



TULSIRAMJI GAIKWAD-PATIL
College of Engineering & Technology, Nagpur

TechEd - 16

2nd Annual International Conference
on

*Encouraging Innovation and Entrepreneurship in
Engineering Education, Global Partnership for Best Practices,
Policy Framework for Governance & Quality Enhancement*

22nd & 23rd January, 2016

In Association with



**Indian Society for
Technical Education, New Delhi**

&



**Rashtrasant Tukdoji Maharaj
Nagpur University, Nagpur**

Department of Mathematics
Department of Chemistry
& Department of Business Management



GAIKWAD-PATIL
GROUP OF INSTITUTIONS

TechEd-16

22nd & 23rd January, 2016

Techsoft | Techantra | ICETCE | ICRTEE | ACUMEN | Techscientia | Tech-Ed



INDEX

Sr. No	Name	Page
1	Shreekant J. Mane & Prof. Mrs. A.V. Nikalje	1
2	Rohan S. Kale & Kartik Ingole	6
3	Sonu Shyam Makde	9
4	Shanklesh M. Vishwakarma & Prof.Tushar uplanchiwar	14
5	Priti V.Shingne & Prof. Rahul Dhature	17
6	Pallavi.S.Chavan & Trupti Mohota	21
7	Bhavana Bhoyar & R. Dhature	26
8	Sneha S. Bonde & Rohini Pochhi	32
9	Ms. Shital G. Nagpurkar & Prof. Rahul Dhature	35
10	Ms. Renuka V. Rithe & Prof.Rahul Dhature	39
11	Ms. Gayatri Datarkar & Prof. Rahul Dhature	43
12	Ms. Sweety S. Kshirsagar , Dr. N.N.Mhala & Prof. B. J. Chilke	47
13	Dhamma A Dahiwale & Prof. Ashish Manusmare	56
14	Brijesh Pathak	60
15	Mr. Vaibhav Agrawal & Prof.Sunil R.Gupta	64
16	Vanshri K.Kadwe & Prof.Supratim Saha	68
17	Abhijit D. Gadge & Prof. Supratim Saha	72
18	Roshan Y Rakhunde & Tushar Uplanchiwar	78
19	Shrutika Vijay Khodankar & Prof. Supratim Saha	83
20	Roshan Bhoyar & Prof. Kanchan Dhote	87
21	Vivek Wanjari & Prof. R. N. Mandavgane	91
22	Shraddhawanjari & Dr.Sanjay Asutkar	100
23	Fatema Anjum & Pooja Thakre	106
24	Shirin Khan & M T Hasan	110
25	Gaurav G. Sambhe	113
26	Vikrant Chhapekar	116
27	Ankit Dandekar & Sagarpradhan	119
28	Ritesh Waghe & Rahul Godghate	122
29	Sonali J. Rewatkar, Sagar Ghormade & Sagar Pradhan	125
30	Nita S. Kalaskar	129
31	Ashwini C. Ingle & Priyanka N. Alone	132
32	Niraj K. Nagrale & Vishakha Nagrale	137
33	Meetal Kalantri, Rahul Dhature & Amit Fulsunge	142
34	Ketan Mishra & Deepak Kumar Sharma	147
35	Bapan Maiti & Deepak Kumar Sharma	150

36	Sneha Chauhan & Deepak Bhoyar	153
37	Prashant G. Bangade	156
38	Bhakti Ganesh Kulkarni, Swapna Dhananjay Kulkarni & Prof.A.M.Ekbote	159
39	Syed Nighat & Prof.M.Nasiruddin	162
40	Ruqaiya Begum & Prof.S.M Ali	166
41	Sharmeen Saba & Prof. A.S.Khan	170
42	Zeba Sheikh & Prof.M.Nasiruddin	173
43	Bushra Firdous & Prof.S.M. Ali	177
44	Zeenat Farzana & Prof. S. R. Ganar	184
45	Rehan. A. Khan & Prof. Tirupati Goskula	187
46	Farha Sabir & Pooja Thakre	190
47	Fiza Firdaus & Dr.Pankaj Agrawal	194
48	Dipti J. Umalkar & Rahul Godghate	197
49	Mr. Amit Bhattacharya & Prof. Nilesh A. Mohota	200
50	Akshay P. Kirmirwar, Sagar Ghormade & Sagar Pradhan	204
51	Sarita Chouhan & Abhishek Misal	208
52	Amruta Pathe	213
53	Madhurima Dubey & Mrs.Yojana Yadav	217
54	Shivangi Namdeo & Mrs. Ashalata Sharma	221
55	Shafaque Farheen Khan	225
56	Tanveer Khan	229
57	Manisha Mankar, Dr. R. V. Kshirsagar & M. V. Vyawahare	233
58	Priti Mankar & Prof.R.H.Khade	240
59	Mrs. Hemlata Meharkure	244
60	Syed Irfan Ali, Sunita Parihar, Deepak Kapgate & Syed Akbar Ali	251
61	Minal A. Kahurke & Shubhangi Dhengre	255
62	Mr. Sanket Yeole & Prof. Sagar Ghormade	259
63	Utkarsha Thatte & Mrs.K.M.Bogawar	261
64	Priyanka Dangore & Prof. Sunil Gupta	265
65	Sneha Metkar & Prof. Sagar Pradhan	269
66	Yogesh Kale, Eqbal Nasim, Parimal Joshi & Akshay Kumar Dhull	272
67	Priyanka G. Kanaskar & Prof. S. Ganar	278
68	Pratik Suresh Bang	280
69	Sonam Fulwadhvani	284
70	Ms. Mithilesh Mahendra	288
71	Deepak Fouzdar	293
72	Diksha Rahangdale, Kalyani Gajpure, Pranjali Deshpande & Prof.. Gaurav Pohane	295
73	Aditya V. Wagh & Prof. Supratim Saha	299
74	Dolly Tambe, Roshani Dekate, Ankit Chauhan, Nikhil Sakhare & Sushma Raut	303
75	Ashwin Shinde, Sumedha Chokandre & Mayuri Marawar	306

blood vessels or capillaries which become thinner, weaker and eventually they leak blood known as micro aneurysms. In figure 3 (b) a patient's sights at this stage is still good but an ophthalmologist can detect and notice the abnormalities in the retina. As the disease progresses some blood vessels are blocked. These trigger the retina to grow new blood vessels those are abnormal, fragile, and easily bleed as shown in figure 3 (c). In the later stage of the disease new blood vessels are grown continuously as well as scar tissue as shown in figure 3 (d). Ultimately retina will be detached from an eye.

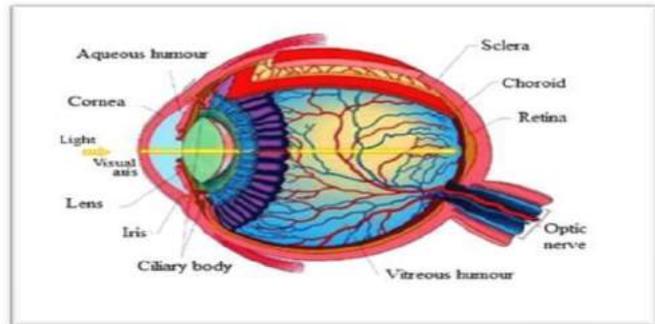


Fig. 2 Human Eye

National Eye Institute recommends everyone with diabetes to have comprehensive eye exam at least once a year because diabetic retinopathy has no early warning symptoms or signs. Failure to undergo universally recommended annual eye examinations is the primary cause of this continued loss of sight. If early diagnosis is done and proper treatment given to patient then the majority of the severe vision loss cases due to diabetic retinopathy can be prevented. Ophthalmologists primarily rely on the results of randomized clinical studies to guide their treatment of patients with diabetes. Retinal photography is important document in the diagnosis of various eye diseases in clinics. Color retinal images are widely used to mass screen systemic diseases such as diabetic retinopathy. Early detection and treatment of these diseases are crucial to avoid preventable vision loss. Early detection of the disease via regular screening is particularly important to prevent vision loss. In this process an automated DR diagnostic system can assist in a big way since a large population has to be screened and that too repeatedly. Color fundus images are used by ophthalmologists to study eye diseases like diabetic retinopathy. Early detection can enable timely treatment minimizing further deterioration. Clinical signs observable by digital film based fundus photography include microaneurysms, dot and blot hemorrhages, exudates and intra retinal micro vascular abnormalities. Following are the types of diabetic retinopathy, classified as per the severity of the disease. DR eye features calculation and identification is possible by using manual or automated method.

A. Mild non proliferative retinopathy: This is earliest stage of diabetic retinopathy where micro aneurysms occur in eye. They are small areas of balloon like swelling in the retina's tiny blood vessels.

Moderate non proliferative retinopathy: As the disease progresses some blood vessels that nourish the retina are blocked and swell.

C. Severe non proliferative retinopathy: Many more blood vessels are blocked, depriving several areas of the retina with their blood supply. These areas of the retina send signals to the body to grow new blood vessels for nourishment. Exudates and hemorrhages are observed due to leaking of blood vessels in eye initially.

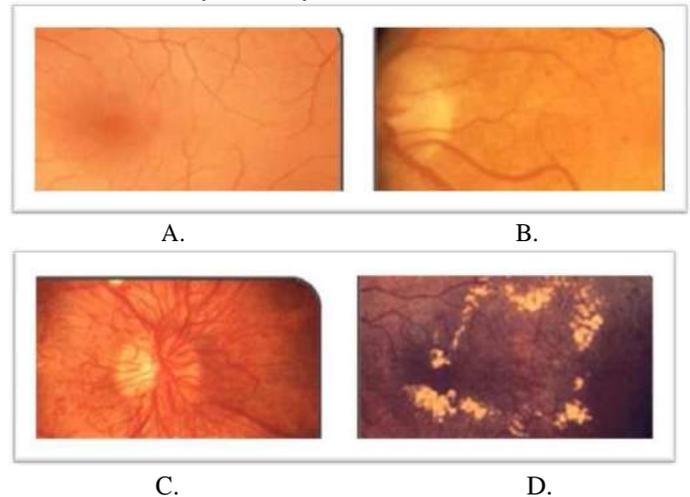


Fig.3 Different Stages of Diabetic Retinopathy A. an example of normal retinal image B. a retinal image with micro aneurysms C. proliferated diabetic retinopathy with fragile newly grown blood vessels and D. a retina image with some types of scar tissues.

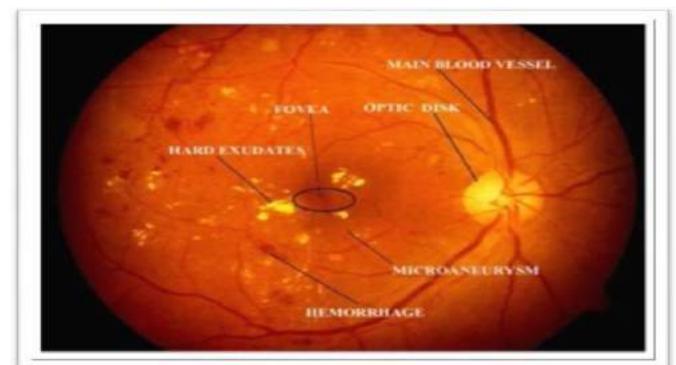


Fig. 4 Defects observed in DR Fundus Image

d) Proliferative retinopathy: This is advanced stage of retinopathy where signals are sent by the retina for nourishment trigger the growth of new blood vessels. This condition is called proliferative retinopathy. These new blood vessels are abnormal and fragile and grow along with the retina and the surface of the clear, vitreous gel that fills the inside of the eye.

Fundus image of DR patient given in figure 4 and labeled various feature components or defects which observed in diabetic retinopathy. Micro aneurysms are small blood clots caused by local distension of capillary walls and appear as

small red dots. This may also lead to big blood clots called hemorrhages. Hard exudates are yellow lipid deposits which appear as bright yellow lesions. The bright circular region from where the blood vessels emanate is called the optic disk. The fovea defines the center of the retina and is the region of highest visual acuity. The spatial distribution of exudates and micro aneurysms and hemorrhages especially in relation to the fovea can be used to determine the severity of diabetic retinopathy. The early treatment diabetic retinopathy study implemented standardized retinal imaging, classification and severity staging for diabetic retinopathy as well as proving the therapeutic of laser photocoagulation surgery in preventing vision loss. This multicenter randomized clinical trial designed to evaluate treatment of patients with non proliferative or early proliferative diabetic retinopathy. The study demonstrated a statistically significant reduction in severe visual loss for those eyes with early treatment. The fundus image required to diagnose DR uses topcons nw series camera which is shown in figure 5 used to capture image for further processing to analyze features to diagnose and treatment of the DR patient.



Fig. 5 Fundal Photography Equipment (Topcon NW Series)

II. NECESSITY

Diabetic retinopathy is one of the most serious complications of diabetes and a major cause of visual morbidity. It is a progressive disease classified according to the presence of various clinical abnormalities. DR is the most common cause of blindness in people aged 30 to 69 years. Manual methods of diagnosis may waste of time, cost and vision of patients. Some manual errors may occur while diagnosis process is going on. Retinal image classification has been done by various methods. Thomas Walter et. al used morphological reconstruction techniques for detection of the exudates known lipids of proteins which come out from damaged capillary vessels which is used to early stages of the Diabetic Retinopathy [1]. Joes Staal et. al performed vessel segmentation using kNN classifier and sequential forward feature selection on fundus Image which is required to extract

features of DR to evaluate stage of the given disease [2]. Alan D. Fleming et. al classify micro aneurysms using contrast normalization are compared where this enables to define early stages of the diabetic retinopathy [3]. Gary G. Yen et. al used hybrid intelligent system using ETDRS protocol developed to study grading of diabetic fundus image [4]. Arturo Aquino et. al used morphological and edge detection techniques followed by the circular hough transform to obtain a circular OD boundary approximation [5]. Keerthi Ram et. al define successive rejection based strategy using anisotropic filters, scale difference of Gaussian and inverted Gaussian methods to detect MA by avoiding clutter to obtain DR but severity of the disease cannot find using this method this limits the scope of the system [6]. Ramon Pires et. al provided theory of soft max bov, soft assignment coding and max pooling classification achieved area under the contours in DR patients which enables the detection of the severity [7].

Limitations of the existing systems or proposed works up till now evaluation of all defects arises due to DR compliances cannot extract using single method. Hence this developed system will overcome and able extract all features using single platform with the help of MATLAB.

III. OBJECTIVE

Various types of health hazards are observe now a days due to hectic life schedule, unhealthy diet plan. Consequences of DR are very complicated and severe so early detection of the disease is required. Following are the objective of this developed system.

1. To develop an efficient feature extraction algorithm that can effectively segment blood vessels and to select reliable point correspondences for latter processing.
2. To displaying the severity of the disease. This can be achieved by the area of the exudates and hemorrhages.
3. To propose a new constraint for optic disk detection where we first detect the major blood vessels first and use the intersection of these to find the approximate location of the optic disk

IV. THEME

In this project, fundus retinal image is used to diagnose diabetic retinopathy patient. Developed system used green plane outoff RGB component of image due more clarity. Green plane is selected because red planes have saturated features and blue plane has low intensity features while contours are easily viewed in green plane due to proper intensity features. Median filtering operation and histogram equalization operations is performing on a green plane to analyze various features in DR patient. Morphological operation like closing and opening (Dilation or Erosion) is required to identify feature accurately with the help of threshold value for Defects. Besides that Hough transform is used to isolate the features of the particular shape within an image. In the given system defects boundaries are created around the affected areas of the retina image and calculating the areas. According to the area of DR feature component and

with the help ANN by training and defining weights to the previous layer. Severity of the disease can be viewed with the help of GUI which display using feed forward back propagation network.

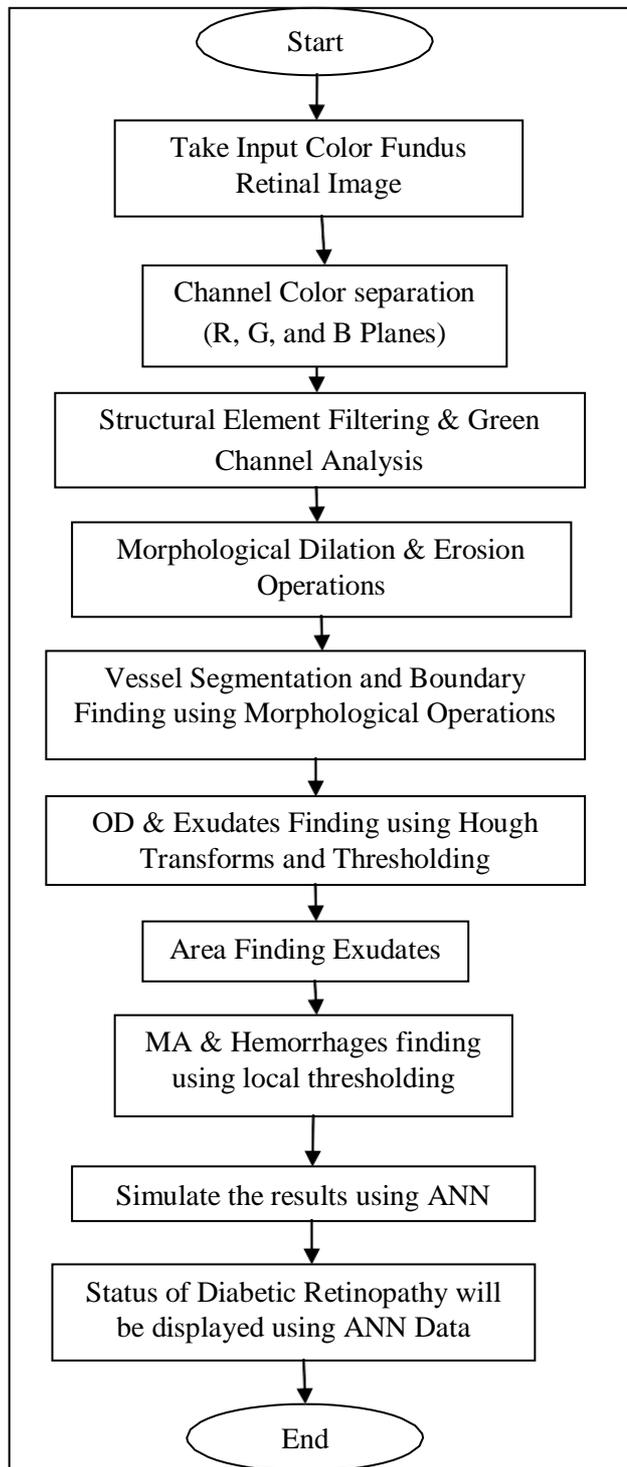


Fig. 6 Design Flow of the System

DR is a common retinal complication associated with diabetes and observes in higher age groups. It is a major cause of blindness in middle as well as older age groups. Therefore early detection through regular screening and timely intervention will be highly beneficial in effectively controlling the progress of the disease. Since the ratio of people afflicted

with the disease to the number of eye specialist who can screen these patients is very high. Need to have automated diagnostic system for diabetic retinopathy changes in the eye so that only diseased persons can be referred to the specialist for further intervention and treatment. Various aspects and stages of retinopathy are analyzed by examining the colored retinal images. Micro aneurysms are small blood clots caused by local distension of capillary walls and appear as small red dots. Blood vessels walls are thin and rupture easily to cause hemorrhages. Hard exudates are yellow lipid deposits which appear as bright yellow lesions. The bright circular region from where the blood vessels originate is called the optic disk. The spatial distribution of exudates and micro aneurysms and hemorrhages, especially in relation to the fovea can be used to determine the severity of diabetic retinopathy.

V. Experimental Results

We used a dataset of 110 images for evaluating the algorithm. The images were obtained from Dr Manoj Saswade one of the renowned Diabetic Eye Specialist and those patients images are used whose treatment is going on. Fundus Images quality and illumination is so important to identify defects present in patients iris due to Diabetes. The images in the dataset were classified by ophthalmologists based on the lesion type (exudates/MAHMs) into those with the lesion and those without it. An image having no lesions is considered normal whereas one that has lesions like exudates, micro aneurysms and hemorrhages is considered abnormal. Among the 110 images obtained from eye hospitals, 78 are diagnosed as Mild Non Proliferative Diabetic Retinopathy and 32 are observe Diabetic Retinopathy patient.

All the images were taken by using fundal equipment i.e. Topcon NW series fundus image camera. Out off 110 images 45 images were identified by ophthalmologists as having exudates and did not have any exudates. A total of 48 images were identified as containing micro aneurysms/ hemorrhages while 21 were free from this lesion type. The entire algorithm was run on the database and results for optic disk localization, exudates detection and MAHMs detection were obtained. The matlab code takes 4 seconds per image on an average to run on a 2 GHz machine with 4GB RAM. The pixel location obtained prior to placing the circular mask is considered for evaluation purposes. If the pixel location indicated by the optic disk algorithm falls within the boundaries of the optic disk, then it is considered a correct detection and vice-versa.

Diabetic retinopathy (DR) is a vascular disorder affecting the microvasculature of the retina. It is estimated that diabetes mellitus affects 4% of the world's population almost half of whom have some degree of DR at any given DR occurs. As we mentioned earlier in Literature survey that there is need of such a automated system to get reed out of it. There are huge number of DR patients who are suffering, and facing vision loss and other micro vascular problems. So in proposed system we obtain sensitivity and specificity results algorithm at both the image and pixel levels.

The main objective of this system is to define severity of the disease using fundus image. In following figure 7 shown that the given fundus image of diabetic patient has mild non proliferative retinopathy.

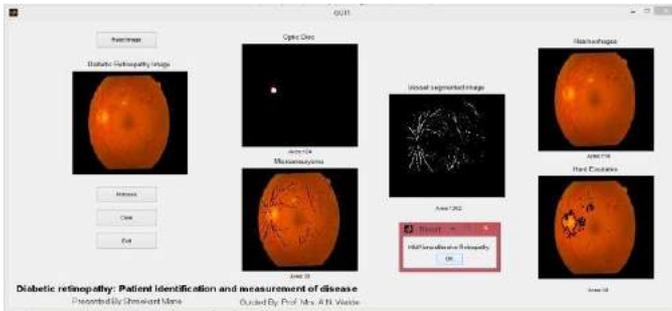


Fig. 7 Mild Non Proliferative Diabetic Retinopathy

This system attenuates image variation by normalizing the original retinal image against a reference model. Variations typically arise within the same image intra image variability as well as between images inter image variability and to enable efficient image analysis which is necessary to compensate for this variability.

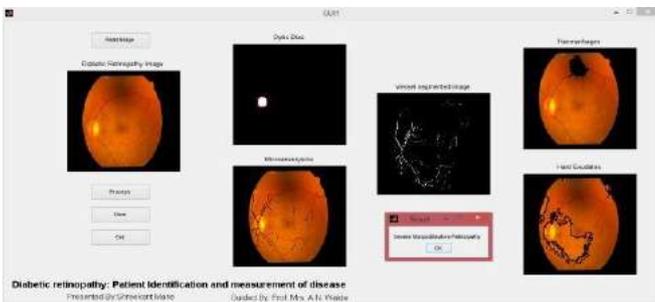


Fig. 8 Severe Non proliferative Diabetic Retinopathy

Diabetic Retinopathy patient identification system is robust to define severity of the Disease. In figure 8 shown that the given patient has severe Diabetic Retinopathy because of exudates and hemorrhages contains available. This Color features can be calculate using morphological classifier, which is used to classify pixel into lesion or non lesion classes. Gold slandered test is used in medical image processing. Given system has accuracy in identifying all the retinal images 100%. The system accuracy to define severity as per fundus image contain is 86.36%. Diabetic Retinopathy and normal retina was classified automatically using image processing and multilayer artificial neural network where input layer outcomes and hidden layer weights which is adjusted accordingly and defines the severity of the disease as per the features of DR fundus image. The system yielded a sensitivity of 87.09% and a specificity of 82.35%. Automated diagnosis based on three lesions exudates, hemorrhages and micro aneurysms.

ACKNOWLEDGMENT

The authors would like to thank the referees and convener of the conference Dr. Seema Biday for their detailed and useful suggestions and giving opportunity to present our proposed work, which have helped to greatly to improve.

REFERENCES

- [1] Thomas Walter, Jean Claude Klein, Pascale Massin, and Ali Erginay, "A Contribution of Image Processing to the Diagnosis of Diabetic Retinopathy Detection of Exudates in Color Fundus Images of the Human Retina", IEEE Transactions on Medical Imaging, Vol. 21, No. 10, pp 1236-1243, October 2002
- [2] Joes Staal, Michael D. Abramoff, Meindert Niemeijer, Max A. Viergever, and Bram van Ginneken, "Ridge-Based Vessel Segmentation

in Color Images of the Retina", IEEE Transactions on Medical Imaging, Vol. 23, No. 4, pp 501-508, April 2004.

Alan D. Fleming, Sam Philip, Keith A. Goatman, John A. Olson, and Peter F. Sharp, "Automated Microaneurysm Detection Using Local Contrast Normalization and Local Vessel Detection", IEEE Transactions on Medical Imaging, Vol. 25, No. 9, pp 1223-1232, September 2006s.

- [3] Gary G. Yen, and Wen Fung Leong, "A Sorting System for Hierarchical Grading of Diabetic Fundus Images: A Preliminary Study", IEEE Transactions on Information Technology in Biomedicine, Vol. 12, No. 1, pp 118-130, January 2008.
- [4] Arturo Aquino, Manuel Emilio Gegundez-Arias, and Diego Marin, "Detecting the Optic Disc Boundary in Digital Fundus Images Using Morphological, Edge Detection, and Feature Extraction Techniques", IEEE Transactions on Medical Imaging, Vol. 29, No. 11, pp 1860-1869, November 2010.
- [5] Keerthi Ram, Gopal Datt Joshi, and Jayanthi Sivaswamy, "A Successive Clutter-Rejection-Based Approach for Early Detection of Diabetic Retinopathy", IEEE Transactions on Biomedical Engineering, Vol. 58, No. 3, pp 664-673, March 2011.
- [6] Ramon Pires, Herbert F. Jelinek, Jacques Wainer, Siome Goldenstein, Eduardo Valle, and Anderson Rocha, "Assessing the Need for Referral in Automatic Diabetic Retinopathy Detection", IEEE Transactions on Biomedical Engineering, Vol. 60, No. 12, pp 3391-3397, December 2013.



AUTOMATIC TOLL COLLECTION SYSTEM

¹Rohan S. Kale
Department of Electronics Engineering
T.G.P.C.E.T.
Rohankale05@yahoo.in

²Kartik Ingole
Department of Electronics Engineering
T.G.P.C.E.T.
kartikzap5@gmail.com

Abstract: ATCS is an Automated Toll Collection System used for collecting tax automatically. A vehicle will hold an RFID tag. This tag is nothing but unique identification number assigned. This will be assigned by RTO or traffic governing authority. In accordance with this number we will store, all basic information as well as the amount he has paid in advance for the TOLL collection. Reader will be strategically placed at toll collection center. Whenever the vehicle passes the toll Plaza, the tax amount will be deducted from his prepaid balance. New balance will be updated. In case if one has insufficient balance, his updated balance will be negative one. To tackle this problem, we are alarming a sound, which will alert the authority that this vehicle doesn't have sufficient balance and that particular vehicle can be trapped. As vehicles don't have to stop in a queue, it assures time saving, fuel conservation and also contributing in saving of money.

Keywords– ATCS, RFID Reader, RFID Tag, Toll Collection, prepaid account

1. INTRODUCTION

Electronic toll collection (ETC) is a technology enabling the electronic collection of toll payments. It has been studied by researchers and applied in various highways, bridges, and tunnels requiring such a process. This system is capable of determining if the car is registered or not, and then informing the authorities of toll payment violations, debits, and participating accounts [2]. The most obvious advantage of this technology is the opportunity to eliminate congestion in tollbooths, especially during festive seasons when traffic tends to be heavier than normal. It is also a method by which to curb complaints from motorists regarding the inconveniences involved in manually making payments at the tollbooths. Other than this obvious advantage, applying ETC could also benefit the toll operators.

The benefits for the motorists include:

1. Fewer or shorter queues at toll plazas by increasing toll booth service turnaround rates;
2. Faster and more efficient service (no exchanging toll fees by hand);

3. The ability to make payments by keeping a balance on the card itself or by loading a registered credit card; and

The use of postpaid toll statements (no need to request for receipts). Other general advantages for the motorists include fuel savings and reduced mobile emissions by reducing or eliminating deceleration, waiting time, and acceleration

An ETC system commonly utilizes radio frequency identification (RFID) technology. RFID is a generic term used to identify technologies utilizing radio waves to automatically identify people or objects. RFID technology has been implemented in various applications, such as in warehouse management, library system, attendance system, theft prevention, and so on. In general, RFID is used for tracking, tracing, and identifying objects.

2. PROPOSED SYSTEM

This project deals with the simplification of procedure followed by passengers to pay toll at toll collection booths, like making it automated, vehicle theft detection etc. All these activities are carried out using single smart card (RFID tag), thus saving the efforts of carrying money and records manually.

Automatic Toll Collection: The RFID Readers mounted at toll booth will read the prepaid RFID tags fixed on vehicles' windshield and automatically respective amount will be deducted. If the tag is removed from the windshield then cameras fixed at two sites at toll plaza take snaps of the front and back number plate. Since every vehicle registration ID is linked to users account, toll can be deducted from the account bank directly.

Signal Breaking Avoidance: The vehicle ignoring the traffic signal will be detected by the RFID readers fixed at signal crossing and will be notified to the traffic police. This can be done efficiently and great accuracy.

Tracking Over speeding Vehicle: Vehicle travelling above speed limit can be tracked with 100 % accuracy.

3. WORKING OF PROPOSED SYSTEM

Whenever any person buys a vehicle, one first needs to get his or her vehicle registered at the RTO office. RTO officials will not only assign a number plate to it but also will give a RFID enabled smart card or a tag. This card will have a unique ID feasible to use with that vehicle only. They will also create an account for the use of that particular smart card and maintain transaction history in database. User needs to deposit some minimum amount to this account.

Whenever a vehicle arrives in toll plaza range antenna sends signals to tag and activate the tag, tag sends back information to the antenna. As data is received to the antenna, it sends the data to central server database. Server checks the information if the consumer/driver, if the account has credit more than required tax, then the tax is subtracted from the account and the vehicle is allowed to pass the toll plaza. Also a transaction message is sent to consumer/driver that how much tax is paid and remaining balance of the account. The passing of vehicle and the transaction of tax is completed within short time. The central server stores all information of transaction, which contains location of toll plaza, date, time and total amount payment of tax. If the credit of account is low then system generates indication for low balance.

4. INTRODUCTION TO RFID

RFID stands for Radio-Frequency Identification. The acronym refers to small electronic devices that consist of a small chip and an antenna. The chip typically is capable of carrying 2,000 bytes of data or less.

The RFID device serves the same purpose as a bar code or a magnetic strip on the back of a credit card or ATM card; it provides a unique identifier for that object. And, just as a bar code or magnetic strip must be scanned to get the information, the RFID device must be scanned to retrieve the identifying information.

5. COMPARISON OF RFID AND BARCODES

A significant advantage of RFID devices over the others mentioned above is that the RFID device does not need to be positioned precisely relative to the scanner. We're all familiar with the difficulty that store checkout clerks sometimes have in making sure that a barcode can be read. And obviously, credit cards and ATM cards must be swiped through a special reader.

In contrast, RFID devices will work within a few feet (up to 20 feet for highfrequency devices) of the scanner. For example, you could just put all of your groceries or purchases in a bag, and set the bag on the scanner. It would be able to query all of the RFID devices and total your purchase immediately.

6. WORKING OF RFID

A Radio-Frequency Identification system has three parts:

- A scanning antenna
- A transceiver with a decoder to interpret the data
- A transponder - the RFID tag - that has been programmed with information.

The scanning antenna puts out radio-frequency signals in a relatively short range. The RF radiation does two things:

- It provides a means of communicating with the transponder (the RFID tag)
- It provides the RFID tag with the energy to communicate (in the case of passive RFID tags).

This is an absolutely key part of the technology; RFID tags do not need to contain batteries, and can therefore remain usable for very long periods of time (maybe decades).

The scanning antennas can be permanently affixed to a surface; handheld antennas are also available. They can take whatever shape you need; for example, you could build them into a door frame to accept data from persons or objects passing through.

When an RFID tag passes through the field of the scanning antenna, it detects the activation signal from the antenna. That "wakes up" the RFID chip, and it transmits the information on its microchip to be picked up by the scanning antenna.

7. RFID TAG

An RFID tag is a microchip combined with an antenna in a compact package; the packaging is structured to allow the RFID tag to be attached to an object to be tracked. "RFID" stands for Radio Frequency Identification and Detection.

The tag's antenna picks up signals from an RFID reader or scanner and then returns the signal, usually with some additional data (like a unique serial number or other customized information).

RFID tags can be very small - the size of a large rice grain. Others may be the size of a small paperback book.

8. ACTIVE RFID TAG

An RFID tag is an active tag when it is equipped with a battery that can be used as a partial or complete source of power for the tag's circuitry and antenna. Some active tags contain replaceable batteries for years of use; others are sealed units. (Note that it is also possible to connect the tag to an external power source.)

The major advantages of an active RFID tag are:

- It can be read at distances of one hundred feet or more, greatly improving the utility of the device
- It may have other sensors that can use electricity for power.

The problems and disadvantages of an active RFID tag are:

- The tag cannot function without battery power, which limits the lifetime of the tag.
- The tag is typically more expensive, often costing \$20 or more each
- The tag is physically larger, which may limit applications.

Active RFID tags may have all or some of the following features:

- Longest communication range of any tag.
- The capability to perform independent monitoring and control.
- The capability of initiating communications.
- The capability of performing diagnostics.
- The highest data bandwidth.
- Active rfid tags may even be equipped with autonomous networking; the tags autonomously determine the best communication path.

9. PASSIVE RFID TAG

A passive tag is an RFID tag that does not contain a battery; the power is supplied by the reader. When radio waves from the reader are encountered by a passive RFID tag, the coiled antenna within the tag forms a magnetic field. The tag draws power from it, energizing the circuits in the tag. The tag then sends the information encoded in the tag's memory.

The major disadvantages of a passive RFID tag are:

- The tag can be read only at very short distances, typically a few feet at most. This greatly limits the device for certain applications.
- It may not be possible to include sensors that can use electricity for power.
- The tag remains readable for a very long time, even after the product to which the tag is attached has been sold and is no longer being tracked.

10. RFID READER

An RFID reader is a device that is used to interrogate an RFID tag. The reader has an antenna that emits radio waves; the tag responds by sending back its data.

A number of factors can affect the distance at which a tag can be read (the read range). The frequency used for identification, the antenna gain, the orientation and polarization of the reader antenna and the transponder antenna, as well as the placement of the tag on the object to be identified will all have an impact on the RFID system's read range.

11. RFID TAG ANTENNA

The antenna in an RFID tag is a conductive element that permits the tag to exchange data with the reader. Passive RFID tags make use of a coiled antenna that can create a magnetic field using the energy provided by the reader's carrier signal

12. ADVANTAGES

- **Financial leakage control.** By utilizing fully automatic mechanism we can nearly able to control this financial loss.
- **Fuel saving** Due to automation of toll plaza their will be large reduction in the rush at toll plaza which will cause indirectly the saving of fuel.
- **Reduced man power** The basic aim of Automation concept is to reduce the man power & to increase the accuracy of the system. So we can able to achieve the same with our on built concept.

- **Reduced time for completion of process** The present system we have in work today consumes nearly 1 minute for each vehicle to complete the process of toll payment. With our automated toll plaza we can able to reduce the time consumption nearly up to 40-42 sec. which will be very important in today's era

13. LIMITATIONS

If RFID fails whole system fails. The RFID system we are here using for detecting the vehicle number means the vehicle identity which we are further using for storing into memory & also to display on the LCD. If the RFID fails to detect the correct identity of the vehicle the data regarding the vehicle will be wrong which will may create many problems & system fails.

14. CONCLUSION

By doing automation of toll plaza we can have the best solution over money loss at toll plaza by reducing the man power required for collection of money and also can reduce the traffic indirectly resulting in reduction of time at toll plaza.

In our paper, we have introduced the techniques such as Radio Frequency Identification. This technique will include the RFID tag & reader which in coordination with each other can be used to detect the vehicle identity.

By effectively utilizing this technique at different stages of our project we are able to represent the automation in toll plaza which will reduce the complete processing time by few seconds which is very important as well as helps to reduce money leakage in a very cost effective manner.

15. REFERENCES

- [1] RFID based toll collection system, 2011 IEEE third international Conference
- [2] D. M. Grimes and T. O. Jones, —Automotive radar: A brief review, Proc. IEEE, vol. 62, no. 6, pp. 804–822, Jun. 1974.
- [3] ActiveWaveInc. <http://www.activewaveinc.co>
- [4] Smart key Access Control System <http://www.smartkey-rfid.com>
- [5] D. M. Grimes and T. O. Jones, —Automotive radar: A brief review, Proc. IEEE, vol. 62, no. 6, pp. 804–822, Jun. 1974.



Efficient Artery/Vein classification in Retinal Images using Discrete Curvelet Transform Algorithm

Sonu Shyam Makde

*4th Sem M.Tech. Electronics & Communication Engineering
Tulsiramji Gaikwad-Patil College of Engineering & Technology
India, Nagpur (Maharashtra State)
sonu7279@gmail.com Contact No.9890302781*

Abstract- The classification of retinal vessels into artery/vein is an important phase for speeding up the detection of vascular changes, and for the calculation of characteristic signs associated with several systemic diseases for example diabetes, hypertension, blood pressure and other cardiovascular diseases. This paper presents an automatic approach for A/V classification based on the critical analysis of a graph extracted from the retinal vasculature. The proposed scheme classifies the whole vascular tree deciding on the type of each intersection point (graph nodes) and assigning one of two labels to each vessel segment (graph links).

Proposed Artery vein classification method on the images of three different databases demonstrate the independence of this method in Artery vein classification of retinal images with different properties, such as differences in size, quality, and camera angle.

On the other hand, the high accuracy achieved by our method, especially for the largest arteries and veins, confirm that this Artery vein classification method is reliable for the calculation of many characteristic signs associated with vascular alterations. In this paper we planned using the graph that represents the vessel tree and the artery vein classification method for Artery vein ratio calculation, as well as identifying other vascular signs, such as vascular bifurcation angles, branching patterns, and fractal-based features, which can have significant impact on the early finding and follow up of diseases, namely diabetes, hypertension, and cardiovascular diseases.

Keywords: *component; Artery/vein classification, graph, retinal images, vessel segmentation.*

INTRODUCTION

There are two types of vessels, arteries and veins. Arteries are bright in color, since they transport blood rich in oxygen to the organs of the body. The veins then transport the blood, which is at low oxygen level and thus darker, to the lungs and the liver. For many medico applications it would be of great benefit, if the vessels could be distinguished into arteries and veins, since many diseases with one symptom being an abnormal ratio of the size of arteries to veins. Like in diabetic patients the veins are abnormally wide, while diseases of the pancreas lead to narrow arteries and high blood

pressure results in thickening of arteries. To detect these diseases the retina is routinely examined.

As a basis for classification a proper segmentation of blood vessels is of course needed.

There are mainly four different features that can be used to classify arteries from veins in general:

- arteries are bright in color than veins
- arteries are thinner than neighboring veins
- the central reflex (the light reflex of the inner parts of the vessels shown in Figure 1) is wide in arteries and smaller in veins.
- arteries and veins usually alternate near the optic disk before they branching out; that means near the optic disk one artery is usually next to two veins and the other way round one important representative of each arteries and veins can be seen in Figure 2.

The mentioned features often provide ample information to successfully classify a vessel as artery or vein. However, in many cases they do not suffice for the following reasons:

- If the image quality is not good enough - which is especially in the outer regions of the image, the central reflex often disappears.
- Vessels in the outer regions of the image are very dark due to the shading effect (in-homogeneous lighting of the image). Here arteries and veins look very much similar, which necessarily leads to the wrong classification of some vessels.
- The width of the vessel is also not very useful for classification, since it is largest near the optic disk and smallest on the outer side of the image.
- The alternation of arteries and veins only found true for the vessels very near to the optic disk. When they start branching out, it is found that two branches of the same vessel go next to each other. So none of the typical features of arteries and veins is globally valid.



Figure 1. One of the most important features for the discrimination of arteries and veins is the central reflex in the red channel: left: original image containing two large veins and an artery in the center, right: red channel



Figure 2. Typical representative of arteries (left) and veins (right), they can be discriminated by color, size, central reflex size and topological properties

To give an overall impression of the difficulty of this classification task, ten cropped veins and ten cropped arteries taken from four different retinal images. The quality of the images, the background and the small size of the vessels and the delicacy of the features themselves make it very hard to distinguish between the two classes. These examples clearly show that a classification method based only on local features may not be able to achieve good results. We compile these features in a learning based approach, which – with the help of global meta-knowledge - is able to classify arteries from veins with a very high classification rate.

LITERATURE SURVEY

Many characteristic signs associated with vascular changes are measured, aiming at finding the stage and severity of some retinal conditions. Generalized arteriolar narrowing, which is inversely related to higher blood pressure levels [5], [6], is expressed by the Arteriolar-to-Venular diameter Ratio. The Atherosclerosis Risk in Communities (ARIC) study previously showed that a smaller retinal Arteriolar-to-Venular diameter ratio might be an independent predictor of incident stroke in middle aged individuals [7].

The Arteriolar-to-Venular diameter Ratio values are also be an indicator of other diseases, like diabetic retinopathy and retinopathy of prematurity [8]. Among other image processing operations, the estimation of Arteriolar-to-Venular diameter Ratio requires vessel segmentation, accurate vessel width measurement, and artery/vein (A/V) classification [9], [10]. Therefore, any automatic Arteriolar-to-Venular diameter ratio measurement system must accurately identify which vessels are arteries and which are veins, some slight classification errors can have a large influence on the final value.

Several works on vessel classification has been proposed [11]–[17], but automated classification of retinal vessels into arteries and veins can received limited attention, and is still an open task in the retinal image analysis field. In recent years, graphs emerge as a unified representation for image analysis and graph-based methods has been used for retinal vessel segmentation [18], retinal image registration [19], and retinal vessel classification [12]. In this paper we propose a graph-based method for automatic A/V classification. The graph extracted from the segmented retinal vasculature can analyzed to decide on the type of intersection points (graph nodes), and afterwards one of two labels is assigned to each vessel segment (graph links).

Finally, intensity features of the vessel segments can measured for assigning the final artery/vein class.

Grisan et al. [13] developed a tracking artery/vein (A/V) classification technique which classifies the vessels only in a well-defined concentric zone around the optic disc. Therefore, by using the vessel structure reconstructed by tracking, the classification can propagated outside this zone, where little or no information is available to discriminate arteries from veins. This algorithm cannot design to consider the vessels in the zone all together, but rather partitions the zone into four quadrants, and works separately and locally on each of them.

Vazquez et al. [14] described a method can combines a color-based clustering algorithm with a vessel tracking method. First the clustering approach divides the retinal image into four quadrants, therefore it can classify separately the vessels detected in each quadrant, and finally it can combine the results.

Therefore, a tracking strategy based on a minimal path approach can applied to join the vessel segments located at different radius in order to support the classification by voting.

A piece wise Gaussian model to elaborate the intensity distribution of vessels profiles has been proposed by Li et al. [15]. In this model, the central reflex is considered. A minimum distance classifier based on the Mahalanobis distance is used to differentiate between the vessels types using features obtained from the estimated parameters.

Kondermann et al. [16] describes two feature extraction methods and two classification methods, which are based on support vector machines and neural networks, to classify retinal vessels.

One of the feature extraction methods is profile based, while the other method is based on the definition of region of interest (ROI) around each center line point. To reduce the dimensionality of the feature vectors, they used the multiclass principal component analysis (MPCA).

PROPOSED SYSTEM

We tried to understand in details which are the most relevant features related to the vascular classes and how they can be used to discriminate veins and arteries on heterogeneous images. For this purpose we considered a large number of features, which includes not only color and size descriptor, but we also adding explicitly context related values like spatial position with respect to the optic disc.

In order to have detailed analysis we tried to separate features that are different in veins and arteries for different reasons, which are trying to analyze their real contribution to the classification.

Central color and within-vessel variations:

The principal features used for vessel classification are related to color. Color space components in a neighborhood of the central pixels or along a profile perpendicular to the vessel are mainly considered, usually after a color component normalization to zero mean and unitary standard deviation.

We similarly tested a large set of color features, but decided to analyze separately color features related to the internal part of the vessel and color features including the contrast with the background. We did not find necessary to consider profiles perpendicular to the vessel direction, due to the fact that we studied variations within circular regions around the central pixel. This makes the technique a more robust and thus not depending on the local estimation of the vessel direction. So to characterize the colors inside the vessel and the central reflex, we used the central pixel color components (R,G,B,H,S,V) and component derivatives, also the mean, minimum, maximum and variance of that values in a disc of diameter equal to the locally estimated vessel diameter (small region in Fig. 1).

Contrast with surrounding pixels it is then interesting to check if the contrast with the background provide relevant information for vessel classification (and to see which are the most discriminating parameters). For this purpose we computed further features averages and standard deviations of color components and color derivatives in a disc with diameter equal to twice the locally estimated vessel diameter (large region in Fig. 1).

In this case the computed features are largely dependent on the contrast between vessel color and background color.

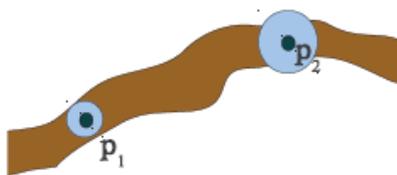


Figure 1. Small (only internal, radius equal to half vessel width) and large (radius equal to vessel width) region used to compute color features potentially characterizing the vessel type.

Position and Size

Vessel size is considered in some work a potentially discriminative feature, but often not considered due to the fact that it changes with the distance from the optical disc .

But this is not a reason to avoid its use, but rather a reason to use it in combination with spatial information. Actually, if we consider the results, where it is reported that color features are more discriminative if used independently in different sectors around the OD, it is reasonable to think that color features

should also be combined with spatial information in order to obtain a better classification.

We decided to test the discriminative power of spatial features like angular and radial distance from the Optic disc center and distance from the image optic center. The analysis of the discriminative power of these features alone and also combined with size and color based one is surely relevant to determine how to improve the performance of classification tools. To compute angular distance from the estimated OD center we used the OD locator developed for the VAMPIRE tool, based on multi scale ellipse fitting. The angular position is computed differently in case of left or right image. In the first case we consider a clockwise orientation, and in the second case counterclockwise as shown in (Fig. 2), so that the possible effects of the variable on the image color should be the same.

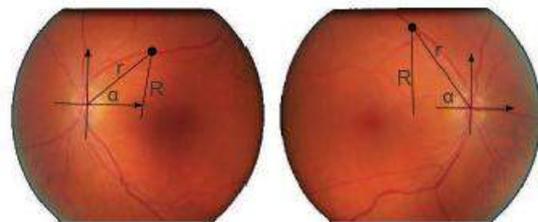


Figure 2. Measurements related to image position: linear distances from the estimated OD center and image center and angular position with respect to the OD center differentiated for left and right images.

MODULES

Image enhancements:

In image enhancements we extract the green channel of image which show the more probability of veins of retina image. Retina image is RGB (red green blue). We extract green channel. After that we enhance the extract image by using histograms adjustment algorithm to improve the image quality.

Vessel segmentation:

After getting the improve image we apply the canny edge detector to finding the edges in image for classifying feature extraction and A/V (artery vein) Classification.

Feature extraction module contain SVM (state vector machine) module which is used to train the project for detection the feature points in image.

Node and Branches descriptor:

Node and branches descriptor used to find the cross section points of edges in image to classify the vein and artery by using graph method with the help of bfs (breath first search) to transverse a graph.

Classification Result:

This module classifies the input image by basic of training of feature detection and node descriptor module and shows the calculated result.

RESULT & DISCUSSION

We will perform several tests aimed to understand which groups of features are useful to discriminate veins and arteries in digital fundus images. Results could be useful to improve the performances of existent systems for the estimation of related biomarkers such as the Artery vein ratio.

First of all, color contrast between vessels and background appear as one of the most important cue for discrimination, but there are vessels that are not well recognized so simply and thus required to add more information. This information can be related to vessel position and to the color variations inside the vessel. While the vessel width does not add much useful information.

Finally, image resolution should be taken into account. It seems that high resolution sensors introduces noise and can reduce the color based information, the same features computed on sub sampled images gave, in fact, better results even if an excessive sub sampling could remove the information about the central reflex in vessels. The dependency of performance on color confirms the importance of normalizing image resolution in studies involving different-resolution fundus cameras. to guarantee consistency.

CONCLUSION

We introduced a technique for unsupervised information extraction from unstructured, ungrammatical text. Previously, unsupervised extraction used patterns that make assumptions about the regularity of the structure in the data. We relax this assumption by exploiting reference sets to aid the extraction. These reference sets are chosen by the algorithm, removing the need for any human intervention.

The main ability of neural network is to learn from its environment and to improve its performance through detailed learning. For this purpose there are two types of learning supervised or active learning – learning with an external supervisor who present a training set to the network. But another type of learning also exists : unsupervised learning . Unsupervised learning is self organized learning doesn't require an external supervisor. During training session neural network receives a number of input patterns , discovers significant features in these patterns and learns to classify input data into appropriate categories. It follows the neuro - biological organization of the brain. These algorithms aim to learn rapidly, so learn much faster than back-propagation

networks and thus can be used in real time. Unsupervised neural networks are effective in dealing with unexpected and changing conditions. We have shown that as compared to Trinity Tree Algorithm Back Propagation is more accurate and less time consuming.

Acknowledgment

The authors would like to thank the authors whose reference are available in this regards.

References

- [1] N. Patton, T. M. Aslam, T. MacGillivray, I. J. Deary, B. Dhillon, R. H. Eikelboom, K. Yogesa, and I. J. Constable, "Retinal image analysis: Concepts, applications and potential," *Progr. Retinal Eye Res.*, vol. 25, p. 99–127, Jan. 2006.
- [2] T. T. Nguyen and T. Y. Wong, "Retinal vascular changes and diabetic retinopathy," *Current Diabetes Rep.*, vol. 9, pp. 277–283, Aug. 2009.
- [3] K. Guan, C. Hudson, T. Wong, M. Kisilevsky, R. K. Nrusimhadevara, W. C. Lam, M. Mandelcorn, R. G. Devenyi, and J. G. Flanagan, "Retinal hemodynamics in early diabetic macular edema," *Diabetes*, vol. 55, pp. 813–818, Mar. 2006.
- [4] A. S. Neubauer, M. Ludtke, C. Haritoglou, S. Priglinger, and A. Kampik, "Retinal vessel analysis reproducibility in assessing cardiovascular disease," *Optometry Vis. Sci.*, vol. 85, p. 247–254, Apr. 2008.
- [5] N. Cheung and T. Y. Wong, "The retinal arteriole to venule ratio: Informative or deceptive?" *Graefe's Archive Clinical Experim. Ophthalmol.*, vol. 245, no. 8, pp. 1245–1246, 2007.
- [6] G. Liew, P. Mitchell, J. Wang, and T. Wong, "Effect of axial length on retinal vascular network geometry," *Amer. J. Ophthalmol.*, vol. 141, pp. 597–598, Mar. 2006.
- [7] S. R. Lesage, T. H. Mosley, T. Y. Wong, M. Szklo, D. Knopman, D. J. Catellier, S. R. Cole, R. Klein, J. Coresh, L. H. Coker, and A. R. Sharrett, "Retinal microvascular abnormalities and cognitive decline: The ARIC 14-year follow-up study," *Neurology*, vol. 73, no. 11, pp. 862–868, 2009.
- [8] C. Sun, J. J. Wang, D. A. Mackey, and T. Y. Wong, "Retinal vascular caliber: Systemic, environmental, and genetic associations," *Survey Ophthalmol.*, vol. 54, no. 1, pp. 74–95, 2009.
- [9] L. D. Hubbard, R. J. Brothers, W. N. King, L. X. Clegg, R. Klein, L. S. Cooper, A. Sharrett, M. D. Davis, and J. Cai, "Methods for evaluation of retinal microvascular abnormalities associated with hypertension / sclerosis in the atherosclerosis risk in communities study," *Ophthalmology*, vol. 106, pp. 2269–2280, Dec. 1999.
- [10] M. D. Knudtson, K. E. Lee, L. D. Hubbard, T. Y. Wong, R. Klein, and B. E. K. Klein, "Revised formulas for summarizing retinal vessel diameters," *Current Eye Res.*, vol. 27, pp. 143–149, Oct. 2003.

- [11] M. E. Martínez-Perez, A. D. Hughes, A. V. Stanton, S. A. Thom, N. Chapman, A. A. Bharath, and K. H. Parker, "Retinal vascular tree morphology: A semi-automatic quantification," *IEEE Trans. Biomed. Eng.*, vol. 49, no. 8, pp. 912–917, Aug. 2002.
- [12] K. Rothaus, X. Jiang, and P. Rhiem, "Separation of the retinal vascular graph in arteries and veins based upon structural knowledge," *Image Vis. Comput.*, vol. 27, pp. 864–875, Jun. 2009.
- [13] E. Grisan and A. Ruggeri, "A divide et impera strategy for automatic classification of retinal vessels into arteries and veins," in *Proc. 25th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Sep. 2003, pp. 890–893.
- [14] S. Vazquez, B. Cancela, N. Barreira, M. Penedo, and M. Saez, "On the automatic computation of the arterio-venous ratio in retinal images: Using minimal paths for the artery/vein classification," in *Proc. Int. Conf. Digital Image Comput., Tech. Appl.*, 2010, pp. 599–604.
- [15] H. Li, W. Hsu, M. Lee, and H. Wang, "A piecewise Gaussian model for profiling and differentiating retinal vessels," in *Proc. Int. Conf. Image Process.*, vol. 1, Sep. 2003, pp. 1069–1072.

A Review Paper on “Performance Analysis of Conventional and Wavelet Based SC-FDMA in LTE”

Shanklesh M. Vishwakarma, Prof. Tushar Uplanchiwar[#]
*[#]Department of Electronics and Communication Engineering,
Tulsiramji Gaikwad Patil College of Engineering and Technology
Nagpur
shankykarma@gmail.com*

Abstract—Single Carrier Frequency Division Multiple Access (SC-FDMA) are the multiple-access version of OFDM and another modulation technique, Single-Carrier Frequency-Domain Equalization (SC-FDE). SC-FDMA and OFDM are two techniques in Long Term Evolution (i.e. 4G). The parameters used for comparison will be capacity, Bit error rate (BER), and peak-to-average power ratio (PAPR). OFDM is used for downlink communication and SC-FDMA is used for uplink. OFDMA has a major drawback which is high PAPR due to this it is not much preferable to be used in uplink broadband wireless systems. To overcome this SC-FDMA is used which has low PAPR. Single carrier FDMA (Frequency division multiple access) has become most popular in broadband uplink wireless systems. Since it has low distortion and is free from PAPR problem which are there in OFDMA (Orthogonal frequency division multiple access) systems. In analysis of conventional and wavelet based OFDM in some previous paper it is found that the output BER curves obtained from wavelet based OFDM are good in performance than that of DFT based OFDM. That is the discrete wavelets prove to be the best when substituted instead of FFT analysis. So in this paper we are checking the performance of conventional and wavelet based SCFDMA.

Keywords— SCFDMA, OFDM, LTE etc..

I. INTRODUCTION

In this article we will provide a performance analysis of both uplink candidates for FFT based SCFDMA and wavelet based SCFDMA. OFDMA transmits data over a large number of subcarriers. These signals are perpendicular to each other and their summation will be null which removes mutual interference. SC-FDMA aggregates multipath interference and flexible subcarrier frequency assignment which provides only one carrier at a time instead of multiple carriers in transmission. For the uplink, the LTE of the 3GPP employs SCFDMA due to its low PAPR properties compared to OFDMA. SC-FDMA is introduced recently and it became popular for uplink multiple access scheme in LTE system which is a project of Third Generation Partnership Project (3GPP). The Multiple Access techniques in Advanced Mobile radio system has to meet the challenging requirements for example efficient Bit Error Rate (BER), high throughput, good robustness, low Peak to Average Power Ratio (PAPR), low delays, low computational complexity, low error probability, high spectral efficiency, etc. Wavelet transform is used to analyze signals by the coefficients of wavelets in both

frequency and time domain. One type of wavelet transform is DWT (Discrete Wavelet transforms) have been considered as alternative platforms for replacing IFFT and FFT. ISI and ICI are generally caused by nonorthogonality between the carriers caused by multipath propagation of the signals in OFDM using Discrete Fourier Transform (DFT). ISI arises in between successive symbols of same sub-carrier and ICI arises in different signals at different subcarriers. ISI and ICI are avoided by using cyclic prefix which causes power loss and bandwidth inefficiency in DFT based OFDM. This paper is organized as: in Section I introduction, II as brief Literature review of the previous work demonstrated on OFDM and SCFDMA, III SCFDMA Transmitter, IV Receiver, V Wavelet based transmitter and receiver, VI Summary, and References.

II. LITERATURE REVIEW

In this paper the author analyzed the wavelet based OFDM system and compared it with the DFT based OFDM system. From the output curve it is observed that the BER curves obtained from wavelet based OFDM are good than that of DFT based OFDM. Here three modulation techniques for implementation are used, that are QPSK, 16 QAM and 64 QAM, which are used in LTE. We can use different types of filters with the help of different wavelets available. In this paper Daubechies² and Haar wavelets are used, at different intervals of SNR both provide their best performances.

In this paper the author has done a survey on different modulation schemes to know their suitability in high data rate uplink communication systems and it was found that SC-FDMA is suitable for that. SC-FDMA provides good PAPR reduction than OFDMA and can overcome many of its drawbacks. Besides uplink communication SC-FDMA is used in various applications like return-link of interactive broadband systems, land mobile satellite communication systems etc. It was also observed that PAPR of signal will change with the modulation used and a trade-off between PAPR and out-of band signal energy has to be considered while choosing the roll-off factor for pulse shaping. Besides this, spreading in SC-FDMA can provide both features of SC-FDMA and CDMA which has good advantages than OFDM-CDMA.

In this paper, author compare the Peak-average-power-ratio characteristics of LTE Frame Structure Type (LTE FDD & LTE TDD) of SC-FDMA and OFDMA. It is found that, LTE FDD has better performance than LTE TDD. PAPR of SC-FDMA and OFDMA in LTE FDD has lower values on average. Also FDD has a continuous reduction of BER (Bit Error Rate) and it minimizes the BER up to a certain values of SNRs. Comparing the Performance analysis it is conclude that LTE FDD is the better choice than in LTE TDD in uplink Transmission-SC-FDMA and downlink Transmission-OFDMA, because of its higher efficiency due to low PAPR.

In this paper Wavelet based single carrier FDMA system is proposed, experiments are conducted on different channels under different equalization techniques. Based on this it was found that the orthogonal wavelets can be replace for better band width preservation and the system provides outstanding performance under Rayleigh fading channel. Zero forcing algorithms may be adapted for better equalization. This work may be further extended with complex channeling models like ETU (extended terrain urban) channels and complex wavelet transforms like dual tree complex wavelets.

III. SC-FDMA TRANSMITTER

SC-FDMA uses an N-point DFT stage at transmitter and an N-point IDFT stage at receiver. The basic block diagram of SC-FDMA transmitter is shown in figure 1. The input to transmitter is a stream of modulated symbols.

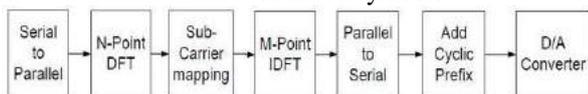


Figure 1: SC-FDMA Transmitter

In SC-FDMA, the data is mapped into signal constellation according to the QPSK, 16-QAM, or 64-QAM modulation, depending upon the channel conditions. Whereas, the QPSK/QAM symbols do not directly modulate the subcarriers. These symbols pass through a serial to parallel converter followed by a DFT block that produce discrete frequency domain representation of the QPSK/QAM symbols. Pulse shaping is followed by DFT element, but it is optional and sometimes needs to shape the output signal from DFT. If pulse shaping is active then in the actual signal, bandwidth extension occurs. The discrete fourier symbols from the output of DFT block are then mapped with the subcarriers in subcarrier mapping block. After mapping these frequency domain modulated subcarriers pass through IDFT for time domain conversion. A guard band is used between OFDMA symbols in order to cancel the Intersymbol Interference at receiver. In LTE, this guard band is called Cyclic Prefix (CP) and the duration of the CP should greater than the channel impulse response or delay spread. After digital to analog conversion signal is send to channel. The sub-carrier mapping plays an important role in the transmitter of SC-FDMA. It maps each of the N-DFT output on a single subcarrier out of M subcarriers, where M is the total number of subcarriers for available bandwidth. The subcarrier mapping is achieved by

two methods; localized subcarrier mapping and distributed subcarrier mapping. The modulation symbols in localized subcarrier mapping are assigned to M adjacent subcarriers, whereas in distributed mode, the symbols are uniformly spaced across the whole channel bandwidth. Localized subcarrier mapping also referred as localized SCFDMA (LFDMA) whereas distributed subcarrier mapping referred as distributed SCFDMA (DFDMA).

IV. SC-FDMA RECEIVER

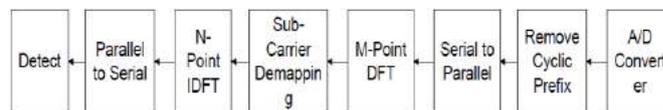


Figure 2: SC-FDMA receiver

A channel model is then applied to the transmitted signal. The model allows for the signal to noise ratio, multipath to be controlled. The signal to noise ratio is set by adding a known amount of white noise to the transmitted signal which is known as AWGN Additive white Gaussian noise. The Receiver basically does the reverse operation of the transmitter. The transmitted signals which pass through the channel are then converted by using Serial to parallel converter and cyclic extension is also removed. The signals pass through an N-point Fast Fourier Transform which converted time domain signal into frequency domain. Then the signal is demapped and performs parallel to serial conversion using Parallel to serial convertor block and the resultant signal is a M sample output

V. WAVELET BASE SCFDMA

Figure show the block diagram of transmitter and receiver of Wavelet base SCFDMA. The modulation processes are applied on the user data. The resulting signal is transformed by the wavelet transform via the DWT. The output of the single-level Haar wavelet transform consists of two signals.

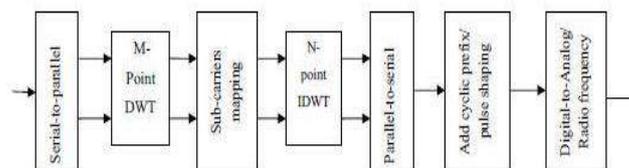


Figure 3: Wavelet based SCFDMA transmitter

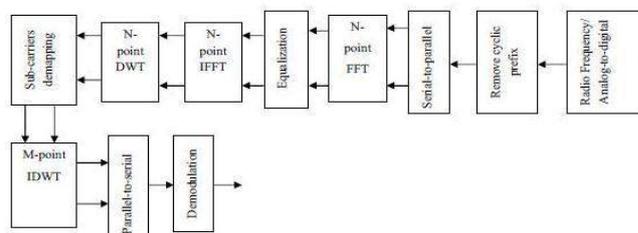


Figure 3: Wavelet based SCFDMA receiver

The resulting signal from the sub-carriers mapping is inserted into the IDWT to produce the signal from the approximation coefficients signal and the detail coefficients signal. After that, we add the CP in order to prevent the ISI. Finally, the resulting signal is transmitted through the wireless channel. At the receiver, the CP is removed from the received signal, and the signal is transformed into the frequency domain via an N-point FFT to apply the equalization process on the signal. The signal is transformed from the frequency domain into the time domain via an N-point IFFT and then it is passed through an N-point DWT to produce the approximation coefficients signal and the detail coefficients signal. Finally, the IDWT and the demodulation processes are performed.

VI. SUMMARY

In this work performance of conventional and wavelet base SCFDMA will be carry out by either comparing PAPR, BER etc. SCFDMA is a modulation technic use for uplink transmission in communication system. If we place N-point DFT in OFDMA then it is converted into SCFDMA structure. From the performance curve of DFT base and wavelet based OFDM it is found that wavelet based OFDM is better than the DFT based OFDM. Wavelet base SCFDMA system is obtain by replacing the DFT blocks by discrete wavelet transform (DWT). Wavelet transform is a new concept in transmission systems. In this a signal is expanded in an orthogonal set called as wavelets. Wavelets provide both frequency and time localization. Wavelet reduces the complexity and power consumption.

REFERENCES

- [1] D.J. Goodman, *Wireless Personal Communications Systems*, Addison-Wesley, 1997.
- [2] R. van Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*, Artech House, 2000.
- [3] H. Ekström, A. Furuskär, J. Karlsson, M. Meyer, S. Parkvall, J. Torsner, and M. Wahlqvist, "Technical Solutions for the 3G Long-Term Evolution," *IEEE Commun. Mag.*, vol. 44, no. 3, pp. 38–45, Mar. 2006.
- [4] 3rd Generation Partnership Project (3GPP); Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN), <http://www.3gpp.org/ftp/Specs/html-info/25913.htm>.
- [5] 3rd Generation Partnership Project (3GPP); Technical Specification Group Radio Access Network; Physical Layer Aspects for Evolved UTRA, <http://www.3gpp.org/ftp/Specs/html-info/25814.htm>.
- [6] U. Sorger, I. De Broeck, and M. Schnell, "Interleaved FDMA—A New Spread-Spectrum Multiple-Access Scheme," *Proc. IEEE ICC '98*, Atlanta, GA, pp. 1013–1017, June 1998.
- [7] H.G. Myung, J. Lim, and D.J. Goodman, "Peak-to-Average Power Ratio of Single Carrier FDMA Signals with Pulse Shaping," to be presented at The 17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '06), Helsinki, Finland, Sep. 2006.
- [8] D. Falconer, S.L. Ariyavisitakul, A. Benyamin-Seeyar, and B. Eidson, "Frequency Domain Equalization for Single-Carrier Broadband Wireless Systems," *IEEE Commun. Mag.*, vol. 40, no. 4, pp. 58–66, Apr. 2002.
- [9] H. Sari, G. Karam, and I. Jeanclaude, "Transmission Techniques for Digital Terrestrial TV Broadcasting," *IEEE Commun. Mag.*, vol. 33, no. 2, pp. 100–109, Feb. 1995.
- [10] J. Lim, H.G. Myung, and D.J. Goodman, "Proportional Fair Scheduling of Uplink Single-Carrier FDMA Systems," to be presented at The 17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '06), Helsinki, Finland, Sep. 2006.
- [11] G. Song and Y. Li, "Cross-layer Optimization for OFDMA Wireless Networks-Part II: Algorithm Development," *IEEE Wireless Commun.*, vol. 4, pp. 625–634, Mar. 2005.
- [12] Z. Han, Z. Ji, and K. Liu, "Fair Multiuser Channel Allocation for OFDMA Networks Using Nash Bargaining Solutions and Coalitions," *IEEE Trans. on Commun.*, pp. 1366–1376, Aug. 2005.
- [13] R. Dinis, D. Falconer, C.T. Lam, and M. Sabbaghian, "A Multiple Access Scheme for the Uplink of Broadband Wireless Systems," *Proc. IEEE GLOBECOM '04*, vol. 6, Dallas, TX, pp. 3808–3812, Dec. 2004.



Design and Implementation of 64 Bit ALU for Power Optimization in Quaternary Four level Using VHDL

Priti V. Shingne

Department of Electronics & Communication
Tulsiramji Gaikwad-Patil College of engineering &
technology
Nagpur
priti_shingane@yahoo.com (+91-8007771245)

Prof. Rahul Dhature

Department of Electronics & Communication
Tulsiramji Gaikwad-Patil College of engineering &
technology
Nagpur
rahuldhature@gmail.com

Abstract—

The Arithmetic Logic Unit (ALU) design is very important in any Integrated Circuit based processing system. An ALU is also called the brain of any computing system. The Arithmetic operation and Logic operations are processed by ALU to serve the execution of hardware computing. In the proposed design a 64-bit ALU with clock gating is implemented on FPGA for low power and high speed applications. A low power consuming system offers the benefits like device portability, long battery life, good performance criteria, etc. To achieve low power operational performance various techniques have been proposed in previous works. Modification of hardware design provides the desired low power feature up to some extent of desired performance. The power consumption can also be affected by controlling the duration of the operation of the circuit. The circuit enable control logic provides transition signals to the operational circuit only for the duration until the results are calculated by the circuit. Once the results are generated the circuit activity is disabled. This saves the power consumption during the extra clock operations that is used after the generation of result by the circuit in the signal transition by the intermediate circuit. The Clock gating reduces power by controlling the clock signal activity that in turn controls the transition of logic values in the sub-blocks of the ALU. The power required in the undesired transitions is thus saved. The proposed design is implemented and simulated on Xilinx XC3S500E FPGA and its software simulation is performed on Xilinx ISE Test-bench Simulator.

Keywords—ALU, Clock Gating, Dynamic Power, FPGA, Opcode, Operand, Xilinx ISE etc.

I. Introduction

The remarkable increase in the density of Very Large Scale Integrated (VLSI) circuits is the result of advanced Integrated Circuits (IC) fabrication processes and the progress of automated design tools. When the number of devices accommodated on VLSI chips increases, many problems arise.

The interconnection between devices inside and outside a chip becomes significantly complicated and the area occupied by interconnections rise in haste. Aggressive interconnect scaling following Moore's law introduces many challenges in integration, performance and reliability. Inappropriate routing results in a larger chip size and cause timing and cross-talk problems. In deep submicron designs these problems are of outstanding importance.

II. ALU ARCHITECTURE IN PROPOSED DESIGN

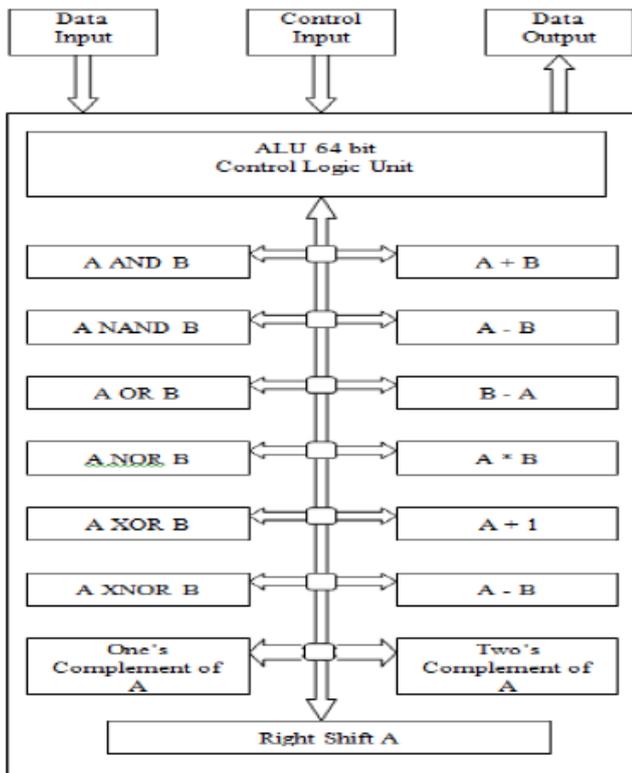


Fig -1: RTL Block of Proposed ALU Design

The ALU generally consists of basic building blocks as AND gate, OR gate, inverters, flip-flops, multiplexers and registers for various arithmetic and logical operation execution and control. A dedicated ALU operates on a fixed length of the input data. The performance of ALU is the main criteria to access the performance of any processing circuit or system. The utilization of different hardware units of ALU varies depending on the application of the system in which ALU is used as processing logic.

III. PRAPOSED DESIGN

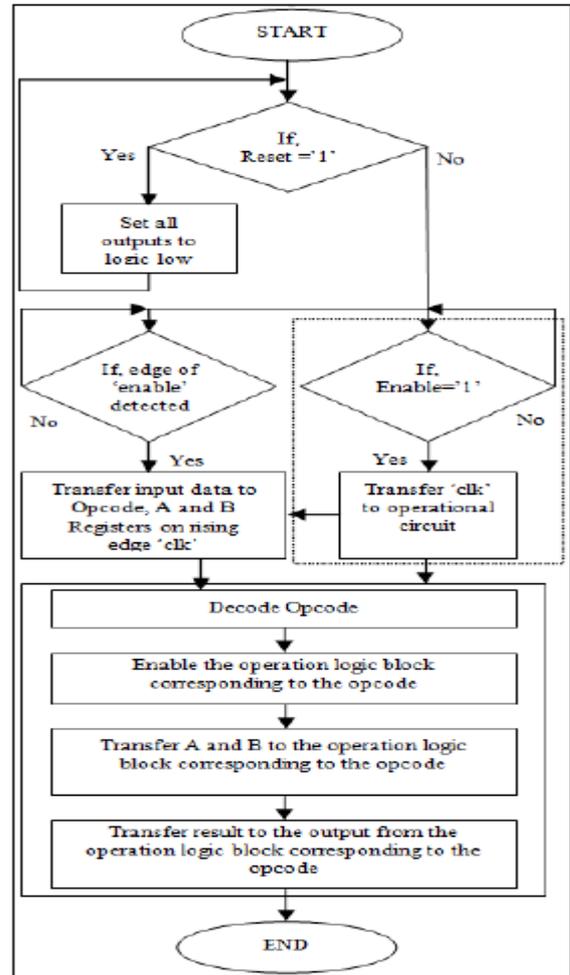


Fig -2: Logic Flow Chart of Proposed ALU Design

Operations are performed on 64-bit input operand values namely A and B. On the basis of the value of input opcode a particular operational logic block will be enabled to perform the logic operation. The output of the logic operation is transferred to the output signal register. The operation by the ALU is performed on the edge of the input clock signal. Once the result value is generated, the next operation can be initialized only when the “Enable” input is given a logic high value followed by a logic low value. The registers and output can be reset to logic low values at any time of operation.

IV. RADIX SELECTION

Several factors have influence in deciding the best radix usable. Obviously, in theory, higher radix would be best to represent as many numbers as possible. But, in practice, the limits of usability and availability of suitable devices limits the usability of higher radix based MVL circuits.

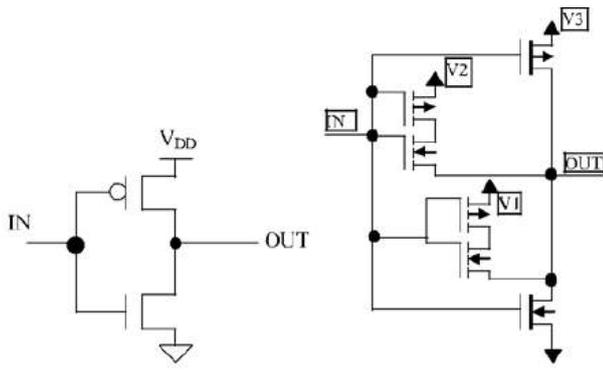
i. Area: Increased data density of multiple valued logic circuits does help, in principle, to reduce the area when compared to equivalent binary circuits. Each of the circuits stores more information per bit. Then net result is that the

large amount of data sets can be combined and implemented in minimum area. At smaller circuits, the additional overhead of “supplementary” logic in the proposed SUSLOC circuit structures does increase the area when compared to their equivalent binary gates.

ii. Performance: Performance of multiple valued circuits gets better with the increased radix. For maximum radix, the more difficult the timing analysis would get because we need to account for several design margins for various physical and electrical effects. But, primarily, the increase in radix would achieve better performance with some caveats of increased complexities in the actual timing closure.

iii. Power consumption: Power primarily consists of three parts: Dynamic power, Active leakage power and Standby leakage power. The Dynamic power is also referred to as the Switching power. Typically, this power is dominant of total power consisting of 70-75% of the total power.

The Active leakage being the next higher component, generally



a) CMOS inverter

b) Quaternary Radix-4 inverter

According to review paper [2] here they propose an arithmetic unit based on QSD number system based on quaternary system. The given design is developed using VHDL and implemented on FPGA device and results are compared with conventional arithmetic unit. Here we can use standard CMOS technology for designing Arithmetic and logical unit. The circuit performed with standard CMOS technology, with a voltage supply and use only simple voltage mode structures. Here, a clock boosting technique is used. It optimizes the switches resistance and power consumption. The proposed implementation reduces limitations seen in previous quaternary implementations published, such as the requirement of special advantages in the CMOS process or power-hungry current-mode cells.

V. DESIGN OF QUATERNARY CONVERTER CIRCUITS

Objective of optimization is to minimize number of gates needed and also to minimize depth of net. Depth of net is the largest number of gates in any path from input to output. The reason for choosing these two objectives is that they will give very good properties when implemented in VLSI. Minimizing number of gates will reduce the chip area, and minimizing depth will give highest clock frequency. A basic Quaternary to binary converter uses three down literal circuits DLC1, DLC2, DLC3. Each DLC having different threshold voltage and also have 2:1 multiplexer. Q is the quaternary input varying as 0, 1, 2 and 3 given to three DLC circuits. The binary outputs thus obtained will be in complemented form and are required to pass through inverters to get actual binary numbers. Down literal circuits are realized from basic CMOS inverter by changing the threshold voltages of p mos and n mos transistors

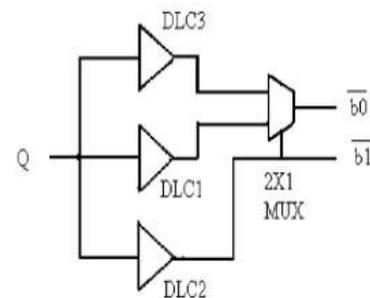


Figure 4: Quaternary to binary converter circuit:

VI. CONCLUSION

The conversion of binary to quaternary circuit is feasible and efficient in terms of power consumption and speed while being implemented in a standard CMOS technology.

As technologies are becoming more complex, multi valued logic (MVL) will be the future of circuit design. Since the research is still in initial stage on MVL the work is fundamental. When hardware implementation using MVL circuits is famous and more exposed to companies then one day MVL will surely turn over the binary logic. The advantages of lower power, higher performance, and reduced interconnect congestion motivate the use of quaternary circuits in a wide variety of applications.

References

- [1] Diogo Brito, Jorge Fernandes, Paulo Flores, Jose Monteiro, Taimur Rabuske, Senior member IEEE “ Quaternary Logic Look up Table in standard CMOS” 2014 IEEE transaction on very large scale integration system.
- [2] Nagamani A. N., Nischai S. PES institute of Technology, Karnataka, “ Quteranary High Performance Arithmetic Logic Unit Design” 2011 Euromica Conference.

- [3] Agarwal S., Pavankumar V. K. and Yokesh R., "Energy-efficient high performance circuits for arithmetic units" IEEE International Conference 2008.
- [4] E. Arbel, C. Eisner and O. Rokhlenko, "Resurrecting infeasible clock-gating functions", Design Automation Conference 46th ACM / IEEE, 2009.
- [5] T. Lam, X. Yang. W. C. Tang and Y. L. Wu, "On Applyinf Erroneous Clock-gating conditions to further cut down Power", Design Automation Conference (ASP-DAC), 2011.
- [6] Deoborah, "High Speed Energy Efficient ALU design using Vedic multiplication Techniques", International Conference on Advances in Computational Tools for Engineering Applications (ICACTEA '09), pp. 600-3, July 2009.
- [7] P. Saha, A. Banerjee, A. Dandapat and P. Bhattacharyya, "Vedic Mathematics based 32-bit Multiplier Design for High Speed Low Power Processors", International Journal on Smart Sensing and Intelligent Systems (IJSSIS), Volume 4, Issue 2, June 2011.
- [8] Tang A. J. J. and Reyes J. A., "Comparative analysis of low power multiplier architectures" IEEE Symposium 2011.



VHDL Implementation of Multistandard Inverse Transform for H.264/MPEG/VC-1

PALLAVI.S.CHAVAN

Electronics and Communication Engineering Dept.
Tulsiramji Giakwad Patil College Of Engg. And Tech.
Nagpur, India
e-mail address- thatzpallavi@gmail.com
Contact No.-9881721232

TRUPTI MOHOTA

Electronics Engineering Dept.
Tulsiramji Giakwad Patil College Of Engg. And Tech.
Nagpur, India
e-mail address- trupti.etrx@tgp cet.com
ContactNo.-8888855875

Abstract— In recent years, different video applications use different video standards, such as H.264/AVC, VC-1, and AVS. To improve the coding efficiency further, recently a joint collaboration team on video coding (JCT-VC) is drafting a next generation video coding standards, known tentatively as high efficient video coding (HEVC or H.265). The target bit rate is half of that of H.264/AVC. Besides, several other effective techniques are proposed in the draft to reduce the complexity of the encoder such as improved intrapicture coding, and simpler VLC coefficients. As a result of these new features, experts predict that the HEVC will dominate the future multimedia market.

Keywords— intrapicture codin ; HEVC;

Introduction

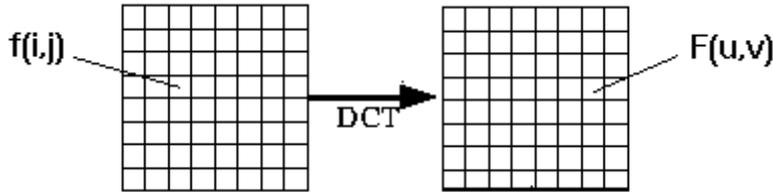
TRANSFORMS are widely used in video and image applications. Several groups, such as The International Organization for Standardization (ISO), International Telecommunication Union Telecommunication Standardization Sector (ITU-T), and Microsoft Corporation, have developed various transform dimensions and coefficients, corresponding to different applications. Numerous researchers have worked on transform core designs, including discrete cosine transform (DCT) and integer transform, using distributed arithmetic, factor sharing (FS), and matrix decomposition methods to reduce hardware cost. The inner product can be implemented using ROMs and accumulators instead of multipliers to reduce the area cost. Yu and Swartzlander present an efficient method for reducing ROMs size with recursive DCT algorithms. Although ROMs are likely to scale much better than other circuits with shrinking technology nodes, several ROM-free DA architectures have recently emerged [3]–[8]. Shams *et al.* [3] employ a bit-level sharing scheme to construct the adder-based

butterfly matrix, called new DA (NEDA). To improve the throughput rate of the NEDA method, high-throughput adder trees are introduced.

a delta matrix to share hardware resources using the FS method. They derive matrices for multistandards as linear combinations from the same matrix and delta matrix, and show that the coefficients in the same matrix can share the same hardware resources by factorization. To further reduce the area, present optimization strategies for FS and adder sharing (AS) for multistandard (MST) applications. Fan and Su use the matrix decomposition method to establish the sharing circuit. Matrices for VC-1 transformations can be decomposed into several small matrices, a number of which are identical for different points transforms. Hardware resources can be shared. Moreover, other previous works on hardware resource sharing are presented in. Recently, reconfigurable architectures have been presented as a solution to achieve a good flexibility of processors in field-programmable gate array (FPGA) platform or application-specific integrated circuit (ASIC), such as ASAP, Ambric, MORA, and SmartCell. Although these reconfigurable architectures have the feature of flexibility, the pure ASIC design can be recommended for a fixed customer application suitably. Because of the same properties in DCT and integer transform applied to Moving Picture Experts Group (MPEG), H.26 and Windows Media Video (WMV-9/VC-1), many MST cores are presented to introduce a fully supported transform core for the H.264 standard, including 8×8 and 4×4 transforms. The eight-point and four-point transform cores for MPEG-1/2/4 and H.264 and cannot support the VC-1 compression standard. In and, 8×8 , 8×4 , 4×8 , and 4×4 transform cores are shown for VC-1, whereas in, and MST cores supporting the MPEG-1/2/4, H.264, and VC-1 Standards are addressed.

1D DCT/IDCT

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain



DCT Encoding

The general equation for a 1D (N data items) DCT is defined by the following equation:

$$F(u) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \Lambda(i) \cdot \cos \left[\frac{\pi \cdot u}{2 \cdot N} (2i + 1) \right] f(i)$$

and the corresponding *inverse* 1D DCT transform is simple $F^{-1}(u)$, i.e.:

where

$$\Lambda(i) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for } \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

The general equation for a 2D (N by M image) DCT is defined by the following equation:

$$F(u, v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(i) \cdot \Lambda(j) \cdot \cos \left[\frac{\pi \cdot u}{2 \cdot N} (2i + 1) \right] \cdot \cos \left[\frac{\pi \cdot v}{2 \cdot M} (2j + 1) \right] \cdot f(i, j)$$

and the corresponding *inverse* 2D DCT transform is simple $F^{-1}(u, v)$, i.e.:

where

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for } \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

The basic operation of the DCT is as follows:

- The input image is N by M ;
- $f(i,j)$ is the intensity of the pixel in row i and column j ;
- $F(u,v)$ is the DCT coefficient in row $k1$ and column $k2$ of the DCT matrix.

- For most images, much of the signal energy lies at low frequencies; these appear in the upper left corner of the DCT.
- DCT is similar to the Fast Fourier Transform (FFT), but can approximate lines well with fewer coefficients.

• Compression is achieved since the lower right values represent higher frequencies, and are often small - small enough to be neglected with little visible distortion.

• The DCT input is an 8 by 8 array of integers. This array contains each pixel's gray scale level;

• 8 bit pixels have levels from 0 to 255.

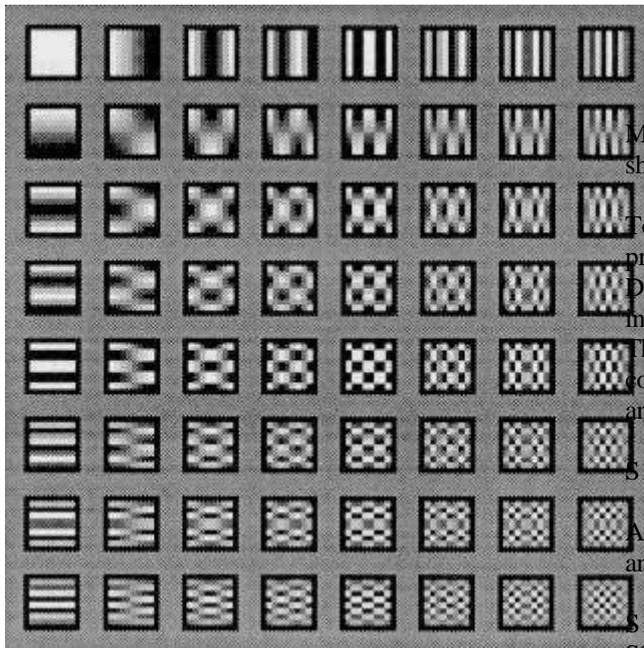
• Therefore an 8 point DCT would be:

where

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for } \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

• The output array of DCT coefficients contains integers; these can range from -1024 to 1023.

• It is computationally easier to implement and more efficient to regard the DCT as a set of **basis functions** which given a known input array size (8×8) can be precomputed and stored. This involves simply computing values for a convolution mask (8×8 window) that get applied (sum values) x pixel the window overlap with image apply window accros all rows/columns of image). The values as simply calculated from the DCT formula. The 64 (8×8) DCT basis functions are illustrated in below fig.



Mathematical derivation of proposed Common Sharing distributed Algorithm

To gain better resource sharing of inner product operation, The proposed CSDA method combines Factor Sharing and Distributed methods. To find FS and DA methods are described in the following. a. Mathematical derivation of Factor Sharing
The factor sharing method shares the same factor in different coefficients of applied input. consider two different elements s_1 and s_2 with same input X as an example.

$$S_1 = C_1 X, S_2 = C_2 X \quad (1)$$

Assuming the same factor F_s can be found in coefficients C_1 and C_2 , S_1 and S_2 can be rewritten as follows.

$$\begin{aligned} S_1 &= (F_s 2^{k_1} + F_{d1}) X \\ S_2 &= (F_s 2^{k_2} + F_{d2}) X \end{aligned} \quad (2)$$

Where k_1 and k_2 indicates the weight position of the sharing factor F_s in C_1 and C_2 respectively. F_{d1} and F_{d2} denote the remainder coefficients after extracting sharing factor F_s for C_1 and C_2 respectively.

$$\begin{aligned} F_{d1} &= C_1 - F_s 2^{k_1} \\ F_{d2} &= C_2 - F_s 2^{k_2} \end{aligned} \quad (3)$$

Mathematical derivation of Common sharing distributed arithmetic:

The inner product for a general multiplication and accumulation can be written as

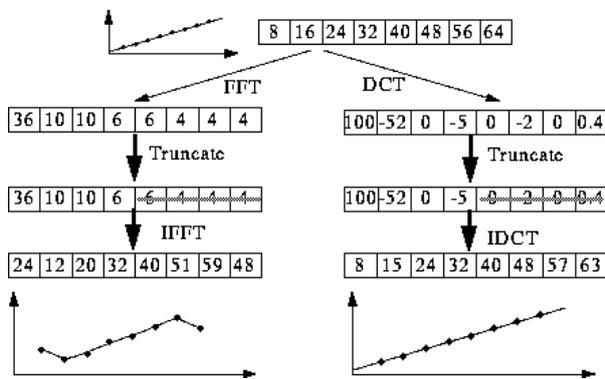
$$Y = \sum_{i=1}^L A_i X_i \quad (4)$$

where X_i is input data, A_i is N -bit CSD coefficient it can be expressed as follow.

$$Y = [2^0 \ 2^{-1} \ \dots \ 2^{-(N-1)}] \cdot \begin{bmatrix} A_{1,0} & A_{2,0} & \dots & A_{L,0} \\ A_{1,1} & A_{2,1} & \dots & A_{L,1} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1,(N-1)} & A_{2,(N-1)} & \dots & A_{L,(N-1)} \end{bmatrix} \begin{bmatrix} X_1 \\ X_2 \\ \vdots \\ X_L \end{bmatrix}$$

$$= [2^0 \ 2^{-1} \ \dots \ 2^{-(N-1)}] \begin{bmatrix} Y_0 \\ Y_1 \\ \vdots \\ Y_{(N-1)} \end{bmatrix}$$

Where $Y_i = \sum A_i X_i$, $A_{i,j} \in \{-1, 0, 1\}$ and

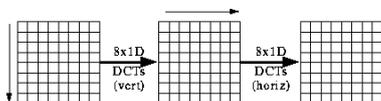


DCT/FFT Comparison

Computing the 2D DCT

- Factoring reduces problem to a series of 1D DCTs
- apply 1D DCT (Vertically) to Columns.
- apply 1D DCT (Horizontally) to resultant Vertical DCT above
- or alternatively Horizontal to Vertical.

The equations are given by:



$i=1$
 $j=0, \dots, (N-1)$. If Y_j can be calculated by adding or subtracting X_i with $A_{i,j} \neq 0$. The product Y can then be obtained by shifting and adding every non-zero Y_j .

1-D Common Sharing Distributed arithmetic-MST:

Based on the proposed CSDA algorithm, the coefficients for MPEG-1/2/4, H.264, and VC-1 transforms are chosen to achieve high sharing capability for arithmetic resources. To adopt the searching flow, software code will help to do the iterative searching loops by setting a constraint with minimum nonzero elements. In this paper, the constraint of minimum nonzero elements is set to be five. After software searching, the coefficients of the CSD expression, where 1 indicates -1. Note that the choice of shared coefficient is obtained by some constraints. Thus, the chosen CSDA coefficient is not a global optimal solution. It is just a local or suboptimal solution. Besides, the CSD codes are not the optimal expression, which have minimal nonzero bits. However, the chosen coefficients of CSD expression can achieve high sharing capability for arithmetic resources by using the proposed CSDA algorithm. More information about CSDA coefficients for MPEG-1/2/4, H.264, and VC-1 transforms.

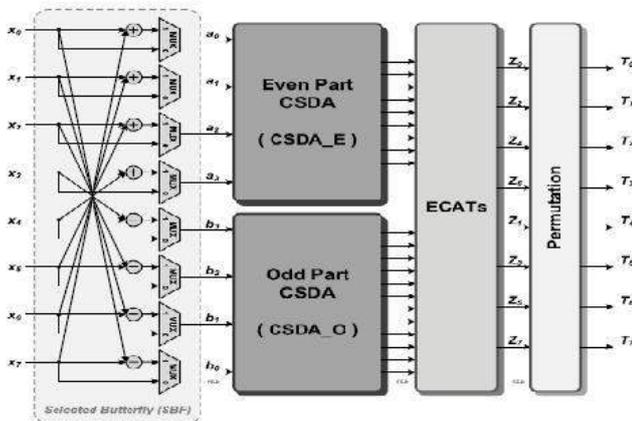


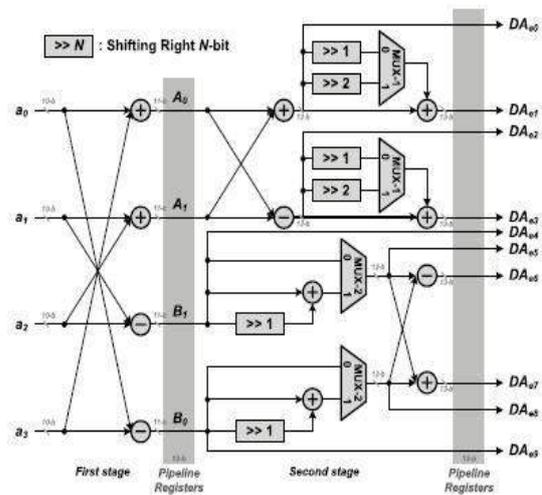
Fig.1. Architecture of proposed 1-D CSDA-MST

Even part common sharing distributed arithmetic circuit:

The SBF module executes for the eight-point transform and bypasses the input data for two four-point transforms. After the SBF module, the CSDA_E and CSDA_O execute and by feeding input data a and b , respectively. The CSDA_E calculates the even part of the eight-point transform, similar to

the four-point Transform for H.264 and VC-1 standards. Within the architecture of CSDA_E, two pipeline stages exist

(12-bit and 13-bit). The first stage executes as a four-input butterfly matrix circuit, and the second stage of CSDA_E then executes by using the proposed CSDA algorithm to share hardware resources in variable standards.



odd part of the eight-point transform and four-point transform

for variable standards. It contains selection signals multiplexers (MUXs) for different standards. Eight adder trees with error compensation (ECATs) are followed by the CSDA_E and CSDA_O, which add the nonzero CSDA coefficients with corresponding weight as the tree-like architectures. The ECATs circuits can alleviate truncation error efficiently in small area design when summing the nonzero data all together.

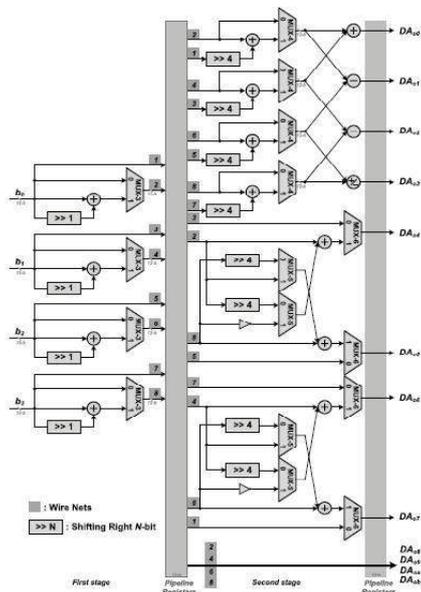


Fig.3 Architecture of odd part CSDA

EXPECTED OUTPUT

The CSDA-MST core can achieve high performance, with a high throughput rate and low-cost VLSI design, supporting MPEG-1/2/4, H.264, and VC-1 MSTs. By using the proposed CSDA method, the number of adders and MUXs in the MST core can be saved efficiently. Measured results show the CSDA-MST core with a throughput rate of 1.28 G-pels/s, which can support $(4928 \times 2048@24 \text{ Hz})$ digital cinema format with only 30 k logic gates. Because visual media technology has advanced rapidly, this approach will help meet the rising high-resolution specifications and future needs as well.

REFERENCES

- [1]:- Yuan-Ho Chen, *Jyun-Neng Chen, Tsin-Yuan Chang, and Chih-Wen Lu*. “High-Throughput Multistandard Transform Core Supporting MPEG/H.264/VC-1 Using Common Sharing Distributed Arithmetic”, 2014.
- [2]:- A. M. Shams, Peng C *et al.*, 2007; Huang C Y *et al.*, 2008; Chen Y H *et al.*, 2011; Chen Y H *et al.*, “NEDA: A low-power high-performance DCT architecture,” 2006.
- [3]:- H. Chang, S. Kim, S. Lee, and K. Cho. , “Design of area-efficient unified transform circuit for multi-standard video decoder,”.
- [4]:- S. R. Chalamalasetti, S. Purohit, M. Margala, and W. Vanderbauwhede, “MORA-an architecture and programming model for a resource efficient coarse grained reconfigurable processor,”.

VLSI ARCHITECTURE OF PARALLEL MULTIPLIER– ACCUMULATOR BASED ON RADIX-2 MODIFIED BOOTH ALGORITHM

Bhavana Bhoyar

M.Tech Student, Department of Electronics and
Communication , Tulsiramji Gaikwad-Patil College of
Engineering &Tech. Nagpur, India.
bhavnabhoyar@gmail.com
Contact No.7276433748

R. Dhature

Asst. Prof., Department of Electronics and Communication ,
Tulsiramji Gaikwad-Patil College of Engineering &Tech.
rahul.etrx@tgp cet.com
Contact No: 9689919712

ABSTRACT - A new architecture of multiplier-and Accumulator (MAC) for high-speed arithmetic. By combining multiplication with accumulation and devising a hybrid type of carry save adder (CSA), the performance was improved. Since the accumulator that has the largest delay in MAC was merged into CSA, the overall performance was elevated. The proposing method CSA tree uses 1's-complement-based radix-2 modified Booth's algorithm (MBA) and has the modified array for the sign extension in order to increase the bit density of the operands. The proposed MAC showed the superior properties to the standard design in many ways and performance twice as much as the previous research in the similar clock frequency. We expect that the proposed MAC can be adapted to various fields requiring high performance such as the signal processing areas

Keywords- Multiplier and accumulator, Carry save adder, Booth algorithm, Standard design

I.INTRODUCTION

Multiplication can be considered as a series of repeated additions. The number to be added is the multiplicand, the number of times that it is added is the multiplier, and the result is the product. Each step of addition generates a partial product. In most computers, the operand usually contains the same number of bits. When the operands are interpreted as integers, the product is generally twice the length of operands in order to preserve the information content. This repeated addition method that is suggested by the arithmetic definition is slow that it is almost always replaced by an algorithm that makes use of positional representation. It is possible to decompose multipliers into two parts. The first part is dedicated to the generation of partial products, and the second one collects and adds them.

A.MULTIPLIER AND ACCUMULATOR

A multiplier can be divided into three operational steps. The first is radix-2 Booth encoding in which a partial product is generated from the multiplicand X and the multiplier Y. The second is adder array or partial product compression to add all partial products. The last is the final addition in which the process to accumulate multiplied results is included.

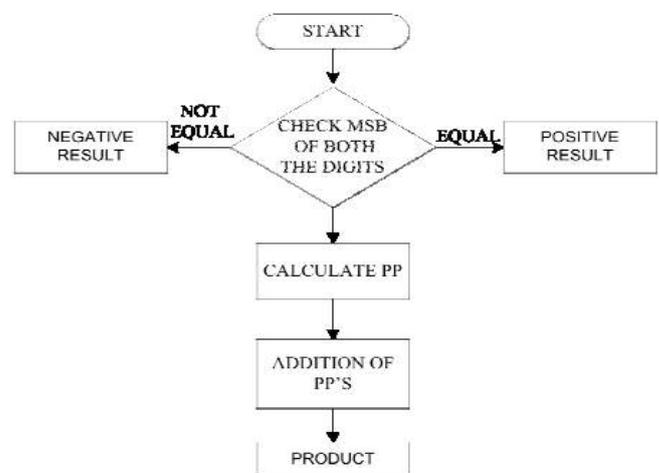


Fig. 1: Signed Multiplication Algorithm

It executes the multiplication operation by multiplying the input multiplier X and the multiplicand Y. This is added to the previous multiplication result Z as the accumulation step. If - bit data are multiplied, the number of the generated partial products is proportional to N. In order to add them serially, the execution time is also proportional to N. The architecture of a multiplier, which is the fastest, uses radix-2 Booth encoding that generates partial products. If radix-2 Booth encoding is used, the number of partial products, is reduced to half, resulting in the decrease in Addition of Partial Products step. In addition, the signed multiplication based on 2's complement numbers is also possible. Due to these reasons, most current used multipliers adopt the Booth encoding.

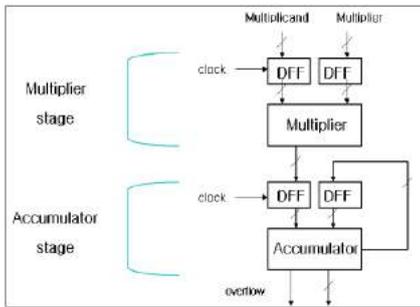


Fig: Simple MAC Architecture

2.1. The product of $A_i \times B_i$ is always fed back into the 32-bit accumulator and then added again with the next product $A_i \times B_i$. This MAC unit is capable of multiplying and adding with previous product consecutively up to as many as times.

3. PROPOSED MAC

If an operation to multiply two N-bit numbers and accumulate into a 2N-bit number is considered, the critical path is determined by the 2N-bit accumulation operation. If a pipeline scheme is applied for each step in the standard design of Fig, the delay of last accumulator must be reduced in order to improve the performance of the MAC.

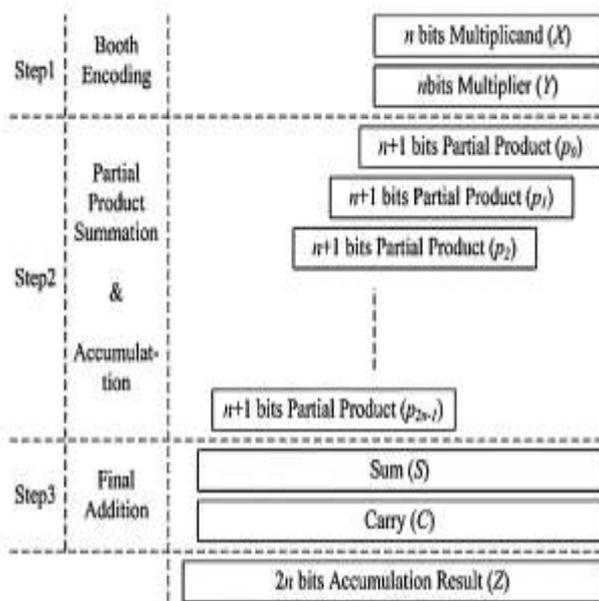


Fig: Arithmetic Operation Of Multiplication And Accumulation

The overall performance of the proposed MAC is improved by eliminating the accumulator itself by combining it with CSA function. If the accumulator has been eliminated the critical path is then determined by the final adder in the multiplier. The basic method to improve the performance of final adder is to decrease the no of input bits. In order to reduce these no input bits, the multiple partial products are compressed into a sum and carry by CSA. The number of bits of sums and carries to be transferred to the final adder is reduced by adding lower bits of sums and carries in advance within the range in which the overall performance will not be degraded.

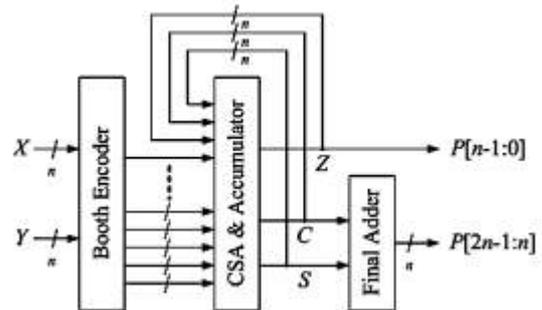


Fig: Hardware Architecture MAC

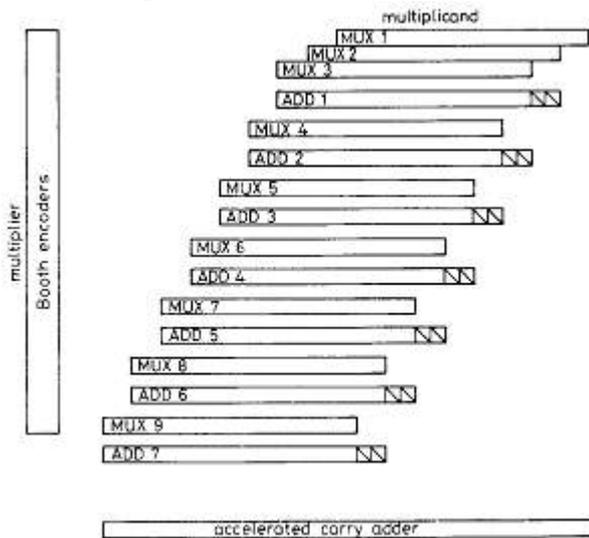
A 2-bit CLA is used to add the lower bits in CSA. In addition to increase the output rate when Pipelining is applied, the sum and carries from the CSA are accumulated instead of outputs from the final adder in the manner that the sum and carry from CSA in the previous cycle are inputted to the CSA. Due to this feedback of sum and carry, the number inputs to the CSA increases compared to standard design. In order to efficiently increase the amount of data, a CSA architecture is modified to treat the sign bit.

III.A. CONVENTIONAL HARDWARE - IMPLEMENTATION OF BOOTH'S ALGORITHM

In the circuit for a Booth multiplier the control signals ADD, SUB, ZERO, ADD x 2 and SUB x 2 are generated from the multiplier operand Y using Booth encoding logic. Fig. shows a multiplexer for a single bit position of the multiplicand X. It consists of five transmission gate switches, which use the five control signals generated by a Booth encoder, to select the appropriate bit of the multiplicand or its inverse. Subtraction is performed using 2's complement addition. This involves adding the inverse of the multiplicand and adding a further '1' at the least significant bit (LSB) position for SUB and at the next most significant bit for SUB x 2.

Fig: Standard 16-bit Booth Multiplier Architecture
The standard 16-bit Booth multiplier block diagram, where the product is formed by summing

the outputs from the nine multiplexers in sequence. There is one multiplexer for each Booth encoder, and for unsigned arithmetic they are each 18 bits in length. Of the two extra zero-bits at the most significant end, one is required so that the MSB of the multiplicand is zero to indicate a positive number in the internal 2's complement format. The second is to allow for the left-shift in the ADD x 2 and SUB x 2 operations.



The 'add' rows are rows of full adders which produce sum and carry outputs that are then used as inputs to the next row. There is no carry propagation along these rows. The first three multiplexers provide the inputs to the first adder row and thereafter a further multiplexer input, together with the sum and carry from the previous adder row, form the inputs to the next adder row. For the conventional Booth multiplier of Fig. , two extra adders, indicated by diagonal lines, are required at the least significant end of each adder row to add in the subtract flags from the preceding row. It is also necessary to sign extend (replicate the MSB) by two bits at each stage before it is added into the next stage, since each add row is left shifted by two bits with respect to the previous row. These sign extensions at each stage are, in total, equivalent to sign extending the multiplicand to the full width of the result.

III.B.MODIFIED BOOTH 'S ALGORITHM

Multiplication consists of three steps: 1) the first step to generate the partial products; 2) the second step to add the generated partial products until the last two rows are remained; 3) the third step to compute the final multiplication results by adding the last two rows. The modified Booth algorithm reduces the number of partial products by half in the first step. We used the modified Booth encoding (MBE) scheme proposed in. It is known as the most efficient Booth encoding and decoding scheme. To multiply X by Y using the modified Booth algorithm starts from grouping Y by three bits and

encoding into one of {-2, -1, 0, 1, 2}. Table I shows the rules to generate the encoded signals by MBE scheme and Fig. 1 (a) shows the corresponding logic diagram. The Booth decoder generates the partial products using the encoded signals as shown in Fig

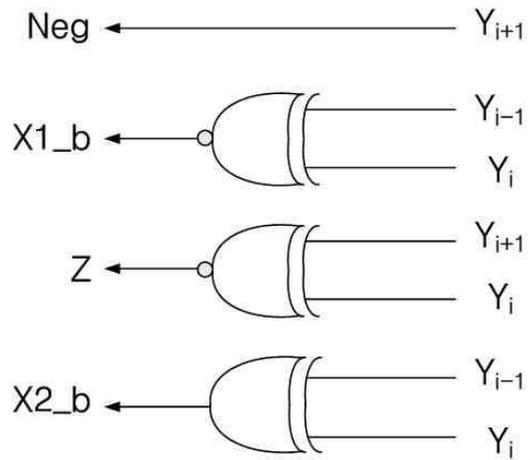


Fig: Booth Encoder

The below fig. shows the generated partial products and sign extension scheme of the 8-bit modified Booth multiplier. The partial products generated by the modified Booth algorithm are added in parallel using the Wallace tree until the last two rows are remained. The final multiplication results are generated by adding the last two rows. The carry propagation adder is usually used in this step.

Booth multiplication is a technique that allows for smaller, faster multiplication circuits, by recoding the numbers that are multiplied. It is possible to reduce the number of partial products by half, by using the technique of radix-4 Booth recoding. The basic idea is that, instead of shifting and adding for every column of the multiplier term and multiplying by 1 or 0, we only take every second column, and multiply by ± 1 , ± 2 , or 0, to obtain the same results. The advantage of this method is the halving of the number of partial products. To Booth recode the multiplier term, we consider the bits in blocks of three, such that each block overlaps the previous block by one bit. Grouping starts from the LSB, and the first block only uses two bits of the multiplier.

The PP generator generates five candidates of the partial products, i.e., $\{-2A, -A, 0, A, 2A\}$. These are then selected according to the Booth encoding results of the operand B. When the operand besides the Booth encoded one has a small absolute value, there are opportunities to reduce the spurious power dissipated in the compression tree

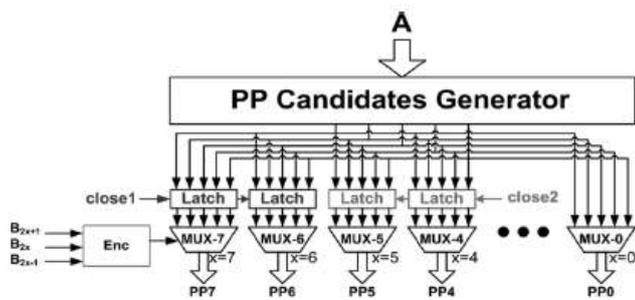


Fig: SPST equipped modified Booth encoder

The multiplication first step generates from A and X a set of bits whose weights sum is the product P. For unsigned multiplication, P most significant bit weight is positive, while in 2's complement it is negative.

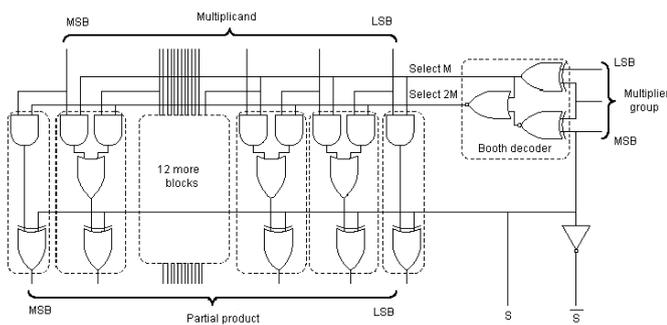


Fig: Booth partial product selector logic

The partial product is generated by doing AND between 'a' and 'b' which are a 4 bit vectors as shown in fig. If we take, four bit multiplier and 4-bit multiplicand we get sixteen partial products in which the first partial product is stored in 'q'. Similarly, the second, third and fourth partial products are stored in 4-bit vector n, x, y.

CONCLUSION

A 16x16 multiplier-accumulator (MAC) is presented in this work. A RADIX- 4 Modified Booth multiplier circuit is used for MAC architecture. Compared to other circuits, the Booth multiplier has the highest operational speed and less hardware count. The basic building blocks for the MAC unit are identified and each of the blocks is analyzed for its performance. Power and delay is calculated for the blocks. 1-bit MAC unit is designed with enable to reduce the total power consumption based on block enable technique. Using this block, the N-bit MAC unit is constructed and the total power consumption is calculated for the MAC unit.

Future Work: The current analysis produces high accuracy for the fixed width output product which is of length $2n$ - bits i.e. n multiplicand n multiplier produce $2n$ - bit output product. There is a further need to produce high accuracy for the fixed width of half, quarter, one by eighth and one by sixteenth of the product term bits. The above need is satisfied by means of comparator and sorting network which uses minimum number of logic gates.

REFERENCES

- [1] J.J.F. Cavanagh, Digital Computer Arithmetic. New York: McGraw-Hill, 1984.
- [2] Information Technology Co dig of Moving Picture and Associated Audio, MPEG 2Draft International Standard, ISO/IEC 13818-1,2,3, 1994.
- [3] JPEG2000 Part I Final 11919 Draft, ISO/IEC JTC1/SC29 WG1.
- [4] O. L. Mac Sorley, "High speed arithmetic in binary computers," Proc. IRE, vol. 49, pp. 6791, Jan. 1961.
- [5] S. Waser and M. J. Flynn, Introduction Arithmetic for Digital Systems Designers. New York: Holt, Rinehart and Winston, 1982.
- [6] A. R. Omondi, Computer Arithmetic Systems. Englewood Cliffs, NJ: Prentice-Hall, 1994.
- [7] A. D. Booth, "Assigned binary multiplication technique," Quart. J. Math., vol. IV, pp. 236-240, 1952.
- [8] C. S. Wallace, "A suggestion for a fast multiplier," IEEE Trans. Elec-tron Comput., vol. EC 13, no. 1, pp. 14-17, Feb. 1964.
- [9] A. R. Cooper, "Parallel architecture modified Booth multiplier," Proc. Inst. Electr. Eng. G, vol. 135, pp. 125-128, 1988.
- [10] N. R. Shanbag and P. Juneja, "Parallel implementation of a 4-bit multiplier using modified Booth's algorithm," IEEE J. Solid-State Circuits, vol. 23, no. 4, pp. 1010-1013, Aug. 1988.
- [11] G. Goto, T. Sato,



FPGA IMPLEMENTATION OF 256 BIT AES FOR SECURED WIRELESS COMMUNICATION

Sneha S. Bonde

*Electronics and Communication Department
Tulsiramji Gaikwad-Patil Clg Of Engg And
Technology,Nagpur
Nagpur,India
Contact no:- 9545409482
e-mail address :- snehabonde77@gmail.com.*

Rohini Pochhi

*Electronics and Communication Department
Tulsiramji Gaikwad-Patil clg of Engg And
Technology,Nagpur
Nagpur,India
Contact no :- 8554982350
e-mail address : - rohini.ece@tgpct.com*

Abstract—The process of encryption translate the original data into a secret code.it is the most effective way to achieve the data security. To read an encrypted file, one must have an access to a secret key or password that enables us to decrypt the information. The unprocessed data is called plain text, the encrypted data is referred to as the cipher text. There are various algorithms available in cryptography like MARS, RSA, TWOFISH, SERPENT & RIJNDAEL. AES is a variant of rijndael which has fixed block size of 128 bits, and a key size 128, 192, 256 bits. By contrast, the rijndael algorithm in itself is specified with block key size that may be any multiple of 32 bits both with a minimum of 128 & a maximum of 256 bits, the advantages of AES are it is the symmetric iterative algorithm, processes data as block of 4 columns of 4bits, operates on entire data block is a every round encryption key. This cryptographic technic not only brings high data security due its increase key length but also make decryption processes more immune towards the problem of breaking key. This work discuss the methodology to implement a 128 bits version of AES on FPGA.

Keywords—component; formatting; style; styling; insert (key words)

Introduction

the AES- Information technology and widespread used, the security of sensitive data on Internet is especially important. Traditional cryptographic methods have failed to meet the requirements, especially to its security, speed and efficiency. AES (Advanced Encryption Standard), also known as the Rijndael Cryptography, is a block encryption algorithm recommended by the NIST (National Institute of Standards and Technology) following the DES (Data Encryption Standard) and 3DES. AES has been extensively analyzed and widely used. Currently, it has become one of the popular algorithms in the symmetric the different lengths of the key, AES can be divided into AES-128, AES-192, AES-256. Till now, there have been many studies on AES implementations. Hammad designed a pipeline structure, with up to 39 GB/s throughput, up to 10662 slice hardware resource consumption. According to the different lengths of the key, AES can be divided into AES-128, AES-192, AES-256. Till now, there have been many studies on AES implementations. Hammad designed a pipeline structure, with up to 39 GB/s throughput, up to 10662 slice hardware resource consumption [1]. Zhang also used the pipeline structure to achieve 128 encryption circuit, using RAM to store S-

box, with up to 34 GB/s throughput. The cost of the hardware resources is up to 2389 slices and 200 RAM [2]. As we can see, even though the pipeline structure can achieve high performance, but for Gigabit Ethernet applications, the required bandwidth is limited, the overcome performance will waste the resources.

In the other hand, it can only realize AES-128 [3-5]. Above all, in this paper, we give a reconfigurable AES on the FPGA (Field Programmable Gate Array) without changing hardware conditions. Depending on the application requirements, it can flexibly choose different key lengths for encryption and decryption according to different needs. Firstly, this paper provides an analysis of framework of the AES algorithm. Secondly, we put forward reconfigurable hardware implementation of AES-128, AES-192, AES-256. Lastly, we take the project to prove the validity of this design and illustrate that the algorithm rate can be increased. Compared to the other implementations with the different key length, this design can efficiently reuse the function modules, greatly reduce the area of the circuit and meet the needs of data exchange-rate of Gigabit Ethernet.

A. FRAME WORK OF AES

According to Rijndael, every group of AES length is fixed at 128 bit, key length is 128, 192 or 256 bits. It is a kind of block cipher algorithms. The number of encryption or decryption rounds is depended on the different key length. The relationship between AES algorithm rounds and key length is shown in table I

TABLE I. AES ALGORITHM ROUND AND KEY LENGTH

AES	Structure of AES algorithm		
	Key length	Group size	Number of rounds
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

As shown in Fig. 1,

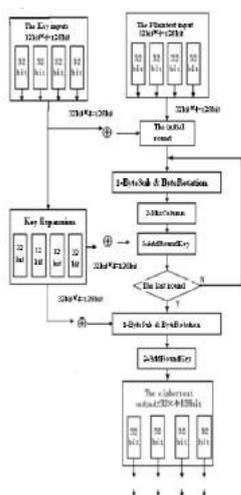
each round of AES encrypted loop

(except the final round) consists of 4 steps:

- **Add Round Key Step.** Every byte in the matrix has been doing operations xor with the rotation key

(round key), and each round key is generated by the key generation algorithm.

- **Sub Bytes Step.** Though using a nonlinear function, each byte is replaced with the corresponding bytes. Sometimes it can be achieved by looking up in the table.
- **Shift Rows Step.** Shift each line according to certain
- **MixColumns Step.** To fully mixed operation of individual row in a matrix, this step uses a linear transformation to be mixed within each of the four bytes. AES is simple, easy and flexibility. Strong function has good parallel characteristics which are
- accommodate to hardware design and implementation.



In the process of the encryption, it should omit them MixColumns step in the last encrypted loop and be replaced by another Add Round Key Step. The decryption process is the reverse of the encryption. More detail information can be found in the paper [6].

III. RECONFIGURABLE AES ENCRYPTION/DECRYPTION CIRCUIT

A .Architecture of Encryption/Decryption Circuit

Using hardware in realizing cryptographic algorithms have been more and more popular and important. Compared with the traditional software realization, hardware has the following advantages: a) having good security, not easy to be attacked; b) calculation in high speed and high efficiency; c) low cost, reliable performance. In order to design and achieve different key length of the AES on the same cipher, this design uses the id reconfigurable hardware, introduces a state machine, uses a controller to keep down the SubBytes module, the ShiftRows modul MixColumns module and the AddRoundKey module. This structure can meet the users' needs of the three different key lengths of AES dynamically. As shown in Fig. 2, the design of AES top module, key encryption generation Encryption/Decryption modules are controlled by the controller.

B. Each Module Based on FPGA Design

1) **SubBytes and InvSubBytes:** SubBytes is based on the inverse operation over finite fields (inverse operation is the only nonlinear transformation in AES algorithm). In thiM paper, we use inverse operation and affine transformations to design SubBytes instead of using S-box.

2) **RhifRows and InvShiftRows:** RhifRows is a step that it makes every row of the data block, 4×4bytes, shift circularly. InvShiftRows is the inverse operation of ShiftRows. In order to reduce the data reading frequency, improving the efficiency of data encryption and decryption, the design usually combine SubBytes and ShiftRows module, InvShiftRows and InvSubBytes modules

3) **Mixcolumns and InvMixcolumns:** Mixcolumns and InvMixcolumns transformation matrix are shown in Fig.9 & Fig.10. Enter the status column in the matrix $(a0j, a1j, a2j, Ma3j)T$, through the (counter) mixing, the columns are transformed into the output matrix analyses the realization methods of Mixcolumns and InvMixcolumns. In terms of resource consumption, bothmixcol-sb is at least, as 398 LUT. Through comparing the two modules, Mixcolumns containing InvMixcolumns, so we combine these two operations. This paper introduces the realization of InvMixcolumns unlike [8]. It uses less hardware resource. Here is the analysis and implementation. In the design of Mixcolumns and InvMixcolumns, the method of table look-up which runs so fast can replace the multiply operation, but it cost so much hardware resources. Defines a table contains 256 bytes, named $X2$, to achieve 8 bits input and 8 bits output, making $X2[ij]=02i$.

This operation is frequently used when hardware resources is sufficient. The circuit use 8 LUT to complete the 8-8 transform. We put 8bits into the upper 4 bits and the lower 4bits, respectively as the addresses of the RAM that is made

of 4LUT. Then combine the two output data (8bits). To sum up, the 8-8 transformation is completed. (as shown in Fig.11). Key expansion module is responsible for each round of

the key. They usually have two ways, internal extensions and external extensions. Using external extensions, we just follow the Rijndael fazed, and then expand into the chip. Using the internal expansion, consideration must be given to the key expansion speed, run time must be less than the encryption and decryption, and otherwise it will be error. But with external key extension, there requires large amounts of storage space to store the intermediate keys, increasing the storage costs. Now many proposals use internal expansion in key expansion module [8]. It is necessary to control cryptographic operations using state machines and key synchronization extension. In decryption operation uses an external expansion, that is, before we decrypt the cipher text will first find the encryption key, stored in the corresponding register. This advantage is only in the design of design cryptographic key expansion module, but not in the additional decryption

key generated module. The drawback for the excessive number of registers holds a key, and consumes hardware resources area when we use the internal expansion. As shown in Fig. 1, each round of AES encrypted loop (except the final round) consists of 4 steps: Σ Add Round Key Step. Every byte in the matrix has been doing operations x or with the rotation key (round key), and each round key is generated by the key generation algorithm. SubBytes Step. Though using a nonlinear function, each byte is replaced with the corresponding bytes. Sometimes it can be achieved by looking up in the table. ShiftRows Step. Shift each line according to certain Srules. MixColumns Step. To fully mixed operation of individual row in a matrix, this step uses a linear transformation to be mixed within each of the four bytes. AES is simple, easy and flexibility. Strong round function has good parallel characteristics which are accommodate to hardware design and implementation.

- dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
- Do not mix complete spellings and abbreviations of units: “Wb/m²” or “webers per square meter,” not “webers/m2.” Spell units when they appear in text: “...a few henries,” not “...a few H.”

A. Equations

The structure of InvMixcolumns is similar to Mixcolumns, but the coefficient of the InvMixcolumns is different from Mixcolumns. So it is waste of resource to additionally defined another table for InvMixcolumns. Through analysis, the Mixcolumns quantic $C(x)$ and the InvMixcolumns quantic $d(x)$ meet the relationship as

$$1) _ d(x) _ (04x2 _ 05)C(x)(mod x4 _ 01) _ ____ (1)$$

provided by the drop down menu to differentiate the head from the text. Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named “Heading 1,” “Heading 2,” “Heading 3,” and “Heading 4” are prescribed.

Acknowledgment

This paper is supported by National 863 Program of

China under Grant No. 2012AA012704, and by National 973 Key Basic Research Development Program of China under Grant No. 2011CB311801.

REFERENCES

- [1] Hammad I, El-Sankary K, El-Masry E, “High-speed AES encrypto with efficient merging techniques,” IEEE Embedded Systems Letters,SS 2010, pp.67-71.
- [2] IZHANG Y L, WANG X G, “Pipelined implementation of AES encryption based on FPGA,” 2010 IEEE International Conference on Information Theory and Information Security, Piscataway: IEEE, 2010, pp. 170-173.
- [3] FAN C-P, HWANG J-K, “Implementations of high throughput sequential and fully pipelined AES processors on FPGA.” ISPACS 2007: Proceeding of 2007 International Symposium on International Signal Processing and Symposium and Communication Systems, Piscataway: IEEE, 2007, pp. 353-356.
- [4] SKLAVOS N, KOUFOPAVLOU O, “Architectures and VLSI implementations of the AES-proposal Rijndael,” IEEE Transactions on Computers, 2002, 51(12), pp. 1454-1459.
- [5] BORKAR A M, KSHIRSAGAR R V, VYAWAHARE M V, “FPGA implementation of AES algorithm,” The 3rd International Conferenc on Electronics Computer Technology, Piscataway: IEEE, 2011, 3, pp. 401-405.
- [6] Joan Daemen, Vincent Rijmen. AES Proposal: Rijndael. The Rijndael Block Cipher.



Analysis & Detecting Emotion Recognition Technique from Speech Signal

Ms. Shital G. Nagpurkar

*Electronics & Communication Engineering,
Tulsiramji Gaikwad-Patil College of Engineering &
Technology, Wardha Road,
Nagpur, Maharashtra, India.
shital_ngp@rediffmail.com*

Prof. Rahul Dhature

*Electronics & Communication Engineering,
Tulsiramji Gaikwad-Patil College of Engineering &
Technology, Wardha Road,
Nagpur, Maharashtra, India.
rmdhature@gmail.com*

Abstract— Emotion recognition based on speech signal is used to know the state of person. There is different state of emotions. Happy, sad, angry and neutral are the primary emotions of a human being are analyzed by speech patterns. In today's era based on human emotion many research are going on. In the field of pattern recognition and speech signal processing in recent years etc. speech recognition by using the Mel-Scale Frequency Cepstral Coefficients (MFCC) extracted from speech signal of spoken words. Support vector machine (SVM) provides better result.

Keywords— MFCC; Support vector machine (SVM); speech features.

I. INTRODUCTION

The human emotions are expressed through speeches and one can judge the emotion of the speech if he is a human, but if we want to make a machine that understands the emotion, we need to design an algorithmic approach as a solution to the problem. The algorithm is a two stage approach the first is to extract features from the speech signal that corresponds to the emotional state of the speaker, and the second is to classify the extracted features into proper emotional state. The accuracy of this type of system is depended upon the accuracy of both the stages, if the features extracted are not proper emotional features, then the system fails, and if the classifier is unable to classify properly, then also the system fails. A lot of research has been done in the field of pattern recognition which has resulted in development of some good classifiers like Neural Networks, Support Vector Machine, Hidden Markov Model, Gaussian Mixture Model, etc. so we have a lot of options for the latter part of the algorithm therefore our main interest is to find the proper technique for emotional features in the speech signals. A speech signal, once recorded is simply a digital signal so when it comes to feature extraction we have different methods that are discussed in this paper and later the emotional features. Speech is a complex signal which contains information about the message, language and emotions. Speech signals produced by human being are time varying signal and it is random in nature. Emotions in the human being

is an individual mental state that arises spontaneously due to extra excitation rather than through conscious effort. There are various kinds of emotions can be detected from speed signal by doing scientific research on it. During this, the basic problem is to cover the gap between the information which is captured by a microphone, corresponding emotion, and model the specific association. This gap can be reduce minimizing various emotions in few, like anger, happiness, sadness, surprise, fear, and neutral. The important fact regarding emotions is that it produced in the speech from the nervous system consciously or unconsciously. Emotions from the speech recognition is a system which basically identifies the mentally as well as physical state of human being from his or her voice [1]. Emotion recognition is having more attention due to the number of applications in various domains like detecting frustration, disappointment, surprise/amusement etc. There are many feature vectors are used towards automatic recognition of emotion in speech. Therefore, a proper choice of feature vectors is one of the most important tasks in the process. The feature vectors can be distinguished into the following four groups: continuous, qualitative, spectral (e.g., MFCC), and TEO autocorrelation envelope area [2]. For classification of speech, the methodologies are as follows: HMM, GMM, ANN, k-NN, and several others. In addition to this their combination are used which enhance the advantages of each classification technique. After studying the related literature it can be identified that, the vector feature sets which is mostly employed are comprised of pitch, MFCCs, and HNR. Apart from this, the HMM technique is most widely and effectively used by the researchers due to its characteristics effectiveness. Paper [3] computes speech features that represent entire utterance using the determined average values which belong to time and frequency domain. For the classification of unknown speech samples used methods are vector quantization, ANN and GMM. One of researcher has developed an emotion recognition system which comprise of combination of both statistic and temporal features. GMM and HMM are combined, which is then provided to a Bayesian and an MLP classifier. Their feature set was combination of F0, feature contours of log energy, and syllable time period. A

different method is followed in paper [4], a variety of descriptors (MFCC, prosodic, speech quality and articulatory) is computed on frame as well as on turn level for further analysis. they used a GMM classifier during the frame level analysis, while for turn level SVM classifier was used. The BERLIN Emotional Speech database, as well as the Speech Under Simulated and Actual Stress (SUSAS) Database were used. They achieve average recognition rates of the order of 89.9 and 83.8 percent respectively. Last but not least, an interesting approach is used in [5], sentence-level emotion recognition is investigated. Segment level emotion classifier used to predict segments within a sentence. Second component in this process combines the predictions from the segments to obtain a sentence level decision. Different segments (words, phrases, time-based) and different decision combination methods (majority vote, average of probabilities, and a Gaussian Mixture Model (GMM)) were evaluated and results show that proposed method significantly gives the standard sentence-based classification approach. In addition to this regards, they analyze that the time based segments provides best output, which is important to develop language dependent emotion recognition systems.

The paper is organized as it describes the overall structure of the speech emotion recognition, different feature extraction and the details about the feature selection and classification schemes which could be use in the speech emotion recognition.

II. Speech Based Emotion Recognition System

Speech based emotion recognition is tends to identification the emotional state of a human being from his or her voice. It is based on in-depth analysis and generation mechanism of speech signal, extracting related parameters which contain emotional information from the speech sample, and adaption of appropriate pattern recognition methods to identify emotional states.

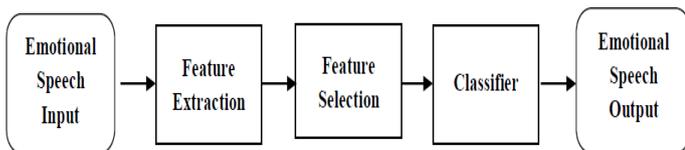


Fig.1 Speech Based Emotion Recognition System

Above figure shows main components in the speech based emotion recognition system. Like typical pattern recognition systems, speech emotion recognition system also contains four main modules: speech input, feature extraction, feature selection, classification, and output. Since a human cannot classify easily natural emotions, it is difficult to expect that machines can offer a higher correct classification. A typical set of emotions contains 300 emotional states which are decomposed into six primary emotions like anger, happiness, sadness, surprise, fear, and neutral. Success of speech emotion recognition depends on naturalness of database. [2] There are six databases available: two publicly available ones, the Danish Emotional Speech corpus (DES), Berlin Emotional Database (EMO-DB), four databases from the Interface project with Spanish, Slovenian, French and English

emotional speech. All of these databases contain acted emotional speech. With respect to authenticity, there seems to be three types of databases used in the SER research: type one is acted emotional speech with human labeling. This database is obtained by asking an actor to speak with a predefined emotion. A recently strong objection has been emerged against the use of acted emotions. It was shown that acted and spontaneous samples differ in the view of features and accuracies [6], second one is authentic emotional speech with human labeling. This databases are coming from real-life systems (for example call-centers) and type third is elicited emotional speech with self-report instead of labeling. Where emotions are provoked and self-report is used for labeling control. [7] Seemingly, different types of databases are suitable for different purposes. Type first still can be of use in, some cases where mainly theoretical research is aimed, rather that construction of a real life application for the industry.

III. Feature Extraction and Selection

Speech signal composed of large number of parameters which indicates emotion contents of it. As the changes occur in these parameters that indicate changes in the emotions. Therefore proper choice of feature vectors is one of the most important tasks to get proper output. There are many approaches towards automatic recognition of emotion from speech signal. Feature vectors can be classified as a long-time and short-time feature vectors. The long-time are estimated over the entire length of the utterance, while the short-time ones are determined over window of usually less than 0.1μs. The long-time approach identifies emotions more efficiently than short time. Short time features uses interrogative phrases which has wider pitch contour and a larger pitch standard deviation. Most common features used by researchers are Energy and its related parameter. The Energy is the basic and one of the most important parameter in speech signal. We can obtain the statistics of energy in the whole speech sample by calculating the energy, such as mean value, average value, max value, variance, variation range, contour of energy [1].

Pitch and related features:

The value of pitch frequency can be calculated in each speech frame and the statistics of pitch can be obtained in the whole speech sample. These statistical values reflect the global properties of characteristic parameters. Each Pitch feature vector has the same 19 dimensions as energy.

Qualitative Features:

An emotional content of an utterance is strongly related with its voice quality. The voice quality can be numerically represented by parameters which are estimated directly from speech signal. The acoustic parameters related to speech quality are: (1) Voice level: signal amplitude, energy and power of signal and duration i.e frequency, period are reliable measures of voice level; (2) voice pitch; (3) phrase,

phoneme, word and feature boundaries; (4) temporal structures. [2]

Linear Prediction Cepstrum Coefficients (LPCC):

LPCC are consists of characteristics of particular channel of speech. A Person with different emotional speech will have different channel characteristics, so we can extract these coefficients to identify the emotions in the speech. The computational method of LPCC is usually a recurrence of computing the linear prediction coefficients (LPC), which is according to the all-pole model.

Mel-Frequency Cepstrum Coefficients (MFCC):

MFCC is based on the characteristics of the human ear's hearing, which uses a nonlinear frequency unit to simulate the human auditory system. Mel frequency scale is the most widely used with a simple calculation, good ability of the distinction, anti-noise and other advantages [8]. The Discrete Wavelet Transform offers the best solution for emotional state identification applications. By employing feature extraction technique we can extract number of features from speech signal. To achieve accurate identification of emotion state, classifier should provide with single best feature. Therefore there is need of systematic feature selection to reduce unwanted features from the base features. For best feature, Forward Selection method can be applied. The remaining features can be used by classifier to increase classification accuracy. [2]

IV. Classifier Selection

The selection of classifier is depends on the geometry of the input feature vector. Some classifiers are more efficient with certain type of class and some are better at dealing with many irrelevant features or with structured features. Comparison in performance of classifiers can be done on the same large and representative database. Most advanced researches on a speaker independent mode achieve recognition rates from 55% to 95%, whereas humans could hardly reach emotion recognition rates of about 60% from unknown speakers [4]. Various Classifiers used by researchers are K-nearest Neighbors (KNN)[1], hidden Markov model(HMM), Gaussian mixtures Model (GMM), support vector machine (SVM) and artificial neural net (ANN). HMM has been studied long time by researchers for speech emotion recognition, as has advantage on dynamic time warping capability. Moreover, it has been proved useful in dealing with the statistical and sequential aspects of the speech signal for emotion recognition [10]. However, the classify property of HMM is not satisfactory. Gaussian mixture model allows training the desired data set from the databases. GMM are known to

capture distribution of data point from the input feature space, therefore GMM are suitable for developing emotion recognition model when large number of feature vector is available. Given a set of inputs, GMM refines the weights of each distribution through expectation-maximization algorithm. GMMs are suitable for developing emotion recognition models using spectral features, as the decision regarding the emotion category of the feature vector is taken based on its probability of coming from the feature vectors of the specific model. Gaussian Mixture Models (GMMs) are among the most statistically matured methods for clustering and for density estimation. They model the probability density function of observed data points using a multivariate Gaussian mixture density. [11] Another common classifier, used for many pattern recognition applications is the artificial neural network (ANN). They are known to be more effective in modeling nonlinear mappings. Also, their classification performance is usually better than HMM and GMM when the number of training examples is relatively low. Almost all ANNs can be categorized into three main basic types: MLP, recurrent neural networks (RNN), and radial basis functions (RBF) network. The classification accuracy of ANN is fairly low compared to other classifiers. The ANN based classifiers may achieve a correct classification rate of 51.19% in speaker dependent recognition, and that of 52.87% for speaker independent recognition. [2] One of the important classifiers is the support vector machine. SVM classifiers are mainly based on the use of kernel functions to nonlinearly map the original features to a high dimensional space where data can be well classified using a linear classifier. SVM classifiers are widely used in many pattern recognition applications and shown to outperform other well-known classifiers [8]. SVM has shown to have better generalization performance than traditional techniques in solving classification problems. The accuracy of the SVM for the speaker independent and dependent classification are 75% and above 80% respectively [1, 8]. There are many other classifiers used for speech emotion recognition such as k-NN classifiers fuzzy classifiers, and decision trees. The GMM and the HMM, are the most used ones for speech emotion recognition. The performance of many of them is not significantly different from the above mentioned classification techniques recognition, and that of 52.87% for speaker independent recognition. [2]

B. SVM training and classification

Now once we have a set of features available with us we can take use of the classifiers to distinguish between the different emotional states. Now we take use of the multiclass SVM classifier for classification purpose. First we train the classifier with some inputs of different emotional states. After training the classifier, we can use it for recognizing the new given input. The process of SVM training contains labeling of extracted features and training SVM. In the training process, every extracted feature has to assign an associated class label. The SVM is trained according to this labeled feature. The SVM kernel functions are used in the training process of

SVM. The result can be improved if we use all the above features properly. One of the important classifiers is the support vector machine. SVM classifiers are mainly based on the use of kernel functions to nonlinearly map the original features to a high dimensional space where data can be well classified using a linear classifier. SVM classifiers are widely used in many pattern recognition applications and shown to outperform other well-known classifiers [8]. SVM has shown to have better generalization performance than traditional techniques in solving classification problems. The accuracy of the SVM for the speaker independent and dependent classification are 75% and above 80% respectively [1, 8].

Conclusion :

In this paper, most recent work done in the field of Speech Emotion Recognition is discussed. Most used methods of feature extraction and several classifier performances are reviewed. Success of emotion recognition is dependent on appropriate feature extraction as well as proper classifier selection from the sample emotional speech. It can be seen that Integration of various features can give the better recognition rate. Classifier performance is need to be increased for recognition of speaker independent systems. The application area of emotion recognition from speech is expanding as it opens the new means of communication between human and machine. It is needed to model effective

method of speech feature extraction so that it can even provide emotion recognition of real time speech.

References

- [1] Kunxia Wang, Ning An, Bing Nan Li "Speech Emotion Recognition Using Fourier Parameters," IEEE TRANSACTIONS ON AFFECTIVE COMPUTING VOL. 6, NO. 1, JANUARY-MARCH 2015.
- [2] Won-Jung Yoon, and Kyu-Sik Park: " Building Robust Emotion Recognition System on Heterogeneous Speech Databases" IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, May 2011.
- [3] Stavros Ntalampiras and Nikos Fakotakis "Modeling the Temporal Evolution of Acoustic Parameters for Speech Emotion Recognition" IEEE TRANSACTIONS ON AFFECTIVE COMPUTING, VOL. 3, NO. 1, JANUARY-MARCH 2012 .
- [4] Steven B. Davis, and Paul Mermelstein, Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences. IEEE Trans. ASSP, 1980. ASSP-28(4): p. 357-366.
- [5] Eun Ho Kim, Kyung Hak Hyun, Soo Hyun Kim, and Yoon Keun Kwak "Improved Emotion Recognition With a Novel Speaker-Independent Feature" IEEE/ASME TRANSACTIONS ON MECHATRONICS, VOL. 14, NO. 3, JUNE 2009 317.
- [6] Chul Min Lee, Student Member, IEEE, and Shrikanth S. Narayanan, Senior Member, IEEE "Toward Detecting Emotions in Spoken Dialogs" IEEE TRANSACTIONS ON SPEECH AND AUDIO PROCESSING, VOL. 13, NO. 2, MARCH 2005 293.



Human Gesture Recognition Analysis Based on Computer Vision Technology

Ms. Renuka V. Rithe

*Electronics and Communication
Engineering
Tulsiramji Gaikwad-Patil College of
Engineering and technology, Wardha
road, Nagpur, Maharashtra, India.
renukarithe@gmail.com*

Prof. Rahul Dhature

*Electronics and Communication
Engineering
Tulsiramji Gaikwad-Patil College of
Engineering and technology,
Wardharoad, Nagpur, Maharashtra,
India.
rmdhature@gmail.com*

Abstract-Face tracking plays major role in many computer vision and relative fields, such as robot vision, intelligent meeting and video surveillance systems. However, in practice, a face tracker often fails to track target under various environmental condition. Therefore a good face tracking algorithm of real-time and robustness becomes a challenging task. These problems are overcome in improving the camshift algorithm. Application of this is used in medical fields such as it is more useful for physically disable person having face movements. The user is ready to use a mouse and open and close a file.

Keywords: *Face tracking , real-time and robustness ,camshift algorithm.*

I. Introduction

Gestures recognition system has now become a significant part of human-computer interaction. Gestures can be formed from any bodily motion or but most commonly it originates from the face or hand. A gesture is a movement of the body parts that has got information about the feelings. Example is waving your hand to say good bye. Pressing keys on the keyboard does not indicate any gesture. All that matters is which key was pressed. The definition of gesture has still remained an arbitrary term as it has been defined by many scholars in different ways .A system that automatically detects and recognizes human head gestures such as nodding and shaking in complex background conditions using Web camera under uncontrolled conditions is head gesture

recognition. The output of a particular procedure is measured in terms of Performance improvement, and then the procedure is modified to increase the output, and efficiency also, or increase the effectiveness of the procedure. Face detection is a technique that finds out the locations and also the size of human faces in digital images. It detects face and other things are ignored by it, such as buildings and trees for instance. Face detection can actually be considered as a more general case of face localization. In face localization, the task is to find the locations and sizes of a known number of faces (usually one). In face detection, first face is processed and then it is matched bitwise with the underlying face image in the database. Even a little change in facial expression, such as smile and movement of lips, will not match the face. Face detection can be considered as a specific case of object-class detection. In object-class detection, the main task is to find the locations and sizes of all objects in an image that belong to a given class. Best instances include upper torsos, pedestrians, and cars. Face-detection algorithms focus on the detection of frontal human faces. It is similar to image detection in which the image of a person is matched bit by bit. Image matches with the image stores in database. Any facial feature changes in the database will invalidate the matching process'

I.1 CAMSHIFT

The Camshift algorithm actually depends on the Mean Shift algorithm. The working of mean shift algorithm is based on statistics distribution. Camshift also depends on dynamically changing distributions. CAMSHIFT's is able to handle dynamic distributions by readjusting the search window size for the next frame based on the zeroth moment of the current frames distribution. So the algorithm can anticipate object movement to quickly track the object in the next scene. The CAMSHIFT algorithm is a variation of the MEAN SHIFT algorithm. CAMSHIFT works by tracking the hue of an object, in this case, flesh color. The movie frames were all converted to HSV space before individual analysis.

I.2 SURF

In image recognition technology, Speeded Up Robust Features (SURF). It is used for object recognition. It is partly inspired by the scale invariant feature transform (SIFT) descriptor. In order to determine the interest point hessian blob determinant is used by SURF.

SURF descriptors can be used to locate and identify objects, people or faces, to make 3D scenes, to track objects and also to extract points of interest. The surf algorithm is work as shown in fig. 1

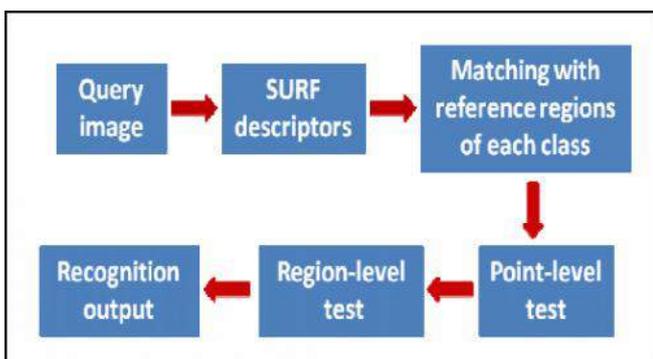


Fig.Flow chart of SURF algorithm.

I.3ADVANCED CAMSHIFT

First of all the position and the size of search window of the object is initialized
 After that the image is converted from RGB color space to YIQ color space, and then the object

back projection is calculated. Next is to calculate the centroid within the search window, and then regard the centroid as the center of the track window.

Return to above step, the iteration will be stopped when the moving distance is less than the threshold value or has reached a certain number of iterations to converge.

In the next frame of video image, with the center which was saved in previous steps to again re-initialize

the size and position of the search window, and next step is to calculate window size, the size of width of search window is: $w = 2 * \sqrt{M_{00}/256}$

Jump to the Step second and then repeat the operation. However, improved Camshift can eliminate these effects of the background and similar skin-color and becomes more robust to noise.

Although, we have been solved the effects of background, when the other object appears around the object, CamShift algorithm will thus automatically include similar skin-color, so the window will expand. So, Surf algorithm will also be employed.

II.LITERATURE REVIEW

1) Parth B. Pancha, Vimal H. Nayak, "A Hand Gesture Based Transceiver System for Multiple Application" IEEE SPONSORED 2ND INTERNATIONAL CONFERENCE ON ELECTRONICS AND COMMUNICATION SYSTEM (ICECS 2015)

Research in hand gesture recognition aims to design and development of such systems than can identify explicit human gestures as input and process these gesture representations for device control through mapping of commands as output. Various different messages can be displayed on touch screen LCD and it can be change according to change in accelerometer position or different angles of accelerometer.

2) Danchi Huang, and Lijuan Li, "Face Tracking Algorithm Based on Improved Camshift and Surf Algorithm", Journal of Computational Information Systems 11: 3 (2015) 893 - 901.

This method can track object correctly, although it is occluded by the similar skin-colour objects. In this method, using the twice-matching to match the object, and update the template, so that the object can be

finding correctly when the appearance of the object is changed. When the object is lost, the algorithm can refund it quickly and continue tracking.

Improvement of this algorithm is needed to better match the object with other features.

3) Yu HuiQiu, Jian Wei Zhang, Guang Lin, Yong Hui Li, and Dong FaGao, "Improved camshift tracking algorithm based on motion detection", *Proceedings of the 2013 International Conference on Machine Learning and Cybernetics, Tianjin, 14 - 17 July, 2013*.

In this paper, it is given that when calculating the colour histogram of a target within the rectangular box, it adds a mask layer to remove background pixels around targets. When calculating the back projection, it adds a mask layer to remove all background pixels within the window to eliminate the interference of similar colour in the background. This improved algorithm utilizes the colour feature better and keeps the tracking right even when background interference exists. The performance of the proposed depends on the accuracy of the moving object detection.

P. Jia, H. Hu, T. Lu, and K. Yuan, "Head Gesture Recognition For Hands Free Control of an Intelligent Wheelchair", *Industrial Robot: An International Journal* 34 / 1 (2007) 60 - 68 [ISSN 0143 - 991X] [DOI10.1108 / 01439910710718469].

A Novel hands-free control system for intelligent Wheelchairs based on visual recognition of head gesture. Adaboost face detection algorithm & Camshift object tracking algorithm are combined in this paper to achieve accurate face detection, tracking, & gesture recognition in real time. Evaluation in both indoor & outdoor environments is not done. Several conditions such as cluttered background, changing lightning conditions, sunshine, and shadows are not taken in consideration.

III. Design Methodology

Face tracking plays an important role in recognizing the face. But sometimes it also happens that the algorithm can also track the face in the incorrect manner. First of all, the face is detected in real time. Then the gesture is recognized. The following things are done to carry out the further steps.

- Basic camera interface is implemented

- Basic algorithm for face detection is implemented
- Study and implementation of real time face detection using Camera
- Study and design of gesture recognition for different gesture based on face.

IV. CONCLUSION

Face recognition is a complex task to perform. Face recognition should be done in a robust manner to correctly detect the face. So we have implemented the improved CAM shift algorithm to make the face recognition a robust task.

V. REFERENCES

- [1] Parth B. Pancha, Vimal H. Nayak, "A Hand Gesture Based Transceiver System for Multiple Application" *IEEE SPONSORED 2ND INTERNATIONAL CONFERENCE ON ELECTRONICS AND COMMUNICATION SYSTEM (ICECS 2015)*
- [2] Danchi Huang, and Lijuan Li, "Face Tracking Algorithm Based on Improved Camshift and Surf Algorithm", *Journal of Computational Information Systems* 11: 3 (2015) 893 - 901.
- [3] Yu HuiQiu, Jian Wei Zhang, Guanglin, Yong Hui Li, and Dong FaGao, "Improved camshift tracking algorithm based on motion detection", *Proceedings of an International Conference on Machine Learning and Cybernetics, Tianjin, 14 - 17 July, 2013*.
- [4] Tao Zhang, and ShuminFei, "Target tracking based on particle filter algorithm with multiple cues fusion", 2014, 26th Chinese Control and Decision Conference (CCDC).
- [5] Amr M. Nagy, Ali Ahmed, and Rala R. Zayed, "Particle Filter Based on Joint Colour Texture Histogram For Object Tracking", *IEEE IPAS'14: International Image Processing Applications & Systems Conference 2014*.
- [6] P. Jia, H. Hu, T. Lu and K. Yuan, "Head Gesture Recognition For Hand Free Control of an Intelligent Wheelchair", *Industrial Robot: An International journal* 34 / 1 (2007) 60 - 68 [ISSN 0143 - 991X] [DOI 10.1108 / 01439910710718469].
- [7] Bradski R. G., and Clara S. C. A., "Computer vision face tracking as a component of a perceptual user interface", In the *Workshop on Applications of Computer Vision, Princeton, PP.* 214 - 219 (1998).
- [8] Wang, Z. W., Yang X. K., and Xu Y., "Camshift guided particle filter for visual tracking", *Pattern Recognition Letters* 30(4), 407 - 413 (2009).
- [9] Ye J. H., Liu Z. G., and Zhang J., "A Face Tracking Algorithm Based on LBP Histograms and Particle Filtering", In: *Proc. 6th*

IEEE International Conference ICNC, Volume 7, PP. 3550 - 3553 (2010).

[10] Wu X., Li L. H., Lai J. H., and Huang J., "A Framework of Face Tracking with Classification Using CAMShift-C and LBP", In: Proc. 6th IEEE International Conference ICIG, PP. 217 - 222 (2010).

[10] AmitSatpathy, Xudong Jiang, *Senior Member* and How-Lung Eng, "LBP-Based Edge-Texture Features for Object Recognition", Ieee Transactions On Image Processing, Vol. 23, No. 5, May 2014



Real Time Object Tracking For Video Surveillance

Ms. Gayatri Datarkar

*Department of Electronics and Communication Engineering
TulsiramjiGaikwad-Patil College of Engineering and
Technology
Nagpur, India
gdkatole@gmail.com*

Prof. Rahul Dhature

*Department of Electronics Engineering
TulsiramjiGaikwad-Patil College of Engineering and
Technology
Nagpur, India
rahul.etrx@tgpacet.com*

Abstract—Real time Object tracking is important task in video surveillance, human-computer interaction, traffic pattern analysis and robotics. The proposed modified mean shift algorithm is used for continuous tracking in complex situations, such as the shape and the illumination of the object change. The mean shift algorithm is utilized here to detect the object target area, and then a decision on the tracking effect is made. If tracking fails, the object area is matched with the target model and a new track position is identified. Otherwise, the target model is periodically updated according to the changing of state of moving object. In the frame of moving object target deformations, such as the uncertainty of scale and illumination, the algorithm is varified and analysed with the mean shift algorithms. Our emphasis will be there on to show, the proposed method can effectively track an object under the condition of videostreamming.

Keywords—*component; formatting; style; styling; insert (key words)*

I. INTRODUCTION

The object tracking is an important elementary operation in several computer vision-based applications including, video monitoring and surveillance, sensing in robotics, key-frame identification, and many more. Object tracking is a mechanism to track an object and to take an action on another object, based on changes occurring in the properties of the object being tracked. There has been a great increase in the availability and amount of video information due to the ever increasing use of videos in several applications such as activity recognition, visual surveillance and intelligence user interface.

Object tracking becomes important because of its several important applications such as: surveillance and Security -to serve better sense of security service, to identify people; Traffic management - to analyze crowd, to detect accidents; Retail space instrumentation - to analyze shopping behavior of customers, to enhance building and environment design;

Tracking of visual objects can be done either by forward-tracking or by back-tracking. The first and foremost

step is to detect the moving object in video streams. We can go for three approaches in object tracking:

- Extraction of characteristics which resembles points, lines, segment from image sequences. In this case tracking stage relies on matching procedures every time this resembles Feature based methods.
- The second approach is Differential method which actually resembles optical flow computation.
- Third approach is measurement of inter image displacement using correlation.

The main obstacle in video tracking is to assign target locations in consecutive video frames, especially when the objects are moving rate is relative fast to the frame rate [1]. Number of approaches for object tracking has been proposed and varified. The appropriate approach which is to be used it depends on the context in which the tracking is to be performed and the end use for which the tracking information is being sought.

II. RELATED WORK

For the purpose of robust object tracking. The MAP based algorithm has been proposed. It is basically based on a sparse collaborative model. This model can exploit both holistic template and local representations to check for drastic appearance changes. It consist of Sparse Discriminative Classifier(SDC) and Sparse Generative model(SGM) for object tracking. It requires online update scheme to update the templates.[2]

Mean shift utilizes color distribution with uniform quantization. But , the quantization method ignores the close relationship of color statistics. The color histogram consists of many empty bins because of uniform distribution. In order to reduce the number of empty bins an optimal color based mean shift algorithm was proposed . In this the histogram agglomeration technique was applied to extract the optimal colors.[3]

In order to determine the candidate target region, mean shift algorithm was utilized and then a judgment on the tracking

effect was made according to the Bhattacharyya coefficient. In case of tracking failure, the candidate area was matched with the target model by SIFT feature. In the next and final step a new track position was determined.[4]

III. MEAN SHIFT

Here, Mean-shift [1] is a nonparametric density gradient estimator is used to identify the image window that is similar to the object's color histogram in the current frame. The mean shift is a non-parametric feature space analysis technique. The basic of mean shift algorithm is that it relies on color cues. It iteratively carries out a kernel based search starting at the last position of the object. Color cues form a most meaningful structure of many tracking algorithms [2–6]. Since color histograms are robust to partial occlusion, are scale and rotation invariant, the resulting algorithm can effectively and successfully handle non-rigid deformation of the object and extensively changing dynamics in complex background posture. The benefit of color is that it is a weak model and is therefore unrestrictive about the type of objects which is being tracked. The main problem regarding tracking with color alone occurs when the region around the target contains objects with same color. When the region is cluttered in this way a single cue does not provide reliable performance because it fails to fully model the target. The texture and edge features have been used for video based tracking purposes but it is not applied to tracking with mean shift technique. In this paper we show that color, texture and edge complete each other and provide reliable performance output. When the region is cluttered, a single cue does not provide reliable performance because it fails to fully model the target. A cue-selection approach is proposed in [7] which present visual cues for object tracking in video sequences is done by particle filtering. A histogram-based framework is developed for the analysis of color, edge and texture features. This paper presents visual features for tracking of moving object in video sequences using Mean Shift algorithm. The features used in this paper are color, edge and texture. Mean shift Algorithm is expanded based on number of features. Object tracking refers to method to track an object (or multiple objects) over a sequence of images. Mean shift analysis is a possible forward-tracking technique because it estimates the positions of the regions in the current frame from the previous frame. Mean-shift tracking is a technique for following an object of interest as it moves through a video sequence. It is a gradient ascent approach that models the image region to be tracked by its color histogram. The mean shift is a method for finding local maxima of a density function from given discrete data samples. It works with a search window that is positioned over a section of the distribution. The mean shift technique is an application independent tool. It is suitable for real data analysis because it does not assume any prior shape (e.g. elliptical) on data clusters. Therefore, there are numerous approaches employing the mean shift algorithm in object tracking. This paper provides a single reference of the great majority of papers and techniques presented on mean shift technique. We compiled over 10 years' papers pertaining to

different Mean shift methods published up to the date of submission of this manuscript. Papers referencing mean shift methods from previous papers without any modification or improvement have been omitted. It is possible that one or more papers were unintentionally omitted. We apologize if an important method or improvement was left out. This manuscript steps through a wide variety of methods with a brief discussion and categorization of each. We have avoided discussing slight modifications of existing methods as distinct methods. Continuously Adaptive Mean shift tracking that is based on adaptation mean-shift. When probability density image is given it finds the mean (mode) of the distribution by iterating in the direction of maximum increase in probability density. This is one of the simplest methods and gives reliable and robust results, if the colors in the background area differs significantly from those in the target object. CAM shift procedure are given below:

1. Set the region of Interest (RoI) of the probability distribution function of the entire image.
2. Select the initial location of the Mean Shift search window.
3. Calculate the color probability distribution of the region centered at the Mean Shift search window.
4. Use Mean Shift algorithm to find the center of the probability image.
5. Store the zero moment (distribution area) and centered location.
6. For the next frame, center the search window at the mean location found in Step 4 and set the window size to a function of the zero moment.
7. Go to Step 3 and repeat the whole process again.

IV. PROPOSED METHOD

In this project modified mean shift algorithm will be utilizing color features and texture features for object tracking. In order to extract the texture features from object we will apply LBP (Local Binary Pattern) technique.

A. LBP

It is a very effective technique to elaborate the texture feature. It has got meritorious qualities such as fast computation and rotation invariance. Thus LBP has wide applications in texture analysis, image retrieval image segmentation etc.

B. COLOR HISTOGRAM

Now coming to the feature like Color feature, we will employ color histogram for extraction of object. Basically, histograms are the collection of data which are organized into a set of predefined bins. Colour histogram is distribution of point sample and it actually represents the object in proper manner. Here color feature is extracted in the form of RGB Colour space which are divided into equal k -intervals which is known as a bin. Number of bins feature is given by $M_c = k^3$. Simple colour histogram ignores the close relationship of colour statistics.

C. JOINT COLOR HISTOGRAM AND LBP

Sometime simple color histogram fails to distinguish between target and background when both seems almost similar. Sometimes the target loses its information in spatial domain. For the above said reason it becomes more convenient to use joint color histogram rather than simple color histogram. The joint color histogram and LBP will be applied together to improve the tracking capability of the conventional mean shift algorithm. In this technique the texture value is assigned to each pixel and then combined with the pixel's color value to represent target features. So a joint color histogram method is proposed for the more differentiated and effective target representation.

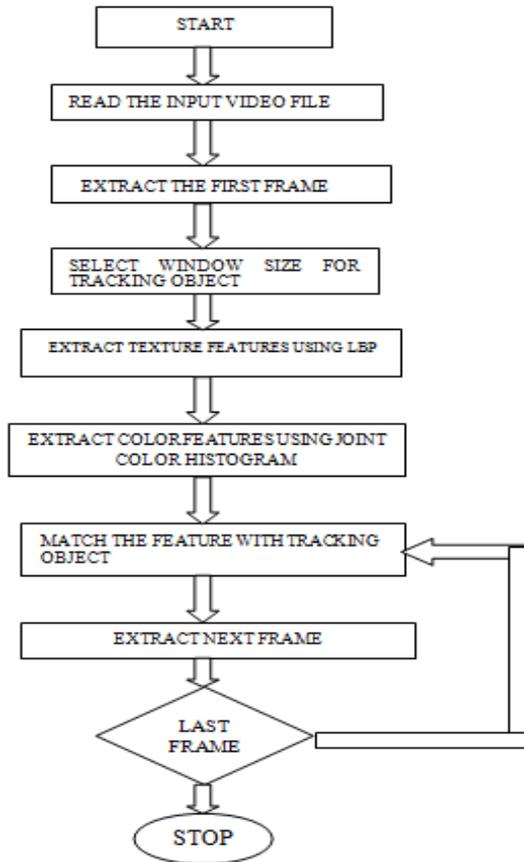


Fig:1 Flow chart of proposed algorithm

V. CONCLUSION

The mean shift algorithm with LBP and color histogram increases the robustness of tracking in different conditions. It is analysed that moving object and tracking are two main core things in video surveillance. The performance of traditional algorithms has been enhanced by joint color histogram and LBP. The accuracy of the algorithm also depends upon the speed of moving object and clarity of a video.

VI. REFERENCES

- 1) "Moving Object Detection: Review of Recent Research Trends" Jaya S. Kulchandani, Kruti J. Dangarwala., 2015 International Conference on Pervasive Computing (ICPC).
- 2) "Optimal color-based mean shift algorithm for tracking objects" Xiaowei An, Jaedo Kim, Youngjoon Han Department of Electronic Engineering, Soongsil University, Seoul, Korea Published in IET Computer Vision 2014
- 3) Oct. 2008. Y. Li, H. Ai, T. Yamashita, S. Lao, and M. Kawade, "Tracking in low frame rate video: A cascade particle filter with discriminative observers of different life spans," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 30, no. 10, pp. 1728–174
- 4) Kernel-Based Structural Binary Pattern Tracking Dae-Hwan Kim, Hyo-Kak Kim, Seung-Jun Lee, Won-Jae Park, and Sung-Jea Ko, Fellow, IEEE
- 5) Z. Khan, I. Y. H. Gu, and A. Backhouse, "Robust visual object tracking using multi-mode anisotropic mean shift and particle filters," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 1, pp. 74–87, Jan. 2011.
- 6) D. Ross, J. Lim, R.-S. Lin, and M.-H. Yang, "Incremental learning for robust visual tracking," *Int. J. Comput. Vis.*, vol. 77, nos. 1–3, pp. 125–141, 2008. J. Kwon and K. M. Lee, "Visual tracking decomposition," in *Proc. IEEE Conf. CVPR, Jun. 2010*, pp. 1–10.
- 7) Zhao, Q., Tao, H.: 'Object tracking using colour correlogram'. Proc. Joint IEEE Int. Workshop on VS-PETS, 2005, pp. 263–270
- 8) X. Wang, T. Han, and S. Yan, "An HOG-LBP human detector with partial occlusion handling," in *Proc. IEEE 12th Int. Conf. Comput. Vis.*, Oct. 2009, pp. 32–39.



Hand Drawn Face Sketch Recognition in Forensic Applications

Ms. Sweety S. Kshirsagar
M.Tech (IV Sem)
Comm. (Electronics) Engg.
SDCOE, Selukate, Wardha
sweety.kshirsagar111@gmail.com

Dr. N.N.Mhala
Professor and Head
Dept. of Electronics Engg.
BDCOE, Sewagram, Wardha
nitiket.mhala@gmail.com

Prof. B. J. Chilke
Assistant Professor
Electronics & Comm. Engg.
SDCOE, Selukate, Wardha
b_kuchewar@rediffmail.com

Abstract— Face is a complex multidimensional structure and needs a good computing techniques for recognition. Forensic Sketch to digital face matching is an important research challenge and is very pertinent to law enforcement agencies. Face sketching is a forensic technique that has been routinely used in criminal investigations. To recognize face sketch through face photo database is a challenging task for today's researchers. Forensic sketches are drawn based on the recollection of an eyewitness person and the expertise of a sketch artist. As a special forensic art, face sketching is traditionally done manually by police sketch artists. Because face sketches represent the original faces in a very concise yet recognizable form, they play an important role in criminal investigations, human visual perception, and face bio- metrics. This paper presents an efficient technique called Cascade object detection with viola jones technique for face detection, also features of face is being extracted by using Extended uniform circular linear binary pattern method. Thereafter, we use SVM classifier and K-NN classifier for better classification. We describe an application of the novel Support Vector Ma- chined Kernel (SVM'ed Kernel) to the Recognition of hand-drawn sketch. The SVM'ed kernel function is itself a support vector machine classifier that is learned statistically from data using an automatically generated training set. Our proposed method is experimentally verified by its robustness against faces.

Keywords— face detection, feature extraction, optical face, sketches, matched output.

I. INTRODUCTION

Face is a very important part of the human body through which and individual can be identified. The Face is a primary focus in the society and it plays a major role in conveying identity and emotions of an individual. Other than identical twins every individual has unique facial features. Facial recognition is a form of computer vision which uses human faces to attempt to identify an individual or verify a person's claimed identity. In many image processing applications, it is essential to represent the information in an image in a form suitable for that application. Since the values of pixels acquired from sensors are affected by lighting conditions and noise, the relevant information needs to be extracted from the image to derive the suitable representation. Deriving a suitable representation from an image is governed by three factors, namely, application, perception and processing. It is difficult to derive a representation which is applicable for all the applications. The representation should contain perceptually significant information of the image, which is specific to the given application. Processing of an image should not add artifacts or enhance noise in the resulting representation. In the context of face recognition (an application where a face image is used to recognize a person), it is difficult to define or articulate the perceptually significant information in a given

face image. The information that makes an individual face unique must be found in the subtle variations of the facial features (e.g., eyes, nose and mouth), since all the faces share the same set of features arranged in roughly similar configuration.

1.1 Biometrics

Biometrics is used in the process of authentication of a person by verifying or identifying that a user requesting a network resource is who he, she, or it claims to be, and vice versa. It uses the property that a human trait associated with a person itself like structure of finger, face details etc. By comparing the existing data with the incoming data we can verify the identity of a particular person. There are many types of biometric system like fingerprint recognition, face detection and recognition, iris recognition etc., these traits are used for human identification in surveillance system, criminal identification. Advantages of using these traits for identification are that they cannot be forgotten or lost. These are unique features of a human being which is being used widely.

1.2 Face Recognition

Face is a complex multidimensional structure and needs good computing techniques for recognition. The face is our primary and first focus of attention in social life playing an important role in identity of individual. We can recognize a number of faces learned throughout our lifespan and identify that faces at a glance even after years. There may be variations in faces due to aging and distractions like beard, glasses or change of hairstyles. Face recognition is an integral part of biometrics. In biometrics basic traits of human is matched to the existing data and depending on result of matching identification of a human being is traced. Facial features are extracted and implemented through algorithms which are efficient and some modifications are done to improve the existing algorithm models. Computers that detect and recognize faces could be applied to a wide variety of practical applications including

criminal identification, security systems, identity verification etc. Face detection and recognition is used in many places nowadays, in websites hosting images and social networking sites. Face recognition and detection can be achieved using technologies related to computer science. Features extracted from a face are processed and compared with similarly processed faces present in the database. If a face is recognized it is known or the system may show a similar face existing in database else it is unknown. In surveillance system if a unknown face appears more than one time then it is stored in database for further recognition. These steps are very useful in criminal identification. In general, face recognition techniques can be divided into two groups based on the face representation they use appearance-based, which uses holistic texture features and is applied to either whole-face or specific regions in a face image and feature-based, which uses geometric facial features (mouth, eyes, eyebrows, cheeks etc), and geometric relationships between them.

Face detection and recognition technology has been widely discussed in relation to computer vision and pattern recognition. Numerous different techniques have been developed owing to the growing number of real world applications. For service robot, face detection and recognition are extremely important, in which the emphasis must be put on security, real-time, high ratio of detection and recognition. Also it plays an important role in a wide range of applications, such as mug-shot database matching, credit card verification, security system, and scene surveillance. However, matching sketches with digital face images is a very important law enforcement application that has received relatively less attention. Forensic sketches are drawn based on the recollection of an eyewitness and the expertise of a sketch artist. One of the important cues in solving crimes and apprehending criminals is matching sketches with digital face images. Generally, forensic sketches are manually matched with the database comprising digital face images of known individuals. The state-of-art face recognition algorithms cannot be used directly and require additional processing to

address the non- linear variations present in sketches and digital face images.

An important application of face recognition is to assist law enforcement. Automatic retrieval of photos of suspects from the police mug shot database can help the police narrow down potential suspects quickly. However, in most cases, the photo image of a suspect is not available. The best substitute is often a sketch drawing based on the recollection of an eyewitness. Therefore, automatically searching through a photo database using a sketch drawing becomes important. It can not only help police locate a group of potential suspects, but also help the witness and the artist modify the sketch drawing of the suspect interactively based on similar photos retrieved. However, due to the great difference between sketches and photos and the unknown psychological mechanism of sketch generation, face sketch recognition is much harder than normal face recognition based on photo images. It is difficult to match photos and sketches in two different modalities. One way to solve this problem is to first transform face photos into sketch drawings and then match a query sketch with the synthesized sketches in the same modality, or first transform a query sketch into a photo image and then match the synthesized photo with real photos in the gallery. Face sketch/photo synthesis not only helps face sketch recognition, but also has many other useful applications for digital entertainment.

Artists have a fascinating ability to capture the most distinctive characteristics of human faces and depict them on sketches. Although sketches are very different from photos in style and appearance, we often can easily recognize a person from his sketch. How to synthesize face sketches from photos by a computer is an interesting problem. The psychological mechanism of sketch generation is difficult to be expressed precisely by rules or grammar. The difference between sketches and photos mainly exists in two aspects: texture and shape.

II. PROPOSED METHODOLOGY

‘Hand drawn face sketch recognition in Forensic application’ shall be implementing in future. Following are the Steps involved in process of matching sketches with digital face images are:

1. First we are going to generate a database simultaneously for both sketches and digital face.
2. The preprocessing technique is used to enhance the quality of both the digital face images and sketch images.
3. Feature Extractions.
4. Then the SVM method is used for recognition.
5. Finally we get the matched output images.

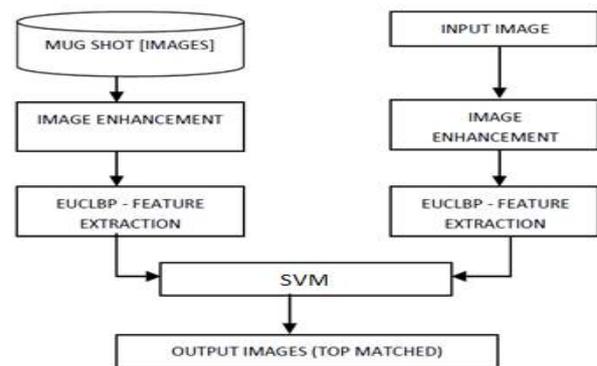


Figure 1: Architecture Diagram

Proposed Methodology will provide:

- To improve recognition rate
- To improve accuracy
- To provide more efficiency

III. FACE DETECTION

There are many techniques available for Face detection. For real time face detection a technique called Cascade object detection with Viola Jones technique can also be used for face detection. For real-time face detection, typically, in 1997, P. Viola presented a machine learning approach based on Adaboost and Cascade technique, which is capable of detecting faces in images in real-time.

3.1 Facial Database



Figure 2: Shows example images used for experiments

3.2 Face Detection

In face detection the elements which we are detecting are Face, Left eye, Right eye, Nose and Mouth along with control point of these Elements.

3.3 Result of face detection

The Result of face detection along with control points is given below :

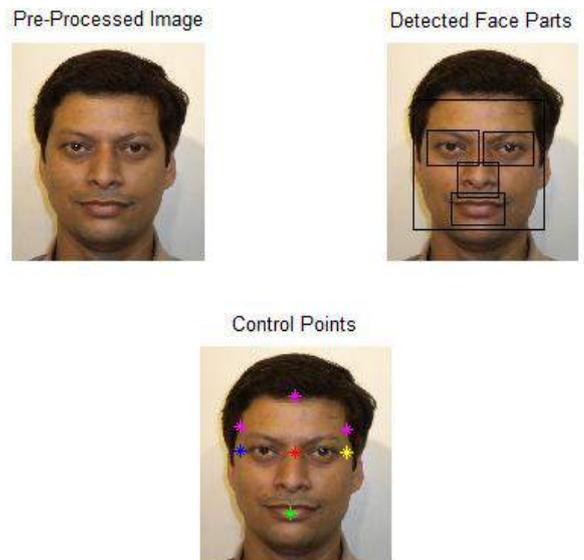


Figure 3: The Result of face detection of sketch along with control points.

The Result of face detection of sketch along with control points is given below :

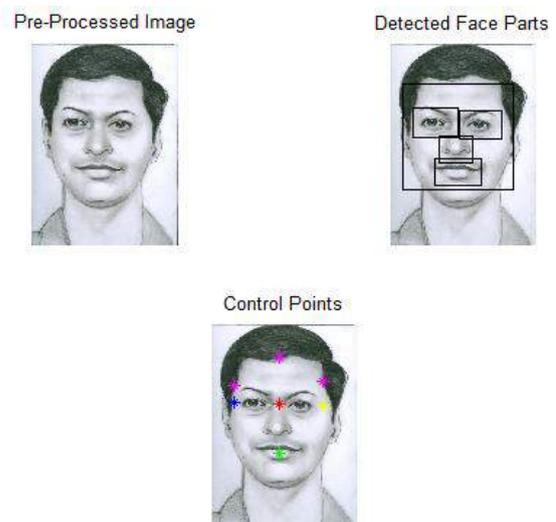


Figure 4: The Result of face detection of sketch along with control points.

IV. FEATURE EXTRACTION

Feature Extraction involves reducing the amount of resources required to describe a large set of data. In image processing, feature extraction starts from an initial set of measured data and builds derived values. Feature Extraction is related to dimensionality reduction.

4.1 Method of Features Extraction

EUCLBP method is used for Feature Extraction. EUCLBP stands for Extended Uniform Circular Local Binary Pattern. Local Binary Pattern (LBP) is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number. The most important property of the LBP operator in real-world applications is its robustness to monotonic gray-scale. In EUCLBP method first step is that both the sketches and digital face images are tessellated into non overlapping local facial regions and then EUCLBP descriptors are computed.

4.2 Result of Features Extraction

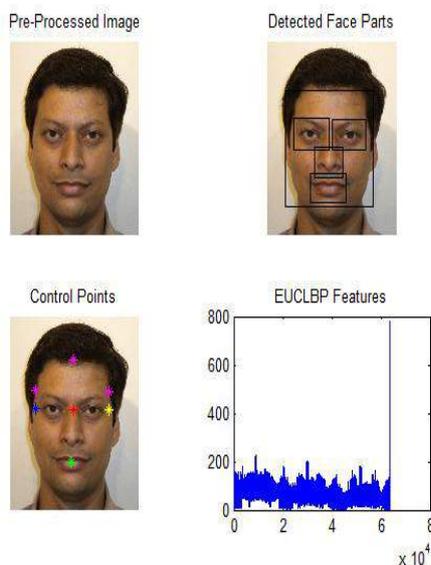


Figure5. : The Result of feature extraction of face.

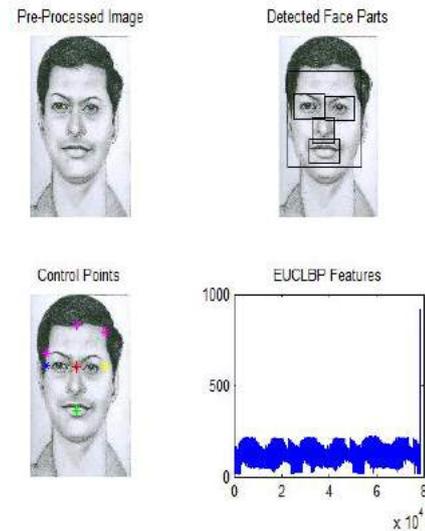


Figure6. : The Result of feature extraction of face sketch

V. SVM (SUPPORT VECTOR MACHINE)

5.1 Introduction:

SVMs were originally proposed by Boser, Guyon and Vapnik in 1992 and gained increasing popularity in late 1990s. Support Vector Machine is machine learning tool that is based on the idea of large margin data. Machine learning is about learning structure from data. Although the class of algorithm called "SVM"s can do more, in this talk we focus on pattern recognition. SVM are among the best of supervised learning algorithm. Theoretically well motivated, developed from statistical learning theory. SVM has Empirically good performance successful applications in many fields (bioinformatics, text, image recognition). A large and diverse community work on them: from machine learning optimization, statistics, neural networks, functional analysis, etc.

Support Vector Machine(SVM) is a machine learning tool that is based on the idea of large margin data classification. The

tool has strong theoretical foundation and the classification algorithms based on it give good generalization performance. Standard implementations, though provide good classification accuracy, are slow and do not scale well. Hence they cannot be applied to large-scale data mining applications. They typically need large number of support vectors. Hence the training as well as the classification times are high.

5.2 SVM:

A Support Vector Machine (SVM) is a discriminative classifier formally defined by a separating hyperplane. SVM locates a separating hyperplane in the feature space and classify points in that space.

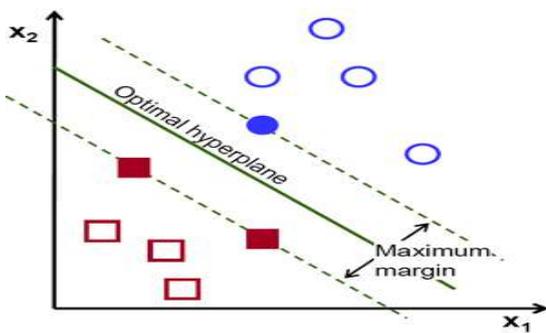


Figure7: Basic diagram

From the above figure Support vectors i.e. closet point to the decision boundary. The margin is defined to be the smallest distance between the decision boundary and any of the sample. Maximizing the margin is good according to intuition and PAC theory. It implies that only support vectors matter; other training examples are ignorable. The classifier is a separating hyperplane. Most important, training points are support vectors; they define the hyperplane.

The features which is being extracted in Feature Extraction process are eye to eye distance, eye width, eye height, nose width, nose height, mouth width, mouth height, left eye to nose distance, right eye to nose distance, mouth to nose distance. These feature values will be given to SVM and SVM

will trained these features and finally we will get matched output images with score card in percentage form. To find score we use nearest neighbour symmetric kernel of SVM and the metric used in Normalized cross correlation.

VI. RESULT

6.1 Result of matched output images:

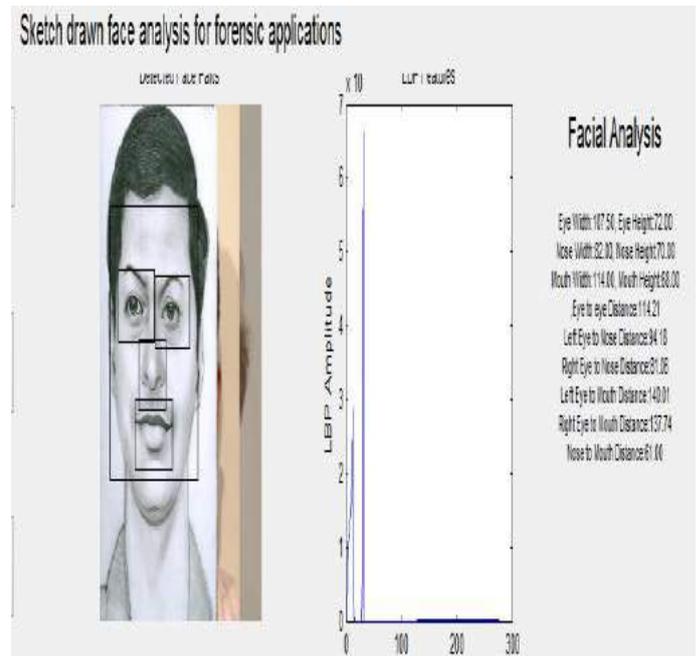


Figure8: Shows the sketch image which is given as an input whose matching image has to be found.

Figure implies that after giving input of sketch image, the face parts are detected and then features of the same is being calculated at the output. Now at final output we should get the optical face of the input sketch with score card and time.



Figure 10: Input sketch image.



Figure 11: Output matching image with score 99.95.

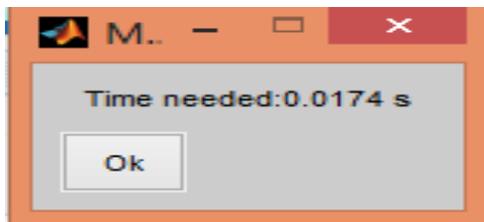


Figure 10: Shows snapshot of time needed to match image. Time required is 0.0174sec.

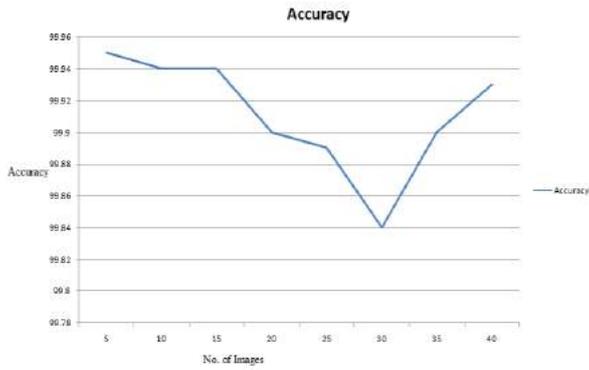
To calculate Accuracy and Time first we have create small database. As shown in table, suppose first database is create by storing 5 no. of images. Then giving required sketch as an input which is to be matched. After applying our proposed method, we will get exact photo image of the sketch image which is given as an input with score card which is nothing but accuracy to match and also time needed to match. We find that when database create of 5 no. of images we found 99.95 accuracy and time needed is 0.017 sec. Similarly, if we store 10 no. of images in database and for matching required sketch image from that 10 no. of image we had found 99.94 accuracy with 0.0289sec. Similarly we have increased no. of images to find of accuracy and time.

No. Of Images	Accuracy	Time
5	99.95	0.0174s
10	99.94	0.0289s
15	99.94	0.0256s
20	99.9	0.0684s
25	99.89	0.08038s
30	99.84	0.0984s
35	99.9	0.1129s
40	99.93	0.1169s

6.2 Finding Accuracy and Time of no. of images:

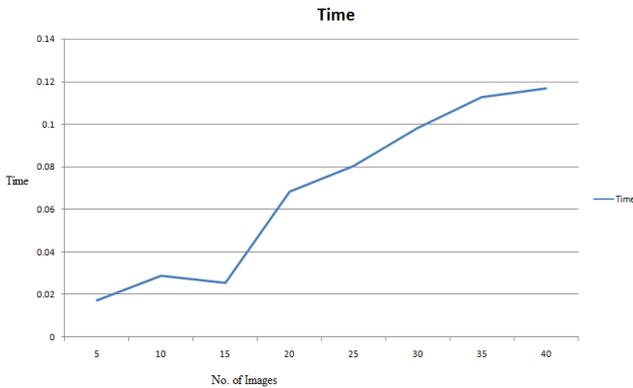
Graph of Accuracy

COMPARISON WITH DIFFERENT METHODS:



No. of Images

6.4 Graph of Time



No. of Images

Rank	1	2	3	4	5
Sketch Transform Method	71	78	81	84	88
Nonlinear face sketch recognition	87.7	92.0	95.0	97.7	98.3
New dimension +PCA+ K-NN	91.4	93	93.5	94.1	95.4
New dimension + PCA + SVM	93	94.2	96.7	97	97.1
EUCLBP + SVM	99.95	99.93	99.93	99.91	99.89

Table : Cumulative Match Scores Of Five Methods

VII. COMPARISON

7.1. Discussion:

In this section, we have given the recognition rate of our system and compared our method with other methods. After extraction of features from images using Extended Uniform Circular Local Binary Pattern (EUCLBP), we have applied two well known K-NN classifier and SVM classifier in a straight forward way for recognition of query face sketch image. Our method significantly good for 1st match in comparison with other methods. Above table shows the

matching percentage of the first five ranks of five methods. In table we compare our proposed method with other methods like : Nonlinear Face Sketch Recognition and Sketch Transform Method and New dimension + PCA. The 1st match for Sketch Transform Method is no more than 80% and the 1st match for Nonlinear Face sketch Recognition is no more than 90% also 1st match of new dimension + PCA is not more than 93%. Our method greatly improves the 1st match to 99.95%.

VII. CONCLUSION

This paper presents matching of sketch images with digital face. The process starts with face detection, feature extraction Support vector machines, and finally matched output images. The method starts with the preprocessing technique to enhance sketches and digital images. However, to find score we use nearest neighbour symmetric kernel of SVM and the metric used in Normalized cross correlation. In this paper we use Cascade object detection with viola jones techniques for face detection and EUCLBP which stands for extended uniform circular linear binary pattern technique is used for feature extraction. Therefore it is concluded that by using Support vector machine we have successfully matched sketch with face image with face with high accuracy and less time. Thus we improve the recognition rate and identification accuracy for the given forensic sketch image.

References

- [1] Hand- Drawn Face Sketch Recognition By Humans and PCA- Based Algorithm for Forensic Applications by Yong Zang, Member, IEEE, Christine McCullough, John R. Sullins, Member, IEEE, and Christine R. Ross, 3 May 2010. [2] X. tang and X. Wang, "Face sketch synthesis and recognition," in proc. IEEE trans. Pattern Anal. Mach. Intell. Vol. 31. No 11 pp Nov 2009.
- [2] X. tang and X. Wang, "Face sketch synthesis and recognition," in proc. IEEE trans. Pattern Anal. Mach. Intell. Vol. 31. No 11 pp Nov 2009.
- [3] EUCLBP Matching Algorithm for Forensic Applications Gnanasoundari. V, Balaji.S PG Scholar , Assistant Professor, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, Feb 2014.
- [4] Anil K. Jain, Brendan Klare and Unsang Park, " Face Matching and Retrieval in Forensics Applications" IEEE Multimedia in Forensics, Security and Intelligence, pp.20-28, 2012.
- [5] B. Klare and A. jain, "Heterogeneous face recognition using kernel prototype similarities, IEEE tranc. On pattern Analysis and Machine Intelligence Vol.35, No. 6 pp.1410- 1422, 2013.
- [6] Hu Han et al [2], Component based recognition (CBR), Active shape modal(ASM) Multiscale local binary pattern(MLBPs) , 2013.
- [7] N. Lavanyaderi et al, Performance Analysis of Face Matching and Retrieval In Forensic Applications ,2013.
- [8] 4B. Klare, L. Zhifeng ,and A. jain, "Matching Sketches to mug Shot photos", IEEE tranc. On pattern Analysis and Machine Intelligence Vol.33, No. 639-646, 2011
- [9] X. Tang and X. Wang, "Face sketch recognition,"IEEE Tranc. Circuits Syst. Video Technol, Vol. 14 no. 1 pp. 50-57, Jan 2004.
- [10] A. S. Georghiadis, P. N. Belhumeur, and D. J. Kriegman, "From few to many: Illumination cone models for face recognition under variable lighting and pose," IEEE Trans. Pattern Anal. Mach. Intell., vol. 23, no. 6, pp. 643–660, Jun. 2001.
- [11] R. Basri and D. W. Jacobs, "Lambertian reflectance and linear subspaces," IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 2, pp. 218–233, Feb. 2003.
- [12] X. Tang and X. Wang, "Face Sketch Recognition," IEEE Trans. Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 50-57, Jan. 2004.



A Survey on Detection and Prevention of Vampire Attack using Time Based Mechanism in Wireless Ad-hoc Sensor Networks

Dhamma A Dahiwale

M.Tech Electronics and Communication
Ballarpur Institute of Technology Bamni, Tah. Ballarpur,
Distr: Chandrapur

Prof. Ashish Manusmare

Department of Electronics and Communication
Ballarpur Institute of Technology Bamni, Tah. Ballarpur,
Distr: Chandrapur

Abstract—A remote sensor system is a class of transducers which is utilized to screen and record the conditions of a remote environment. Disavowal of administration is one of the regular assaults in the remote sensor system. Vampire assault is a sort of disavowal of administration which expends vitality that prompts depleting battery - life of the hubs in the system. Subsequent to the hubs are battery fueled, the system lifetime is minimized. So correspondence between hubs can't be made appropriately furthermore the parcel does not achieve the destination amid transmission. This assault should be possible by either amplifying the way of hubs or it might form a circle in bundle transmission course. In this paper, we display different calculations on secure bundle transmission against vampire assault. This review gives diverse calculations to succeed the vampire assault and give secure bundle transmission in wireless notice- hoc sensor systems.

Keywords-- *Wireless sensor networks, Wireless ad-hoc networks, Denial of service, Vampire attack.*

I. INTRODUCTION

A remote sensor system comprises of various sensors that are spatially circulated over a land region . A n self-ruling sensor structure s a constitute system which is utilized for a few applications. The applications are observing an ecological conditions, wellbeing - care checking, mechanical checking, in a split second deployable correspondence for military, power administration, manufacturing plant execution, on - request figuring power, keen detecting in this way data or information assembling and handling, stock following, seismic location and acoustic recognition. Remote sensor system comprise s of a few qualities such as, versatility of hubs, usability, heartiness, vitality proficiency, heterogeneity, methodical outline, adaptability, responsiveness, self - arrangement and adjustment.

A remote specially appointed sensor system comprises of various sensors sent over a geological range. Each sensor has

remote correspondence ability and some level of knowledge for sign preparing and systems administration of the information. There are two approaches to order remote specially appointed sensor systems. Initially, whether the hubs are independently addressable, and second, whether the information in the system is totaled.

Because of Denial of service assault, the system might prompt execution debasement and loss of profitability. The assault should be possible by enemy hubs. The aim of foe hubs is to "asset exhaustion assault", by incapacitating the system which influences the correspondence way between hubs. It is one of the sorts of foreswearing of administration assault which makes harm system by totally drains vitality of hub's battery - life.

"Vampire - assault" is a sort of dissent of administration. The vampire assault is made by foe hub which makes vitality utilization between hubs in this way depleting the battery - life. Thus, the correspondence can't be made legitimately and the bundle transmits particle may not achieve the objective. The vampire assault can be finished by two ways. The principal assault is merry go round assault which shapes steering circles. Following, the vindictive hub send s parcel in circle that permits a solitary bundle to over and over cross the same arrangement of no des which lead depleting of battery life. The second assault is stretch assault; the foe hub can build the length of way between hubs in a system. So the parcel will go alongside superfluous hub rather than straightforward way to achieve destination.

Those sorts of pernicious hubs must be recognized to give an important action to maintain a strategic distance from these assaults. It should be possible through course disclosure and course upkeep process. The course revelation should be possible by including history along these lines it will maintain

a strategic distance from party I assault and course upkeep to ensure security by performing the mark between imparting way hubs. The distinguished issue can be fathomed by recently - provable calculation called "secure parcel transmission".

Vindictive hubs have infused necessary data or modifying legitimate hub's messages. For instance, an aggressor can produce messages to persuade legit hubs to course parcels in a path from the right destination. Vampire assault is additionally called as asset consumption assault. It predominantly concentrates on depleting hub's battery life which comes about that the system lifetime is lessened.

Whatever is left of the paper is arranged as takes after. Area II characterizes the vampire assault and its sorts. We examine the different calculations to beat the vampire assault and give secure bundle transmission in Section I II. Segment I V at long last finishes up the paper.

II. BACKGROUND

In genuine there are numerous movement administration plans built up as of now. These plans are portrayed underneath:

A. Vampire Attack

Vampire attack is creating and sending messages by malicious node which causes more energy consumption. It will lead to the depletion of node's battery life. Types of vampire attack are given as follows.

i. *Carousel attack*: Malicious nodes purposely introduced routing loops in a packet. This attack sends packets in circles. Its target is source routing protocols, allowing a single packet to repeatedly traverse the same set of nodes which forms a series of loops, so the same node appears in the route many times.

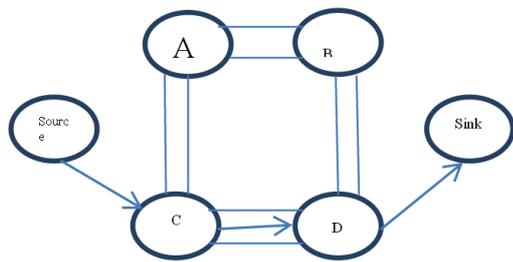


Fig. 1 Carousel Attack

ii. *Stretch attack*: Vindictive hubs intentionally presented directing circles in a parcel. This assault sends bundles in circles. Its objective is source steering conventions, permitting a solitary bundle to over and again cross the same arrangement of hubs which frames a progression of circles, so the same hub shows up in the course ordinarily.

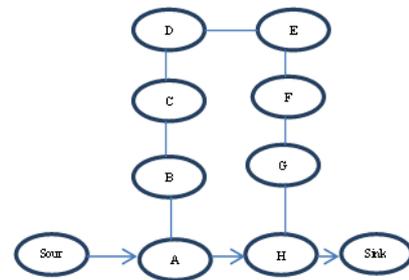


Fig. 2 Stretch Attack

III. ALGORITHM

David Johnson, et al [1] proposed a new type of routing protocol called Ariadne that prevents the attacker in ad-hoc network. Here the compromised nodes tampering with un-compromised routes. Ariadne is based on DSR routing protocol which is applied to route discovery and route maintenance to avoid attacks and also provide security by means of one-time signature.

Gergely ACS, et al [2] depicted, another source steering convention "EndairA" is utilized to give security to keep the assaults of malicious hubs. In EndairA, source hub makes a course demand that is telecast to its neighbor hub. In course revelation prepare a middle of the road hub can get that demand and adds their marks that are rebroadcast to its target. The destination hub makes a computerized signature as a course answer that can be sent to source hub. The given framework gives security against the vicinity of an enemy.

David Johnson, et al [3] introduced another kind of assault called "hurrying - assault". The previously accessible convention might come up short under hurrying assault furthermore they built up another avoidance strategy called "surging - assault counteractive action". Here, the banner marker is connected to determine the issue of noxious hubs.

R.Sangeetha, et al [4] concentrated on vitality accessible at every sensor hub. An unmistakable vampire can contract sufficiently vast use in general system to waste vitality of hubs. All past methodologies are powerless against vampire assaults which are dangerous, difficult to judgment and simple to do malicious insider sending convention yielding messages. The executed a methodology "secure parcel traversal" to accomplish expanded force utilization by compelling hubs.

Santhosh L, et al [5] discussed another variant of vampire assault that incapacitates a whole network for all time by rapidly depleting of hub's battery power. Location Algorithm is connected to each directing hub in a system. On the off chance that a hub gets a parcel it has to create a mark for that bundle and it is added to a rundown in the event that they are not as of now p hated. On the off chance that the mark as of now exists in the rundown then the steering hub will drop that bundle.

Achuthan Ganthi, et al [6] considered worm - opening assault. Because of this assault the bundle can't reach to its destination. The parcel sending should be possible by AODV steering convention. This convention can distinguish the parcel droppers. AODV steering convention will distinguish the assailant hub then locate an option way to cross a bundle that the way ought not to have any sort of assaults. One more point of preference of this protocol is to figure the packet conveyance proportion. They proposed a framework which helps us to accomplish dependable parcel conveyance and set aside just less time to cross the bundles. It distinguishes the course droppers before the transmission of the parcels.

Bryan Parno, et al [7] evaluated another secure steering convention called "clean - slate approach" for sensor systems. The proposed model has centering message conveyance even in a situation containing with a dynamic enemies. They proposed another sensor system routing convention called Geographic hash tables (GHTS) and a key dispersion plan like PIKE with high security proficiency.

Chris Karlof David Wagner, et al [8] for the most part centered around security issues in directing layer . They talked about how the promotion - hoc and peer - to - peer systems can embrace to intense assaults. They centered two sorts of assaults that are sink opening and hi surges. Link layer encryption and validation instruments work with guard against vindictive hubs.

Qing Cao, et al [9] considered a bunch. In group any hub in next - bounce can assume sending liability that extraordinarily intended for remote sensor systems. By utilizing they accomplished better vitality efficiency and that will lessen retransmission. The outcome is effective and improves end - to - end energy and dormancy of current steering conventions.

Chung Kei Wong, et al [10] presented a Feige - fiat - shamir digital signature scheme to speed up both signing and verification operations as well as they allowed adjustable and incremental verification operations. These operations are done through tree chaining techniques. The proposed signing and verification process (eFFS) is more efficient than DSA and Elgammal. An adjustable and incremental verification are more useful in large - scale multicast applications that work with a variety of receivers including limited resources.

Joongseok Park SartajSahni, et al [11] analyzed a lot of routing problem by on - line heuristics in wireless sensor network. In on - line models, each message has to be routed without knowledge of future route request. They developed an on - line heuristic that will maximize network life - time by performing two - shortest path computation for routing their messages. The capacity metrics are increased by using heuristic. The on - line maximum lifetime heuristic (OML) is used to maximize the network life - time that deals with delay depletion of sensor's energy nodes.

Youngsoo Kim, et al [12] proposed a new scheme to transfer an active packet to all neighboring nodes securely. They used public - key crypto system and asymmetric key crypto system. Lakshminarayanan, et al [13] provided two results to overcome attacks in the network. First, they provided a distributed algorithm that can achieve a reliable broadcast in an unknown fixed identity network even an adversary presence. Second, the problem of reliable broadcast in sparse network even if there is a single adversary present. They have developed decentralized security measures to protect internet against adversaries and achieved decentralized public key distribution in static networks.

M.BalaGanesh, et al [14] proposed 2 - ACK plan to send two - jump affirmation of bundles the other way of the steering way. They outlined another interruption - location framework called "EAACK" (Enhanced versatile affirmation) that can recognize profoundly noxious conduct rates and enhance the system execution. The system issues can be handled by EAACK. EAACK can likewise stretch out with computerized mark to keep the assailant from manufacturing affirmation parcel.

Tarun Kumar Mishra, et al [15] promotion - hoc system can help settling issues of assault from private hubs by confirmation procedures that give shared trust between hubs. They additionally conjured advanced marks for security. They utilized AODV convention to give course on - request and coordinated numerous elements to amplify execution at decreased directing overhead. Additionally they have included expense of many-sided quality for effective breaks down. They additionally included course accessibility and acceptance process.

Marcin Poturski, et al [16] gave an essential variation of neighbor revelation issue. They have inferred a convention named as time - based convention and time - area based conventions. The secure neighbor revelation procedure should be possible effectively by utilizing these protocols. The time based conventions are utilized to trade a message between an arrangements of hubs and to quantify those hubs precisely with time element. They proposed a system which gives a protected neighbor disclosure process with basic topology. This system is additionally used to control a hub's transmission power.

Amitabh Saxena, et al [17] presented one - way signature chaining which generates a chain of signature on the same message by different users. Here, each signature can act as a link. An intermediate node can be infeasible to remove links. This chain signature can be constructed by computational Diffie - Hellman (CDH) method. The chain signature is similar to transitive signature. It considered verification encrypted signature (VES) and sequential aggregate signature (SAS). It also provides truncation resilience from that will distinguish it from other multiuser signature schemes.

IV. CONCLUSION

Vampire assault is an asset utilization assault that utilization directing conventions to make a refusal of administration keeping in mind the end goal to handicap whole notice - hoc remote sensor system by waste of hub's battery life. In this paper, we talked about distinctive calculations to beat vampire assault and give secure bundle transmission. By maintaining a strategic distance from these assaults, we can enhance the lifetime of the system.

REFERENCES

- [1] David B.Johnson , Yih - Chun Hu and Adrian Perrig,"Ariadne: A secure On - demand Routing protocol for Ad Hoc Networks " ,In Wireless Networks 11, 21 – 38 , 2005 .
- [2] GergelyAcs, LeventeButtyan, and IstvanVajda,"Provably Secure On - demand Source Routing in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, mar. 2005 .
- [3] David B.Johnson, Yih - Chun Hu and Adrian Perrig, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols " , 2nd ACM workshop on Wireless security, 2003.
- [4] R. Sangeetha, R.Deepa, C.Balasubramanian, " Provably Secure Routing and Defending Against Vampire Attacks in Wireless Ad Hoc Sensor Networks " , IEEE International Conference on - ICIET'14,mar. 2014 .
- [5] Santhosh L, A.V.Krishna Mohan, "Prevention of Resource Depletion Attack in Wireless Sensor Network " , 5th Proceedings of SARC - IRF International Conference , may.2014
- [6] Achuthan Gandhi G and G. Vijayalakshmi, "Identification of Packet Droppers and Effective Routing of Packets in Wireless Sensor Networks", International journal of technology enhancement, 2014 .
- [7] Bryan Parno, MarkLuk, Evan Gaustad, and AdrianPerrig, "Secure Sensor Network Routing: A Clean - Slate Approach " , Proceedings of the 2006 ACM CoNEXT conference2006.
- [8] Chris Karlof David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Article in Elsevier , 2002.
- [9] Qing Cao, TarekAbdelzaher, Tian He, Robin Kravets,"Cluster - Based Forwarding for Reliable End - to - End Delivery in W SN " , IEEE INFOCOM , 2007 .
- [10] Chung Kei Wong and Simon S. Lam,"Digital Signatures for Flows and Multicasts " , IEEE transaction on networking, VOL. 7, NO. 4, aug.1999 .
- [11] Joongseok Park SartajSahni, "Maximum Lifetime Routing In Wireless Sensor Networks", IEEE/ACM Transactions on Networking 2005.
- [12] Youngsoo Kim , Jungchan Na , Seungwon Sohn , " A secure method for transferring active packets " , Proceedings of WSEAS, 1997.
- [13] Lakshminarayanan SubramanianRandy H. KatzVolker RothScott Shenker Ion Stoica, "Reliable Broadcast in Unknown Fixed Identity Networks " , 24 th Proceedings of annual ACM symposium on distributed computing , 2005.
- [14] M.BalaGanesh, M.Mohamed Faisal, "Enhance the Security Level of MANET's Using Digital Signature", IEEE Transactions on Networking, Aug.2004.
- [15] Sureka.N, S. Chandra Sekaran," Securable Routing and elimination of Adversary Attack from Manet", proceedings of ICGICT'14, Mar.2014
- [16] Tarun Kumar Mishra, Bhupendra Singh, ArunKumar,"A Security Scheme for Mobile Ad - hoc Network with Reduced Routing Overhead " , International journal of advanced research computer science and software engineering, 2013.
- [17] MarcinPoturalski, PanosPapadimitratos, Jean - Pierre Hubaux,"Secure Neighbor Discovery in Wireless Network s: Formal Investigation of Possibility", Proceedings of ASIACCS, 2008.
- [18] Sharon Goldberg, David Xiao, EranTromer, Boaz Barak, Jennifer Rexford,"Path - Quality Monitoring in the Presence of Adversaries", Proceedings of ASIACCS, 2008.
- [19] Amitabh Saxena and Ben Soh,"One - Way Signature Chaining - A New Paradigm For GroupCryptosystems", International Journal of Information and computer Security, 2006.
- [20] Prosenjit Bose and Pat Morin and Ivan Stojmenović and Jorge Urrutia,"Routing with Guaranteed Delivery in Ad Hoc Wireless Networks", Journal Wireless Networks vol 7 Issue 6, Nov 2001.

BIOGRAPHIES

Mr.Dhamma Dahiwale is doing his M.Tech in Electronics and Communication at Ballarpur Institute of Technology, Chandrapur. He completed his Bachelor of Technology in Information Technology at Nandha Engineering College, Erode. Her area of interest is Wireless Sensor Networks.

Prof. Ashish Manusmare is working as a Professor in Ballarpur Institute of Technology, Chandrapur. He has completed his ME in Electronics and Communication at Technocrat institute of technology, Bhopal. His area of interest is Wireless Sensor Networks.

An Application Based On Brain Computer Interface(BCI) For Controlling the Speed of Motor Using Mind Wave Signal

Brijesh Pathak

*Department of electronic and telecommunication
RasthrasaniTukadojiMaharaj, Nagpur University*

Nagpur, India.

brijpush3@gmail.com

Abstract—The main idea of this project is to control the speed of DC motor by using the mind wave signal such as attention signal .For example if attention level of the particular person who is wearing the mind wave mobile headset is increases the speed of the DC motor increases and if the attention level decreases the speed of motor also decreases

Keywords—*EEG,BCI,FUZZY LOGIC*

1) INTRODUCTION

Electroencephalography (EEG) is the measurement of electrical activity in the living brain. The first electrical neural activities of the human brain were registered by Hans Berger (1924) using a simple galvanometer. On the human scalp was placed only one electrode, and one wave was identified. It was alpha wave (also called Berger's wave). Nowadays in clinical use of EEG, 21 electrodes are used to identify 5 fundamental waves, but this kind of the device costs thousands of dollars. In recent years, inexpensive mobile EEG devices have been developed by Avatar EEG Solutions, Neurosky, OCZ Technology, InteraXon, PLX Devices and Emotiv Systems. These devices are not used in clinical use, but are used in the Brain Control Interface (BCI) and neurofeedback (one of biofeedback types). The BCI is a direct communication pathway between the brain and an external device. The cheapest EEG device is single-channel MindWave MW001 produced by Neurosky Inc., San Jose, CA. It costs only around \$80. The device consists of eight main parts, ear clip, flexible ear arm, battery area, power switch, adjustable head band, sensor tip, sensor arm and inside thinkgear chipset. Figure 1 presents the device design. The principle of operation is quite simple. Two dry sensors are used to detect and filter the EEG signals. The sensor tip detects electrical signals from the forehead of the brain. At the same time, the sensor picks up ambient noise generated by human muscle, computers, light bulbs, electrical sockets and other electrical devices. The

second sensor, ear clip, is a ground and reference, which allows thinkgear chip to filter out the electrical noise. The device measures the raw signal, power spectrum (alpha, beta, delta, gamma, theta), attention level, meditation level and blink detection. The raw EEG data received at a rate of 512 Hz. Other measured values are made every second. Therefore, raw EEG data is a main source of information on EEG signals using Mind-Wave MW001.

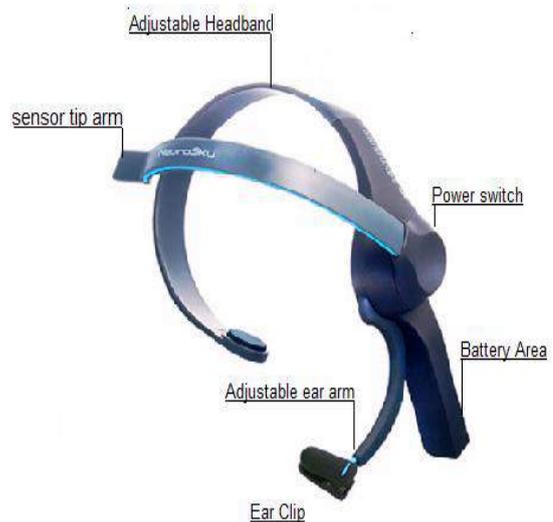


Fig 1. mind wave mobile design

2) METHOD

A. Types of wave:

In human brain there are different wave with its own particular frequency range such as alpha, beta, gamma, delta and theta

1. **Gamma wave** are in the frequency range of 31 Hz and up. It is thought that it reflect the mechanism of consciousness. Beta and Gamma waves together have been associated with attention, perception and cognition.

2. **Beta wave** is in the frequency range of 12 and 30 Hz, but are often divided into β_1 and β_2 to get a more specific range. The wave is small and fast, associated with focused concentration and best defined in central and frontal areas. When resisting or suppressing movement, or solving a math task, there is an increase of beta activity.

3. **Alpha wave** ranging from 7.5 to 12 Hz is slower and associated with relaxation and disengagement. Thinking of something peaceful with eye closed should give an increase of alpha activity. It is also called as Berger's wave.

4. **Theta wave** ranging from 3.5 to 7.5 Hz, are linked to inefficiency, day dreaming and the very lowest wave of theta represent line between being awake or in a sleep state. Theta arises from emotional stress, especially frustration or disappointment. It has also been associated with access to unconsciousness material, creative inspiration and deep meditation.

5. **Delta wave** ranging from 0.5 TO 3.5 Hz is the slowest wave occurs when sleeping. If this wave occurs in the awake state, it thought to indicate physical defect in the brain. Movement can make artificial delta wave.

B. Selection of signal

There is a particular frequency range for an attention and meditation level of a person. For calculating level of attention and meditation we have eSense meter through which we can get the attention and meditation level of a person. For all the different types of eSenses (i.e. Attention, Meditation), the meter value is reported on a relative eSense scale of 1 to 100. On this scale, a value between 40 to 60 at any given moment in time is considered "neutral", and is similar in notion to "baselines" that are established in conventional EEG measurement techniques (though the method for determining a ThinkGear baseline is proprietary and may differ from conventional EEG). A value from 60 to 80 is considered "slightly elevated", and may be interpreted as levels being possibly higher than normal (levels of Attention or Meditation that may be higher than normal for a given person). Values from 80 to 100 are considered "elevated", meaning they are strongly indicative of heightened levels of that eSense. An eSense meter value of 0 is a special value indicating the ThinkGear is unable to calculate an e-Sense level with a reasonable amount of reliability. This may be (and usually is) due to excessive noise.

ATTENTIONeSense

This unsigned one-byte value reports the current e-Sense Attention meter of the user, which indicates the intensity of a user's level of mental "focus" or "attention", such as that which occurs during intense concentration and directed (but stable) mental activity. Its value ranges from 0 to 100. Distractions, wandering thoughts, lack of focus, or anxiety may lower the Attention meter levels. See eSense(tm) Meters above for details about interpreting eSense levels in general. By default, output of this Data Value is enabled. It is typically output once a second.

MEDITATIONeSense

This unsigned one-byte value reports the current e-Sense Meditation meter of the user, which indicates the level of a user's mental "calmness" or "relaxation". Its value ranges from 0 to 100. Note that Meditation is a measure of a person's **mental** levels, not **physical** levels, so simply relaxing all the muscles of the body may not immediately result in a heightened Meditation level. However, for most people in most normal circumstances, relaxing the body often helps the mind to relax as well. Meditation is related to reduced activity by the active mental processes in the brain, and it has long been an observed effect that closing one's eyes turns off the mental activities which process images from the eyes, so closing the eyes is often an effective method for increasing the Meditation meter level. Distractions, wandering thoughts, anxiety, agitation, and sensory stimuli may lower the Meditation meter levels. See "eSense Meters" above for details about interpreting eSense levels in general. By default, output of this Data Value is enabled. It is typically output once a second. From both of the eSenses above we are using the attention signal for controlling the speed of motor. It will be more beneficial and useful for controlling the speed of motor. We have to just focus on controlling the speed of motor so by attention signal we can control the speed of motor. If the attention level increases the speed of the motor increases and if the attention level decreases the speed of motor also decreases.

C. Fuzzy logic

Fuzzy logic can be conceptualized as a generalization of classical logic. Modern fuzzy logic was developed by Lotfi Zadeh in the mid-1960s to model those problems in which imprecise data must be used or in which the rules of inference are formulated in a very general way making use of diffuse categories. In fuzzy logic, which is also sometimes called diffuse logic, there are not just two alternatives but a whole continuum of truth values for logical propositions. Here we are using fuzzy logic such as for controlling the speed of motor. As attention level ranges from 0-100 so we divide the level of attention with the particular value of voltage. If the attention level of the person is 20 so DC motor will be getting 1 volt supply voltage. So DC motor will run according to the power getting from 1 volt. If the attention level increases the

supply voltage to the DC motor increases which would help in increasing the speed of motor.

S.NO	ATTENTION LEVEL	DC MOTOR VOLTAGE
1	0-20	1
2	21-40	2
3	41-60	3
4	61-80	4
5	81-100	5

D. Working

The headset delivers digital data in an asynchronous serial stream of byte which is of 173 byte. It is in packet format consist of three part 1) Packet Header 2) Packet Payload 3) Payload Checksum

Packets are sent as an asynchronous serial stream of bytes. The transportmedium may be UART, serial COM, USB, bluetooth, file, or any othermechanism which can stream bytes.Each Packet begins with its Header, followed by its Data Payload, and endswith the Payload's Checksum Byte The [PAYLOAD...] section is allowed to be up to 169 bytes long, while each of [SYNC], [PLENGTH], and [CHKSUM] are a single byte each. This means that a complete, valid Packet is a minimum of 4 bytes long (possible if theData Payload is zero bytes long, i.e. empty) and a maximum of 173 byteslong (possible if the Data Payload is the maximum 169 bytes long).The [CHKSUM] Byte must be used to verify the integrity of the Packet's DataPayload.The Header of a Packet consists of 3 bytes: two synchronization [SYNC]bytes (0xAA 0xAA), followed by a [PLENGTH]the two [SYNC] bytes are used to signal the beginning of a new arrivingPacket and are bytes with the value 0xAA (decimal 170). Synchronization is two bytes long, instead of only one, to reduce the chance that [SYNC] (0xAA) bytes occurring within the Packet could be mistaken for thebeginning of a Packet. Although it is still possible for two consecutive[SYNC] bytes to appear within a Packet (leading to a parser attempting to begin parsing the middle of a Packet as the beginning of a Packet) the[PLENGTH] and [CHKSUM] combined ensure that such a "mis-sync'dPacket" will never be accidentally interpreted as a valid packet. The [PLENGTH] byte indicates the length, in bytes, of the Packet's Data Payload [PAYLOAD...] section, and may be any value from 0 up to 169. Any higher value indicates an error (PLENGTH TOO LARGE). Be sure to note that [PLENGTH] is the length of the Packet's Data Payload,

NOT of the entire Packet. The Packet's complete length will always be [PLENGTH] + 4. The Payload's Checksum is defined as:

1. Summing all the bytes of the Packet's Data Payload
2. Taking the lowest 8 bits of the sum
- 3.Performing the bit inverse (one's compliment inverse) on thoselowest 8 bits

A receiver receiving a Packet must use those 3 steps to calculate thechecksum for the Data Payload they received, and then compare it to the[CHKSUM] Checksum Byte received with the Packet. If the calculated payload checksum and received [CHKSUM] values do not match, the entire Packet should be discarded as invalid.

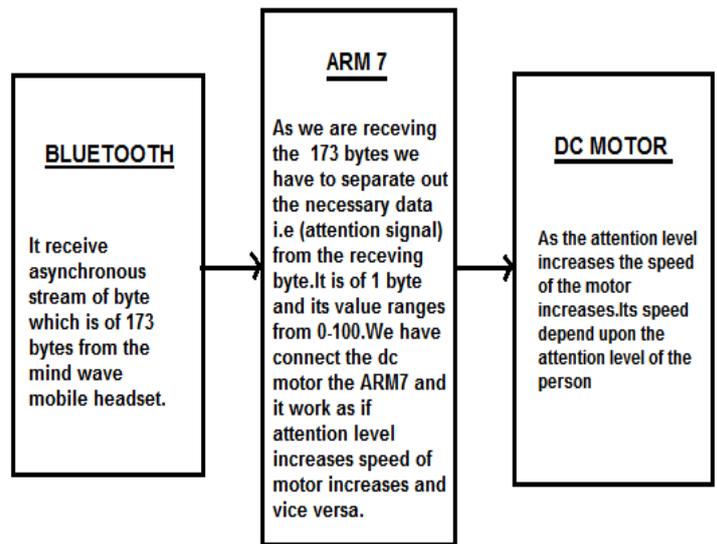


Fig. 2 Block diagram of interfacing of Bluetooth and dc motor the arm controller

From the block diagram we can see that the headset transmitting the signal in an asynchronous stream of byte which can be receive by the Bluetooth at 57k baud rate . It receives 173 byte of data from the headset and it has to follow certain procedure to parse the data which has been discussed above. As this procedure gets complete we can select the data which is required there is particular code for selection of particular signal. If we want attention signal we have to use the code 0x04 which give the attention level of the person who is wearing the headset. Every second its provide the value of the attention signal so we have to store the attention level of the person to a particular memory location so we can get continuously the fresh data .This data has to be used with DC motor so that we can provide the supply voltage according to level of attention signal .If the attention level increases the

speed of the motor increases and if the attention level decreases the speed of the motor decreases.

3) CONCLUSION

We have been working on the project yet we have not finished with the programming. We will finish with programming as soon as possible.

4) ACKNOWLEDGEMENT

I would like to express sincere gratitude and appreciation to all those who gave me the possibility to complete this paper. A special thanks to my Project Guide Prof. Anil Bavaskar, whose help, simulating suggestions and encouragement, helped to coordinate project especially in writing this paper. Word often fail to pay one's gratitude oneself, still we would like to convey sincere thanks to our H.O.D Prof. Sanjeev Sharma, without whose encouragement and guidance this project would not have materialized.

REFERENCE

1. Processing and spectral analysis of the raw EEG signal from the MindWave by WojciechSalabunISSN 0033-2097, R. 90 NR 2/2014.
2. Fuzzy Logic Technique to Control a Robot Based on Non-Invasive Brain Computer Interface by Human Group by Hassan Samadi, Mahdi Karimi. IEEE International Conference on Robotics and Mechatronics -2014.
3. Developing brain computer interface by fuzzy logic by MandeepKaurand PoonamTanwar.
4. Neuro-fuzzy classification of brain computer interface data using phase based feature by AtiyePourbakhtiar, MousaShamsi, and FatemeFarrokhshad.IEEE2013.
5. Brain-Computer Interface Analysis using Continuous Wavelet Transform and Adaptive Neuro-Fuzzy Classifier by Sam Darvishi and Ahmed Al-Ani.IEEE EMBS 2007.
6. Use of fuzzy logic for segmenting of brain images by multi-agent system by S. Nasser, R. Mekki. IEEE International Conference onSystems and Control 2013.
7. BCI revolutionizing human computer interaction by Bernhard Graimann, Brenda ALLISON, Gertfurtscheller.
8. Toward BCI byGuido Dornhege, José del R. Millán, ThiloHinterberger, Dennis J. McFarland,and Klaus-Robert Müller.

Removal of Salt and Pepper Noise Using Unsymmetrical Trimmed Adaptive Median Filter

Mr. Vaibhav Agrawal

Electronic Engineering,
J D Collage of Engineering and Management
RTMN University, Nagpur, India
E-mail ID vaibhavachalpur@gmail.com

Prof. Sunil R. Gupta

Guide and Asso.
Prof of Electronic Engineering,
J D Collage of Engineering and Management
E-mail ID sungt_in@rediffmail.com

Abstract— Digital image contains impulse noise and removal of impulse noise from the image is very challenging area in digital image processing. In recent years many developments were made for removal of such noise which helps to improve quality of image. For the removal of salt and pepper noise this paper is been proposed. This paper proposes unsymmetrical trimmed adaptive median filter algorithm is used for restoration of image quality. The algorithm proposed replaces the noisy pixels i.e. either salt value or pepper value by trimmed median value. 0's or 255's in a window is replaced by median value in the window. This paper is combination of adaptive filter and unsymmetrical trimmed median filter to overcome the flaws in them.

Keywords— Impulse noise, median filter, adaptive filter, unsymmetrical trimmed adaptive median filter.

Introduction

An image is an array or a matrix of square pixels (pictures elements) arranged in rows and columns. Digital images are normally corrupted by noises such as impulse noise which is subdivided as salt and pepper noise and random valued noise. Impulse noise is introduced in images due to various reasons such as malfunctioning of pixels in camera sensors, faulty locations in hardware, acquisition and during transmission. Images corrupted by salt and pepper noise takes maximum or minimum value. Many works were done for the restoration of image. Initially introduced median filter, which is non-linear filter, replaces the center pixel with a value equal to the median of all pixels in current window. Various filters were introduced with different algorithms but basically they all work on median filter with some additional features to overcome the flaws and shortcomings seen in median filter.

Ease of Use

A. Standard median filter

(SMF) removes impulse noise by changing luminance value of the center pixel of the filtering window with the median of the luminance values of pixels contained within the window. It removes thin lines but blurs the image. It cannot differentiate between corrupted and non-corrupted value, so all the values are altered increasing the time of processing and for high

intensity of noise, window size is increased which reduces the originality of image

B. Weighted median filter

(WMF) is similar to SMF, except that WMF has weight associated with each of its filter element. These weights correspond to number of sample duplication for calculation of median value. It is classified as (a) central weighted median filter i.e. it gives more weight only to central value of window (b) adaptive weighted median filter.

C. Directional median filter

It works by separating its 2-D filter into several 1-D filter

D. Iterative median filter:

In this same procedure is repeated several times and the number of iterations needed is depended on level of corruption and also the nature of input image. In general iterative median filter, with (n) iterations requires (n-1) temporary images

E. Adaptive median filter

It is designed to eliminate problems faced with SMF. In AMF the size of window surrounding each pixel is variable and variation depends on median of pixels in present window. If median value is an impulse, then the size of window is expanded else processing is done in current window specifications. The center pixel of the window is evaluated to verify whether it is an impulse or not.

F. Switching median filter

It minimizes the undesired alteration of non-corrupted pixels by the filter. It involves two stages: noise detection and noise cancellation. Decision based filter is based on predefined threshold value. The major drawback of this filter is robust decision. Robust decision is difficult and also it does not consider the local features of image, resulting unsatisfactorily recovered images when noise level is high. Also it causes streaking effect due to repeated use of neighboring element so to avoid this, decision based unsymmetrical trimmed median filter is proposed. It also fails for more than 80% of noise. so this paper proposes the combination of adaptive filter and

decision based unsymmetrical trimmed adaptive median filter. It can remove salt and pepper noise with intensity as high as 90%. The outline is as follows: section 2 describes unsymmetrical trimmed adaptive median filter, section 3 describes its algorithm, section 4 shows its flow chart, section 5 is all about result and conclusion.

II. UNSYMMETRICAL TRIMMED ADAPTIVE MEDIAN FILTER

Salt and pepper noise only takes maximum or minimum value i.e. positive or negative value. Positive impulse appears as white (salt) with intensity 255 and negative impulse appears as black (pepper) with intensity 0. The idea behind this is to reject noisy pixel from selected window (3*3 or 5*5). In unsymmetrical trimmed median filter (UTMF) window size is fixed i.e. (3*3). In this UTMF the selected 3*3 window elements are arranged in either increasing or decreasing order.

Then the pixel values 0's or 255's are removed from the image. Then the median value of the remaining pixels is taken. This median value is used to replace noisy pixel. But at high noise intensity when more than 75% of pixels are corrupted at most only two pixels will be available for reference. So to overcome this problem (UTAMF) is introduced. In this the window size is selected dynamically depending on the total number of noisy or corrupted pixels i.e. if more than 75% or more pixels are noisy in window of size (3*3), then window size is increased to 5*5 and elements are arranged either in their increasing or decreasing order and then 0's and 255's in window removed i.e. salt and pepper value. The noisy pixel is then replaced by median value of remaining pixels.

III. ALGORITHM:

The proposed Unsymmetrical Trimmed Adaptive Median Filter (UTAMF) algorithm processes the corrupted images by first detecting the salt and pepper noise. The processing pixel is checked whether it is noisy or noise free. If the processing pixel lies between maximum and minimum gray level values, then it is noise-free pixel and it is left unchanged. If the processing pixel takes the maximum or minimum gray level, then it is noisy pixel which is processed by UTAMF. While processing image, always noisy image is taken as reference for calculation of median and processing pixel is replaced median in output image. This is explained as follows. Let A be the input noisy image and B be the output image which initially is a copy of the input noisy image A. Now the image A acts as the reference image and it is processed pixel-by-pixel and the corresponding pixel in the image B is replaced with the output pixel which is obtained as a result of processing done on image A. The steps of the UTMAF are explained as follows.

Step 1: Read Noisy Image.

Step 2: Select 2D window of size 3x3 with center element as processing pixel. Assume that the pixel being processed is P_{ij} .

Step 3: If P_{ij} is an uncorrupted pixel (that is, $0 < P_{ij} < 255$), then its value is left unchanged.

Step 4: If $P_{ij} = 0$ or $P_{ij} = 255$, then P_{ij} is a corrupted pixel.

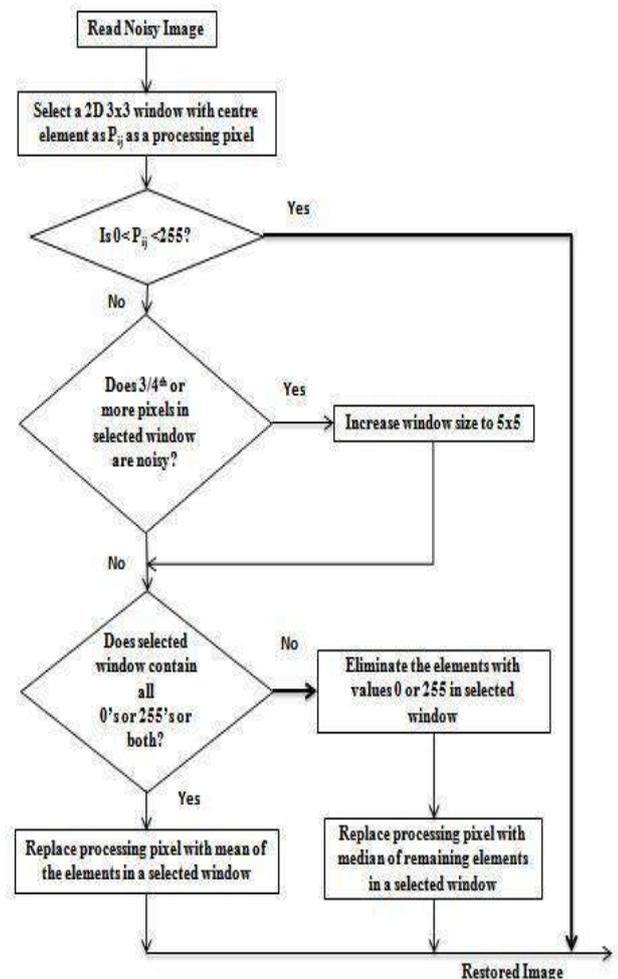
Step 5: If 75% or more pixels in selected window are noisy then increase window size to 5x5.

Step 6: If all the elements in the selected window are 0's and 255's, then replace P_{ij} with the median of the elements in the window else go to step 6.

Step 7: Eliminate 0's and 255's from the selected window and find the median value of the remaining elements. Replace P_{ij} with the median value.

Step 8: Repeat steps 2 to 6 until all the pixels in the entire image are processed

FLOW CHART



A. Figures and Table

The performance of the proposed algorithm is tested with different greyscale and colour images. The noise density (intensity)

TABLE I
COMPARISON OF PSNR VALUES OF DIFFERENT ALGORITHMS FOR LENA IMAGE AT DIFFERENT NOISE DENSITIES

Noise in %	PSNR in dB					
	MF	AMF	PSMF	DBA	MDBA	MDBUTMF
10	26.34	28.43	30.22	36.4	36.94	37.91
20	25.66	27.40	28.39	32.9	32.69	34.78
30	21.86	26.11	25.52	30.15	30.41	32.29
40	18.21	24.40	22.49	28.49	28.49	30.32
50	15.04	23.36	19.13	26.41	26.52	28.18
60	11.08	20.60	12.10	24.83	24.41	26.43
70	9.93	15.25	9.84	22.64	22.47	24.30
80	8.68	10.31	8.02	20.32	20.44	21.70
90	6.65	7.93	6.57	17.14	17.56	18.40

TABLE II
COMPARISON OF IEF VALUES OF DIFFERENT ALGORITHMS FOR LENA IMAGE AT DIFFERENT NOISE DENSITIES

Noise Density in %	IEF					
	MF	AMF	PSMF	DBA	MDBA	MDBUTMF
10	10.36	23.20	171.63	390.67	422.58	648.98
20	28.17	37.76	207.31	358.91	377.42	568.43
30	30.02	42.57	190.92	322.89	324.74	590.83
40	23.12	40.98	143.49	268.49	275.24	424.18
50	11.72	36.11	62.98	208.77	217.18	345.13
60	6.73	25.21	6.61	190.70	175.89	261.66
70	3.31	7.89	3.28	128.58	129.65	171.69
80	2.00	2.91	1.98	67.42	73.24	101.72
90	1.37	1.31	1.37	33.85	33.33	34.23

is varied from 10% to 90%. Denoising performances are quantitatively measured by the PSNR and IEF as defined in (1) and (3), respectively:

$$PSNR \text{ in dB} = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \quad (1)$$

$$MSE = \frac{\sum_i \sum_j (Y(i, j) - \hat{Y}(i, j))^2}{M \times N} \quad (2)$$

$$IEF = \frac{\sum_i \sum_j (\eta(i, j) - Y(i, j))^2}{\sum_i \sum_j (\hat{Y}(i, j) - Y(i, j))^2} \quad (3)$$

where MSE stands for mean square error, IEF stands for image enhancement factor, $M \times N$ is size of the image, Y represents the original image, \hat{Y} denotes the denoised image, η representsthe noisy image.

The PSNR and IEF values of the proposed algorithm are compared

against the existing algorithms by varying the noise density from 10% to 90% and are shown in Table I and Table II.

From the Tables I and II, it is observed that the performance of the proposed algorithm (MDBUTMF) is better than the existing algorithms at both low and high noise densities.

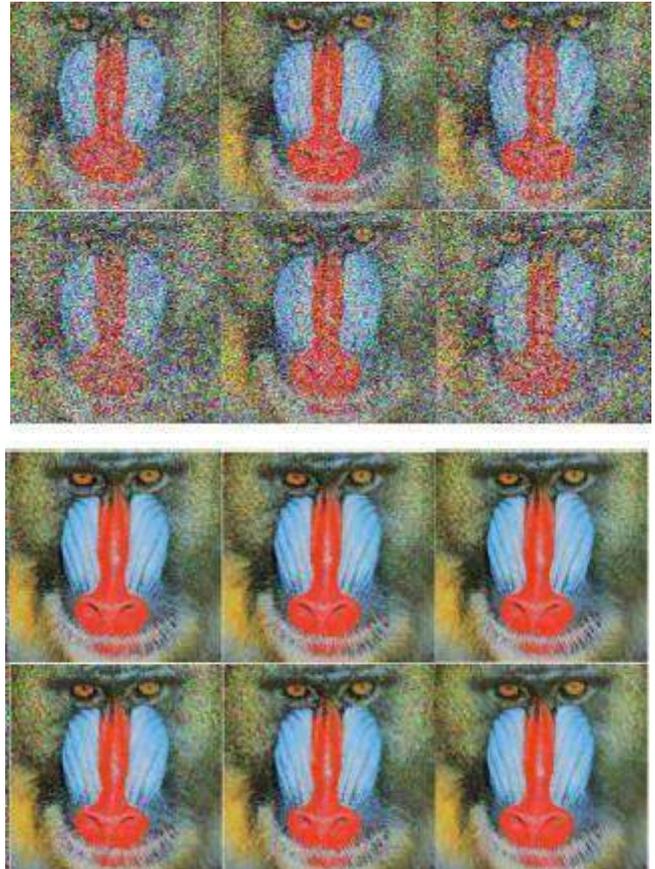


Fig. 1. Results of different algorithms for color Baboon image.

CONCLUSION

Removal of Salt and Pepper Noise Using Unsymmetrical Trimmed Adaptive Median Filter from the corrupted image. The directional difference based noise detector can realize accurate noise detection, thus facilitating the prevention of image degradation resulting from the undetected noise pixels and noise-free pixels. The adaptive mean filter can remove the detected impulses effectively while preserving the details very well because it adaptively determines the filtering window size and attaches different importance to the noise-free pixels in the filtering window. The combination of the noise detector with the distinctive median filter provides the adaptive median filter with significantly better noise detection performance, restoration performance and computational efficiency than numerous switching-based filters.

REFERENCES

- [1] H. Hwang and R. A. Haddad, "Adaptive median filters: New algorithms and results," *IEEE Trans. Image Process.*, vol. 4, no. 4, pp. 499–502, Apr. 1995.
- [2] A. Bovik, *Handbook of Image and Video Processing*. New York: Academic, 2000.
- [3] I. Aizenberg and C. Butakoff, "Effective impulse detector based on rank-order criteria," *IEEE Signal Process. Lett.*, vol. 11, no. 3, pp. 363–366, Mar. 2004.
- [4] W. Luo, "Efficient removal of impulse noise from digital images," *IEEE Trans. Consumer Electron.*, vol. 52, no. 2, pp. 523–527, May 2006.
- [5] F. Russo, "FIRE operators for image processing," *Fuzzy Sets Syst.*, vol. 103, pp. 265–275, Apr. 1999.
- [6] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, Englewood Cliffs, NJ: Prentice Hall, 2002.
- [7] E. Abreu, M. Lightstone, S. K. Mitra, and K. Arakawa, "A new efficient approach for the removal of impulse noise from highly corrupted images," *IEEE Trans. Image Process.*, vol. 5, no. 6, pp. 1012–1025, June 1996.
- [8] T. Chen, K. Ma and L. Chen, "Tri-state median filter for image denoising," *IEEE Trans. Image Process.*, vol. 8, no. 12, pp. 1834–1838, Dec 1999.
- [9] S. Schulte, M. Nachtegael, V. De Witte, D. Van der Waken and E. E. Kerre, "A fuzzy impulse noise detection and reduction method," *IEEE Trans. Image Process.*, vol. 15, no. 5, pp. 1153–1162, May 2006.
- [10] T. Chen, K. K. Ma, and L. H. Chen, "Tri-state median filter for image denoising," *IEEE Trans. Image Process.*, vol. 8, no. 12, pp. 1834–1838, Dec. 1999.
- [11] T. Chen and H. R. Wu, "Adaptive impulse detection using center-weighted median filters," *IEEE Signal Process. Lett.*, vol. 8, no. 1, pp. 1–3, Jan. 2001.
- [12] T. Chen and H. R. Wu, "Space variant median filters for the restoration of impulse noise corrupted images," *IEEE Trans. Circuits Syst. II*, vol. 48, no. 8, pp. 784–789, Aug. 2001.
- [13] R. H. Chan, C. Hu, and M. Nikolova, "An iterative procedure for removing random-valued impulse noise," *IEEE Signal Process. Lett.*, vol. 11, no. 12, pp. 921–924, Dec. 2004.
- [14] I. Aizenberg, C. Butakoff, and D. Paliy, "Impulsive noise removal using threshold Boolean filtering based on the impulse detecting functions," *IEEE Signal Process. Lett.*, vol. 12, no. 1, pp. 63–66, Jan. 2005.
- [15] S. Zhang and M. A. Karim, "A new impulse detector for switching median filters," *IEEE Signal Process. Lett.*, vol. 9, no. 11, pp. 360–363, Nov. 2002.

Review of Design of Area Efficient FFT Processor for DSP Application

Vanshri K.Kadwe

Department of Electronics and Communication Engineering
Tulsiramji Gaikwad Patil College of Engineering
Nagpur, Maharashtra, India
kvanshri@gmail.com

Prof.Supratim Saha

Department of Electronics and Communication Engineering
Tulsiramji Gaikwad Patil College of Engineering
Nagpur, Maharashtra, India
v.principal@tgpcet.com

Abstract— The discrete Fourier transform is an important operation in digital communication systems. However, the DFT is computationally very expensive, and the fast Fourier transform is an algorithm that has been proposed to compute the discrete Fourier transform efficiently. FFT can be implemented as either decimation in time or decimation in frequency. Also, depending on the decomposition, FFT can be radix-2 or radix-4. We propose a split radix FFT design where we apply a radix-2 mapping to the even index terms and we apply a radix-4 mapping to the odd index terms. The design is to be implemented on Xilinx Spartan FPGA. We present speed, area, and power results showing a comparison between split radix implementation and single radix implementation.

Keywords— FFT, fast fourier transform, discrete fourier transform, FPGA, decimation in time, decimation in frequency

I. INTRODUCTION

The fast Fourier transform is a fast implementation of the DFT. It is based on a divide-and-conquer approach in which the DFT computation is divided into smaller, simpler, problems and the final DFT is rebuilt from the simpler DFTs. Another application of this divide-and-conquer approach is the computation of very large FFTs, in which the time data and their DFT are too large to be stored in main memory. In such cases the FFT is done in parts and the results are pieced together to form the overall FFT, and saved in secondary storage such as on hard disk. In the simplest Cooley-Tukey version of the FFT, the dimension of the DFT is successively divided in half until it becomes unity. This requires the initial dimension N to be a power of two:

$$N = 2^B \text{ or } B = \log_2(N)$$

The problem of computing the N-point DFT is replaced by the simpler problems of computing two (N/2)-point DFTs. Each of these is replaced by two (N/4)-point DFTs, and so on. We will see shortly that an N-point DFT can be rebuilt from two (N/2)-point DFTs by an additional cost of N/2 complex multiplications. This basic merging step is shown in Fig. 1.

Thus, if we compute the two (N/2)-DFTs directly, at a cost of $(N/2)^2$ multiplications each, the total cost of rebuilding the full N-DFT will be:

$$2 \left(\frac{N}{2} \right)^2 + \frac{N}{2} = \frac{N^2}{2} + \frac{N}{2} = \frac{N^2}{2} \text{ (approximately)} \dots \text{eq.(1)}$$

where for large N the quadratic term dominates. This amounts to 50 percent savings over computing the N-point DFT directly at a cost of N^2 .

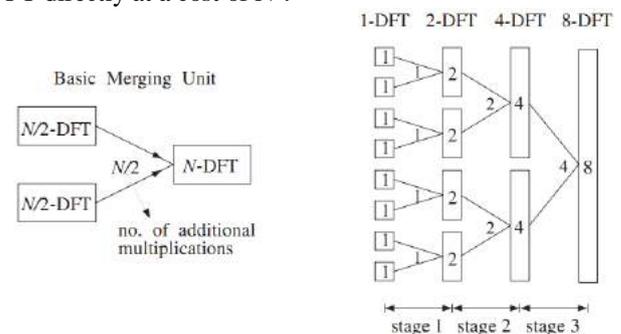


Fig.1.Basic merging step of (N/2)-point DFT

Merging two N/2-DFTs into an N-DFT and its repeated application

Similarly, if the two (N/2)-DFTs were computed indirectly by rebuilding each of them from two (N/4)-DFTs, the total cost for rebuilding an N-DFT would be:

$$4 \left(\frac{N}{4} \right)^2 + 2 \left(\frac{N}{4} \right) + \frac{N}{2} = \frac{N^2}{4} + 2 \left(\frac{N}{2} \right) = \frac{N^2}{4} \text{ (approximately)}$$

Thus, we gain another factor of two, or a factor of four in efficiency over the direct N-point DFT. In the above equation, there are 4 direct (N/4)-DFTs at a cost of $(N/4)^2$ each, requiring an additional cost of N/4 each to merge them into (N/2)-DFTs, which require another N/2 for the final merge. Proceeding in a similar fashion, we can show that if we start with (N/2^m)-point DFTs and perform m successive merging steps, the total cost to rebuild the final N-DFT will be:

$$\frac{N^2}{2^m} + \frac{N}{2} m \dots \text{eq.(2)}$$

The first term, $N^2/2m$, corresponds to performing the initial $(N/2^m)$ -point DFTs directly. Because there are 2^m of them, they will require a total cost of $2^m(N/2^m)2 = N^2/2^m$. However, if the subdivision process is continued for $m = B$ stages, as shown in Fig.1, the final dimension will be $N/2^m = N/2^B = 1$, which requires no computation at all because the 1-point DFT of a 1-point signal is itself. In this case, the first term in Eq. (2) will be absent, and the total cost will arise from the second term. Thus, carrying out the subdivision/merging process to its logical extreme of $m = B = \log(N)$ stages, allows the computation to be done in:

$$\frac{1}{2}NB = \frac{1}{2}N \log_2(N) \quad \dots \text{eq.(3)}$$

It can be seen Fig.1 that the total number of multiplications needed to perform all the mergings in each stage is $N/2$, and B is the number of stages. Thus, we may interpret Eq. (3) as (total multiplications) = (multiplications per stage) \times (no. stages) = $(N/2) \cdot B$

For the $N = 8$ example shown in Fig. 1, we have $B = \log_2(8) = 3$ stages and $N/2 = 8/2 = 4$ multiplications per stage. Therefore, the total cost is $BN/2 = 3 \cdot 4 = 12$ multiplications. Next, we discuss the so-called decimation-in-time radix-2 FFT algorithm. There is also a decimation-in-frequency version, which is very similar. The term radix-2 refers to the choice of N as a power of 2, in Eq. (1). Given a length- N sequence $x(n)$, $n = 0, 1, \dots, N-1$, its N -point DFT $X(k) = X(\omega k)$ can be written in the component-form of Eq. (2):

$$X(k) = \sum_{n=0}^{N-1} W_N^{kn} x(n), \quad k = 0, 1, \dots, N-1 \quad \dots \text{eq.(4)}$$

The summation index n ranges over both even and odd values in the range $0 \leq n \leq N-1$. By grouping the even-indexed and odd-indexed terms, we may rewrite Eq. (4) as

$$X(k) = \sum_n W_N^{k(2n)} x(2n) + \sum_n W_N^{k(2n+1)} x(2n+1) \quad \dots \text{eq.(5)}$$

To determine the proper range of summations over n , we consider the two terms separately. For the even-indexed terms, the index $2n$ must be within the range $0 \leq 2n \leq N-1$. But, because N is even (a power of two), the upper limit $N-1$ will be odd. Therefore, the highest even index will be $N-2$. This gives the range:

$$0 \leq 2n \leq N-2 \text{ or } 0 \leq n \leq \frac{N}{2} - 1$$

Similarly, for the odd-indexed terms, we must have $0 \leq 2n+1 \leq N-1$. Now the upper limit can be realized, but the lower one cannot; the smallest odd index is unity. Thus, we have:

$$1 \leq 2n+1 \leq N-1 \text{ or } 0 \leq 2n \leq N-2 \text{ or } 0 \leq n \leq \frac{N}{2} - 1$$

Therefore, the summation limits are the same for both terms:

$$X(k) = \sum_{n=0}^{N/2-1} W_N^{k(2n)} x(2n) + \sum_{n=0}^{N/2-1} W_N^{k(2n+1)} x(2n+1)$$

This expression leads us to define the two length- $(N/2)$ subsequences:

$$g(n) = x(2n) \\ h(n) = x(2n+1)$$

$$n = 0, 1, \dots, \frac{N}{2} - 1$$

and their $(N/2)$ -point DFTs:

$$\begin{matrix} G(k) = \sum_{n=0}^{N/2-1} W_{N/2}^{kn} g(n) \\ H(k) = \sum_{n=0}^{N/2-1} W_{N/2}^{kn} h(n) \end{matrix}, \quad k = 0, 1, \dots, \frac{N}{2} - 1$$

Then, the two terms of Eq.(5) can be expressed in terms of $G(k)$ and $H(k)$. We note that the twiddle factors W_N and $W_{N/2}$ of orders N and $N/2$ are related as follows:

$$W_{N/2} = e^{-2\pi j/(N/2)} = e^{-4\pi j/N} = W_N^2$$

or

$$W_N^{k(2n)} = W_N^{2(kn)} = W_{N/2}^{kn}$$

and

$$W_N^{k(2n+1)} = W_N^k W_N^{2kn} = W_N^k W_{N/2}^{kn}$$

So,

$$X(k) = \sum_{n=0}^{N/2-1} W_{N/2}^{kn} g(n) + W_N^k \sum_{n=0}^{N/2-1} W_{N/2}^{kn} h(n) \quad \dots \text{eq.(6)}$$

and

$$X(k) = G(k) W_N^k H(k)$$

$$k = 0, 1, \dots, N-1$$

This is the basic merging result. It states that $X(k)$ can be rebuilt out of the two $(N/2)$ -point DFTs $G(k)$ and $H(k)$. There are N additional multiplications, $W_N^k H(k)$. Using the periodicity of $G(k)$ and $H(k)$, the additional multiplications may be reduced by half to $N/2$. To see this, we split the full index range $0 \leq k \leq N-1$ into two half-ranges parametrized by the two indices k and $k+N/2$:

$$0 \leq k \leq \frac{N}{2} - 1 \quad \text{or} \quad \frac{N}{2} \leq k + \frac{N}{2} \leq N-1$$

Therefore, we may write the N equations (6) as two groups of $N/2$ equations:

$$X(k) = G(k) + W_N^k H(k)$$

$$X(k + N/2) = G(k + N/2) + W_N^{(k+N/2)} H(k + N/2)$$

Using the periodicity property that any DFT is periodic in k with period its length, we have $G(k + N/2) = G(k)$ and $H(k + N/2) = H(k)$. We also have the twiddle factor property:

$$W_N^{N/2} = (e^{-j2\pi/N})^{N/2} = e^{-j\pi} = -1$$

Then, the DFT merging equations become:

$$X(k) = G(k) + W_N^k H(k)$$

$$X(k + N/2) = G(k) - W_N^k H(k)$$

$$k = 0, 1, \dots, N/2 - 1$$

They are known as the butterfly merging equations. The upper group generates the upper half of the N -dimensional DFT vector X , and the lower group generates the lower half. The $N/2$ multiplications $W_N^k H(k)$ may be used both in the upper and the lower equations, thus reducing the total extra merging cost to $N/2$. Vectorially, we may write them in the form:

$$\begin{bmatrix} X_0 \\ X_1 \\ \vdots \\ X_{N/2-1} \end{bmatrix} = \begin{bmatrix} G_0 \\ G_1 \\ \vdots \\ G_{N/2-1} \end{bmatrix} + \begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_{N/2-1} \end{bmatrix} \times \begin{bmatrix} W_N^0 \\ W_N^1 \\ \vdots \\ W_N^{N/2-1} \end{bmatrix}$$

$$\begin{bmatrix} X_{N/2} \\ X_{N/2+1} \\ \vdots \\ X_{N-1} \end{bmatrix} = \begin{bmatrix} G_0 \\ G_1 \\ \vdots \\ G_{N/2-1} \end{bmatrix} - \begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_{N/2-1} \end{bmatrix} \times \begin{bmatrix} W_N^0 \\ W_N^1 \\ \vdots \\ W_N^{N/2-1} \end{bmatrix}$$

where the indicated multiplication is meant to be component-wise. Together, the two equations generate the full DFT vector X. The operations are shown in Fig.2.

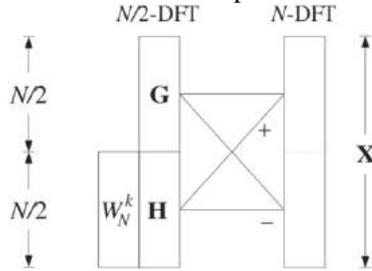


Fig.2. Butterfly merging builds upper and lower halves of length-N DFT.

As an example, consider the case $N = 2$. The twiddle factor is now $W_2 = -1$, but only its zeroth power appears $W_2^0 = 1$. Thus, we get two 1-dimensional vectors, making up the final 2-dimensional DFT:

$$\begin{aligned} [X_0] &= [G_0] + [H_0 W_2^0] \\ [X_1] &= [G_0] - [H_0 W_2^0] \end{aligned}$$

For $N = 4$

$$\begin{bmatrix} X_0 \\ X_1 \end{bmatrix} = \begin{bmatrix} G_0 \\ G_1 \end{bmatrix} + \begin{bmatrix} H_0 W_4^0 \\ H_1 W_4^1 \end{bmatrix}$$

$$\begin{bmatrix} X_2 \\ X_3 \end{bmatrix} = \begin{bmatrix} G_0 \\ G_1 \end{bmatrix} - \begin{bmatrix} H_0 W_4^0 \\ H_1 W_4^1 \end{bmatrix}$$

For $N = 8$

$$\begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{bmatrix} = \begin{bmatrix} G_0 \\ G_1 \\ G_2 \\ G_3 \end{bmatrix} + \begin{bmatrix} H_0 W_8^0 \\ H_1 W_8^1 \\ H_2 W_8^2 \\ H_3 W_8^3 \end{bmatrix}$$

$$\begin{bmatrix} X_4 \\ X_5 \\ X_6 \\ X_7 \end{bmatrix} = \begin{bmatrix} G_0 \\ G_1 \\ G_2 \\ G_3 \end{bmatrix} - \begin{bmatrix} H_0 W_8^0 \\ H_1 W_8^1 \\ H_2 W_8^2 \\ H_3 W_8^3 \end{bmatrix}$$

To begin the merging process shown in Fig.1, we need to know the starting one-dimensional DFTs. Once these are known, they may be merged into DFTs of dimension 2,4,8, and so on. The starting one-point DFTs are obtained by the so-called shuffling or bit reversal of the input time sequence. Thus, the typical FFT algorithm consists of three conceptual parts:

1. Shuffling the N-dimensional input into N one-dimensional signals.
2. Performing N one-point DFTs.
3. Merging the N one-point DFTs into one N-point DFT.

Performing the one-dimensional DFTs is only a conceptual part that lets us pass from the time to the frequency domain. Computationally, it is trivial because the one-point DFT $X =$

$[X_0]$ of a 1-point signal $x = [x_0]$ is itself, that is, $X_0 = x_0$, as follows by setting $N = 1$ in Eq. (4). The shuffling process is shown in Fig.2 for $N = 8$. It has $B = \log_2(N)$ stages. During the first stage, the given length-N signal block x is divided into two length-($N/2$) blocks g and h by putting every other sample into g and the remaining samples into h . During the second stage, the same subdivision is applied to g , resulting into the length-($N/4$) blocks $\{a, b\}$ and to h resulting into the blocks $\{c, d\}$, and so on. Eventually, the signal x is time-decimated down to N length-1 subsequence's. These subsequence's form the starting point of the DFT merging process, which is depicted in Fig. 4 for $N = 8$. The butterfly merging operations are applied to each pair of DFTs to generate the next DFT of doubled dimension.

II. FFT IMPLEMENTATIONS

The Fast Fourier Transform (FFT), as an efficient algorithm to compute the Discrete Fourier Transform (DFT), is one of the most important operations in modern digital signal processing and communication systems. The pipeline FFT is a special class of FFT algorithms which can compute the FFT in a sequential manner; it achieves real-time behavior with nonstop processing when data is continually fed through the processor. Pipeline FFT architectures have been studied since the 1970's when real-time large scale signal processing requirements became prevalent. Several different architectures have been proposed, based on different decomposition methods, such as the Radix-2 Multipath Delay Commutator (R2MDC), Radix-2 Single-Path Delay Feedback (R2SDF), Radix-4 Single-Path Delay Commutator (R4SDC), and Radix-2³Single-Path Delay Feedback (R2³SDF). More recently, Radix-2³ to Radix-2⁴ SDF FFTs were studied and R2³SDF was implemented and shown to be area efficient for 2 or 3 multipath channels. Each of these architectures can be classified as multipath or single-path. Multipath approaches can process data inputs simultaneously, though they have limitations on the number of parallel data-paths, FFT points, and radix. This paper focuses on single-path architectures.

From the hardware perspective, Field Programmable Gate Array (FPGA) devices are increasingly being used for hardware implementations in communications applications. FPGAs at advanced technology nodes can achieve high performance, while having more flexibility, faster design time, and lower cost. As such, FPGAs are becoming more attractive for FFT processing applications and are the target platform of this paper.

The primary goal of this research is to optimize pipeline FFT processors to achieve better performance and lower cost than prior art implementations.

The FFT processor is an inevitable component used for implementing the systems of OFDM. The pipeline architectures in structured form are adopted to satisfy the requirements of energy and signal processing as far as mobile environment is concerned. The architectures of FFT based on decomposition method and radix-2 algorithm were proposed by He et al (1998). The algorithm was exploited for the implementation of dominant elements to decrease the count of manipulations and the 21 storage capacity. The storage capacity had been optimized by adjusting the word length in a

progressive manner. The efficiency of the design with respect to area and power was improved by using a multiplier based on distributed arithmetic. The specifications of the design were obtained by using a 1024 point FFT processor. Song-Nien Tang et al (2012) proposed a FFT processor for various types of wireless networks such as wireless LAN, wireless MAN etc. By adopting the Flexible-Radix Configuration Multiple Delay Feedback (FRCMDF) commutator, a high performance could be obtained by FFTs of variable-length in an efficient manner. In order to improve the efficiency with respect to area and energy, an optimized method of multiplication was also suggested. In addition, the architecture could provide a support for scaling the power across the modes of FFT. The chip had been realized with a size of 3.2 mm², a signal to noise ratio of 40 dB, power consumption of 507 mW at 300 MHz. This FFT processor of length 512-point was able to give higher performance and lower consumption of power when compared to other designs.

Taesang Cho (2013) presented a radix-2 5 fast Fourier transform (FFT) processor of length 512-point for applications of personal area wireless networks. A modified version of radix-2 5 algorithm of FFT was used to decrease the level of hardware required. This technique could decrease the count of manipulations and the capacity of memory required. A complex multiplier was employed in the place of a Booth multiplier. The architecture obtained a SNR value of 35 dB with a word length of '12' bits at 1.2 V. This design had been implemented using 90-nm technology with the specifications - gate count was 2, 90, 000, the rate of throughput was 2.5 Gigabits per second at 310 MHz.

Kyung Heo et al (2003) proposed a FFT processor using mixed radix algorithm and a new in-place technique. This processor employed only two numbers of N-word memories for implementation of FFT when compared to existing FFT processors which employ four numbers of N-word memories. Further this architecture obtained the optimum requirements with respect to area and signal processing. The number of clock cycles and number of gates were 640 and 37, 000 respectively for a FFT processor of length 512-point. Hence this design could reduce size of memory and gate count when compared to other FFT processors.

Shousheng He et al (1998) discussed a FFT processor of length 1024-point using pipeline architecture. This architecture utilized the regularity of radix-2 2 FFT algorithm. The implementation of FFT processor was obtained with only four numbers of complex multipliers and a data memory of 1024 points. The chip had been realized with 0.5 μ m CMOS technology with an area of 40 mm² at a frequency of 30 MHz.

Han Ying et al (2003) introduced a FFT processor based on Xilinx FPGA. To reduce the complexity of logic, the serial mode was adopted to subject the data into three operations such as inclusion of multiplying window, manipulation of FFT and computation of module-square. The frequency of the clock was increased to obtain better performance by employing the serial and parallel architectures thereby avoiding the bottleneck. It was shown that the processor obtained high performance and was suitable for applications of Digital signal processing.

Chang et al (2003) presented an architecture based on algorithm of Radix-4. By integrating the styles of feed forward and feedback commutators, this architecture obtained better usage of hardware and memory when compared to other FFT processors. Moreover various components of ROM were needed for storing the 23 twiddle values. The size of ROM was decremented by an integer of '2' using the concept of redundancy. The single-frequency networks are constructed on a large scale using Coded Orthogonal Frequency Division Multiplexing (COFDM) system, with appropriate guard durations to make the echoes invalid. The fast Fourier transforms of longer length have to be implemented for demodulating every symbol in order to reduce the losses of spectral efficiency to about 20%.

Petrovsky et al (2006) proposed a technique for synthesizing the split radix FFT processors using pipeline architecture. This technique was adopted using hardware design of FPGA by considering the constraints of practical applications such as frequency, length of transform, performance etc into account. The illustrated examples of architecture showed the abilities of the technique to optimize the hardware. The transition from variable arithmetic to fixed arithmetic along with appropriate issues of accuracy was also discussed.

III. EXPECTED RESULTS AND CONCLUSION

By using various optimization techniques such as pipelining, parallel architecture, and split-radix implementation, we propose an FFT architecture that is optimized in terms of speed, power, and area. We will also show the interplay of these parameters and the tradeoffs involved in efficient design

REFERENCES

- [1] Jaishri Katekhaye, Mr.Amit Lamba, Mr. Vipin —REVIEW ON FFT PROCESSOR FOR OFDM SYSTEM IJAICT Vol-1,NOV:2014
- [2] Z.Qian and M.Margala, —ANovel Low-Power and In-Place Split-Radix FFT Processor, | IEEE Trans.in ACM Proc.of the 24th Great Lakes Symp.on VLSI (GVLSI'14),Houston,TX,USA,2014,pp.81-82
- [3] Z.Qian and M.Margala, —FPGA Implementation of Low-Power Split-Radix FFT Processor,| IEEE Trans.24th International Conference Sept.2014,USA
- [4] Anwar Bhasha Pattan, Dr. Madhavi Latha —FastFourier Transform Architectures: A Survey| —IJAECT Weidong Li and Lars Wanhammar —LOW- POWER FFT PROCESSORS| —IJAECT.
- [5] Weidong Li and Lars Wanhammar—VLSI based FFT processor with improvement in computation speed and area reduction| —IJECSE 2013.
- [6] M. Ayinala, M. Brown, and K. K. Parhi, —Pipelined parallel FFT architectures via folding transformation,| IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 20, no. 6, pp. 1068–1081, Jun. 2012.
- [7] S. He and M. Torkelson, —Design and implementation of a 1024-point pipeline FFT processor,| in Proc. IEEE Custom Integr. Circuits Conf.,
- [8] J. Lee, H. Lee, S. I. Cho, and S. S. Choi, —A high-speed two parallel radix-24 FFT/IFFT processor for MBOFDM UWB systems,| in Proc. IEEE Int. Symp. Circuits Syst., May 2006, pp. 4719–4722.
- [9] H. Sorensen, D. Jones, M. Heideman, and C. Burrus, —Real-valued fast Fourier transform algorithms,| IEEE Trans. Acoust., Speech Signal Process., vol. 35, no. 6, pp. 849–863, Jun. 1987.
- [10] R. Radhouane, P. Liu, and C. Modin, —Minimizing the memory requirement for continuous flow FFT implementation: Continuous flow mixed mode FFT (CFMM-FFT),| in Proc. IEEE Int. Symp. Circuits Syst., May 2000, pp. 116–119.



Review on Dual Clock Wormhole NoC Router for FPGA

Abhijit D. Gadge

*Department of Electronics and Comm Engineering,
Tulsiram Gaikwad Patil College of Engg Nagpur
abhijitgadge23@gmail.com*

Prof. Supratim Saha

*Department of Electronics and Comm Engineering,
Tulsiram Gaikwad Patil College of Engg Nagpur*

Abstract—A number of real world applications are implemented as SoC (system on chip). SoC consists of a number of interconnected processing elements. Traditional interconnects are point to point and bus based. These interconnects become inefficient for SoC with a large number of components. NoC is an interconnect scheme that aims to overcome the limitations of bus based and point to point connections. An NoC consists of three components - router, link, and adapter. The router is the most important component of an NoC. We propose a router optimized for speed by using a dual edge clock sensitive scheme. The routing is a five port design based on round robin arbitration and FIFO queues.

Keywords--*Network on Chip, FIFO, router, arbiter.*

I. Introduction

The complexity of a system on silicon is comparable to other macro systems such as space shuttle or skyscrapers, when measured in terms of the number of basic elements intricately connected together, but at a micro level. Moore's law describes an important trend in the history of the integrated circuit (IC): the number of transistors that can be placed on an IC is increasing exponentially, doubling approximately every two years. This trend has continued for more than half a century. Increasing transistor density, higher operating frequencies, shorter time-to-market and reduced product life cycle, characterize today's semiconductor industry. As semiconductor technology evolves, electronic industries continually push the envelope for greater functional and performance capabilities in new electronic systems. This is creating a continuing need for new design methodologies and design space exploration.

An embedded system is a special-purpose computer system designed to perform one or a few dedicated functions, often with real-time computing constraints. Embedded systems range from portable devices such as digital watches, cameras and MP3 players, to large stationary units like traffic lights and factory controllers. Complexity varies from low, with a single micro-controller chip, to very high with multiple intellectual property (IP) cores and peripherals. The exponential growth in chip density is opening the door for the

implementation of even larger and more complex systems, where complete embedded systems can be built onto a single chip. This paradigm shift is known as System-on-Chip (SoC) and is becoming increasingly common and complex. SoCs may contain many hardware and/or software blocks, such as processors, DSPs, memories, peripheral controllers, gateways, and other custom logic blocks.

The communication architecture implemented in SoCs is an important contribution to the overall performance. Since the introduction of SoC concept, designers relied on a custom-designed ad-hoc mixture of buses and dedicated wires as communication mechanisms. Dedicated wires are effective for systems with a small number of cores, but available routing resources are quickly used up as system complexity grows. They also provide poor reusability and flexibility. A shared bus is a set of wires common to multiple cores, which increases both reusability and scalability. This scheme works well for Master-Slave communication patterns, where peripherals (slaves) wait for data to be received or requested from a more complex processing IP core (master). However, when there are several masters in the system, contention creates a bottleneck which gets worse as complexity grows. And although using hierarchical bus models separated by bridges may reduce some of these constraints, it also complicates protocols while failing to fully eliminate the scalability problem. Design and verification times also grow with SoC complexity.

With the current trend in integration of more complex SoCs, there is a need for better communication infrastructure on chip that will solve the scalability problem by supporting multiple concurrent connections between IP cores, allow for pre-tested design reuse to minimize design and verification times, all while maintaining a low area-overhead. Many architectural templates have been proposed for hardware platforms for future SoCs to provide standardized communication. NoC has been introduced as a new interconnection paradigm able to integrate IP cores in a structured and scalable way. This idea aims to allow system modules to communicate with each other over an on-chip network and has been gaining support world-wide. NoCs are based on the concepts adopted on the building of

interconnection networks for parallel computers. Each router has a set of ports which are used to connect routers with its neighboring routers and with the IP cores of the system. This solution also promotes independent design of IP cores. NoC is still an active area of research, but many works have provided promising performance results over current communication strategies (dedicated wires, shared and locked buses) for FPGAs. There is a great need for research in hardware implementation of NoC systems to determine the feasibility of implementing various parameters, and also to accurately determine what design tradeoffs are involved in NoC implementation.

ASICs are increasingly being replaced by Field Programmable Gate Arrays (FPGAs) for applications with low to medium volume, due to longer design cycles and high cost. FPGA's have also continued to grow with the increase in chip density. Modern FPGA's have various hardware and/or software blocks embedded within them such as DSP blocks, memory, and even processors. These blocks, along with customizable logic blocks, makes them the perfect candidate for NoC designs. A fundamental difference between ASICs and FPGAs is that wires in ASICs are designed such that they match the requirements of a particular design. Wire parameters such as length, width, layout and the number of wires can be varied to implement a desired circuit. Conversely, in an FPGA, area is fixed and routing resources exist whether or no they are used. The electrical characteristics of the FPGA are solved by the chip vendor not by the user [3]. Exploiting the advantages of NoC in FPGAs for implementing SoC designs is an active area of research where the goal becomes implementing a circuit within the limits of available resources. Hence, the importance of designing a generic light-weight router whose area can be traded-off for performance in many different ways to meet applications requirements.

II. Building Blocks

NoC aims to allow computational components (IP cores) to communicate over an on-chip network. An example of a NoC interconnection network is shown in Figure 2.1, which consists of four basic functional blocks. These blocks include the IP cores, the network adaptor, the routing node, and the links. IP cores are specific to the application and not considered part of the NoC design.

NoC aims to allow computational components (IP cores) to communicate over an on-chip network. An example of a NoC interconnection network is shown in Figure 2.1, which consists of four basic functional blocks. These blocks include the IP cores, the network adaptor, the routing node, and the links. IP cores are specific to the application and not considered part of the NoC design.

A. Links

This component provides connections for a routing node with a network interface or another routing node. It may provide buffer resources and separate control lines for connection establishment and teardown.

B. Network Interface

This component provides the conversion between the high level protocol (HLP) that the IP uses and the packet-based communication protocol of the NoC. This component may be responsible for buffering packets, storing IP core addresses, creating and disassembling messages, implementing end-to-end flow control, crossing clock domains, and other higher level network issues.

C. Routing Node

This component carries out the task of receiving and forwarding messages inside the network based on NoC parameters. The Router is the central component in a NoC interconnection network. Therefore, its area and speed play a big role in the performance of the overall system. NoC interconnection networks have a large range of parameters which are all focused around router design. Research in this area still lacks in useful implementation results.

III. NoC Parameters

A. Channel Width

This parameter describes the size of the data passed between routers. It is important since it directly affects bandwidth but can lead to the side affects of increased area/power. Our library allows for a parameterizable channel width which will also be tested for resulting area and latency tradeoffs.

B. Topology

This parameter refers to the way routers are connected in the network. It should be chosen to minimize area, while maximizing utilization without causing bottlenecks. Saldana et al. evaluate different topologies in terms of area and routing resources [3]. Figure 2.2 shows some popular NoC topologies. Ring and star achieve slightly better results, although both fail to provide solutions to the scalability problem. As the number of nodes increases, ring suffers large end to end delay and star suffers from a central bottleneck. Narasimhan et al. compare the performance of a two dimensional torus to mesh, showing a slight edge for two dimensional torus [4]. They however, do not compare the extra routing resources needed or the increase area of each router due to a more complex routing algorithm. We restrict the topology to mesh, which is most common among FPGA networks, but allow for various implementation sizes up to an 8 x 8 network. We also create multiple local ports (up to four per router), which allows for multiple IP cores connected to each router or multiple router connections for single IP cores. This increases the possible number of IP cores connected in the network from 64 to 256. With available FPGAs, it would be impractical to build anything larger due to area and routing resource constraints.

C. Communication Mechanism

Communication mechanism deals with how data flows through the network and includes flow control, switching mode, switching mechanism, and routing algorithm. These parameters are usually set when designing the NoC platform.

D. Flow Control

This parameter deals with the allocation of channels and buffers to data as it travels from source to destination. The two extremes are packet switching (PS) and circuit switching (CS). In circuit switching, there is a dedicated connection between the two modules in which raw data can be transmitted freely. This technique requires a setup time to build and tear down connections, and its channel reservation nature often leads to idle times and causes unreliable blocking. The only upside to this method is its ability to provide guaranteed bandwidth during connection times. This method does not scale as well and is not a popular choice for NoC systems. In packet switching, data is broken into packets which carry routing information. Packets can further be broken down into flow control units (flits). Modules can send packets at any time and there are often many different packets in flight at a given time. The routers must process and redirect each packet accordingly.

E. Switching Mode

This parameter only exists in PS networks and defines how packets move through the network. The most important schemes are store-and-forward (SAF), virtual cut-through (VCT), and wormhole (WH). In SAF, a router cannot forward a packet until all its flits have been received. Therefore, latency is proportional to packet size and it carries large buffer requirements. In WH, the first flit (header) determines the next hop and all remaining flits follow and can be sent as soon as it's received. Therefore, latency is proportional to flit size. This method combines packet switched flow control with circuit switched ideas but also leads to channel reservation. It also requires a complex routing algorithm. VCT uses a combination of both ideas to provide latency based on flit size without idle times by guaranteeing buffering before setting up the connection. However, this method uses large buffer amounts and very complex routing algorithms making it unsuitable for light-weight networks. We have chosen SAF for its light-weight algorithm and to prevent channel reservation. Future testing may extend flexibility to include WH as well.

F. Switching Mechanism

This parameter refers to how connections are made inside a router. Common architectures include fully connected, crossbar matrix, and partial crossbar matrix. We use a partial crossbar scheme to save area as it is the smallest configuration. We have also implemented optimizations based on the chosen routing algorithm which we will discuss later.

G. Routing Algorithm

The routing algorithm determines the path the packet will take. There is not much research guidance available on effectiveness of available routing algorithms for NoC implementations. We use XY routing for its simplicity and low area overhead. This scheme also prevents livelock and assures flits and packets arrive in order. Routing schemes can also require congestion control and recovery mechanisms, which can lead to added area overhead. We allow this to be handled by the application layer.

IV. NoC Evaluation Metrics

NoC architectures are designed to meet certain cost and performance constraints, which include, but are not limited to, speed, area, energy/power consumption, Quality of Service (QoS) and flexibility. Through parameter selection, one or more metrics can often be improved at the cost of other(s). In the following sections we will discuss the evaluation metrics for NoC router architectures and their relevance to this thesis.

A. Latency/Throughput

When using FPGA technologies, evaluating speed can often be as easy as obtaining the synthesized maximum frequency the clock is capable of running at. For NoC routers, this is not the case. Although still important to the overall performance, NoC routers have multiple ports which can send, receive and process simultaneously. Therefore, it is important to observe data transaction times.

Speed can be measured in delay, which is referred to as latency. Latency can be the overall run time, it can be decomposed into several intervals such as packet or flit latency, calculated as an average, along with other creative possibilities. We use the overall application run time measured in cycles, which is converted to time as a function of the maximum clock frequency.

Speed can also be measured in bandwidth, which is referred to as throughput. Throughput is the amount data transferred over a period of time. Throughput can be; the ideal data processing rate (system working under the best possible conditions), it can be decomposed into several intervals such as overall application, packet or flit throughput, measured per system, IP core, router, or port, calculated as an average, along with other creative possibilities. We use the overall application/simulation throughput measured in packet and flits per cycle, which is converted to time as a function of the maximum clock frequency.

Finally, some papers suggest NoC router speed be measured in terms of bottlenecks. Either the number of occurring bottlenecks, or the time in which a router has a bottleneck occurring. This metric was not used in our experiments but is very interesting to note.

It is important to understand that speed characteristics for NoC routers are application specific and do not represent speed characteristics of the router alone. This makes comparing different router performances quite hard.

B. Area

In an FPGA, overall system area is limited and therefore important to keep minimal. Area can be measured as a number or a percent of available resources. Area is a very vague term. In an FPGA, there are many components which occupy area. For our experiments, we use area in terms of logic elements (LE's), memory blocks, and routing resources (direct wires, interconnects, and clocks). This information is obtained from Altera Quartus II CAD tool after compiling and synthesizing the VHDL code. Altera Quartus II CAD tool gives the option to synthesize for the lowest area or highest speed.

C. Energy/Power Consumption

For FPGA technologies, power consumption is a metric not often evaluated. This is due to the fact that power consumption has a direct relation with area. Also, designing low power circuits for FPGA implementation is based on trial and error. Therefore, most research including ours focuses on area and excludes the use of power estimation tools.

D. Quality of Service (QoS)

Quality-of-Service (QoS) is a networking term that refers to guarantees that the system can make about its performance. In computer networks, certain application such as video streaming are required to give a guarantee of high uninterrupted bandwidth because of the uniqueness of the application. It is difficult to actually predict the behavioral nature of the data in the network, thus making it nearly impossible to guarantee the required bandwidth without some margin of error. PS suffers even more in its ability to predict the timing of its services. To help provide QoS, NoCs must provide service free of the following causes of failure.

1. Livelock: data is prevented from reaching its destination because it is in a cyclic path.
2. Starvation: data is prevented from reaching its destination because some resource does not grant access.
3. Deadlock: data is prevented from reaching its destination because it is blocked at some intermediate resource.

Live lock occurs when the packets are being routed around their destination and are placed in a cyclic holding manner. Live lock can be avoided by allowing the packet to travel the shortest route. XY routing avoids this situation. Starvation is a common PS problem. It occurs when the packet is discriminated against as low-priority data, thus never getting service. This can be avoided by allocating resources to process all packets equally, automatically dropping and resending packets in the network for too long, or by use of dynamic arbitration insuring all ports receive service.

Deadlock is cause by packet being continuously blocked and it is the hardest problem to solve because packets that are blocked stay blocked while waiting for an event that cannot happen. This problem is solved by restricting channel reservation.

V. FPGA Technology

A field-programmable gate array (FPGA) is an integrated circuit (IC) which can be reprogrammed many times to implement any desired digital circuit which doesn't exceed the limits of the device. An FPGA contains a two dimensional array of programmable logic components, called logic elements (LEs), a hierarchy of wires and buses with reconfigurable interconnects that allow the LEs to be physically connected and is surrounded by configurable I/O blocks (IOB's). Figure 2.3 shows this two dimensional FPGA architecture. In addition, FPGAs typically include other specialized blocks, such as block random access memories (B BRAMs) and digital signal processors (DSPs) which still provide some degree of configurability. An FPGA is programmed by loading data bits in memory cells which

control transistor switches to establish non-permanent connections. An FPGA can support hundreds of thousands of gates of logic operating at speeds of tens of megahertz. We can use an FPGA to implement any logical function that an application-specific integrated circuit (ASIC) could perform, however FPGAs tend to run slower and consume more area and energy compared to application-specific integrated circuits (ASICs). The use of FPGA to implement digital circuits is on the rise over ASIC designs. FPGA allows for faster prototyping, shorter time to market, and lower NRE costs compared to ASIC. The main advantage comes from the ability to fix bugs in the field through reprogramming.

The first working implementation of FPGAs was presented by Marescaux et al. [6]. It has many faults mainly large size, and a one dimensional architecture which fails to provide a high degree of scalability. They extend their work in [7], allowing a more flexible architecture, but still suffering from large area overhead. They use VCT flow control which is now considered too area-intensive for FPGA platforms because of complex routing logic without eliminating any buffer constraints.

Moraes et al, present Hermes, a router with parameterizable data width and buffer depth. They perform simulations of a 5 x 5 mesh while varying buffer depth. They conclude with the notion that increased buffer size reduced latency, but only to a saturation point. Their design uses centralized arbitration and routing units, which decreases area but stalls performance as routing requests are queued to be handled one at a time. Their design also suffers from a very low clock speed. They later extend their work to provide an automatic router generation and traffic analyzer [9].

A comparable router, RASoC [10], was presented by Zeferino et al. The main difference being they use a WH flow control. Performance differences are yet to be compared and may be considered for future work as a WH downfall is that it reserves channels which can cause blocking. However, WH also requires complex routing logic as well as extra bits in the datapath for framing. They also used Altera to synthesis their 5-port, 8-bit router which occupies 486 LE's and has a clock frequency of approximately 57MHz. This area is quite large for a router whose buffers are limited to 4 per port. PNoc, proposed by Hilton et al, gives us a router with circuit switched flow control. They test their router against bus based approaches to show improvements. However, routing complexity grows as the number of ports, or number of routers increase and therefore reduces scalability. It also suffers typical CS setup and teardown latencies and possible blocked idle time.

Sethuraman et al. propose LiPaR, which was a starting point of our design, but significant improvements were added by us. They use SAF, input and output buffering, and decentralized components. Optimizations are made in the crossbar matrix to reduce area through careful analysis of the XY routing algorithm. However, we extend these optimizations to the arbitration unit. They use a single 5x5 crossbar matrix for switching rather than 5 5x1 partial crossbars leading to a larger area. Their complex crossbar design results in a slower clock speed and increased area.

They later propose multi-local port routers (MLPR), which have the potential of improving area and performance metrics. However, the authors fail to provide any synthesis results to support their proposal. Another extension the authors propose is Optimap, an exhaustive CAD tool for mapping IP's and choosing network size.

Vestias et al. propose GNoC, a generic router which supports a range of routing, switching and arbitration protocols. They create a tool for exploring the sharing of some decentralized components to reduce area that is based on the injection rate of ports. Unfortunately, they lock all protocols to certain values and do not explore them further. Their tool shows how they can save area when injection rates are low but does not test to see if performance is degraded. MoCres, designed by Janarthanan et al., uses complex VCT flow control and attempts to reduce area by sacrificing area through centralizing components. They create multi-clock domain to enable high clock frequencies during transfers. Optimizations from XY routing in the crossbar matrix have been extended to the routing algorithm, and gave us the idea for a further arbitration unit extension. We have also used their idea of creating VHDL wrappers to simulate the stand-alone router or routing configurations to compare parameters.

VI. Router Architecture

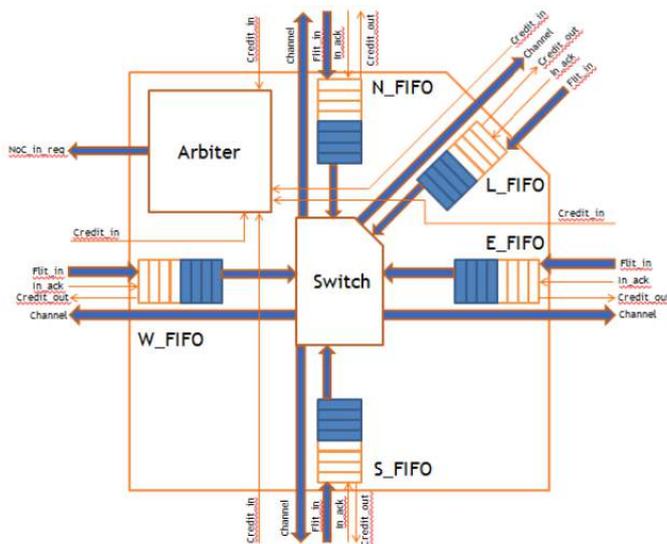


Fig 2 shows the block diagram of FLNR and that connect it to the adjacent (North, East, S IPs/routers, as well as the local IP core. d its external links South, and West)

Associated with each input port, we temporarily storing the coming flits the final destination. The FIFO de equal to the number of possible flits routing decision time, in order to get design the routing decision time is time needed to write each body because we use credit-based protocol (one for head flit, one for body minimum latency in the absence buffer size is parameterizable and w make fair comparison with other router locations will be useful in handling t Upon the arrival of the packet at the FIFO buffer flit by flit every available. At the same time and w buffer will be evacuated as long as finding a free space at the adjacent evacuation stops when the control s that adjacent node is not valid; indicating that no more space is available. However, the storing in the current FIFO will

continue. The control signal “credit” representing this port is sent as back pressure to the adjacent source nearly full. As soon as the first flit location of the FIFO, which is conn stage as well as the switch, the packet information included in this header flit will notify the Arbiter about the arrival of packet in this port, and provide Direction Decoder to calculate the d XY routing scheme is used in some drawbacks, it is one of the cheapest approaches to obtain a deadlock free network [8]. The a using the round-robin method. The n use an input FIFO buffer for s until they find their way to depth must be greater than or that can be stored during the t the best case latency. In our s only one clock cycle. The flit is also one clock cycle ol. Note that only two buffers flit) are enough to get the of blocking. However, the buffer size is parameterizable and was chosen to be 8 in order to make fair comparison with other routers. Also, these extra buffer the contention if needed. the input port, it is stored in clock cycle if free space is with the same speed, FIFO s the assigned output port is destination’s input port. The signal “credit” coming from indicating that no more space is he current FIFO will continue entering this port is sent as a e node, when FIFO becomes t (head_flit) reaches the first connected directly to the routing ckt information included in biter about the arrival of the destination address to direction decoder to calculate the direction .XY routing scheme is used in our design because, despite cheapest approaches to obtain a arbitration in FLNR is done notifications arriving from the input ports are served in the following order: North, East, South, West, and Local. Last port served is given the least priority in the following transmission. Upon granting an input port, the Arbiter configures the Direction Decoder unit asking it to provide the direction based on the information provided by the current processed packet from the current corresponding port. Then, the availability of free buffer locations in the neighboring destination hop is checked through examining the validity of the signal Credit before opening the channel. As well, the Arbiter will acknowledge the FIFO Buffer unit and enable the multiplexers in the cross point matrix to establish a connection. The Switch is the final stage of the router that maps the packets coming from input ports to assigned channels. It was implemented using five 5-to-1 multiplexers supporting all possible connections between input and output buffers. Enabling the multiplexers and selecting the appropriate inputs is accomplished via control signals provided by the Arbiter.

VII. Expected Results and Conclusions

We have proposed a router for network on chip paradigm. The router is consists of a FIFO queues, arbiter, and crossbar switch. The design is proposed to operate on dual clock principle to improve throughput. Also, due to the use of smaller flit sizes, we will see a reduction in the area requirement of the router, and as a result, the total area requirement of the NoC implementation, as the router is the most area intensive component of the network on chip.

References

[1] William J. Dally and Brian Towles, Route Packets, Not Wires: On-Chip Interconnection Networks, DAC 2001, June 18-22, 2001, ACM 1-58113-297-2/01/0006, ACM 2001.

- [2] Luca Benini Giovanni De Micheli, Networks on Chip: A New Paradigm for Systems on Chip Design, IEEE Proceedings of the 2002 Design, Automation and Test in Europe Conference and Exhibition (DATE 02) IEEE 2002.
- [3] Davide Bertozzi, Shashi Kumar, and Maurizio Palesi, Networks-on-Chip: Emerging Research Topics and Novel Ideas, Hindawi Publishing Corporation, VLSI Design, Volume 2007, Article ID 26454, 3 pages, Hindawi 2007.
- [4] Giorgos Passas, Manolis Katevenis, and Dionisis Pnevmatikatos, A $128 \times 128 \times 24$ Gb/s Crossbar Interconnecting 128 tiles in a single hop and Occupying 6% of their area, ACM/IEEE Proceedings of the 4th Int. Symposium on Networks on Chip – NOCS 2010, Grenoble, France, May 2010.
- [5] Mohammad Abdullah Al Faruque, Thomas Ebi, and Jörg Henkel, Configurable Links for Runtime Adaptive On-chip Communication, DATE09, 2009 EDAA IEEE.
- [6] Lotfi Mhamdi, A Partially Buffered Crossbar Packet Switch, IEEE Transactions on Computers, Vol. 58, No. 11, November 2009.
- [7] Jonathan Turner, Design and Evaluation of a Practical, High Performance Crossbar Scheduler, Department of Computer Science & Engineering - Washington University in St. Louis, 2009.
- [8] Rwei-Xi Chen, Wei Zhao, Jeffrey Fan and Asad Davari, Vector Bank Based Multimedia Codec System-on-a-Chip (SoC) Design, IEEE 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009.
- [9] Ankur Agarwal, Cyril Iskander, Ravi Shankar, Survey of Network on Chip (NoC) Architectures & Contributions, Journal of Engineering, Computing, and Architecture, ISSN 1934-7197, Volume 3, Issue 1, 2009.
- [10] R.Dafali, J-Ph.Diguët and M.Sevaux, Key Research Issues for Reconfigurable Network-on-Chip, IEEE 2008 International Conference on Reconfigurable Computing and FPGAs, 2008.
- [11] Salminen et al., Survey of Network-on-Chip Proposals, White Paper, OCP-IP, March 2008
- [12] Pascal T. Wolkotte, Exploration within the Network-on-Chip Paradigm, ISSN 1381-3617, CTIT Ph.D.-thesis series No. 09-133, 2008.
- [13] David Atienza, Federico Angiolini, Srinivasan Murali, Antonio Pullini, Luca Benini, Giovanni De Micheli, Network-on-Chip design and synthesis outlook, Elsevier INTEGRATION, the VLSI journal 41 (2008) 340–359, Elsevier 2008.



Review on Design of Performance Monitoring Unit for Reconfigurable Embedded Processor

Roshan Y Rakhunde

Department of Electronics and Communication Engineering
Tulsiram Gaikwad Patil College of Engg Nagpur
roshanrakhunde@gmail.com

Tushar Uplanchiwar

Department of Electronics and Communication Engineering
Tulsiram Gaikwad Patil College of Engg Nagpur

Abstract— Current embedded systems make use of soft-core processors such as LEON, Nios, Micro-blaze. Because these processors are designed for embedded systems, they lack a number of features that are present in more powerful desktop and server processors such as Xeon, SPARC and Itanium. One of these features is performance monitoring unit. In order to design optimized software, its execution needs to be monitored on the target processor. This is done by the use of multiple counters and control logic. This helps to record a number of events such CPU cycles, number of instructions, and data and instruction cache hit or miss, this paper proposed the RTL design and simulation of a performance monitoring unit for the Altera Nios II processor and quantifies the overhead incurred on hardware resources of the underlying programmable hardware.

Keywords— Performance monitoring unit, embedded processor, soft-core processor.

I. Introduction

Performance Monitoring counters is a valuable tool for measuring performance of a program which can be analysed to identify the bottlenecks in the program. These counters are present in the most modern processors including Intel Pentium, Pentium Pro, P6, Pentium 4, AMD, Cyrix etc. These counters are hardware registers attached with the processor which measures various programmable events occurring in the processor. They do not require any additional overhead and supports a wide range of events.

This section introduces the relevant background on hardware performance counters and the software used to configure and use them.

Hardware Performance Counters. Most modern processors contain hardware performance counters [2], special-purpose registers that can count the occurrence of micro-architectural events. Often these counters are programmable: They can be enabled or disabled, they can be configured to cause an interrupt at overflow, and they can be configured to count different types of events. Commonly supported events include the number of committed instructions, clock cycles, cache misses, or branch mispredictions. As processors differ

in their micro-architectures, they necessarily differ in the type of countable events. The number of counter registers also differs greatly between different micro-architectures. In addition to programmable counters, some processors also support fixed-function counters which provide limited programmability (i.e. they always count the same event, or they cannot be disabled).

Configuring & Accessing Counters. Processors provide special registers to configure the hardware performance counters (e.g. to enable or disable a counter, or to determine which event to count). They also provide special instructions to access the counter and the counter configuration registers. For example, on processors supporting the IA32 instruction set architecture, the RDPMC instruction reads the value of a performance counter into general purpose registers, RDTSC reads the value of the time stamp counter (a special kind of fixed-function performance counter), and RDMSR/WRMSR read/write the value of any model-specific register (such the time stamp counter, a performance counter, or the registers used to configure the counters).

All the above mentioned IA32 instructions can be executed when in kernel mode. RDMSR and WRMSR are unavailable in user mode. Whether RDPMC and RDTSC work in user mode is configurable by software and depends on the operating system.

Per-Thread Counters. Hardware performance counters count events happening on a given processor. The counter register does not distinguish between different software threads that run on its processor. Performance analysts often need to know the number of events incurred by specific threads. To support this per-thread counting, the operating system's context switch code has to be extended to save and restore the counter registers in addition to the general purpose registers.

Software Support for Hardware Counters. The fact that some of the counter configuration or access instructions require kernel mode privileges, and the need to provide per-thread counts, have lead to the development of kernel extensions that provide user mode applications access to the

counters. For Linux, the two frequently used kernel extensions are perfctr [3] and perfmon2 [4].

These kernel extensions are specific to an operating system. Thus, measurement code using these extensions becomes platform dependent. Moreover, even when using the same kernel extension, configuring counters for different processors requires processor-specific code. For this reason, many performance analysts use PAPI [5], a higher level API to access performance counters. PAPI provides a platform (OS and processor) independent programming interface. It achieves OS-independence by providing a layer of abstraction over the interface provided by kernel extensions that provide access to counters. It achieves processor-independence by providing a set of high level events that are mapped to the corresponding low-level events available on specific processors. PAPI also provides access to the machine-specific low-level events. To allow an even simpler programming model, PAPI provides a high level API that requires almost no configuration.

Performance analysis based on performance monitoring units (PMUs) requires both, hardware and software infrastructure. The hardware infrastructure for recording statistical data at the micro-architectural level during program execution basically includes sets of control registers and counters. The control registers can be programmed to specific events that should be captured which are then counted. The configuration written to control registers also determines whether and which interrupts are generated on a counter overflow, whether data is collected only for user mode or also for kernel mode execution, and generally to enable or disable data collection. While most modern processors include some form of PMU [11], the number of measurable events and hardware counters varies [4], [12]. Events commonly available for monitoring include the number of CPU cycles, access and miss rates for caches and TLBs, and IPC values.

The software infrastructure for a PMU needs to configure the measurement infrastructure, start and stop data collection, and finally read out and aggregate counter values. There exist several tools and system interfaces supporting the collection of statistical data from PMUs. Among them, PAPI and the perf tool are commonly used in high-performance computing. These tools rely on a system interface running in kernel mode to access the PMU hardware counters. Running the system interface in kernel mode is advantageous since the hardware counters can easily be saved and restored during a context switch, allowing for per-thread performance monitoring. In the Linux operating system, two patches for performance monitoring are widely used: perfctr and perfmon2. More recently, the perf_event interface and the perf tool have been included into the main Linux kernel source code. The perf tool works tightly with the perf_event interface and makes performance monitoring straight-forward for users.

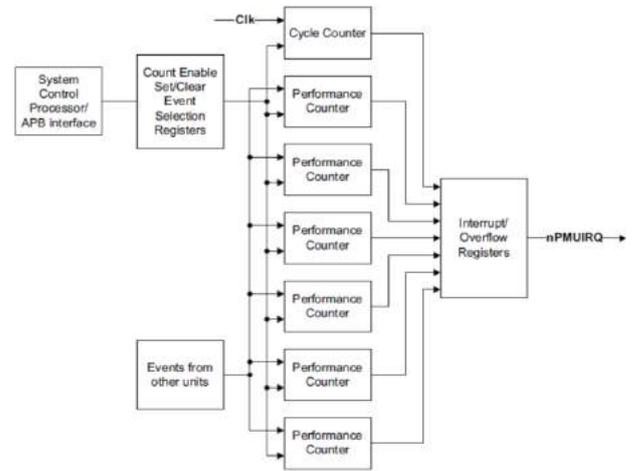


Figure 1: Performance Monitoring Unit

Performance events can be grouped into five categories: program characterization, memory accesses, pipeline stalls, branch prediction, and resource utilization. Program characterization events help define the attributes of a program (and/or the operating system) that are largely independent of the processor’s implementation. The most common examples of these events are the number and type of instructions (for example, loads, stores, floating point, branches, and so on) completed by the program. Memory access events often comprise the largest event category and aid performance analysis of the processor’s memory hierarchy. For example, memory events can count references and misses to various caches and transactions on the processor memory bus. Pipeline stall event information helps users analyse how well the program’s instructions flow through the pipeline. Processors with deep pipelines rely heavily on branch prediction hardware to keep the pipeline filled with useful instructions. Branch prediction events let users analyse the performance of branch prediction hardware (for example, by providing counts of mispredicted branches). Resource utilization events let users monitor how often a processor uses certain resources (for example, the number of cycles spent using a floating-point divider).

II. Performance-monitoring hardware

Performance-monitoring hardware typically has two components: performance event detectors and event counters. By properly configuring the event detectors and counters, users can obtain counts of a variety of performance events under various conditions. Users can configure performance event detectors to detect any one of several performance events (for example, cache misses or branch mispredictions). Often, event detectors have an event mask field that allows further qualification of the event. For example, the Intel Pentium III’s event to count load accesses to the level 2 cache (L2_LD) has an event mask that lets event detectors monitor only accesses to cache lines in a specific state— modified, shared, exclusive, or invalid.

The event detector configuration also allows qualification by the processor’s current privilege mode. Operating systems

use supervisor and user privilege modes to prevent applications from accessing and manipulating critical data structures and hardware that only the operating system should use directly. When the operating system is executing on the processor, the privilege mode is supervisor; when an application is executing on the processor, the privilege mode is user. As such, the ability to qualify event detection by the processor's privilege mode allows counting of events caused only by the operating system or only by an application. Configuring the event detector to detect events for both privilege modes counts all events.

In addition to counting events detected by the performance event detectors, users can configure performance event counters to count only under certain edge and threshold conditions. The edge detection feature is most often used for performance events that detect the presence or absence of certain conditions every cycle. For these events, an event count of one represents a condition's presence and zero indicates its absence. For example, a pipeline stall event indicates the presence or absence of a pipeline stall on each cycle. Counting the number of these events gives the number of cycles that the pipeline stalled. However, the edge detection feature can also count the number of stalls (more specifically, the number of times a stall began) rather than just the total number of cycles stalled. With edge detect enabled, the performance counter will increment by one only when the previous number of performance events reported by the event detector is less than the current number being reported. So when the event detector reports zero events on a cycle followed by one event on the next cycle, the event counter has detected a rising edge and will increment by one. It's usually possible to invert the sense of the edge detection to count falling edges..

The event counter's second major feature is threshold support. This capability lets the event counter compare the value it reports each cycle to a threshold value. If the reported value exceeds the threshold, the counter increments by one. The threshold feature is only useful for performance events that report values greater than one each cycle. For example, superscalar processors can complete more than one instruction per cycle. Selecting instructions completed as the performance event and setting the counter threshold to two would increment the counter by one whenever three or more instructions complete in one cycle. This provides a count of how many times three or more instructions completed per cycle.

III. Performance profiles

Although performance event detectors and counters can easily detect the presence of a performance problem and let the user estimate the severity of the problem, it's often necessary to find the locations of the code (whether in the application or the operating system) that are causing the performance problem. Knowing the source of the performance problem lets programmers alter the high-level algorithms used by the application and/or the low-level code to avoid or reduce the problem's impact. To illustrate how performance counters can help create a profile that identifies the major sources of performance problems, let's first review the goals and techniques used to create time-based profiles.

A. Time-based profiles

A common technique to identify areas upon which to focus tuning efforts is to obtain a time-based profile of the application. A time-based profile estimates the percentage of time an application spends in its major sections.

Focusing tuning efforts on the application's most frequently executed sections maximizes the benefits of any performance-tuning changes made to the code. A time-based profile relies upon interrupting an application's execution at regular time intervals. During each interrupt, the interrupt service routine saves the value of the program counter. Once the application completes, the user can create a histogram that shows the number of samples collected for each program counter value. Assuming that the histogram draws from many program counter samples, it will show the applications most frequently executed sections.

B. Event-based profiles

A technique similar to that for creating a time-based profile can help collect an event-based profile. An event-based profile is a histogram that plots performance event counts as a function of code location. Instead of interrupting the application at regular time intervals (as is done to create a time-based profile), the performance-monitoring hardware interrupts the application after a specific number of performance events has occurred. So just as a time-based profile indicates the most frequently executed instructions, an event-based profile indicates the most frequently executed instructions that cause a given performance event.

To support event-based sampling (EBS), performance-monitoring hardware typically generates a performance monitor interrupt when a performance event counter overflows. To generate an interrupt after N performance events, the performance counter is initialized to a value of overflow minus N before being enabled. A performance monitor interrupt service routine (ISR) handles these interrupts. The ISR saves sample data from the program (for example, the program counter) and re-enables the performance event counter to cause another interrupt after N occurrences of a certain performance event. After the application finishes executing, the user can plot the data samples saved by the ISR to create an event-based profile.

IV. Performance-monitoring capabilities

Intel's P5-based processors (these include the original Pentium and Pentium MMX) and P6-based processors provide two performance counters that support privilege mode qualification, threshold comparisons, and interrupt generation on counter overflow. 1

These processors also provide a large set of performance events (more than 80 on the Pentium III). AMD's Athlon processor⁸ provides four performance counters with capabilities similar to the Pentium III, but with a smaller set of performance events (about 25). IBM's PowerPC 750 processor⁹ provides four counters with capabilities similar to the Pentium III and supports more than 40 events. Motorola's PowerPC 7450 provides six counters and over 200 events. 10

An additional feature of the PowerPC performance-monitoring hardware is the ability to count performance events only for marked processes on a system running multiple processes. This feature lets a process indicate that its events should be counted, excluding those events generated by any unmarked process.

Intel's Itanium processor provides four performance counters and over 90 performance events. In addition to supporting privilege-mode qualification, threshold comparisons, and interrupt generation on counter overflow, Itanium allows event qualification by opcode as well as instruction and/or data address range. Itanium events also account for all major single- and multicycle stall and flush conditions. These events let the user determine the percentage of all cycles spent on various activities, such as execution, data and instruction accesses, and branch mispredictions. Unlike most other processors, Itanium contains a set of event address registers that records the instruction and data addresses for cache and transition look-aside buffer (TLB) misses. These event address registers identify data addresses and structures that cause frequent cache and TLB misses.

Sun's UltraSparc I and II provide two performance counters and qualification by privilege mode for over 20 events, but they have no threshold support and cannot generate interrupts on counter overflow. Compaq's Alpha 21264 provides two performance counters that support privilege-mode qualification and interrupt generation on counter overflow. The Alpha 21264 was also the first processor to support Pro-fileMe, a novel pro- filing technique, discussed in the "Alpha's Pro- fileMe approach" sidebar.

v. Nios II System

The Nios II processor can be used with a variety of other components to form a complete system. These components include a number of standard peripherals, but it is also possible to define custom peripherals. Altera's DE2 Development and Education board contains several components that can be integrated into a Nios II system. An example of such a system is shown in Figure 2.

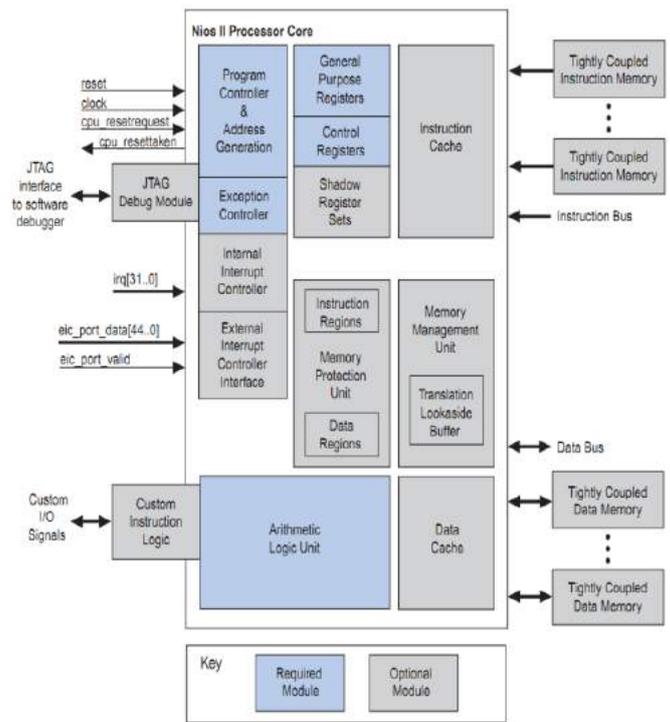


Figure 2: Nios II Microprocessor

The Nios II processor and the interfaces needed to connect to other chips on the DE2 board are implemented in the Cyclone II FPGA chip. These components are interconnected by means of the interconnection network called the Avalon Switch Fabric. Memory blocks in the Cyclone II device can be used to provide an on-chip memory for the Nios II processor. They can be connected to the processor either directly or through the Avalon network. The SRAM and SDRAM memory chips on the DE2 board are accessed through the appropriate interfaces. Input/output interfaces are instantiated to provide connection to the I/O devices used in the system. A special JTAG UART interface is used to connect to the circuitry that provides a Universal Serial Bus (USB) link to the host computer to which the DE2 board is connected. This circuitry and the associated software is called the USB-Blaster. Another module, called the JTAG Debug module, is provided to allow the host computer to control the Nios II processor. It makes it possible to perform operations such as downloading programs into memory, starting and stopping execution, setting program breakpoints, and collecting real-time execution trace data. Since all parts of the Nios II system implemented on the FPGA chip are defined by using a hardware description language, a knowledgeable user could write such code to implement any part of the system. This would be an onerous and time consuming task. Instead, one can use the SOPC Builder tool in the Quartus II software to implement a desired system simply by choosing the required components and specifying the parameters needed to make each component fit the overall requirements of the system.

vi. Conclusions

We propose a performance monitoring unit to be implemented for a Nios II soft-core processor that is used as a configurable processor in embedded systems. Traditionally,

soft-core processors intended for embedded systems lack a performance monitoring unit so that area and power footprints are minimized. However, as the complexity of embedded system software increases, there is a need for hardware support to monitor performance so as to optimize embedded system applications. Performance monitoring units are an integral part of advanced workstation and server processors. We will show the impact on silicon area as a result of implementation of the performance monitoring unit.

References

- [1] N. L. Binkert, B. M. Beckmann, G. Black, S. K. Reinhardt, A. G. Sadi, A. Basu, J. Hestness, D. Hower, T. Krishna, S. Sardashti, R. Sen, K. Sewell, M. Shoaib, N. Vaish, M. D. Hill, and D. A. Wood, "The Gem5 Simulator," SIGARCH Computer Architecture News. ACM, vol. 39, no. 2, pp. 1–7, 2011.
- [2] D. Zapanuks, M. Jovic, and M. Hauswirth, "Accuracy of Performance Counter Measurements," in Intl. Symposium on Performance Analysis of Systems and Software (ISPASS). IEEE, pp. 23–32, 2009.
- [3] A. Gordon-Ross and F. Vahid, "A Self-Tuning Configurable Cache," in Design Automation Conference (DAC). ACM, pp. 234–237, 2007.
- [4] ARM, ARM Cortex-A9, Technical Reference Manual, ARM Inc., 2009.
- [5] Analog Devices, ADSP-BF535 Blackfin Processor Hardware Reference, Analog Devices, Inc., 2004.
- [6] Renesas, SuperHTM Family, User Manual, Renesas Inc., 2004.
- [7] Xilinx, Zynq-7000 All Programmable SoC Technical Reference Manual, UG585 (v1.7) ed., Xilinx Inc., 2014.
- [8] S. Koehler, J. Curreri, and A. D. George, "Performance Analysis Challenges and Framework for High-Performance Reconfigurable Computing," Parallel Computing. Elsevier Science Publishers B. V., vol. 34, no. 4–5, pp. 217–230, 2008.
- [9] A. G. Schmidt, N. Steiner, M. French, and R. Sass, "HwPMI: An Extensible Performance Monitoring Infrastructure for Improving Hardware Design and Productivity on FPGAs," Intl. J. of Reconfigurable Computing. Hindawi Publishing Corp., vol. 2012, pp. 2:2–2:2, 2012.
- [10] Aeroflex Gaisler, GRLIB IP Library User's Manual, 2014.
- [11] B. Sprunt, "The Basics of Performance Monitoring Hardware," IEEE Micro, vol. 22, no. 4, pp. 64–71, 2002.
- [12] SUN Microsystems, OpenSPARC T2 Core Microarchitecture Specification, Sun Microsystems, Inc., 2007.

Review on efficient fixed point LMS Adaptive Filter for Noise Cancellation

Shrutika Vijay Khodankar

*Department of Electronics and Communication Engineering
Tulsiramji Gaikwad Patil College of Engineering
Nagpur
shruti.kh0110@gmail.com*

Prof. Supratim Saha

*Department of Electronics and Communication Engineering
Tulsiramji Gaikwad Patil College of Engineering
Nagpur
v.principal@tgpct.com*

Abstract— An important step in digital signal processing (DSP) is the filtering operation. Digital filters are commonly implemented as finite impulse response (FIR) filters. In applications such as mobile communication, the filtering process needs to be adaptive as the DSP operations are performed in varying environments, and each environment presents a different noise profile. There are a number of adaptation schemes for FIR filters, and one of the most common adaptation schemes is the least mean square (LMS) algorithm. The important components of a digital filter are delay elements, multipliers, and adders. The multipliers are the most demanding components in terms of both area and critical path length. In this paper we present an adaptive FIR filter based on the LMS algorithm. We present simulation and synthesis results for implementation on Xilinx Spartan programmable gate arrays (FPGA). We propose a design optimized for area and power by replacing multipliers with a distributed arithmetic scheme that is well suited for FPGA implementation due to the use of look up tables (LUT).

Keywords— LMS, FPGA, adaptive filtering, noise cancellation.

I. Introduction

An adaptive filter is a computational device that attempts to model the relationship between two signals in real time in an iterative manner. Adaptive filters are often realized either as a set of program instructions running on an arithmetical processing device such as a microprocessor or DSP chip, or as a set of logic operations implemented in a field-programmable gate array (FPGA) or in a semi- custom or custom VLSI integrated circuit. However, ignoring any errors introduced by numerical precision effects in these implementations, the fundamental operation of an adaptive filter can be characterized independently of the specific physical realization that it takes. For this reason, we shall focus on the mathematical forms of adaptive filters as opposed to their specific realizations in software or hardware. Descriptions of adaptive filters as implemented on DSP chips and on a dedicated integrated circuit can be found in [1, 2, 3], and [4], respectively.

An adaptive filter is defined by four aspects:

1. The signals being processed by the filter.
2. The structure that defines how the output signal of the filter is computed from its input signal.
3. The parameters within this structure that can be iteratively changed to alter the filters input-output relationship.
4. The adaptive algorithm that describes how the parameters are adjusted from one time instant to the next.

By choosing a particular adaptive filter structure, one specifies the number and type of parameters that can be adjusted. The adaptive algorithm used to update the parameter values of the system can take on a myriad of forms and is often derived as a form of optimization procedure that minimizes an error criterion that is useful for the task at hand.

In this section, we present the general adaptive filtering problem and introduce the mathematical notation for representing the form and operation of the adaptive filter. We then discuss several different structures that have been proven to be useful in practical applications. We provide an overview of the many and varied applications in which adaptive filters have been successfully used. Finally, we give a simple derivation of the least-mean-square (LMS) algorithm, which is perhaps the most popular method for adjusting the coefficient of an adaptive filter, and we discuss some of this algorithm's properties. As for the mathematical notation used throughout this section, all quantities are assumed to be real-valued. Scalar and vector quantities shall be indicated by lowercase (e.g., x) and uppercase-bold (e.g., \mathbf{X}) letters, respectively. We represent scalar and vector sequences or signals as $x(n)$ and $\mathbf{X}(n)$, respectively, where n denotes the discrete time or discrete spatial index, depending on the application. Matrices and indices of vector and matrix elements shall be understood through the context of the discussion.

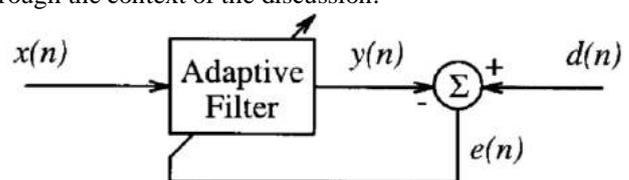


Figure 1 shows a block diagram in which a sample from a

digital input signal $x(n)$ is fed into a device, called an adaptive filter that computes a corresponding output signal sample $y(n)$ at time n . For the moment, the structure of the adaptive filter is not important, except for the fact that it contains adjustable parameters whose values affect how $y(n)$ is computed. The output signal is compared to a second signal $d(n)$, called the desired response signal, by subtracting the two samples at time n . This difference signal, given by $e(n) = d(n) - y(n)$

This $e(n)$ is known as the error signal. The error signal is fed into a procedure which alters or adapts the parameters of the filter from time n to time $n + 1$ in a well-defined manner. This process of adaptation is represented by the oblique arrow that pierces the adaptive filter block in the figure. As the time index n is incremented, it is hoped that the output of the adaptive filter becomes a better and better match to the desired response signal through this adaptation process, such that the magnitude of $e(n)$ decreases over time. In this context, what is meant by “better” is specified by the form of the adaptive algorithm used to adjust the parameters of the adaptive filter. In the adaptive filtering task, adaptation refers to the method by which the parameters of the system are changed from time index n to time index $n + 1$. The number and types of parameters within this system depend on the computational structure chosen for the system. We now discuss different filter structures that have been proven useful for adaptive filtering tasks.

II. FILTER STRUCTURE

In general, any system with a finite number of parameters that affect how $y(n)$ is computed from $x(n)$ could be used for the adaptive filter in Fig. 1. Define the parameter or coefficient vector $W(n)$ as

$$W(n) = [w_0(n) \ w_1(n) \ \dots \ w_{L-1}(n)]^T$$

Where $\{w_i(n)\}$, $0 \leq i \leq L-1$ are the L parameters of the system at time n : With this definition, we could define a general input-output relationship for the adaptive filter as

$$y(n) = f(W(n), y(n-1), y(n-2), \dots, y(n-N), x(n), x(n-1), \dots, x(n-M+1)).$$

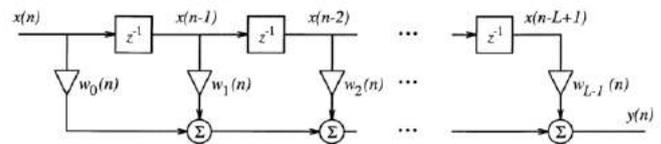
Where f represents any well-defined linear or nonlinear function and M and N are positive integers. Implicit in this definition is the fact that the filter is causal, such that future values of $x(n)$ are not needed to compute $y(n)$. While non causal filters can be handled in practice by suitably buffering or storing the input signal samples, we do not consider this possibility.

Although (3) is the most general description of an adaptive filter structure, we are interested in determining the best linear relationship between the input and desired response signals for many problems. This relationship typically takes the form of a finite-impulse-response (FIR) or infinite-impulse-response (IIR) filter. Figure 2 shows the structure of a direct-form FIR filter, also known as a tapped-delay-line or transversal filter, where z^{-1} denotes the unit delay element and each $w_i(n)$ is a multiplicative gain within the system. In this case, the

parameters in $W(n)$ correspond to the impulse response values of the filter at time n . We can write the output signal $y(n)$ as

$$\begin{aligned} y(n) &= \sum_{i=0}^{L-1} w_i(n)x(n-i) \\ &= \mathbf{W}^T(n)\mathbf{X}(n), \end{aligned}$$

Where $\mathbf{X}(n) = [x(n) \ x(n-1) \ \dots \ x(n-L+1)]^T$ denotes the input signal vector and T denotes vector transpose. Note that this system requires L multiplies and $L - 1$ adds to implement, and these computations are easily performed by a processor or circuit so long as L is not too large and the sampling period for the signals is not too short. It also requires a total of $2L$ memory locations to store the L input signal samples and the L coefficient values, respectively.



Structure of an FIR filter.

I. ADAPTIVE FILTER APPLICATIONS

Perhaps the most important driving forces behind the developments in adaptive filters throughout their history have been the wide range of applications in which such systems can be used. We now discuss the forms of these applications in terms of more-general problem classes that describe the assumed relationship between $d(n)$ and $x(n)$. Our discussion illustrates the key issues in selecting an adaptive filter for a particular task. Extensive details concerning the specific issues and problems associated with each problem genre can be found in the references at the end of this chapter.

A. Channel Identification

In communication systems, useful information is transmitted from one point to another across a medium such as an electrical wire, an optical fiber, or a wireless radio link. Non idealities of the transmission medium or channel distort the fidelity of the transmitted signals, making the deciphering of the received information difficult. In cases where the effects of the distortion can be modeled as a linear filter, the resulting “smearing” of the transmitted symbols is known as inter-symbol interference (ISI). In such cases, an adaptive filter can be used to model the effects of the channel ISI for purposes of deciphering the received information in an optimal manner. In this problems cenario, the transmitter sends to the receiver a sample sequence $x(n)$ that is known to both the transmitter and receiver. The receiver then attempts to model the received signal $d(n)$ using an adaptive filter whose input is the known transmitted sequence $x(n)$. After a suitable period of adaptation, the parameters of the adaptive filter in $W(n)$ are fixed and then used in a procedure to decode future signals transmitted across the channel. Channel identification is typically employed when the fidelity of the transmitted channel is severely compromised or when simpler techniques for sequence detection cannot be used. Techniques for detecting digital signals in communication systems can be found in [9].

B. Plant Identification

In many control tasks, knowledge of the transfer function of a linear plant is required by the physical controller so that a suitable control signal can be calculated and applied. In such cases, we can characterize the transfer function of the plant by exciting it with a known signal $x(n)$ and then attempting to match the output of the plant $d(n)$ with a linear adaptive filter. After a suitable period of adaptation, the system has been adequately modelled, and the resulting adaptive filter coefficients in $W(n)$ can be used in a control scheme to enable the overall closed-loop system to behave in the desired manner. In certain scenarios, continuous updates of the plant transfer function estimate provided by $W(n)$ are needed to allow the controller to function properly. A discussion of these adaptive control schemes and the subtle issues in their use is given in [10, 11].

C. Echo Cancellation for Long-Distance Transmission

In voice communication across telephone networks, the existence of junction boxes called hybrids near either end of the network link hampers the ability of the system to cleanly transmit voice signals. Each hybrid allows voices that are transmitted via separate lines or channels across a long-distance network to be carried locally on a single telephone line, thus lowering the wiring costs of the local network. However, when small impedance mismatches between the long distance lines and the hybrid junctions occur, these hybrids can reflect the transmitted signals back to their sources, and the long transmission times of the long-distance network—about 0.3 s for a trans-oceanic call via a satellite link—turn these reflections into a noticeable echo that makes the understanding of conversation difficult for both callers. The traditional solution to this problem prior to the advent of the adaptive filtering solution was to introduce significant loss into the long-distance network so that echoes would decay to an acceptable level before they became perceptible to the callers. Unfortunately, this solution also reduces the transmission quality of the telephone link and makes the task of connecting long distance calls more difficult. An adaptive filter can be used to cancel the echoes caused by the hybrids in this situation. Adaptive filters are employed at each of the two hybrids within the network. The input $x(n)$ to each adaptive filter is the speech signal being received prior to the hybrid junction, and the desired response signal $d(n)$ is the signal being sent out from the hybrid across the long-distance connection. The adaptive filter attempts to model the transmission characteristics of the hybrid junction as well as any echoes that appear across the long-distance portion of the network. When the system is properly designed, the error signal $e(n)$ consists almost totally of the local talker's speech signal, which is then transmitted over the network. Such systems were first proposed in the mid-1960s [12] and are commonly used today. For more details on this application, see [13, 14].

D. Acoustic Echo Cancellation

A related problem to echo cancellation for telephone transmission systems is that of acoustic echo cancellation for conference-style speakerphones. When using a speakerphone,

a caller would like to turn up the amplifier gains of both the microphone and the audio loudspeaker in order to transmit and hear the voice signals more clearly. However, the feedback path from the device's loudspeaker to its input microphone causes a distinctive howling sound if these gains are too high. In this case, the culprit is the room's response to the voice signal being broadcast by the speaker; in effect, the room acts as an extremely poor hybrid junction, in analogy with the echo cancellation task discussed previously. A simple solution to this problem is to only allow one person to speak at a time, a form of operation called half-duplex transmission. However, studies have indicated that half-duplex transmission causes problems with normal conversations, as people typically overlap their phrases with others when conversing. To maintain full-duplex transmission, an acoustic echo canceller is employed in the speakerphone to model the acoustic transmission path from the speaker to the microphone. The input signal $x(n)$ to the acoustic echo canceller is the signal being sent to the speaker, and the desired response signal $d(n)$ is measured at the microphone on the device. Adaptation of the system occurs continually throughout a telephone call to model any physical changes in the room acoustics. Such devices are readily available in the marketplace today. In addition, similar technology can and is used to remove the echo that occurs through the combined radio/room/telephone transmission path when one places a call to a radio or television talk show. Details of the acoustic echo cancellation problem can be found in [14].

E. Adaptive Noise Cancelling

When collecting measurements of certain signals or processes, physical constraints often limit our ability to cleanly measure the quantities of interest. Typically, a signal of interest is linearly mixed with other extraneous noises in the measurement process, and these extraneous noises introduce unacceptable errors in the measurements. However, if a linearly related reference version of any one of the extraneous noises can be cleanly sensed at some other physical location in the system, an adaptive filter can be used to determine the relationship between the noise reference $x(n)$ and the component of this noise that is contained in the measured signal $d(n)$. After adaptively subtracting out this component, what remains in $e(n)$ is the signal of interest. If several extraneous noises corrupt the measurement of interest, several adaptive filters can be used in parallel as long as suitable noise reference signals are available within the system. Adaptive noise cancelling has been used for several applications. One of the first was a medical application that enabled the electroencephalogram (EEG) of the fetal heartbeat of an unborn child to be cleanly extracted from the much-stronger interfering EEG of the maternal heartbeat signal. Details of this application as well as several others are described in the seminal paper by Widrow and his colleagues [15].

III. LMS ADAPTIVE ALGORITHM

The cost function $J(n)$ chosen for the steepest descent algorithm of (18.25) determine the coefficient solution obtained by the adaptive filter. If the MSE cost function in (18.16) is chosen, the resulting algorithm depends on the

statistics of $x(n)$ and $d(n)$ because of the expectation operation that defines this cost function. Since we typically only have measurements of $d(n)$ and of $x(n)$ available to us, we substitute an alternative cost function that depends only on these measurements. One such cost function is the least-squares cost function given

$$J_{LS}(n) = \sum_{k=0}^n \alpha(k)(d(k) - \mathbf{W}^T(n)\mathbf{X}(k))^2$$

Where $\alpha(n)$ is a suitable weighting sequence for the terms within the summation. This cost function, however, is complicated by the fact that it requires numerous computations to calculate its value as well as its derivatives with respect to each $w_i(n)$, although efficient recursive methods for its minimization can be developed. Alternatively, we can propose the simplified cost function JLMS(n) given by

$$J_{LMS}(n) = \frac{1}{2}e^2(n)$$

This cost function can be thought of as an instantaneous estimate of the MSE cost function. Although it might not appear to be useful, the resulting algorithm obtained when JLMS(n) is used for $J(n)$ in (25) is extremely useful for practical applications. Taking derivatives of JLMS(n) with respect to the elements of $\mathbf{W}(n)$ and substituting the result into (25), we obtain the LMS adaptive algorithm given by

$$\mathbf{W}(n+1) = \mathbf{W}(n) + \mu(n)e(n)\mathbf{X}(n)$$

Note that this algorithm is of the general form in (14). It also requires only multiplications and additions to implement. In fact, the number and type of operations needed for the LMS algorithm is nearly the same as that of the FIR filter structure with fixed coefficient values, which is one of the reasons for the algorithm's popularity. The behaviour of the LMS algorithm has been widely studied, and numerous results concerning its adaptation characteristics under different situations have been developed. For now, we indicate its useful behaviour by noting that the solution obtained by the LMS algorithm near its convergent point is related to the Wiener solution. In fact, analyses of the LMS algorithm under certain statistical assumptions about the input and desired response signals show that

$$\lim_{n \rightarrow \infty} E\{\mathbf{W}(n)\} = \mathbf{W}_{MSE}$$

when the Wiener solution \mathbf{W}_{MSE}/n is a fixed vector. Moreover, the average behaviour of the LMS algorithm is quite similar to that of the steepest descent algorithm in (27) that depends explicitly on the statistics of the input and desired response signals. In effect, the iterative nature of the LMS coefficient updates is a form of time-averaging that smooths the errors in the instantaneous gradient calculations to obtain a more reasonable estimate of the true gradient.

IV. EXPECTED RESULTS AND CONCLUSIONS

We have proposed an HDL design and simulation of an adaptive filter using the LMS algorithm. The intended application for the LMS filter is adaptive noise cancellation. We propose a pipelined design of the LMS filter that results in higher throughput at the cost of a slight increase in area.

References

- [1] Pramod Kumar Meher, Sang Yoon Park -Adaptive-Delay-power Efficient fFixed-point LMS Adaptive Filter With Low Adaptation Delay, IEEE transaction on very large scale integration system vol.22 no 2. feb 2014.
- [2] Mrs. S. Savitha, Ms. S. lakshmi on Implimentation of Efficient LMS Adaptive Filter With Low Adaptation Delay in IEEE sponsored 2nd International Conference on Electronics and Communication(ICECS 2015)
- [3] Bhumika Chandrakar A SURVEY OF NOISE REMOVAL TECHNIQUES FOR ECG SIGNALS International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2013
- [4] Sachin singh Performance Evaluation Of Different Adaptive Filters For ECG Signal Processing International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1880-1883.
- [5] Vinay Dawar, Mohit Bansal Denoising of Image Using Least Minimum Mean Square Error International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-1, October 2012
- [6] J.Nandini Meeraa Survey on Adaptive LMS Algorithm to Cancel Noise and Improve Audio Quality in VOIP International Journal of Computer Science and Management Research Vol 2 Issue 1 January 2013 ISSN 2278-733X
- [7] Suman Swapna Devi Malay Dutta Optimized Noise Canceller for ECG Signals International Conference on Intelligent Systems and Data Processing (ICISD) 2011 Special Issue published by International Journal of Computer Applications® (IJCA)
- [8] Daniel Olgun Adaptive Notch Filter for EEG Signals Based on the LMS Algorithm with Variable Step-Size Parameter Conference on Information Sciences and Systems, The Johns Hopkins University, March 16–18, 2005
- [9] Keigo Hirakawa Image Denoising Using Total Least Squares IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 9, SEPTEMBER 2006.
- [10] SHAUL FLORIAN Performance Analysis of the LMS Algorithm with a Tapped Delay Line (Two-Dimensional Case) IEEE TRANSACTIONS ON ACOUSTICS, SPEECH, AND SIGNAL PROCESSING, VOL. ASSP-34, NO. 6, DECEMBER 1986
- [11] M. Shams Esfand Abadi Image Denoising with Two-Dimensional Adaptive Filter Algorithms Iranian Journal of Electrical & Electronic Engineering, Vol. 7, No. 2, June 2011
- [12] Lilatul Ferdouse Simulation and Performance Analysis of Adaptive Filtering Algorithms in Noise Cancellation IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011 ISSN (Online): 1694-0814
- [13] Pranjali M. Awachat A Design Approach For Noise Cancellation In Adaptive LMS Predictor Using MATLAB. International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue4, July-august 2012, pp.2388-2391

“Power Optimization in Wireless Sensor Networks”

Roshan Bhoyar

Department of Electronics and Comm Engineering,
Tulsiram Gaikwad Patil College of Engg Nagpur
bhoyar.roshan@gmail.com

Prof. Kanchan Dhote

Department of Electronics and Comm Engineering,
Tulsiram Gaikwad Patil College of Engg Nagpur
Kanchan.dhote@rediffmail.com

Abstract-- Wireless sensor network is design by wireless sensor nodes and various types of sensors are deployed in various areas such as offices, wild life, college etc. The sensed data is transferred using wireless sensor network through these nodes. These devices are cheap and require low power for operation. The nodes integrate programming, communication and it provides easy user interface for operation and deploying it.

I. Introduction

In recent year the field of wireless sensor network has a various development and it is very useful in domestics, environment sensing , smart building and physiological monitoring , which makes our life easy. It has disadvantages of synchronization and energy consumption, this problem has been tackled by using techniques to secure a perfect synchronization through the network to reduce the loss of data packages or by modifying the medium control and avoiding the collision of data.

The environmental conditions such as temperature, sound, pressure are monitored by using wireless sensor network and corporately transfer these data through the network to the main location. The wireless sensor network was developed for military applications but now days it is used in many industrial and consumer application such as industrial process monitoring and to monitor the machine health and so on.

The wireless sensor network is design by using several nodes it can be from few to several hundred or even thousand and every node consist of antenna for interfacing with the sensors and an energy source. The sensing nodes can be variable size. A “node” in a wireless sensor network gather the formation, process that information and communicate with other connected nodes in the network. The topology of wireless sensor network can vary from simple star network to an advanced multi-hop wireless mesh network. The sensors in the node sense the data and send this data (Analog signal) to analog to digital converter and then send to controller for further processing.

WSN can be considered an innovative paradigm, which permits the emergence of several new monitoring applications, but introduces challenges intrinsic to this technology. Some of these challenges are

1) *Paradigm change:*

WSN are deployed in order to collect scalars from the environment and to support control applications. The WSN application must sense the environment and sometimes it must act in one way or the other on the environment. Thus, it is considered critical to obtain a cooperative behavior of thousands of sensor nodes, where the data from just one node may not be important. The identification address for the sensor nodes does not have permanent, due to the fact that generally messages are not sent to a specific node but to a space or area. Users can be interested in the information about a specific monitoring area, thus the sensed data from a specific node may not be important, representing the data centric approach in Wireless sensor networks.

2) *Resource Constraints:*

WSNs faces severe resource limitations. Some of them are limited energy budget, restricted CPU clock, restricted memory as well as network bandwidth. That causes the implementations of wireless sensor network. The Wireless sensor network topologies are composed of a huge number of nodes represents a new issue that had not been considered in simple ad-hoc networks.

3) *Self:*

One of the biggest challenges is to create the wireless sensor network vision in the network application layer. Due to the fact that WSNs are deployed to operate with few or none human intervention, self characteristics like self-organization, and self-healing become necessary. These characteristics are easily listed as challenge, however are extremely difficult to achieve.

4) *High scale/density:*

There are number of Wireless sensor network approaches that consider a large number of nodes in order to overcome hardware or software problems, thus there is a

minimum number of nodes that is necessary to provide the Wireless sensor network service. The main challenges include the processing of the large number of generated data, the assurance that the particular Wireless sensor network requires the minimum desirable density, and the development of solutions that require the lowest density and energy consumption in order to maximize the Wireless sensor networks lifetime. A WSN based on a large number of nodes that are deployed in large areas is considered a large-scale system. Due to its characteristics, these systems are subject to faults, noise, which sometimes can be caused by the WSN itself, and other uncertainties. Moreover, when a WSN is deployed, it might be self-operational and present self-maintenance, due to that human intervention is very expensive or even impossible. Therefore, all these characteristics impose several conflicting goals.

5)Security:

Wireless sensor networks can be used in safety critical applications, thus its security is an essential issue to be considered. Moreover, the security issues is consider for coordination and real time communication approaches.Thus, some intruder can easily exploit these Wireless sensor network security faults. The great dilemma is how to implement security techniques that need large computational resources in a technology that deals with severe hardware constraints.

6)Real-time:

Wireless sensor networks operate in the real world, for correct functionality real-time features are necessary. These systems present implicit real-time constraints. The response time of its tasks is also important, thus the system tasks must be completed as fast as possible. Several Wireless sensor networks present explicit real-time constraints. For example, a structural monitoring application imposes explicit deadlines for the data sensing However, due to the large number of nodes, non-determinism and noise, it might be extremely hard to guarantee real-time properties.

II. DESSIGNING OF WIRELESS SENSOR NETWORK

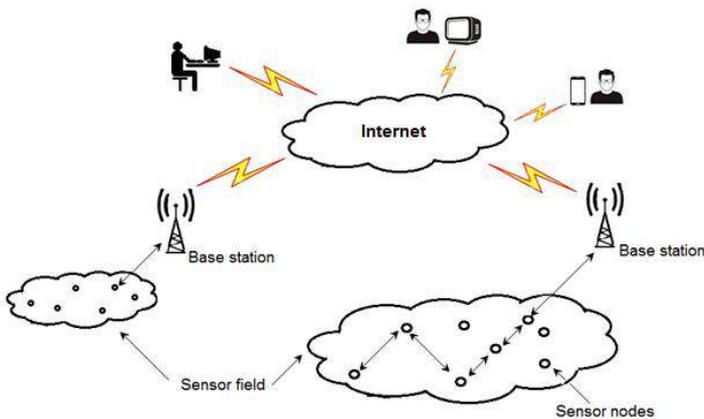


fig. Wireless sensor network

1. Network Dynamics

There are three main components in a sensor network. These are the sensor nodes, sink and monitored events. Supporting the mobility of sink nodes is an important issue in WSN design. Routing plays important role as routing messages from or to moving nodes is more challenging since route stability becomes an important optimization factor, in addition to energy, bandwidth etc
Sensor network has three main components these are sensor nodes, sink and monitored events. For wireless sensor designing supporting the mobility of sink node is an important issue in wireless sensor network design. as the messages routes from or to moving nodes is more challenging since route stability becomes an important optimization factor, in addition to energy, bandwidth etc

2. Placement of Nodes

Another consideration is the topological deployment of nodes topology can be simple star network to an advanced multi-hop wireless mesh network. . This is application dependent and affects the performance of the routing protocol. The deployment is either deterministic or self-organizing

3. Energy Considerations:

While designing the infrastructure, the process of setting up the routes is greatly influenced by energy considerations. Since the transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multi hop routing will consume less energy than direct communication.

4. Node Capabilities:

In a Wireless sensor networks, different functionalities can be associated with the sensor nodes. According to previous studies, all sensor nodes are assumed to be homogenous, having equal capacity in terms of computation, communication and power. Depending on the application a node can be dedicated to a particular special function such as relaying, sensing and aggregation since engaging the three functionalities at the same time on a node might quickly drain the energy of that node. Including of heterogeneous set of sensors raises multiple technical issues related to data routing. The results generated from these sensors can be at different rates, subject to diverse quality of service constraints and following multiple data delivery models. Therefore, such a heterogeneous environment makes data routing more challenging.

III. OVERVIEW OF WIRELESS SENSOR NETWORK

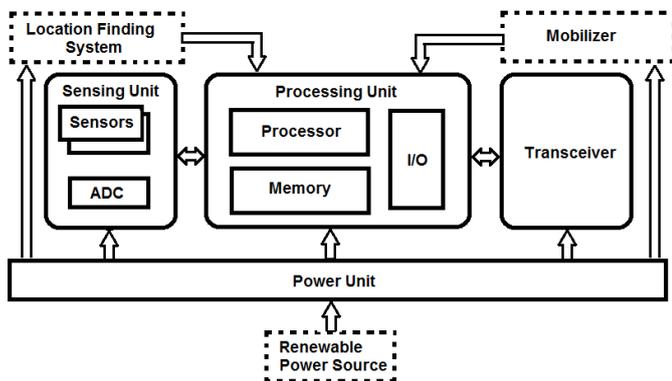


Fig. Node architecture

Number of fields where wireless sensor networks are used that are ranging from spatial application field such as wild environment monitoring, industrial machine measurement and military purpose measurement to daily application fields such as fire monitoring and pollution monitoring. A wireless sensor network can be wire or wireless network, which has several sensors nodes installed in certain field. A sensor node should have computation, sensing and wireless communication functionalities. The number of sensors are used for delivering information in real-time from environments and processes, where data collection is impossible previously.

wireless sensor networks consist of low power sensor nodes and integrate general-purpose computing with heterogeneous sensing and wireless communication. Power unit is One of the most important components of a sensor node. A wireless sensor network limits the radio frequency channel, due to, that is to say, unstable links, limit of physical protection of each sensor node, actual of each nodes connection, variation topology in addition dangerousness about routing security is high by activity spite nodes. A wireless sensor network consists of spatially distributed autonomous sensors which cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants.

IV. POWER CONSTRAINTS IN WSN

Limited energy resource is the main drawback of wireless sensor network. The lifetime of the wireless sensor network is limited as there are no external power supply through wires. There are many researches in the field of energy optimization & energy supply for the wireless sensor network like photovoltaic but these techniques are not sufficient to improve the life time of wireless sensor network.

To make the wireless sensor network more efficient & to extend the life time of the wireless sensor network it is required that battery life of every participating sensor should be improved and then the total energy of the WSN should be optimized. To achieve this nodes remain functional or activated only when they have to transmit or receive any signal from other nodes. Every node has a radio transceiver that has four modes of operation:-

Transmission: -

Information transmission b/w sensor nodes. It consumes the maximum power in the WSN.

Receiving: -

Information received b/w sensor nodes. It consumes the medium power.

Stand-by: -

Sensor node is currently inactive and turned on & ready for data transmission.

Sleep: -

Sensor node is in OFF state.

A finite number of bits are transmitted by sensor nodes before running out of battery power. To make the network life time longer it is essential to reduce the energy consumption per bit. To achieve this it is taken in to consideration that every information bit is valid for only a particular time frame and sensor nodes have to send all the bits to a hub before this particular time frame. Using this approach the end to end transmission delay can be controlled to some extent. Layers of the protocol stack also affect the energy consumption in the WSN. So there is requirement where all the hardware & protocol layers can be used in an efficient manner to improve the life time of the WSN.

V. CONCLUSION

In this paper power related problems in WSN are presented. The power and communication of data are the main problems of a wireless sensor network. With its limitations, it is important to design a network that uses optimal energy resources while transferring reliable data.

VI. REFERENCES

- [1]Warneke, Liebowitz, B., Last, M., B., and Pister, K. S. J. Smartdust: Communicating with a cubic-millimeter computer. *Computer* 34, 1(2001), 44–51.
- [2] W. Su, Sankarasubramaniam Akyildiz, and E.Cayirci, "A survey on sensor networks", *IEEE Communications Magazine*, Volume: 40 Issue: 8, August 2002, pp.102-114.
- [3]Akyildiz, I. F.; Su W.; Sankarasubramaniam Y. & Cayirci E. (2002). A Survey on Sensor Networks. *IEEE Communications Magazine*, pp. 102-114

[4] D.Culler, D.Estrin and M.Srivastava, "Overview of Sensor Networks", IEEE Computer Society, August 2004.

[5] Ayad Salhieh Jennifer Weinmann _ Manish Kochhal _ Loren Schwiebert, "Power Efficient Topologies for Wireless Sensor Networks" reference.kfupm.edu.sa/.../power_efficient_topologies_for_wireless_529104.pdf

[6] Ewa Niewiadomska-Szynkiewicz, Piotr Kwaśniewski, Izabela Windyga, "Comparative Study of Wireless Sensor Networks Energy-Efficient Topologies and Power Save Protocols"

[7] <http://snap.cs.berkeley.edu/documents/architecture.pdf>

[8] Kemal Akkaya and Mohamed Younis , "A Survey on Routing Protocols for Wireless Sensor Networks" http://www.cs.umbc.edu/~kemal1/mypapers/Akkaya_Younis_JoAdHocRevised.pdf

[9]M.Ismail, M.Y.Sanavullah, "Security Topology in Wireless Sensor Networks With Routing Optimisation"IEEE 2008.

[10]IEEE/ACM Transactions on Networking, Vol. 20, No. 1
Chen, W.; Neely, M. J. & Mitra, U. (2008). Energy-Efficient Transmissions With Individual Packet Delay Constraints. *IEEE Transactions on Information Theory*, Vol. 54, No. 5.

[11]Akyildiz, I. F.; Brunetti, F. & Blazquez, C. (2008). Nanonetworks: A new communication paradigm. *Computer Networks*, No. 52, pp. 2260–2279

[12] Young-Jun Jeon, Yong-Sik Choi, Sang-Hyun Park, "A study on sensor nodes attestation protocol in a Wireless Sensor Network", ICACT 2010.

[13]Allipi, C. & Galperti, C. (2008). An Adaptive System for Optimal Solar Energy Harvesting in

[14]Wireless Sensor Networks Nodes. *IEEE Transactions on Circuits and Systems*, Vol. 55, No. 6, pp. 1742-1750

[15]Campobello, G.; Leonardi, A. & Palazzo, S. (2012). Improving Energy Saving and Reliability in Wireless Sensor Networks Using a Simple CRT-Based Packet-Forwarding Solution.



Design of 8 x 8 Vedic Multiplier using Quaternary-Logic & Pipelining Architecture

Vivek Wanjari
M.Tech (IV SEM).
Electronics Engg. (Communication)
SDCOE, Selukate, Wardha.
compactvivek30@gmail.com

Prof. R. N. Mandavgane
Asso. Professor and Head
Dept. of E&T Engg.
BDCOE, Sewagram, Wardha.
rmandavgane@rediffmail.com

Abstract - In recent years the growth of the portable electronic is forcing the designers to optimize the existing design for better performance. There are different entities that one would like to optimize when designing a VLSI circuit. These entities can often not be optimized simultaneously, only improve one entity at the expense of one or more others. A multiplication is the important operation used in various applications like DSP processor, math processor and in various arithmetic circuits. In VLSI system the overall performance is strongly depends on the performance of arithmetic circuits like multiplier. Designers find the solution of these by implementing technique of calculation based on Indian Vedas mathematics called as Vedic multiplier, which offers simple way of multiplication. The design of an efficient multiplier circuit in terms of power, area, and speed simultaneously, has become a very challenging problem. Power dissipation is recognized as a critical parameter in modern VLSI design field. The multi valued logic (MVL) provides the key benefit of a higher density per integration circuit area compared to traditional two valued binary logic. All so the Quaternary logic offers the benefit of easy interfacing to binary logic because radix 4 allow for the use of simple encoding/decoding circuits. This paper present design of 8x8 Vedic multiplier using Tanner EDA tool & simulated using T-spice simulator. With the help of pipelining technique 8x8 Vedic multiplier circuit level has been proposed in these paper, as it does not increase the hardware that much, but which increase the speed and requires less computation gives us better speed. The two stages pipelining is used to optimize Delay compared with previously normal 8x8 Vedic multiplier results.

Keywords - VLSI, Multi-valued logic (MVL), Quaternary logic, Vedic multiplier, Digital signals processing.

I. INTRODUCTION

A multiplier is one of the most important parts in any processor and most of the instruction in a typical processor is multiplication. Multiplication process is used in many neural computing and DSP applications like Instrumentation and

Measurement, Communications, and Audio and Video processing, Graphics, Image Enhancement, 3-D Rendering, Navigation, Radar, GPS, and control applications like Robotics, Machine Vision and Guidance. In binary logic, the size of the device is reduced by reducing the size of the transistor. But up to a limit, because the size of transistor cannot be reduced indefinitely. The multi-valued logic apply to the multiplier design, word length & no of transistor can be greatly reduced. There are various multipliers for binary logic Such as Array multiplier, Booth multiplier, and Wallace tree multiplier and a Vedic multiplier. In recent years Vedic multiplier has caught the Attention because of its superiority over other multipliers. If the Functional blocks designed in multi-valued logic are used in Vedic multiplier's architecture, it will surely enhance the performance of multiplier and hence the whole area & power consumption of chip. The performance of two levels binary logic is limited due to interconnects which occupy a large area on a VLSI chip. In VLSI circuit, total 70% of the area is divided to interconnection, 20% to insulation, and 10% to device. One can achieve a cost-effective way of utilizing Interconnections by using a larger set of signals over the same area in multiple-Valued logic (MVL) devices, allowing easy implementation of circuits. In MVL advantage of binary logic is retained. The higher radix in Use is the ternary and the quaternary logic. The Binary logic has many drawbacks and limitations. A signal cannot always be just ON or OFF or DON'T CARE, and HIGH IMPEDANCE. It does not mean that these states can result in inefficient processing of the data. Also, binary logic results in longer word-lengths which increase the number of interconnections and hence the chip size. Multiplier design in Vedic mathematics has improved conventional delay time, area size to minimizing power dissipation while still maintaining the high performance. The low power and high speed multipliers can be implemented with different logic style.

II. VEDIC MATHEMATICS

A 'Veda' is a Sanskrit word that means 'knowledge'. The name Vedic Mathematics which is used & heard many times with reference to the techniques for solving problems mentally. The techniques of math that is Vedic mathematics were rediscovered in the early twentieth century from ancient Indian sculptures by Sri Bharati Krishna Tirthaji Maharaj. These methods can be directly applied to Trigonometry, plain & spherical geometry, conics, calculus and applied mathematics of various kinds. Total 16 sutras or formulae given in ancient Vedas out of these two sutras are useful for multiplication namely Nikhilam sutra and Urdhva Tiryakbhyam sutra. Means "all from 9 and last from 10" and "vertically and crosswise". The Urdhva Tiryakbhyam sutra is more popular than Nikhilam sutra since it is applicable in all cases.

III. MULTI-VALUE LOGIC (MVL)

It was first proposed by Jan Lukasiewicz, Polish minister of Education in 1919. Followed by Emil Post, American logician born in Poland the MVL employs more than two discrete levels of a signal, such as ternary & quaternary logic. Two logic systems are available in ternary logic, balanced ternary logic -1, 0 and 1 and simple ternary logic 0, 1 and 2. The quaternary logic uses 0, 1, 2 and 3 logic levels.

IV. OPERATING MODE OF MVL

MVL can be employed in either Voltage-Mode or Current-Mode. In voltage-mode MVL, operating voltage range is divided into the number of logical values to be represented, whereas, in current-mode MVL, currents are usually defined to have logical levels that are integer multiples of a reference current unit. For higher radix MVL system, current-mode is always preferred over voltage-mode because currents can be copied, scaled and algebraically sign-changed with a simple current mirror. The frequently used linear sum operation can be performed simply by wiring, resulting in a reduced number of active devices in the circuit. It is believed that current-mode MVL designs can allow better noise margin than voltage-mode MVL designs.

V. URDHVA-TIRYAKBHYAM SUTRA

Urdhva Tiryakbhyam Sutra is a general multiplication formula applicable to all cases of multiplication. It literally means "Vertically and crosswise". It is based on a novel concept through which the generation of all partial products can be done and then, concurrent addition of these partial products can be done. Thus parallelism in generation of partial products and their summation is obtained. The Urdhva Tiryakbhyam sutra (method) was selected for implementation since it is applicable to all cases of multiplication. Multiplication of two no's using Urdhva Tiryakbhyam sutra is

performed by vertically and crosswise, crosswise means diagonal multiplication and vertically means straight above multiplication and taking their sum. Thus any multi-bit multiplication can be reduced down to single bit multiplication and addition using this method. Moreover, the carry propagation from LSB to MSB is reduced due to one step generation of partial product.

VI. CONCEPT OF PIPELINING

Pipelining is one of the popular methods to realize high performance computing platform. Pipelining is a technique where multiple instruction executions are overlapped. It comes from the idea of a water pipe continue sending water without waiting the water in the pipe to be out. By pipelining the unit of a system we can produce result in every clock cycle. It leads to a reduction in the critical path. It can either increase the clock speed (or sampling speed) or reduces the power consumption at same speed in a system.

VII. Multiplier

A multiplier is an essential component. Longer word-lengths in binary logic make the multiplier large and complex. In binary logic, the size of the device is reduced by reducing the sizes of the transistors. But it has a limit, since the sizes of transistors cannot be reduced indefinitely. By applying MVL to the multiplier design, word-lengths and the area can be reduced. This will enhance the performance of multipliers and hence the whole chip.

A. 2X2 Vedic Multiplier

In 2x2 bit multiplier, the multiplicand has 2 bits each and the result of multiplication is of 4 bits. So in input the range of inputs goes from (00) to (11), output lies in the set of (0000, 0001, 0010, 0011, 0100, 0110, 1001). By using Urdhva Tiryakbhyam, the multiplication takes place. Here multiplicands a And b are taken to be (10) both. The first step is the vertical multiplication of LSB of both multiplicands, and second step is the crosswise multiplication and addition of the partial products. Then Step 3 involves vertical multiplication of MSB of the multiplicands and addition with the carry propagated from Step 2.

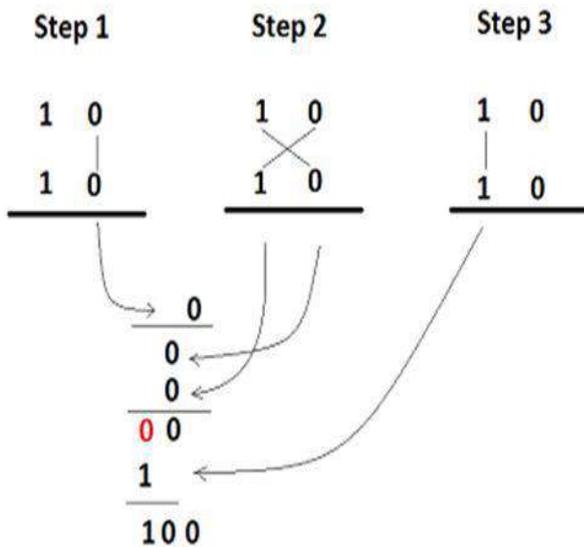
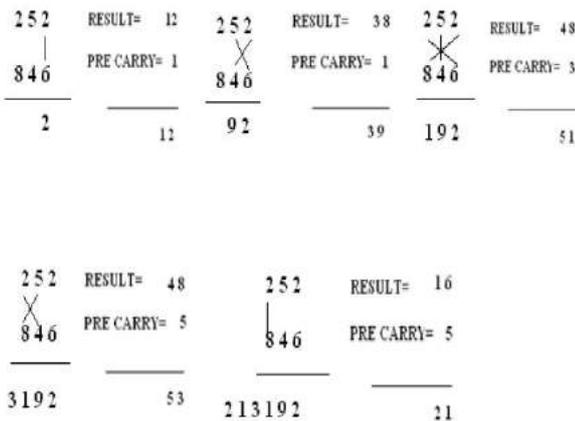


Fig 1: 2X2 Multiplication using Urdhva Tiryakbhyam Sutra.

B. Multiplication of two Decimal Numbers 252 x 846.

For Example, let us consider the multiplication of two decimal numbers 252 x 846 by Urdhva-Tiryakbhyam method. The digits on the both sides of the line are multiplied and added with the carry from the previous step. This generates one of the bits of the result and a carry. This carry is added in the next step and hence the process goes on. If more than one line are there in one step, all the results are added to the previous carry. In each step, least significant bit acts as the result bit and all other bits act as carry for the next step. Initially the carry is taken to be zero.



C. 4X4 Vedic Multiplier

The block diagram of 4x4 Vedic Multiplier is shown in Figure2. This multiplier is modelled using structural style of modelling using VHDL. In this paper first a 2x2 Vedic Multiplier is implemented using the above mentioned method. The 4x4Vedic Multiplier is designed. Using four 2x2 Vedic

Multipliers After that 8x8 Vedic Multiplier is implemented using four 4x4 Vedic Multipliers by using pipeline concept. Finally the results will be compared with the standard results.

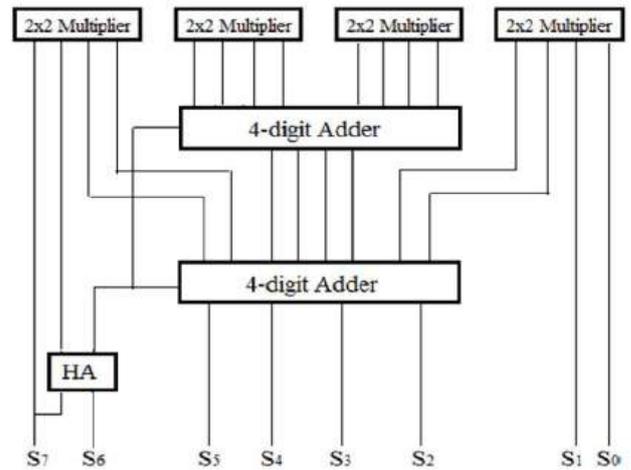


Fig 2:- Quaternary 4x4 Vedic Multiplier.

VIII. Simulation & Results

Fig.3 shows Four Quadrant Vedic multiplier. It can be surely concluded that the Application of current-mode MVL reduces the number of adders in the multiplier architecture as the number of bits to be processed goes on increasing. Furthermore, proposed 4x4 quaternary multiplier and by using pipeline architecture design of 8x8 Vedic Multiplier, which shows great reduction in the circuitry because of MVL.

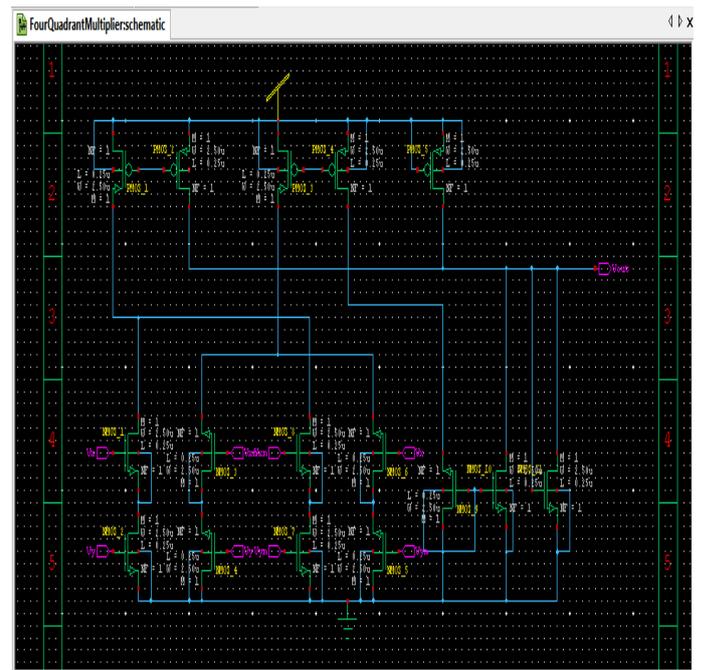


Fig.3. Synthesize result of Four Quadrant Vedic Multiplier.

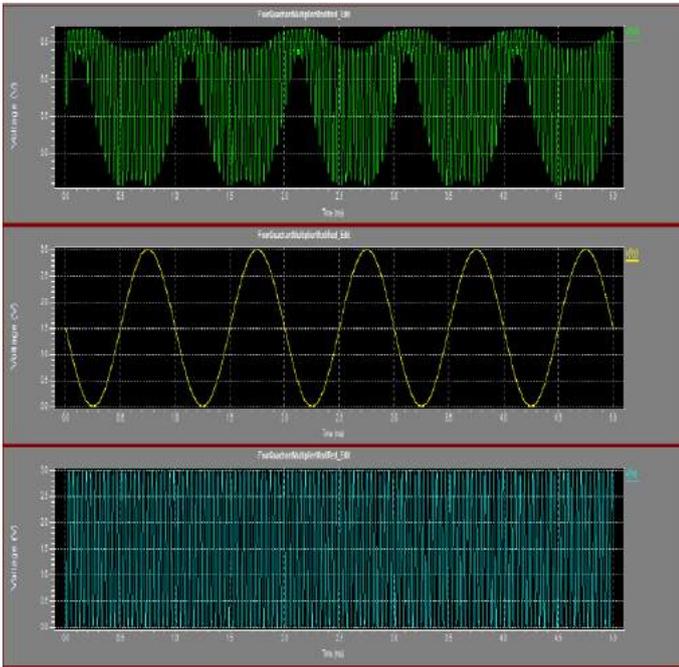


Fig.4. Simulation result of Four Quadrant Vedic Multiplier.

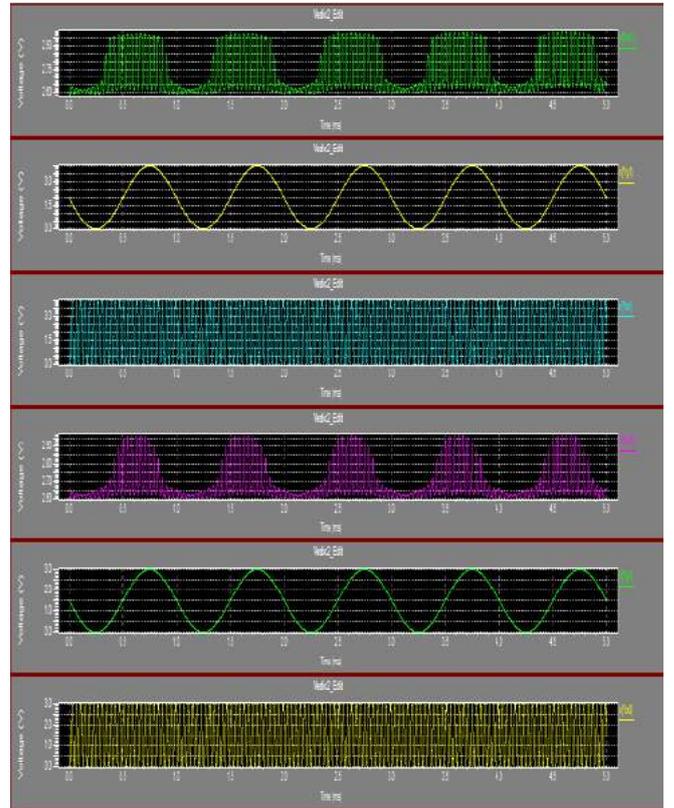


Fig.6:-Simulation result of 2-Bit Vedic Multiplier

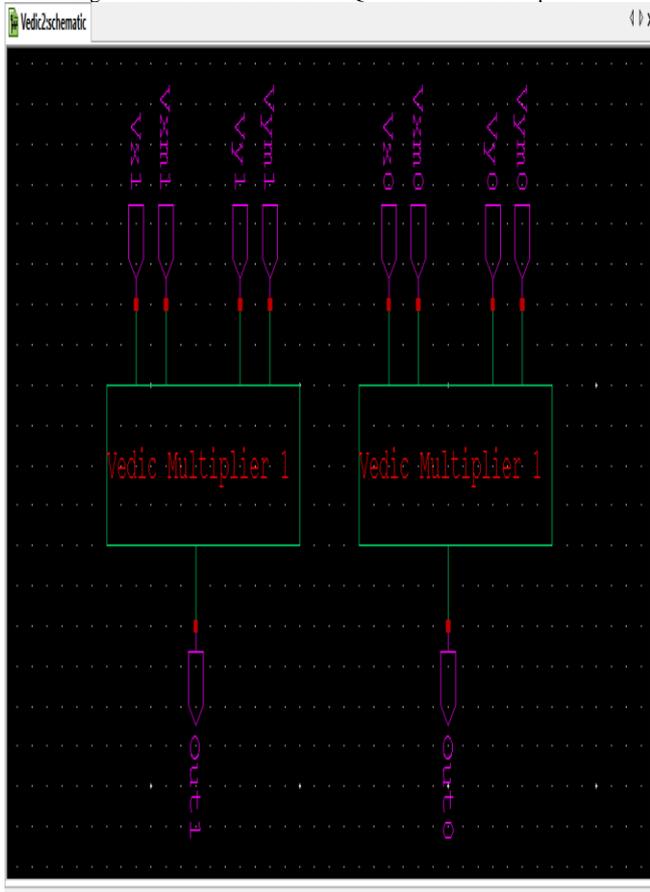


Fig 5:- 2-Sample/Bit Vedic Multiplier

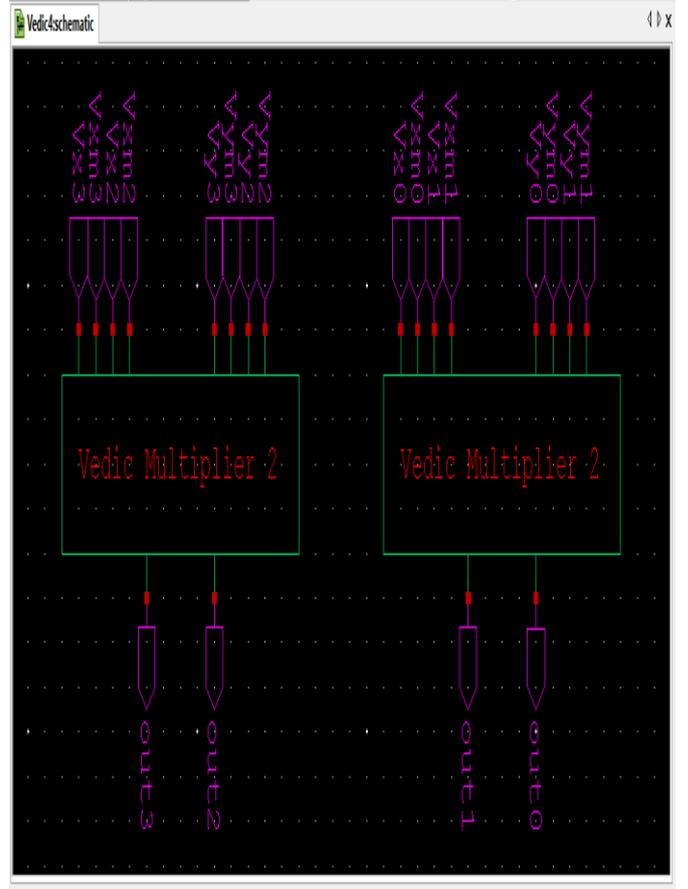


Fig 7:- 4-Sample/Bit Vedic Multiplier

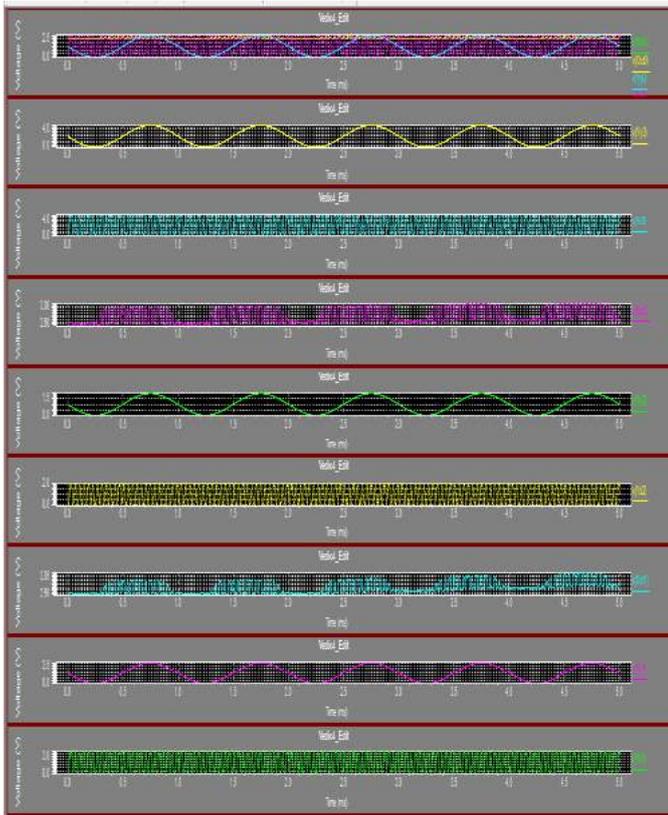


Fig.8:-Simulation result of 4-bit Vedic Multiplier

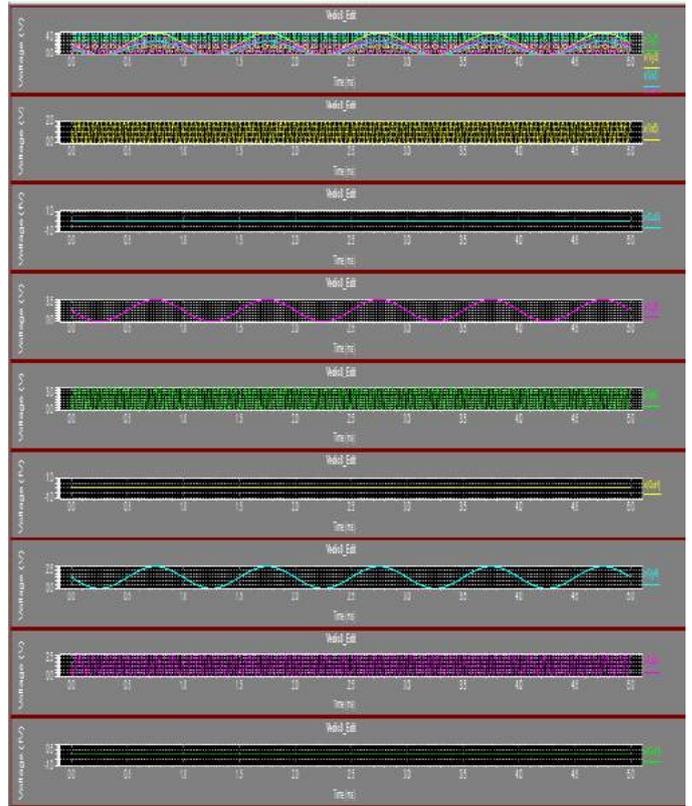


Fig. 10:-Simulation result of 8-bit Vedic Multiplier

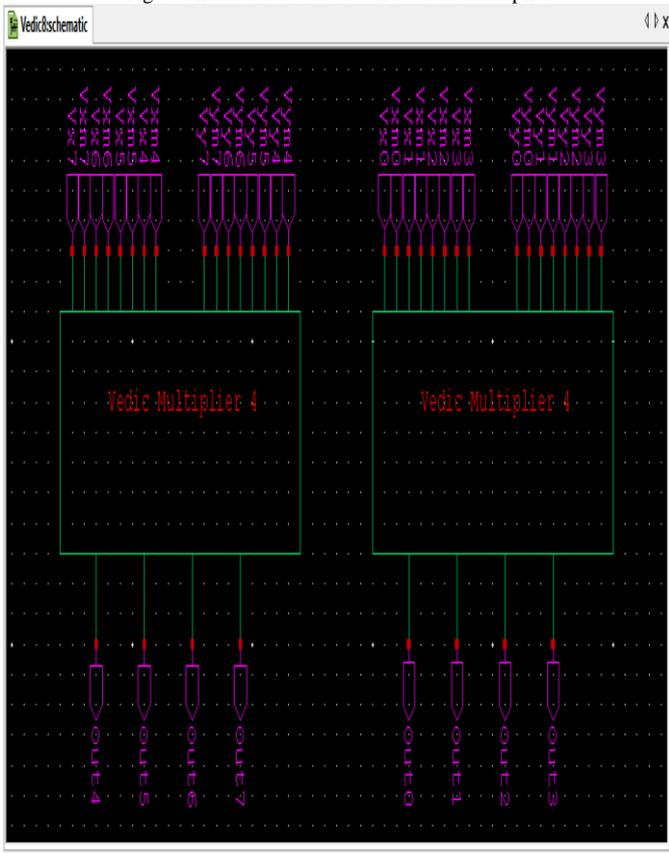


Fig 9:- 8-Sample/Bit Vedic Multiplier

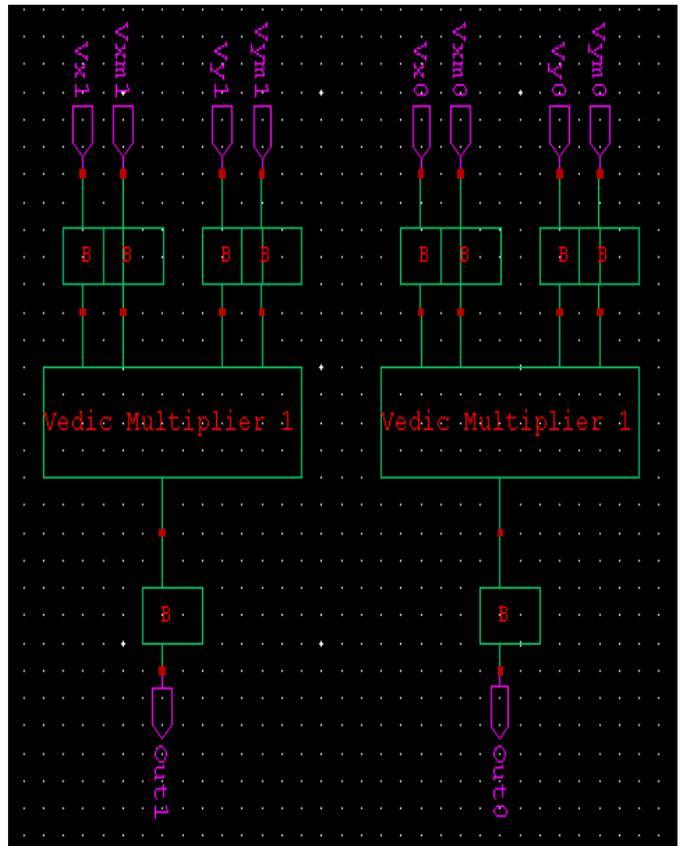


Fig 11:- 2-Sample/Bit pipeline Vedic Multiplier

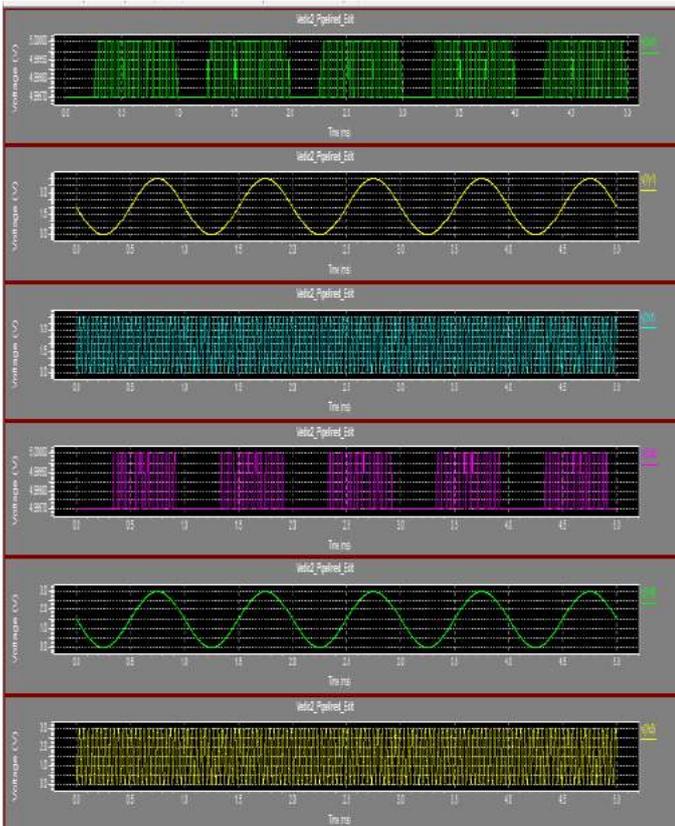


Fig. 12:-Simulation result of 2-Bit pipeline Vedic Multiplier

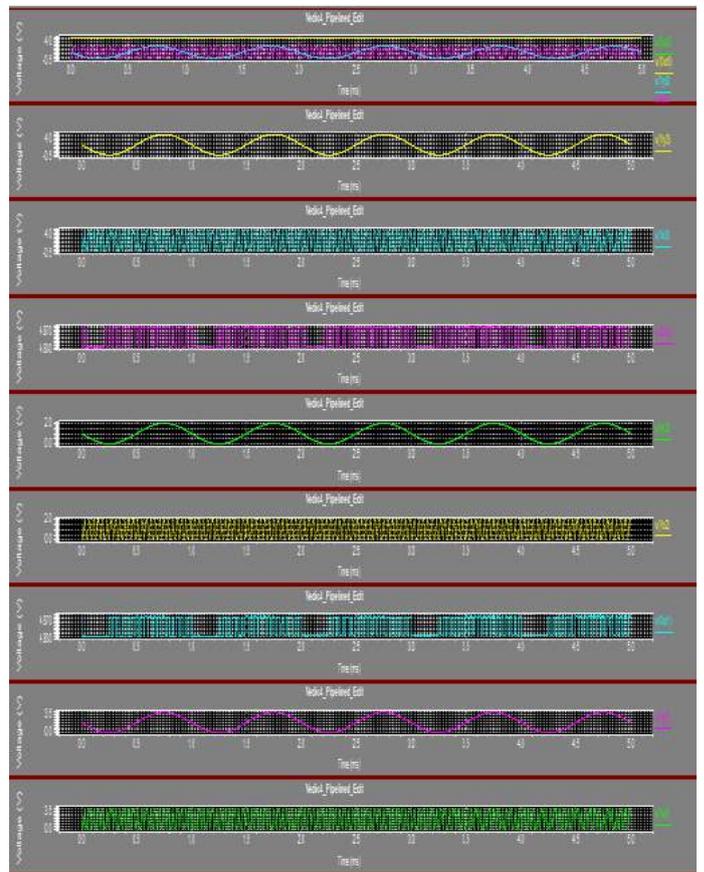


Fig. 14:-Simulation result of 4-bit pipeline Vedic Multiplier

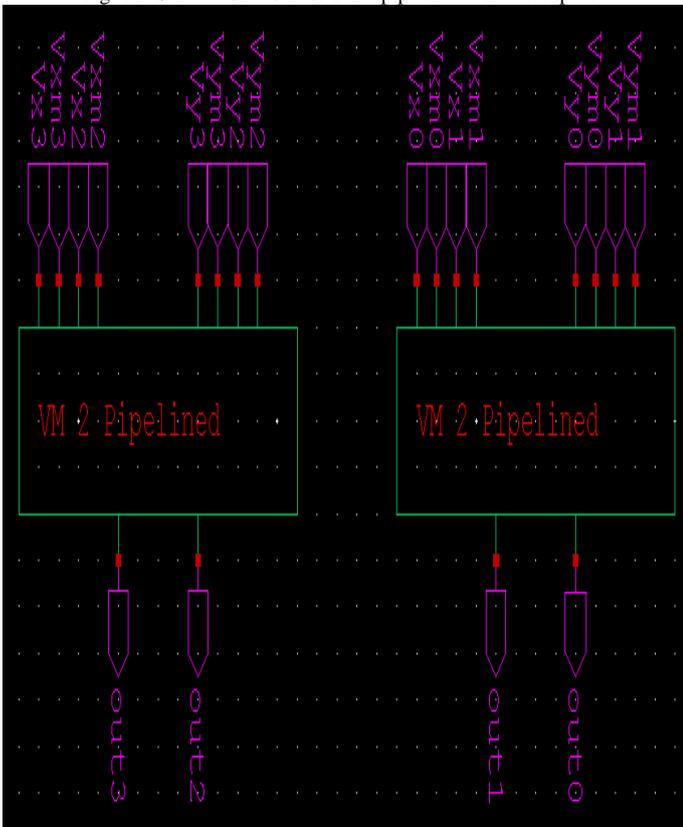


Fig 13:- 4-Sample/Bit pipeline Vedic Multiplier

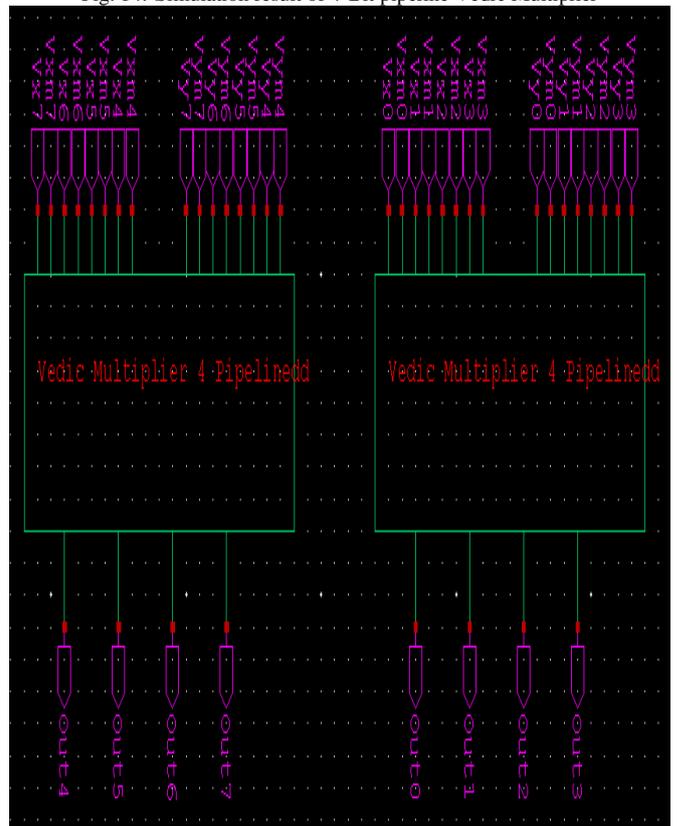


Fig 15:- 8-Sample/Bit pipeline Vedic Multiplier

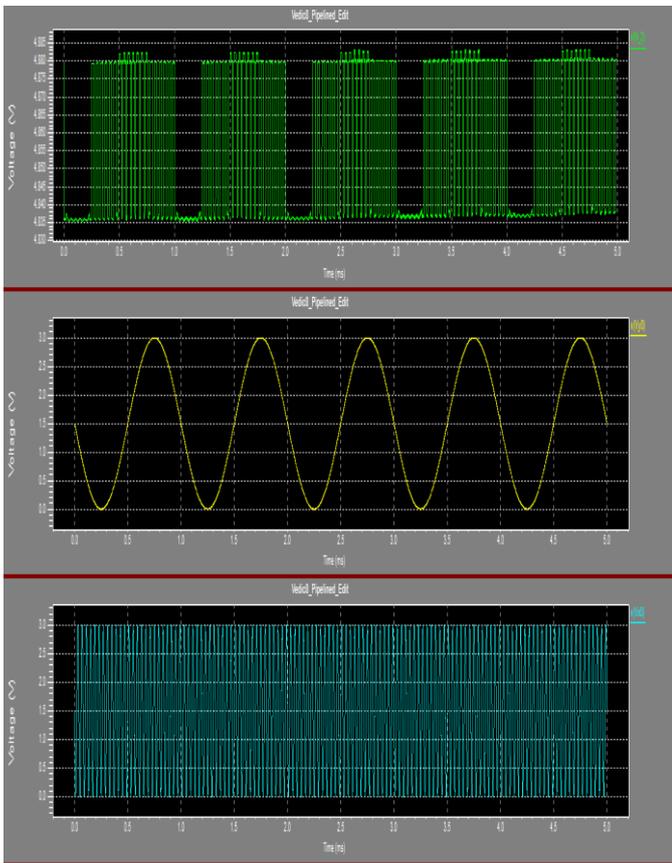


Fig. 16:-Simulation result of 8-Bit pipeline Vedic Multiplier
Table 1

Sr. no	Type of Vedic multiplier	Tech. file used	power	No. of Mossfet	Delay
1	Four quadrant multiplier	180 nm	7.2885e-003 watt	11	13.44 u sec

-	90 nm	4.3559e-004 watt	11	19.85 u sec
-	65 nm	1.8783e-004 watt	11	21.03 u sec

Table1. Results analyses of four Quadrant Multipliers

Table 2

Sr. no	Type of Vedic multiplier	Tech. file used	power	No. of Mossfet	Delay
1	2 – bit multiplier	180 nm	1.7158e-002 watt	41	13.76 u sec
-	-	90 nm	8.3993e-003 watt	41	18.97 u sec
-	-	65 nm	8.0685e-003 watt	41	19.77 u sec

2	4 – bit multiplier	180 nm	3.4457e-002 watt	81	19.93 u sec
	-	90 nm	1.6947e-002 watt	81	19.46 u sec
	-	65 nm	1.6214e-002 watt	81	19.30 u sec
3	8 – bit multiplier	180 nm	6.8853e-002 watt	161	19.26 u sec
	-	90 nm	3.3894e-002 watt	161	18.82 u sec
	-	65 nm	3.2427e-002 watt	161	18.73 u sec

Table2. Results analyses of different Multipliers

Table 3

Sr. no	Type of Vedic multiplier	Tech. file used	power	No. of Mosfet	Delay
1	2 – bit pip. multiplier	180 nm	3.5239e-002 watt	81	6.02 u sec
	-	90 nm	1.7618e-002 watt	81	2.56 u sec
	-	65 nm	1.5759e-002 watt	81	2.45 u sec

2	4 – bit pip. multiplier	180 nm	7.3417e-002 watt	161	5.68 u sec
	-	90 nm	2.2848e-002 watt	161	2.88 u sec
	-	65 nm	3.0772e-002 watt	161	1.76 u sec
3	8 – bit pip. multiplier	180 nm	1.4683e-001 watt	321	4.93 u sec
	-	90 nm	4.5696e-002 watt	321	4.47 u sec
	-	65 nm	6.1530e-002 watt	321	4.16 u sec

Table3. Results analyses of different pipeline Vedic Multipliers

XI. CONCLUSION

The paper shows the efficient use of Vedic multiplication method in order to multiply two numbers. Here we introduce the concept of pipelining so that lesser number of LUTs verifies that the hardware requirement is reduced, Thereby reducing the time consumption without compromising power so much.

X. SCOPE OF FUTURE WORK

An improvement in power by using new techniques can greatly improve system performance. This project can be extended for the reconfigurable architecture.

Acknowledgement

I wish to Prof. R. N. Mandavgane and other contributor to give their contribution for developing this topic related search. I also thankful to all the authors of different books which guide me a lot.

REFERENCES

1. Ashish S. Shende, M. A. Gaikwad, D. R. Dandekar. "Design of Efficient 4x4 Quaternary Vedic Multiplier Using Current-Mode Multi-Valued

- Logic”, *Int. J. on Recent Trends in Engineering and Technology*, Vol. 10, No. 2, Jan 2014.
2. Diogo Brito, Jorge R. Fernandez, Jose Monteiro. “Quaternary Logic Lookup Table in Standard CMOS”, *IEEE Transaction on Very Large Scale Integration (VLSI) System* 2014.
 3. Riya Saini, Tina G. Galani, R. D. Daruwala. “Efficient Implementation of Pipelined Double Precision Floating Point Unit on FPGA”, *International Journal of Emerging Trends in Electrical and Electronics (IJETEE – ISSN: 2320-9569)* Vol. 5, Issue. 1, July-2013.
 4. Ashish S. Shende, M. A. Gaikwad, D. R. Dandekar. “Application of Current-Mode Multi-Valued Logic in the Design of Vedic Multiplier”, *International Journal of Computer Applications (0975 – 8887) Recent Trends in Engineering Technology-2013*.
 5. Deeraj Jain, Dr. Ajay Somkuwar. “Implementation and Performance Analysis of a Vedic Multiplier Using Tanner EDA Tool”, *IJSRD–International Journal for Scientific Research & Development* vol. 1, Issue 5, 2013.
 6. Arun K. Patro, Kunal N. Dekate. “A Transistor Level Analysis For a 8-Bit Vedic Multiplier”, *International Journal of Electronics Signals and Systems (IJESS) ISSN: 2231- 5969, Vol-1 Iss-3, 2012*.
 7. S. Kokila, R.Ramadhurai, L.Sarah. “VHDL Implementation of Fast 32X32 Multiplier based on Vedic Mathematics”, *International Journal of Engineering Technology and Computer Applications* Vol.2, No.1, Apr 2012.
 8. Aniruddha Kanhe, Shishir Kumar Das, Ankit Kumar Singh. “Design and Implementation of Floating Point Multiplier based on Vedic Multiplication Technique”, *International Conference on Communication, Information & Computing Technology (ICCICT)*, Oct. 19-20, 2012.
 9. Sumit R. Vaidya. “Design of High Performance 8x8-bit Multiplier Based on Vedic Mathematics in ASIC”, *Dissertation for M.Tech. Project, BDCOE, RTM Nagpur University, January 2011*
 10. Sumit R.Vaidya and Deepak Dandekar. “Delay-Power Performance Comparison of Multipliers in VLSI Circuit Design”, *International Journal of Computer Networks & Communications (IJCNC)*, Vol.2, No.4, July 2010

A 32 BIT MAC Unit Design Using Vedic Multiplier and Reversible Logic Gate

ShraddhaWanjari,
Nuva college of Engg. & Tech
shraddhawanjari0@gmail.com

Dr.SanjayAsutkar
MIT,Gondia

Abstract—In the accumulate adder the previous MAC output and the present output will added and it consists of Multiplier unit, one adder unit and both will get be combined by an accumulate unit. The major applications of Multiply-Accumulate (MAC) unit are microprocessors, logic units and digital signal processors, since it determines the speed of the overall system . The efficient designs by MAC unit are Nonlinear Computation like Discrete Cosine or wavelet Transform (DCT), FFT/IFFT. Since, they are basically executed by insistent application of multiplication and addition, the entire speed and performance can be compute by the speed of the addition and multiplication taking place in the system. general MAC architecture consists of a conventional multiplier, adder and an accumulator. Where the output is added to the previous MAC output result by an accumulate adder. The Multiply-Accumulate (MAC) unit is extensively used in microprocessors and digital signal processors for data-intensive applications, such as filtering, convolution, and inner products.

Keywords—Reversible Logic, Quantum Computing, Kogge Stone Adder

I. INTRODUCTION

In the accumulate adder the previous MAC output and the present output will added and it consists of Multiplier unit, one adder unit and both will get be combined by an accumulate unit. The major applications of Multiply-Accumulate (MAC) unit are microprocessors, logic units and digital signal processors, since it determines the speed of the overall system [13]. The efficient designs by MAC unit are Nonlinear Computation like Discrete Cosine or wavelet Transform (DCT), FFT/IFFT. Since, they are basically executed by insistent application of multiplication and addition, the entire

speed and performance can be compute by the speed of the addition and multiplication taking place in the system. Generally the delay, mainly critical delay, happens due to the long multiplication process and the propagation delay is observed because of parallel adders in the addition stage.

The main idea of this paper is comparison of area, speed and other parameters of Conventional MAC unit with the Vedic MAC design.

II. Literature Survey

A. MAC Unit

A multiplying function can be carried out in three ways: partial product Generation (PPG), partial product addition (PPA), and final conventional addition. The two bottle necks that should be considered are increasing the speed of MAC are partial product reduction and accumulator block.

The 32 bit Mac design by using Vedic multiplier and reversible logic gate can be done in two parts. First, multiplier unit, where a conventional multiplier is replaced by Vedic multiplier using Urdhava Triyagbhayamsutra.

Multiplication is the fundamental operation of MAC unit [1]. Power consumption, dissipation, area, speed and latency are the major issues in the multiplier unit. So, to avoid them, we go for fast multipliers in various applications of DSP, networking, etc. There are two major criterion that improve the speed of the MAC units are reducing the partial products and because of that accumulator burden is getting reduced. The basic operational blocks in digital system in which the multiplier determines the critical path and the delay. The $(\log_2 N + 1)$ partial products are produced by $2N-1$ cross products of different widths for $N*N$. The partial products are generated by Urdhava sutra is by Criss Cross Method. The maximum number of bits in partial products will lead to Critical path.

The second part of MAC is Reversible logic gate. In modern VLSI, fast switching of signals leads to more power

dissipation. Loss of every bit of information in the computations that are not reversible is $kT \cdot \log_2$ joules of heat energy is generated, where k is Boltzmann's constant and T the absolute temperature at which computation is performed. In recent years, reversible logic functions has emerged and played a vital role in several fields such as Optical, Nano, Cryptography, etc.

III. DESIGN OF MAC ARCHITECTURE

The design of MAC architecture consists of 3 subdesigns.

- Design of 32x32 bit Vedic multiplier.
- Design of adder using DKG gate reversible logic.
- Design of accumulator which integrates both multiplier and adder stages.

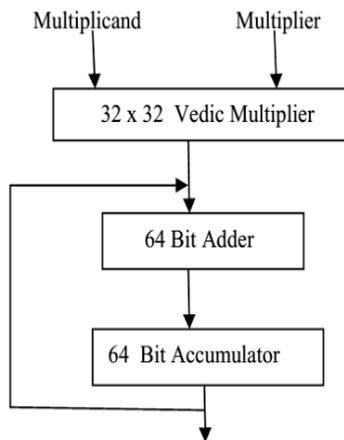


Fig 1: Modified MAC Architecture

A. 32 x 32 bit Vedic Multiplier

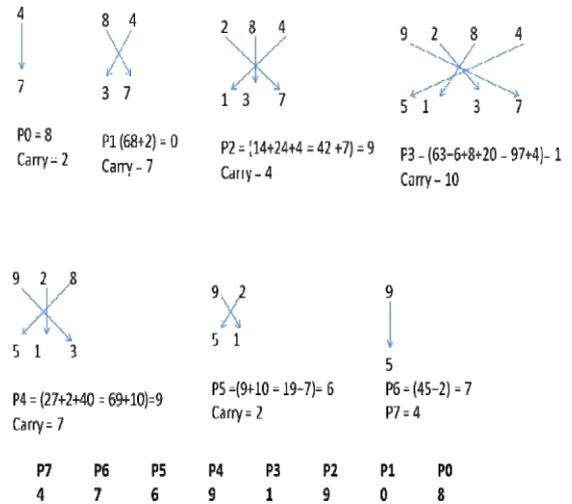
Vedic mathematics is an ancient system of mathematics, which was formulated by Sri Jagadguru Swami Bharati Krishna Tirthaji (1884 - 1960). After a research of eight years, he developed sixteen mathematical formulae from Atharvana Veda [11]. The sutras (aphorisms) covered each and every topic of Mathematics such as Arithmetic, Algebra, Geometry, Trigonometry, differential, integral, etc., The word "Vedic" is derived from the word "Veda" which means the power house of all knowledge and divine [2, 3]. The proposed Vedic multiplier is based on the "UrdhvaTriyagbhayam" sutra (algorithm). These Sutras have been traditionally used for the multiplication of two numbers in the decimal number system. In this work, we will utilize similar techniques to solve the binary number system to make the new aphorism, which will be more compatible for the digital systems. It is a general multiplication formula applicable to all cases of multiplication.

B. UrdhvaTriyagbhayam Sutra

It literally means "Vertically and Crosswise". Shift operation is not necessary because the partial product calculation will perform it in a single step, which in turn saves time and

power. This is the main advantage of the Vedic multiplier [14].

An example for the UrdhvaTriyagbhayam sutra is as follows: $9284 * 5137$



IV. IMPLEMENTATION OF VEDIC MULTIPLIER USING MODEL ARCHITECTURE IN DESIGN

The following fig. 2 shows the design of a 16x16 Vedic multiplier using an 8x8 Vedic multiplier and the design can be implemented using Verilog HDL. Using a 16x16 Vedic multiplier we can design 32 x 32 Vedic multiplier with carry save adder as shown in fig.3. We have modified the final adder stage with the Kogge stone adder which is more efficient than the Carry save adder which is shown in the fig. 4.

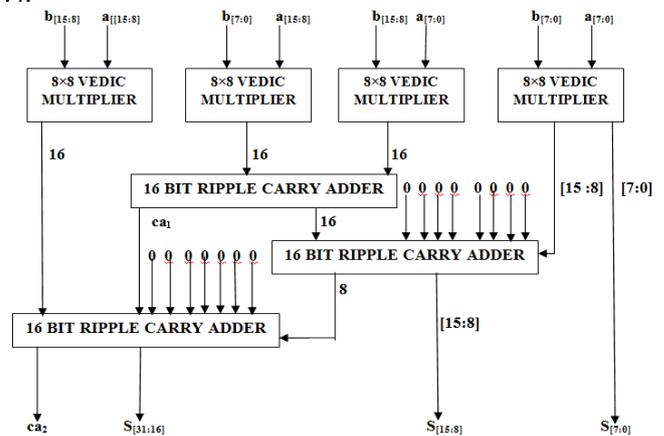


Fig 2: 16x16 Vedic multiplier using 8x8 Vedic multiplier

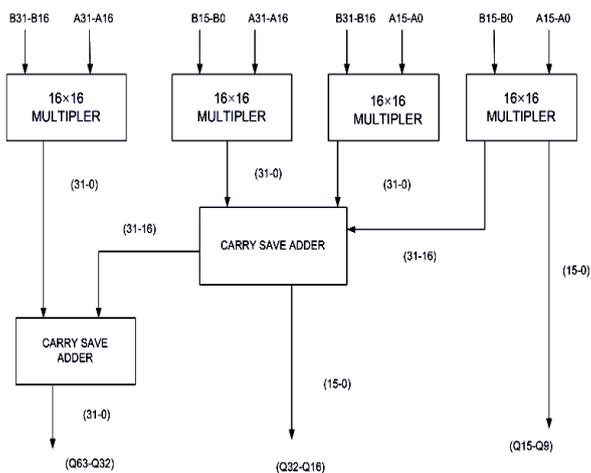


Fig 3: 32 × 32 Vedic Multiplier with Carry saveAdder

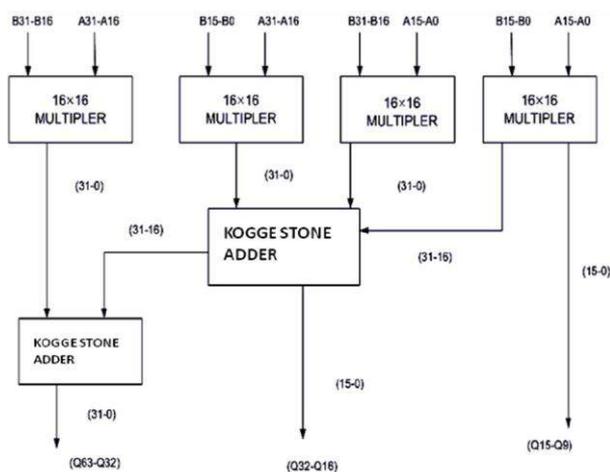


Fig 4: 32 × 32 Vedic Multiplier with Kogge StoneAdder

By using the Vedic multiplier we can achieve lesser partial products as the table shows that the multiplier and adder stages for Vedic multiplier for higher bit are lesser as compared to the conventional multiplier.

The multiplier design has been simulated and synthesized using Xilinx. The floor plan, device and port details of the multiplier are shown in the fig.5.



Fig. 5 device level diagram of 32 bit multiplier with Kogge StoneAdder

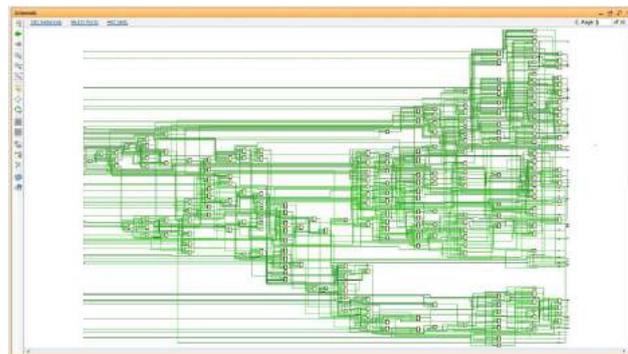


Fig . 5a. schematic floor plan of 32 bit Vedic multiplier with Kogge StoneAdder

V. KOGGE STONEADDER

It's a parallel prefix adder, which is the one of the fastest adder. Carry stages: $\log_2 n$; The number of cells: $n(\log_2 n - 1) + 1$; Maximum fan-out: 2 (extrawiring). So, it will reduce the power consumption as well as the power dissipation.

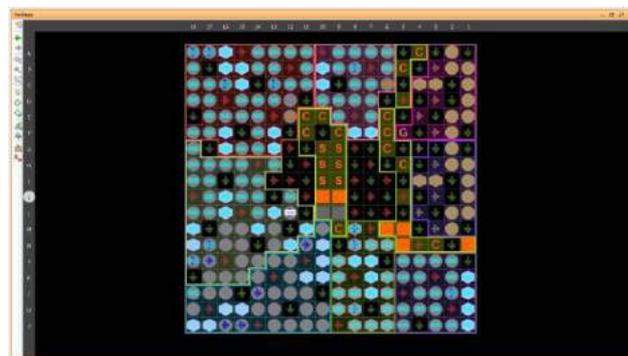


Fig. 5b. I/O package of 32 bit Vedic multiplier with Kogge StoneAdder

Table 1: comparison of no of additions and multiplications required in various Multipliers

	M= MULTIPLICATION A= ADDITION		
Multiplier	8 x 8 BIT	16x16 BIT	32 x 32 BIT
Conventional	64M 56A	256M 240A	1024M 1022A
Vedic multiplier with RCA	8M 4A	16M 8A	32M 16A
Booth	40M 26A	96M 72A	288M 243A
Vedic multiplier with Kogge stone Adder	8M 4A	17M 7A	35M 13A

VI. Design Of Adder Using Reversible Logic DkgGate

A. Reversiblelogic

Reversible logic is a unique technique (different from other logic). Loss of information is not possible in here. In this, the numbers of outputs are equal to the number of inputs.

1. General consideration for reversible logicgate

A Boolean function is reversible if each value in the input set can be mapped with a unique value in the output set. Landauer [18] proved that the usage of traditional irreversible circuits leads to power dissipation and Bennet [17] showed that a circuit consisting of only reversible gates does not dissipate power. In the design of reversible logic circuits, the following points must be kept in mind to achieve an optimized circuit:

- Fan-out is not permitted
- Loops or feedbacks are not permitted
- Garbage outputs must be minimum
- Minimum delay
- Minimum quantum cost
- Zero energy dissipation [17]

2. DKGGate

A 4*4 reversible DKG gate [6] that can work singly as a reversible full adder and a reversible full subtractor is shown below. If input A=0, the DKG gate works as a reversible Full adder, and if input A=1 then it works as a reversible Full subtractor. It has been verified that a reversible full-adder circuit requires at least two or three garbage outputs to make the output combinations unique [5],[6].

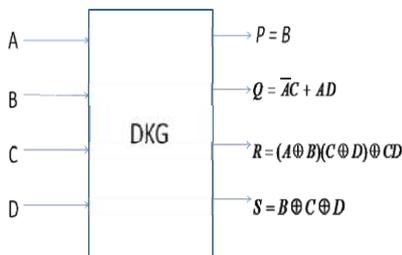


Fig. 6a [6] DKGgate

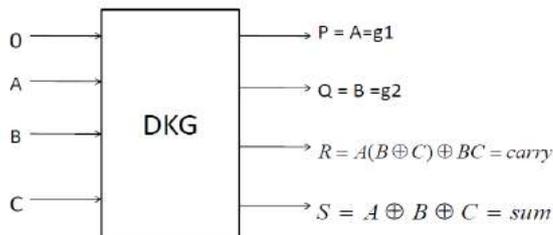


Fig. 6b DKG gate as a Fulladder

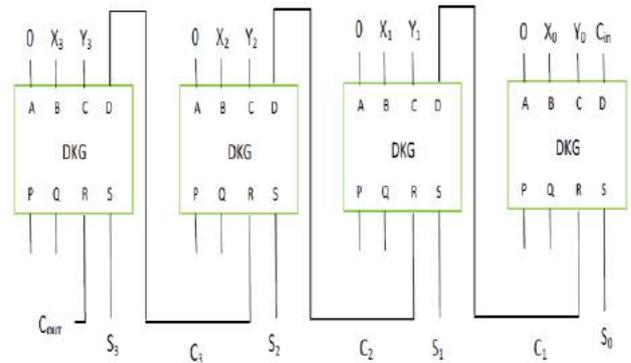


Fig. 6c Parallel adder using DKGgate

VII. AccumulatorStage

Accumulator has an important role in the DSP applications in various ranges and is a very basic and common method. The register designed in the accumulator is used to add the multiplied numbers. Multiplier, adder and an accumulator are forming the essential foundation for the MAC unit. The conventional MAC unit has a multiplier and multiplicand to do the basic multiplication and some parallel adders to add the partial products generated in the previous step. To get the final multiplication output we add the partial product to these results. Vedic Multiplier has put forward to intensify the action of the MAC Unit. The suggested MAC is compared with the conventional MAC and the results are analyzed. The results obtained using our design had better performance when compared to the previous MAC designs.

VIII. Result AndDiscussion

The modified multiplier using the Kogge Stone Adder is fast and the design of 32 bit MAC is done in Modelsim. The synthesis is performed out in Cadence RTL compiler. The above design is implemented in Verilog Code using mentor graphics modelsim 6.5b. Synthesis of the RTL code is done using Cadence RC compiler in 45nm technology. RTL Schematic view is given in the fig. 7. Comparison of area, speed and power reports is made with other methods as shown in table2.

Table 2: Analysis report of 32-bit MAC using Booth, Wallace tree and Vedic with Reversible logicmultiplier.

PARAMETER	Booth multiplier	Booth recoded Wallace tree multiplier	Vedic multiplier with Kogge Stone Adder and reversible logic (proposed model)	Vedic multiplier and reversible logic (proposed model)
POWER(μ W)	18398.67	17567.678	15621.12	15546.567
SPEED(ns)	6.567	6.436	4.932	5.667
AREA(μ m ²)	2322	2379	1972	2123

Comparison of parameters with different 2 bit MAC architectures is shown in fig.8

Simulation of 32 bit MAC output is shown in fig.9

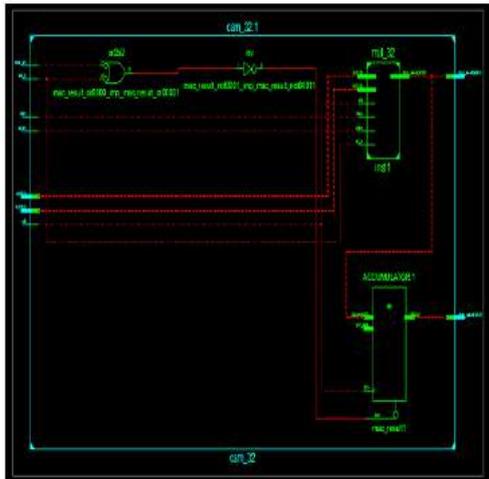


Fig 7: RTL schematic of 32 bit MAC architecture

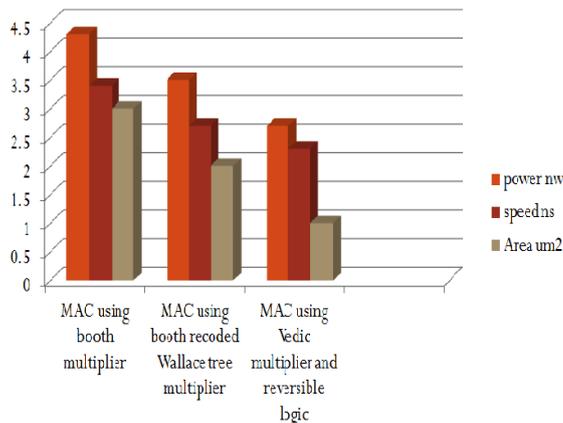


Fig 8: Comparison of different 32 BIT MAC architectures

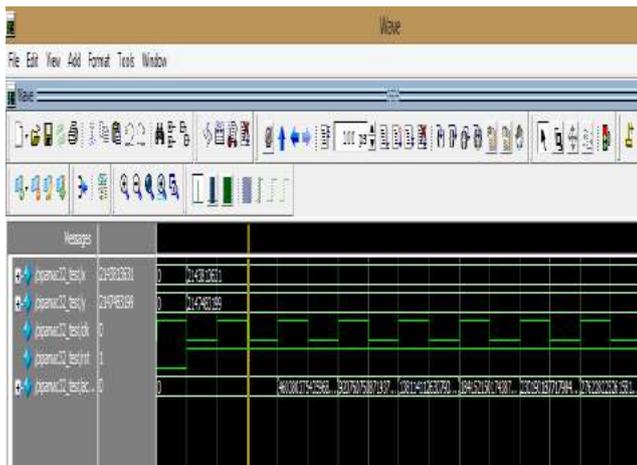


Fig 9: 32 BIT MAC simulated output in modelsim6.5b

IX. Conclusion And Future Work

The results obtained by the design of Vedic multiplier with 32 bits and reversible logic are quite good. The work presented is based on 32 – bit MAC unit with Vedic Multipliers. We have designed MAC unit basic building blocks and its performance has been analyzed for all the blocks. Therefore, we can say that the UrdhavaTriyagbhayam sutra with 32-bit Multiplier and reversible logic is the best in all aspects like speed, delay, area and complexity as compared to other architectures which are shown in table2.

Many researchers are reconfiguring the structure of MAC unit, which is the basic block in different designs and aspects especially using reversible logic which evolves recent days. Spectrum Analysis and Correlation linear filtering which are the applications of transform algorithm further add to the field of communication, signal and image processing and instrumentation, and some other. Combining the Vedic and reversible logic will lead to new and efficient achievements in developing various fields of Mathematics, science as well engineering.

References

- [1] VaijyanathKunchigi ,LinganagoudaKulkarni, SubhashKulkarni 32-bit MAC unit design using Vedic multiplier International Journal of Scientific and Research Publications, Volume3, Issue 2, February2013
- [2] Ramalatha, M.Dayalan, K D Dharani, P Priya, and S Deborah, High Speed Energy Efficient ALU design using Vedic multiplication techniques, International Conference on Advances in Computational Tools for Engineering Applications, 2009. ACTEA '09.pp. 600 -3, Jul 15-17,2009.
- [3] SreeNivas A and Kayalvizhi N. Article: Implementation of Power Efficient Vedic Multiplier. International Journal of Computer Applications 43(16):21-24, April 2012. Published by Foundation of Computer Science, New York,USA
- [4] VaijyanathKunchigi, LinganaGoudaKulkarni, SubhashKulkarni, High Speed and Area Efficient Vedic Multiplier, International Conference on Devices, Circuits and Systems (ICDCS),2012.
- [5] D.P.Vasudevan, P.K.Lala, J.Di and J.P.Parkerson, “Reversible- logic design with online testability”, IEEE Trans. on Instrumentation and Measurement, vol.55., no.2, pp.406-414, April2006.
- [6] RaghavaGaripelly , P.MadhuKiran , A.Santhosh Kumar A Review on Reversible Logic Gates and their Implementation International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 3, March2013.
- [7] Wikipedia.org/ macdesign
- [8] PrabirSaha, Arindam Banerjee, Partha Bhattacharyya, AnupDandapat, High Speed ASIC Design of Complex Multiplier Using Vedic Mathematics, Proceeding of the 2011 IEEE Students' Technology Symposium 14-16 January, 2011, IIT Kharagpur.
- [9] AsmitaHaveliya, A Novel Design for High Speed Multiplier for Digital Signal Processing Applications (Ancient Indian Vedic mathematics approach), International Journal of Technology and

- [10] AniruddhaKanhe, Shishir Kumar Das and Ankit Kumar Singh, Design and Implementation of Low Power Multiplier Using Vedic Multiplication Technique, (IJCS) International Journal of Computer Science and Communication Vol. 3, No. 1, January- June 2012, pp. 131-132 International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013ISSN 2250-315.
- [11] www.hinduism.co.za/vedic.htm#VedicMathematics.
- [12] www.vedicmaths.org/
- [13] A. Abdelgawad, MagdyBayoumi ,” High Speed and Area- Efficient Multiply Accumulate (MAC) Unit for Digital Signal Processing Applications”, IEEE Int. Symp. Circuits Syst. (2007) 3199–3202.
- [14] R.Bhaskar, GanapathiHegde, P.R.Vaya,” An efficient hardware model for RSA Encryption system using Vedic mathematics”, International Conference on Communication Technology and System Design 2011 Procedia Engineering 30 (2012) 124 –128.
- [15] FatemehKashfi, S. Mehdi Fakhraie, Saeed Safari,” Designing an ultra-high-speed multiply-accumulate structure”, Microelectronics Journal 39 (2008)1476–1484.
- [16] Jagadguru Swami Sri BharatiKrisnaTirthaji Maharaja, “Vedic mathematics”, MotilalBanarsidass Publishers Pvt. Ltd, Delhi, 2009.
- [17] C.H. Bennett,” Logical reversibility of computation”, IBM J. Res. Dev. 17 (1973)525–532.
- [18] R. Landauer, Irreversibility and heat generation in the computational process’s, IBM J. Res. Dev. 5 (1961)183–191.
- [19] AshisKumerBiswas, Md. MahmudulHasan, Ahsan Raja Chowdhury, Hafiz Md. HasanBabu, “Efficient approaches for designing reversible Binary Coded Decimaladders”.

DESIGN OF 9-BIT UART MODULE BASED ON VHDL

Fatema Anjum

Department of Electronics and Telecommunication
Nuva College of Engineering and Technology
Nagpur, India
fatemashadaan@gmail.com

Pooja Thakre

Department of Electronics and Telecommunication
Nuva College of Engineering and Technology
Nagpur, India

Abstract— Serial transmission is normally used with modems and for non-networked communication between computers, terminals and other devices. Fast, secure, reliable and long distance communication is crucial to meet user requirement. Universal Asynchronous Receiver Transmitter (UART) is widely used in serial data communication because of its advantages of high reliability, long distance and low cost. In this paper, we have presented the important modules of UART for reliable, efficient and secure data transmission. We have presented baud rate generator, also known as prescaler and asynchronous first in first out (FIFO) buffer for smooth data transmission. Simulation result and register transfer view of both modules are presented in this paper.

Keywords—prescaler; uart; serial communication; fifo; buffer; asynchronous

I. INTRODUCTION

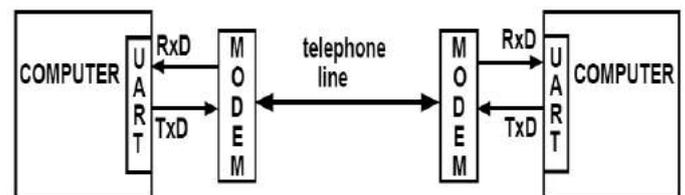
A UART (Universal Asynchronous Receiver/Transmitter) is the microchip with programming that controls a computer's interface to its attached serial devices. Specifically, it provides the computer with the RS-232C Data Terminal Equipment (DTE) interface so that it can "talk" to and exchange data with modems and other serial devices. As part of this interface, the UART also:

- Converts the bytes it receives from the computer along parallel circuits into a single serial bit stream for outbound transmission
- On inbound transmission, converts the serial bit stream into the bytes that the computer handles
- Adds a parity bit (if it's been selected) on outbound transmissions and checks the parity of incoming bytes (if selected) and discards the parity bit
- Adds start and stop delineators on outbound and strips them from inbound transmissions
- Handles interrupts from the keyboard and mouse (which are serial devices with special ports)

- May handle other kinds of interrupt and device management that require coordinating the computer's speed of operation with device speeds

Serial transmission is commonly used with modems and for non-networked communication between computers, terminals and other devices.

Serial Data Transmission



higher data rate. In many cases, serial is a better option because it is cheaper to implement. Many ICs have serial interfaces, as opposed to parallel ones, so that they have fewer pins and are therefore cheaper.

In telecommunications and computer science, serial communications is the process of sending data one bit at one time, sequentially, over a communications channel or computer bus. This is in contrast to parallel communications, where all the bits of each symbol are sent together. Serial communications is used for all long-haul communications and most computer networks, where the cost of cable and synchronization difficulties makes parallel communications impractical. Serial computer buses are becoming more common as improved technology enables them to transfer data at higher speed.

II. LITERATURE SURVEY

From review of related work and published literature, it is observed that many researchers have designed UART by

applying different techniques like algorithms, logical relations. Researchers have undertaken different methodologies with regards to UART design and its implementation on hardware platform.

Mohd Yamani, Idna Idris, Mashkuri Yaacob and Zaidi Razak have design UART with BIST capability[1]. In this designed, To increase reliability, manufacturers must be able to discover a high percentage of defective chips during their testing procedures. They highlight the attention given by most customers who are expecting the designer to include testability features that will increase their product reliability. They suggested the design of a UART chip with embedded built-in-self-test (BIST) architecture using FPGA technology. In this technique the behavior of UART circuit is describe by using VHISC hardware description language (VHDL). In the implementation phase, the BIST technique will be incorporated into the UART design before the overall design is synthesized by means of reconfiguring the existing design to match testability requirements.

One of the most important applications of UART is Multi-channel UART Controller designed by Shouqian Yu, Lili Yi, Weihai Chen and Zhaojin Wen.[2]. The proposed method paper presents a multi-channel UART controller based on FIFO technique and FPGA. This controller is designed with FIFO circuit block and UART circuit block to implement communication in modern complex control systems quickly and effectively. In this, the flow charts of data processing as well as the implementation state machine are also presented in detail. This controller can be used to implement communication when master equipment and slaver equipment are set at different Baud Rate. It also can be used to reduce synchronization error between sub-systems in a system with several sub-systems. The controller is reconfigurable and scalable.

From the survey it is observe that the implementation of UART basically uses the on-chip UART IP hard core because it has high performance but it has poor flexibility and poor transportability, hence it is usually unable to meet the high requirements of the customer. With the rapid development of FPGA soft core plays an increasingly important role in embedded system depending on the high performance, high flexibility, transportability and configuration. Huimei Yuan, Junyou Yang and Peipei Pan presented new methodology that provide Optimized Design of UART IP Soft Core based on DMA Mode [3]. They provide UART IP soft core based on DMA mode. The IP core is AVALON bus-compatible with the control and arithmetic logic of entire IP core completed by a single FPGA chip so that it is very suited to NIOSII embedded system. Since the two kinds of transmission will often interrupt the operation of CPU during the data transmission process, especially when transmitting large data, it will occupy a lot of time of CPU, thus greatly reducing the performance of the overall NIOSII system. The whole IP core is tested and verified in a simple NIOSII embedded hardware system. It turns out that UART IP soft core based on DMA mode can reduce elapsed time of CPU greatly in data transmission process so that the performance of NIOSII system can be improved and design requirement can be better met with less resources occupied, high speed, high flexibility and high transportability. Researchers have undertaken

different design processes or phenomena with regards to use serial communication as it reduces signal distortion.

Naresh Patel, Vatsalkumar Patel and Vikaskumar Patel proposed design of UART with Status register [4] which includes three modules which are the baud rate generator, receiver and transmitter that satisfies the system requirements of high integration, stabilization, low bit error rate, and low cost. The work also supports configurable baud rate generator and variable data length from 5-8 bits per frame. This work detect the different types of errors occurred during communication and hence correct them. In recent year, a need of high speed UART might be the first demand in serial communication.

Hazim Kamal Ansari and Asad Suhail Farooqi introduces concept of high speed UART for programming FPGA [5]. They suggested that to maintain time triggered communication within FPGA a separate controller must be designed within it and this controller is called UART. FPGAs are suited to I/O intensive operations and it is very fast. Design Partitioning across the two devices can increase overall system speeds, reduce costs, and potentially absorb all of the other discrete logic functions in a design – thus presenting a truly reconfigurable system. They describe UART controller which is designed within FPGA based on SRAM with high speed and high reliability. The controller can be used to implement communications in complex system and it also can be used to reduce time delays between sub-controllers of a complex control system to improve the synchronization of each sub-controller. According to them, FPGAs are replacing convention programmable logic devices and within next few years they would be required at each and every application.

III. PROPOSED WORK

The UART serial communication module is divided into three sub-modules: the baud rate generator, receiver module and transmitter module Therefore, the implementation of the UART communication module is actually the realization of the three sub-modules as shown in fig.1.

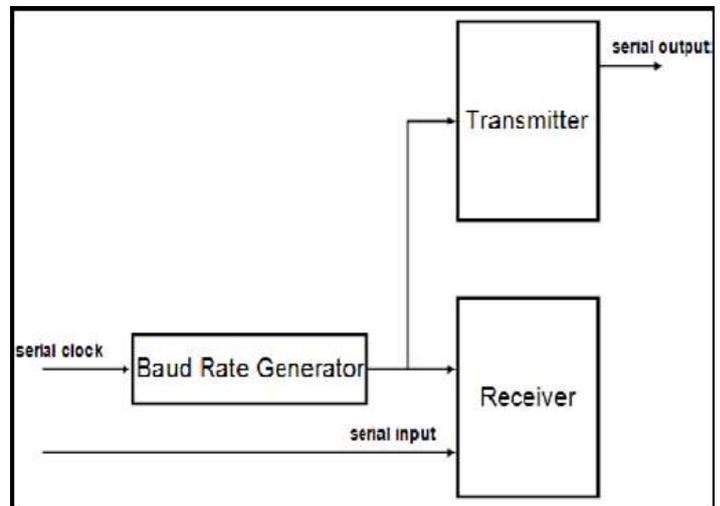


Fig. 1 UART Module

Proposed UART design consists of the three sub-modules of a UART which are the receiver, transmitter and baud rate generator that we called prescaler with internal first in first out

asynchronous buffer. Proposed design has internal buffers in both receiver and transmitter. Because design operates in serial clock domain and interfaces with parallel clock domain of the processor, we implement the buffers to provide smooth data transfer between two different clock domains. This UART design can operate at any defined serial clock frequency and at the same time follows the desired baud rate. Here is where the prescaler module comes in hand where it acts as a baud rate generator module that calculates the divider factor. The divider factor will then generate prescaler pulse that acts as a baud clock. The prescaler module is used in this design for the transmission and reception to be at the desired baud rate. Fig. 2 below shows the register transfer level (RTL) view of proposed baud rate generator which is sub-module of proposed design.

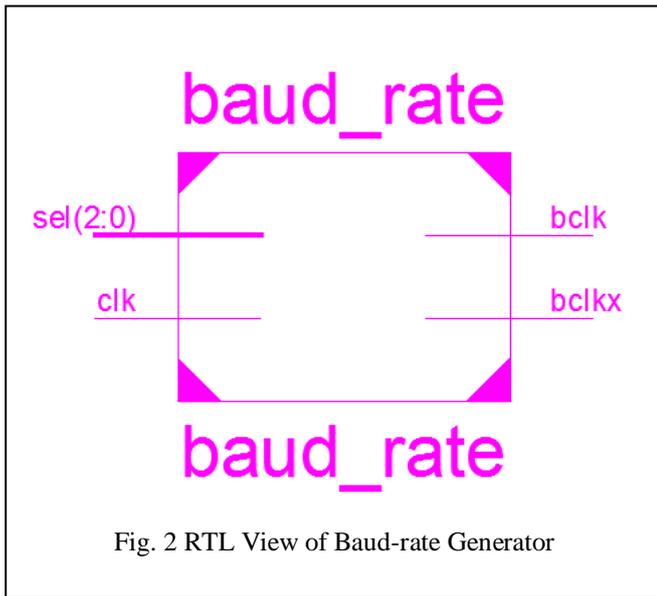


Fig. 2 RTL View of Baud-rate Generator

The serial clock is set to 100MHz and the desired baud clock rate is 1562500bps. The calculation to get prescaler divide ratio is shown below:

$$\text{Divide ratio} = \text{Serial clock frequency} / (16 * \text{Baud rate})$$

In serial data transmission, a huge stream of data can come in too fast and UART may not be quick enough to process what it is receiving. This causes data overrun which then results in data loss or other serious errors. This is why we need flow control in the UART where it will halt the flow of data bytes until UART is ready to receive more data. There are many ways to implement flow control mechanism. One of the older methods used back then is to add bunch of zeros while receiving line is busy. This method is called padding. UART will ignore the zeros while it processes current data. To make it efficient, we need to provide just enough number of zeros and figuring this out is not easy. Another method is to use RTS (Request to Send) and CTS (Clear to Send) flow control mechanism which is part of RS-232 standard. These two lines allow both sender and receiver to communicate and alert each other on their status. When sender has data to be sent, it will assert RTS to ask receiver whether it is ready to receive data or not. If receiver is free, it will reply by asserting CTS and

sender will start transferring data. But if receiver is busy, CTS line will maintain low and sender needs to halt the data and wait until CTS goes high. This method however requires additional wires to the UART design. Most UART nowadays has internal buffer with the size big enough to hold the data and that is less likely to overrun. The buffer can be set to interrupt the processor when the buffer reaches certain threshold level. In this paper, we are using this method to do flow control. Asynchronous FIFOs are being used as an internal TX buffer and RX buffer in transmitter and receiver module respectively. The asynchronous FIFO allows smooth data transmission between two different clock domains and provides reliable empty and full status [14-16].

During reception, receiver module writes the received data bytes into RX buffer using serial clock. When RX buffer is almost full, receiver will interrupt the processor to start reading the data (using parallel clock) before RX buffer starts to overflow. While in transmission, processor writes data into TX buffer using parallel clock. When there is at least one data byte inside TX buffer, transmitter will start reading the data in serial clock, process the data byte and transmit out serial bits. If TX buffer is almost full, an interrupt is sent to processor to halt writing into the buffer. The register transfer level view of designed asynchronous first in first out (FIFO) buffer is shown below in fig. 3.

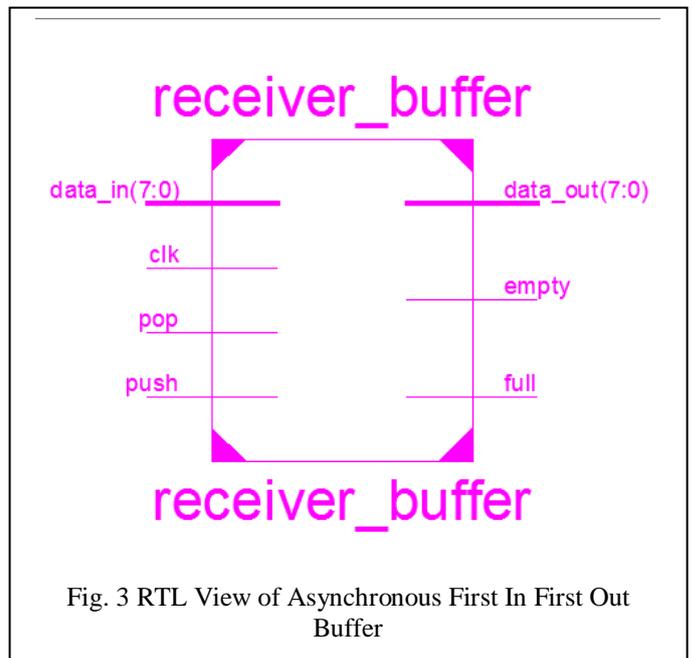


Fig. 3 RTL View of Asynchronous First In First Out Buffer

IV. SIMULATION RESULTS

In this paper, we have presented simulation results of prescaler i.e. baud rate generator which divides serial clock as per user requirement and asynchronous first in first out buffer for smooth data flow. Simulation result shows baud rate generator consists of two different clocks for receiver and transmitter. We can select different baud rate using select input which divides clock as per input given to sel signal. Fig. 4 shows simulation result of proposed baud rate generator with 100MHz frequency and division ratio of 4.

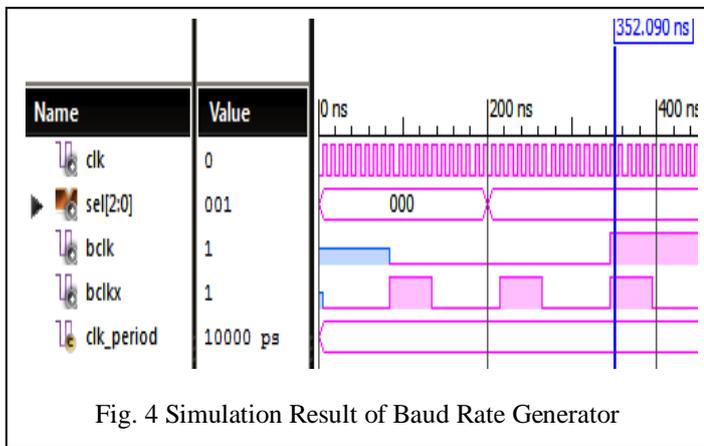


Fig. 4 Simulation Result of Baud Rate Generator

RELIABLE AND SECURE DATA TRANSMISSION CAN BE POSSIBLE USING PROPOSED SUB MODULE OF UART DESIGN. WITH ALL THE FEATURES STATED, IT ENHANCES FLEXIBILITY, STABILITY AND RELIABILITY TO THE NORMAL UART DESIGN THAT IS WIDELY BEING USED.

References

- [1] Mohd Yamani Idna Idris, Mashkuri Yaacob, Zaidi Razak, "A VHDL implementation of UART design with BIST capability" *Malaysian Journal of Computer Science*, Vol. 19 (1), 2006.
- [2] Shouqian Yu, Lili Yi ,Weiha Chen,Zhaojin Wen," Implementation of a Multi-channel UART Controller Based on FIFO Technique and FPGA" 1-4244-0737-0/07/\$20.00 c 2007 IEEE
- [3] Huimei Yuan, Junyou Yang,Peipei Pan," Optimized Design of UART IP Soft Core based on DMA Mode" 978-1-4244-5046-6/10/\$26.00 c 2010 IEEE.
- [4] Naresh patel, Vatsalkumar Patel and Vikaskumar Patel "VHDL Implementation of UART with Status Register" *2012 International Conference on Communication Systems and Network Technologies(IEEE)*.
- [5] Hazim Kamal Ansari, Asad Suhail Farooqi," Design Of High Speed Uart For Programming FPGA" *International Journal Of Engineering And Computer Science* Volume1 Issue 1 Oct 2012.
- [6] Nennie Farina Mahat, Member, IEEE, "Design of a 9-bit UART Module Based on Verilog HDL," *IEEE-ICSE2012 Proc., 2012*, Kuala Lumpur, Malaysia, 978-1-4673-2396-3/12/\$31.00 ©2012 IEEE.
- [7] J. Norhuzaimin, and H.H. Maimun, "The design of high speed UART," *Asia Pac. Conf. on Appl. Electromagnetics (APACE 2005)*, Johor, Malaysia, Dec. 2005.
- [8] C. He, Y. Xia, and L. Wang, "A universal asynchronous receiver transmitter design," *Int'l Conf. on Elect. Comm. and Control (ICECC 2011)*, Ningbo, China, Sept. 2011.
- [9] Y. Wang, and K. Song, "A new approach to realize UART," *Int'l Conf. on Elect. and Mech. Eng. and IT (EMEIT 2011)*, Harbin, Heilongjiang, China, Aug. 2011.
- [10] Using a 9-bit Software UART with Stellaris® Microcontrollers Application Note (AN01280), Texas Instruments, P.O. Box 655303, Dallas, Texas 75265, USA, Aug. 2010.
- [11] Zilog Z8 Encore! XP® 9-bit UART Implementation Application Note (AN014602-1207), Zilog Inc., Dec. 2007.
- [12] Z. Zhang, and W. Wu, "UART integration in OR1200 based SoC Design," *2nd Int'l Conf. on Comp. Eng. and Tech. (ICCET 2010)*, Chengdu, China, Apr. 2010.
- [13] Y. Fang, and X. Chen, "Design and simulation of UART serial communication module based on VHDL," *3rd Int'l Workshop on Intel. Sys. and App. (ISA 2011)*, Wuhan, China, May 2011.
- [14] C.E. Cummings, "Simulation and synthesis techniques for asynchronous FIFO design," *Synopsys User Group (SNUG), San Jose, USA, 2002*.
- [15] X. Wang, and J. Nurmi, "A RTL asynchronous FIFO design using modified micropipeline," *The 10th Biennial Baltic Elect. Conf. (BEC 2006)*, Tallinn, Estonia, Oct. 2006.
- [16] X. Wang, T. Ahonen, and J. Nurmi, "A synthesizable RTL design of asynchronous FIFO," in *Proc. Int'l Sympo. on SoC 2004*, Tampere, Finland, Nov. 2004.

Fig. 5 shows simulation result of internal asynchronous first in first out buffer for 8-bit input data. Here, different two clocks are used for writing and reading operation named wclk and rclk respectively. To enable read and write operation two inputs are used which are readen_in and writen_in respectively.

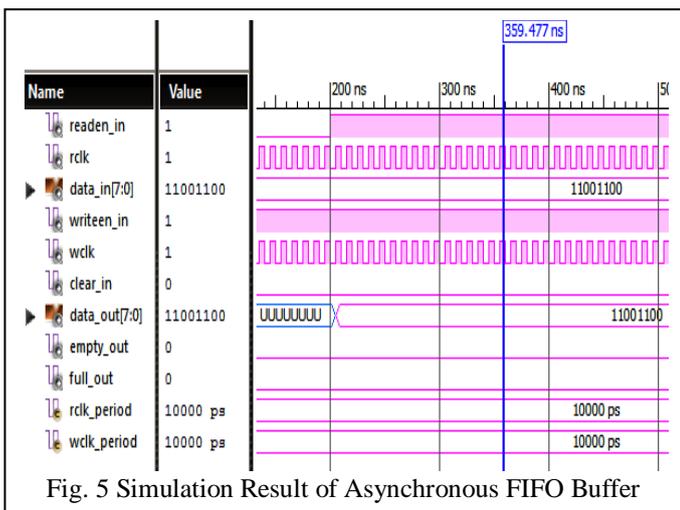


Fig. 5 Simulation Result of Asynchronous FIFO Buffer

V. CONCLUSION

IN THIS PAPER, A MODIFIED UART DESIGN IS PROPOSED WITH ADDITIONAL INTERNAL BUFFER AND PROGRAMMABLE BAUD RATE GENERATOR FOR SMOOTH DATA FLOW AND TO GET DESIRED BAUD RATE. THE SUB-MODULE OF UART DESIGN IS IMPLEMENTED USING VHDL AND SIMULATED AND SYNTHESIS OF SUB-MODULES TO SEE THE FUNCTIONALITY USING XILINX ISE 13.1 DESIGN SUITE. THIS DESIGN SHOWS THAT FAST,



Video Steganography Encoding MPEG-4 Part 10 VideoStreams By CodeWord Substitution

Shirin Khan

M.TECH Student

*Department of Electronics and Communication
Anjuman College of Engineering & Technology
Sadar, Nagpur*

Email ID: shirin.khan210@gmail.com

M T Hasan

Professor

*Department of Electronics and Communication
Anjuman College of Engineering & Technology
Sadar, Nagpur*

Email ID: mthasan21@gmail.com

Abstract—Now a days somewhere Digital video needs to be stored and processed in an encrypted format to maintain security and privacy. For this purpose, it is necessary to perform data hiding in these encrypted videos. In this way, data hiding in encrypted domain without decryption preserves the confidentiality of the content. In addition, it is more efficient without decryption followed by data hiding and re-encryption. In this paper, a novel scheme of data hiding directly in the encrypted version of H.264/AVC video stream is proposed, which includes the following three parts, i.e., H.264/AVC video encryption, data embedding, and data extraction. A data hider may embed additional data in the encrypted domain by using codeword substitution technique, without knowing the original video content. In order to adapt to different application scenarios, data extraction can be done either in the encrypted domain or in the decrypted domain. Furthermore, video file size is strictly preserved even after encryption and data embedding.

Keywords—Data hiding, encrypted domain, H.264/AVC, codeword substituting.

I. Introduction

CLOUD computing has become an important technology trend, which can provide highly efficient computation and large-scale storage solution for video data. Given that cloud services may attract more attacks and are vulnerable to untrustworthy system administrators, it is desired that the video content is accessible in encrypted form. The capability of performing data hiding directly in encrypted H.264/AVC video streams would avoid the leakage of video content, which can help address the security and privacy concerns with cloud computing. For example, a cloud server can embed the additional information (e.g., video notation, or authentication data) into an encrypted version of an H.264/AVC video by using data hiding technique. With the hidden information, the server can manage the video or verify its integrity without knowing the original content, and thus the security and

privacy can be protected. In addition to cloud computing, this technology can also be applied to other prominent application scenarios. For example, when medical videos or surveillance videos have been encrypted for protecting the privacy of the people, a database manager may embed the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain. The encryption is performed by using bit-XOR (exclusive-OR) operation.

With the increasing demands of providing video data security and privacy protection, data hiding in encrypted H.264/AVC videos will undoubtedly become popular in the future. Obviously, due to the constraint of the underlying encryption, it is very difficult and sometimes impossible to transplant the existing data hiding algorithms to the encrypted domain.

II. literature review

In this section we review various studies and development carried out by many researchers. We will also see various detection techniques.

[1] W. J. Lu, A. Varna, and M. Wu has proposed a work on “Secure video processing: Problems and challenges,” Secure signal processing is an emerging technology to enable signal processing tasks in a secure and privacy preserving fashion. It has attracted a great amount of research attention due to the increasing demand to enable rich functionalities for private data stored online. In this paper, discussion on the research issues and challenges in secure video processing with focus on the application of secure online video management. To be practical, secure video processing requires efficient solutions that may involve a trade-off between security and complexity.

[2] B. Zhao, W. D. Kou, and H. Li proposed a work on “Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol,” In most watermarking schemes for copyright protection, a seller usually embeds a watermark in multimedia content to identify a buyer. When an unauthorized copy is found by the seller, the traitor’s identity can be traced by the embedded watermark. In this paper, an enhanced watermarking scheme is presented.

[3] X. P. Zhang proposed a work on “Separable reversible data hiding in encrypted image,” This work proposes a novel scheme for separable reversible data hiding in encrypted images. In this a content owner encrypts the original uncompressed image using an encryption key. Then a data hider hide some additional data with the data hiding key, if receiver has both the data hiding key and the encryption key, he extract the additional data and recover the original image.

[4] Z. Shahid, M. Chaumont, and W. Puech proposed a work on video streams “Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames,” This paper presents a novel method for the protection of bitstreams of state of the art video codec H.264/AVC. The problem of selective encryption is addressed along with the compression in the entropy coding modules. H.264/AVC supports two types of entropy coding modules. Context-adaptive variable length coding (CAVLC) is support in H.264/AVC baseline profile and context-adaptive binary arithmetic coding (CABAC) is support in H.264/AVC main profile.

[5] Dawen Xu, Rangding Wang,& Yun Q Shi proposed a work that is “ Data hiding in encrypted H.264/AVC video streams by codeword substitution” Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. For the purpose of content notation and/or tampering detection, it is necessary to perform data hiding in these encrypted videos. In this way, data hiding in encrypted domain without decryption preserves the confidentiality of the content. In addition, it is more efficient without decryption followed by data hiding and re-encryption. In this, a novel scheme of data hiding directly in the encrypted version of H.264/AVC video stream is proposed.

III. CONCLUSION

Video steganography in encrypted media has started to draw attention because of the privacy-preserving requirements from cloud data management. In this paper, an algorithm to embed additional data in encrypted H.264/AVC bitstream is presented, which consists of video encryption, data embedding and data extraction phases. The algorithm can preserve the bit-rate exactly even after encryption and data embedding, and is simple to implement as it is directly performed in the compressed and encrypted domain, i.e., it does not require decrypting or partial decompression of the video stream thus making it ideal for real-time video applications. It is concluded that the proposed encryption and data embedding

scheme can preserve file-size, whereas the degradation in video quality caused by data hiding is quite small.

IV. REFERENCE

[1] W. J. Lu, A. Varna, and M. Wu, “Secure video processing: Problems and challenges,” in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.

[2] B. Zhao, W. D. Kou, and H. Li, “Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol,” *Inf. Sci.*, vol. 180, no. 23, pp. 4672–4684, 2010.

[3] X. P. Zhang, “Reversible data hiding in encrypted image,” *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[4] Z. Shahid, M. Chaumont, and W. Puech, “Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 5, pp. 565–576, May 2011.

[5] Dawen Xu, Rangding Wang,& Yun Q Shi, “ Data hiding in encrypted H.264/AVC video streams by codeword substitution”, *IEEE Trans. Inf. Forensics Security*, vol.9,No.4, pp.596- 606, Apr.2014.

[6] P. J. Zheng and J. W. Huang, “Walsh-Hadamard transform in the homo- morphic encrypted domain and its application in image watermarking,” in Proc. 14th Inf. Hiding Conf., Berkeley, CA, USA, 2012, pp. 1–15.

[7] W. Puech, M. Chaumont, and O. Strauss, “A reversible data hiding method for encrypted images,” *Proc. SPIE*, vol. 6819, pp. 68191E-1–68191E-9, Jan. 2008.

[8] W. Hong, T. S. Chen, and H. Y. Wu, “An improved reversible data hiding in encrypted images using side match,” *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.

[9] X. P. Zhang, “Separable reversible data hiding in encrypted image,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[10] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.

- [11] A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robust watermarking of compressed and encrypted JPEG2000 images," *IEEE Trans. Multimedia*, vol. 14, no. 3, pp. 703–716, Jun. 2012.
- [12] S. G. Lian, Z. X. Liu, and Z. Ren, "Commutative encryption and watermarking in video compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.
- [13] S. W. Park and S. U. Shin, "Combined scheme of encryption and watermarking in H.264/scalable video coding (SVC)," *New Directions Intell. Interact. Multimedia*, vol. 142, no. 1, pp. 351–361, 2008.
- [14] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560–576, Jul. 2003.
- [15] S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, "Secure advanced video coding based on selective encryption algorithms," *IEEE Trans. Consumer Electron.*, vol. 52, no. 2, pp. 621–629, May 2006.
- [16] M. N. Asghar and M. Ghanbari, "An efficient security system for CABAC bin-strings of H.264/SVC," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 3, pp. 425–437, Mar. 2013.
- [17] T. Stutz and A. Uhl, "A survey of H.264 AVC/SVC encryption," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 3, pp. 325–339, Mar. 2012.
- [18] *Advanced Video Coding for Generic Audiovisual Services*, ITU, Geneva, Switzerland, Mar. 2005.
- [19] J. G. Jiang, Y. Liu, Z. P. Su, G. Zhang, and S. Xing, "An improved selective encryption for H.264 video based on intra prediction mode scrambling," *J. Multimedia*, vol. 5, no. 5, pp. 464–472, 2010.
- [20] I. E. G. Richardson, *H.264 and MPEG-4 Video Compression: Video Coding for Next Generation Multimedia*. Hoboken, NJ, USA: Wiley, 2003.
- [21] D. K. Zou and J. A. Bloom, "H.264 stream replacement watermarking with CABAC encoding," in *Proc. IEEE ICME*, Singapore, Jul. 2010, pp. 117–121.
- [22] D. W. Xu and R. D. Wang, "Watermarking in H.264/AVC compressed domain using Exp-Golomb code words mapping," *Opt. Eng.*, vol. 50, no. 9, p. 097402, 2011.
- [23] D. W. Xu, R. D. Wang, and J. C. Wang, "Prediction mode modulated data-hiding algorithm for H.264/AVC," *J. Real-Time Image Process.*, vol. 7, no. 4, pp. 205–214, 2012.
- [24] T. Shanableh, "Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 455–464, Apr. 2012.



Research & Implementation of Gesture Spotting Techniques

Gaurav G. Sambhe

Department of M.Tech (VLSI Design)

Jhulelal Institute of Technology, Lonara, Nagpur

gauravsambhe@gmail.com

Abstract— Gesture recognition can be seen as a way for computers to begin to understand human body language, thus building a richer bridge between machines and humans than primitive text user interfaces or even GUIs (graphical user interfaces), which still limit the majority of input to keyboard and mouse. The applications of gesture recognition are manifold, ranging from sign language through medical rehabilitation to virtual reality, keeping in this mind we proposed a system, which will allow humans, to control the machines by simple human gesture.

Keywords—*Gesture Spotting, Gesture Recognition, Pattern Recognition, Computer Vision.*

I. INTRODUCTION

Gesture recognition is a topic of modern technology with the goal of interpreting human gestures via mathematical algorithms. Reliable and natural human-robot interaction is a subject that has been extensively studied by researchers in the last few decades. Nevertheless, in most of cases, human beings continue to interact with robots recurring to the traditional process. Probably, this is because these “more natural” interaction modalities have not yet reached the desired level of maturity and reliability.

Gestures are one of the most important modes of communicating with computer in an interactive environment. Recent advances in computer vision and machine learning have led to a number of techniques for modeling gestures in real-time environment. Gestures can originate from any bodily motion or state but commonly originate from the face or hand. Human motion recognition is a field with a wide variety of applications. Of particular interest is gesture recognition for new modes of human-computer interaction, and gait recognition for video surveillance systems and intrusion detection.

It is very common to see a human being explaining something to another human being using hand gestures. Making an analogy, and given our demand for natural human-robot interfaces, gestures can be used to interact with machines in an intuitive way.

Recent research in gesture spotting (gesture segmentation plus gesture recognition) aimed at applications in many different fields, such as sign language (SL) recognition, electronic appliances control, video-game control and human-computer/robot interaction. The development of reliable and

natural human-robot interaction platforms can open the door to new robot users and thus contribute to increase the number of existing robots.

II. GESTURE ONLY INTERFACES

The gestural equivalent of direct manipulation interfaces is those which use gesture alone. These can range from interfaces that recognize a few symbolic gestures to those that implement fully fledged sign language interpretation. Similarly interfaces may recognize static hand poses, or dynamic hand motion, or a combination of both. In all cases each gesture has an unambiguous semantic meaning associated with it that can be used in the interface.

A. Tracking Technologies

Gesture only interfaces with syntax of many gestures typically require precise hand pose tracking. A common technique is to instrument the hand with a glove which is equipped with a number of sensors which provide information about hand position, orientation, and flex of the fingers.

B. Natural Gesture Only Interfaces

At the simplest level, effective gesture interfaces can be developed which respond to natural gestures, especially dynamic hand motion

III. GESTURE TYPES

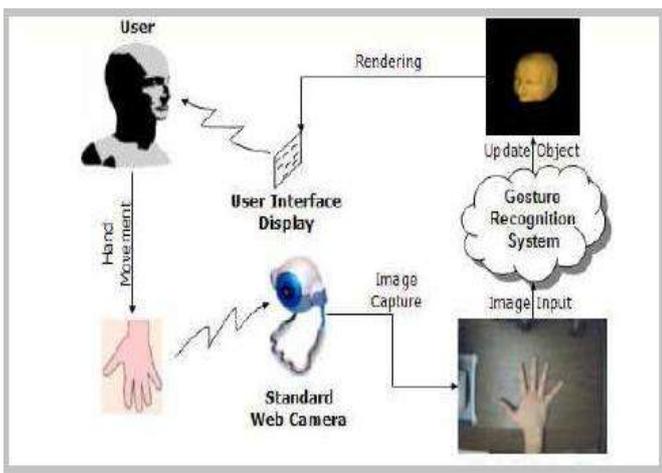
In computer interfaces, two types of gestures are distinguished:

- a. **Offline gestures:** Those gestures that are processed after the user interaction with the object. An example is the gesture to activate a menu.
- b. **Online gestures:** Direct manipulation gestures. They are used to scale or rotate a tangible object.

A. Types of Gestures

- 1) **Gesticulation:** Spontaneous movements of the hands and arms that accompany speech.
- 2) **Language-like gestures:** Gesticulation that is integrated into a spoken utterance, replacing a particular spoken word or phrase.
- 3) **Pantomimes:** Gestures that depict objects or actions, with or without accompanying speech.
- 4) **Emblems:** Familiar gestures such as V for victory, thumbs up, and assorted rude gestures.
- 5) **Sign languages:** Linguistic systems, such as American Sign Language, which are well defined.

IV. SYSTEM ARCHITECTURE



Here we can see that the user action is captured by a camera and the image input is fed into the gesture recognition system, in which it is processed and compared efficiently with the help of an algorithm. The virtual object or the 3-d model is then updated accordingly and the user interfaces with machine with the help of a user interface display.

V. USES

Gesture recognition is useful for processing information from humans which is not conveyed through speech or type. As well, there are various types of gestures which can be identified by computers.

- 1) **Sign language recognition:** Just as speech recognition can transcribe speech to text, certain types of gesture recognition software can transcribe the symbols represented through sign language into text.
- 2) **For socially assistive robotics:** By using proper sensors (accelerometers and gyros) worn on the body of a patient and by reading the values from those sensors, robots can assist in patient rehabilitation. The best example can be stroke rehabilitation.

- 3) **Directional indication through pointing:** Pointing has a very specific purpose in our society, to reference an object or location based on its position relative to ourselves. The use of gesture recognition to determine where a person is pointing is useful for identifying the context of statements or instructions. This application is of particular interest in the field of robotics.
- 4) **Control through facial gestures:** Controlling a computer through facial gestures is a useful application of gesture recognition for users who may not physically be able to use a mouse or keyboard. Eye tracking in particular may be of use for controlling cursor motion or focusing on elements of a display.
- 5) **Alternative computer interfaces:** Foregoing the traditional keyboard and mouse setup to interact with a computer, strong gesture recognition could allow users to accomplish frequent or common tasks using hand or face gestures to a camera.
- 6) **Immersive game technology:** Gestures can be used to control interactions within video games to try and make the game player's experience more interactive or immersive.
- 7) **Virtual controllers:** For systems where the act of finding or acquiring a physical controller could require too much time, gestures can be used as an alternative control mechanism. Controlling secondary devices in a car or controlling a television set are examples of such usage.
- 8) **Affective computing:** In affective computing, gesture recognition is used in the process of identifying emotional expression through computer systems.
- 9) **Remote control:** Through the use of gesture recognition, "remote control with the wave of a hand" of various devices is possible. The signal must not only indicate the desired response, but also which device to be controlled.

VI. CHALLENGES

There are many challenges associated with the accuracy and usefulness of gesture recognition software. For image-based gesture recognition there are limitations on the equipment used and image noise. Images or video may not be under consistent lighting, or in the same location. Items in the background or distinct features of the users may make recognition more difficult.

Gesture Recognition Challenges:

- 1) **Latency:** Image processing can be significantly slow creating unacceptable latency for video games and other similar applications.
- 2) **Lack of Gesture Language:** Different users make gestures differently, causing difficulty in identifying motions.

- 3) **Robustness:** Many gesture recognition systems do not read motions accurately or optimally due to factors like insufficient background light, high background noise etc.
- 4) **Performance:** Image processing involved in gesture recognition is quite resource intensive and the applications may found difficult to run on resource constrained devices.

VII. CONCLUSION

This paper proposes robust methods for hand gesture spotting and recognition. A method for real-time and continuous hand gesture spotting has been presented. Our methods perform the hand gesture spotting and recognition tasks simultaneously. Furthermore, they are suitable for real-time applications and solve the issues of time delay between the spotting and the recognition tasks.

Acknowledgment

I would like to express sincere gratitude and appreciation to all those who gave me the possibility to complete this paper. A special thanks to my Project Guide Prof. (Mr.) Nakul Nagpal, Whose help, stimulating suggestions and encouragement, helped to coordinate project especially in writing this paper. Words often fail to pay one's gratitude oneself, still we would like to convey sincere thanks to our H.O.D Prof. (Mr.) Sanjeev Sharma , without whose encouragement and guidance this project would not have materialized.

References

- [1] S. Mitra and T. Acharya, "Gesture recognition: a survey," *IEEE Trans. Systems, Man Cybernetics*, vol. 37, no. 3, pp. 311–324, 2007.
- [2] H. Francke, J. R. del Solar and R. Verschae, "Real-time hand gesture detection recognition using boosted classifiers and active learning," in *Proc. Pacific Rim Adv. Image and Video Tech.*, 2007, pp. 533–547.
- [3] T. Kirishima, K. Sato and K. Chihara, "Real-time gesture recognition by learning and selective control of visual interest points," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 27, no. 3, pp. 351–364, 2005.
- [4] D. Weinland, R. Ronfard and E. Boyer, "Free viewpoint action recognition using motion history volumes," *Computer Vision and Image Understanding*, vol. 104, no. 2/3, pp. 249–257, 2006.
- [5] I. Mihara, Y. Yamauchi and M. Doi, "A real-time vision-based interface using motion processor and applications to robotics," *Systems and Computers in Japan*, vol. 34, no. 3, pp. 10–19, 2003.
- [6] G. Lalit and M. Suei, "Gesture-based interaction and communication: automated classification of hand gesture contours," *IEEE Trans. Systems, Man and Cybernetics*, vol. 31, no. 1, pp. 114–120, 2001.
- [7] J. Yang, W. Bang, E. Choi, S. Cho, J. Oh, J. Cho, S. Kim, E. Ki and D. Kim, "A 3D hand-drawn gesture input device using fuzzy ARTMAP-based recognizer," *J. of Systemics, Cybernetics and Informatics*, vol. 4, no. 3, pp. 1–7, 2006.
- [8] Y. Yamashita and J. Tani, "Emergence of functional hierarchy in a multiple timescale neural network model: a humanoid robot experiment," *PLoS Comput. Biol.*, vol. 4, no. 11, pp. 1–17, 2008.
- [9] B. Peng and G. Qian, "Online gesture spotting from visual hull data," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 33, no. 6, pp. 1175–1188, 2011.
- [10] H. H. Avilés, W. Aguilar and L. A. Pineda, "On the selection of a classification technique for the representation and recognition of dynamic gestures," in *IBERAMIA 2008*, H. Geffner et al., Ed. Berlin-Heidelberg: Springer, 2008, pp. 412–421.
- [11] H. D. Yang, S. Sclaroff and S. W. Lee, "Sign language spotting with a threshold model based on conditional random fields," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 31, no. 7, pp. 1264–1277, 2009.

Efficient Electricity Management System Using Power Factor Correction Method Based on ARM Cortex

Vikrant Chhapekar, M.Tech
Department of Electronics Engineering,
Jhulelal Institute of Technology, Lonara, Nagpur, India
vickychhapekar@gmail.com

Abstract---With the continuous rise in the demand and cost of energy, increased power efficiency and quality is very desirable. Power quality can be fairly increased through Power Factor Correction (PFC). In this paper aims to build a simple, compact and energy-efficient system for automatic power factor monitoring and control. This proposed solution based on ARM -Cortex. The use of ARM based 32-bit microcontroller promises for complete power management unit. Apart from lower power consumption, it allow easy extension of functionalities from power data logging, remote monitoring and control, emergency alarm etc.

Keywords-Efficient Electricity Management System Using Power Factor Correction, PFC ARM Cortex.

I. INTRODUCTION

As we see that electricity is playing most important role everywhere like industries, home appliances are utilised more power but electricity is limited sources so we have to utilise it wisely. Due to this limited source we have to face many problems so we need to find some solution so we can avoid electricity scarcity problem. This paper proposed a solution which can be solve the problem electricity using Power Factor Correction (PFC). Power factor is playing very vital role in electricity distribution and utilisation process. A compact and efficient system for power factor control and power management can be very useful in industries with high inductive loads. Its use can be extended to within a building or a single machine or appliances. Embedded technology is one of the biggest boons to mankind. Its use greatly reduces Manpower, saves time and space. Moreover, it increases efficiency without human interference and can incorporate built-in intelligence. So, embedded technology is incorporated for a compact and efficient power management system. Power Factor is defined as the ratio of the real power delivered to the load to the apparent power. It is a direct measure of the power quality. In an electric power system, a load with a low power factor draws more current than a load

with a high power factor for the same amount of useful power transferred. The higher currents increase the energy lost in the distribution system, and require larger wires and other equipment. Because of the costs of larger equipment and wasted energy, electrical utilities usually charge a higher cost to industrial or commercial customers where there is a low power factor. Poor power factor costs our community in increased electricity charges and unnecessary greenhouse gases. While some countries provide incentives for customers to maintain the required power factor, some impose penalties for power factor dropping beyond a limit. Thus, power factor control is a vital part of efficient power management.

II. TECHNICAL BACKGROUND

The power factor correction is necessary using we can see that using power factor correction we can improve the system efficiency and also increased power handling capacity using.

A. What is Power Factor

Power factor is the ratio of Active Power (KW) to Apparent Power (KVA). Where, KW is Working Power or Active Power or Real Power, KVAR is Reactive Power, KVA is Apparent Power. It is the "vectorial summation" of KVAR and KW.

B. Dragging Mac's Analogy

Let us understand What Causes Low Power Factor why should we improve power factor in detail. Take an example of Dragging Mac's BMI Analogy (Figure 1). Here we can see that Mac dragging a heavy load in forward direction lets Mac working power is KW. But his shoulder height adds little Reactive Power i.e. KVAR. Apparent power of Mac dragging load is vectorial summation of KW & KVAR. From the Dragging Mac's BMI Analogy a Power Triangle is formed.

Dragging Mac's BMI Analogy

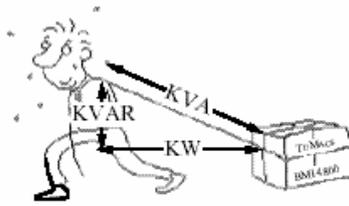
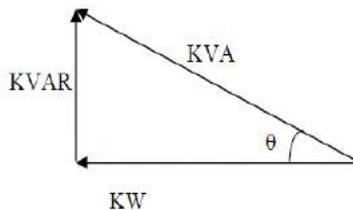


Figure 1



$$\text{P.F.} = \frac{\text{KW}}{\text{KVA}} = \cos \theta$$

$$\frac{\text{KVAR}}{\text{KVA}} = \sin \theta$$

$$\text{KVA} = \sqrt{\text{KW}^2 + \text{KVAR}^2} = \text{KV} * \text{I} * \sqrt{3}$$

Above power triangle represent what is power factor cosine θ . From that we can better understand the significance of power factor correction.

III.OBJECTIVE

The main objective of this project to power factor correction by reducing the effect of reactive power in apparent power.

A. Causes of Low Power Factor

Power Triangle shows the power factor cosine θ , so the lowering power factor is due to Reactive power KVAR. KVAR increases the amount of apparent power (KVA) in your distribution system. As increase in reactive and apparent power results in a larger angle θ , as θ increases, cosine θ (or power factor) decreases.

B. Necessity to Improve Power Factor

By lowering the utility bill by reducing peak KW billing demand & eliminating the power factor penalty, in your electricity system if you want to increase in system capacity and reduced system losses power factor must improve. Increase voltage level in your electrical system and cooler, more efficient motor.

C. Way to Improve Power Factor

The main reason for lower power factor is Sources of Reactive Power (inductive loads) like Transformer, Induction motors, Induction, generators (wind mill generators), High intensity discharge (HID) and lighting. Thus for the Power Factor Correction we have to add Capacitors in to the system and improve lowering power factor. By adding equal and opposite effect of capacitor (capacitive reactance) in against of inductive effect (inductive reactance) so both the effect cancel each other. The effect of reactive power get reduces and hence power factor get improve.

IV.METHODOLOGY

The power factor correction its proposed block diagram as shown in figure 2 below. As we can see in block diagram the heart is ARM-cortex which performs the complete operation switching, monitoring, calculation etc. The power factor meter is present which giving continues data of how much power factor lowered to ARM. A set of relays are present which switches the capacitors according to instructions of ARM. Capacitor bank which provide for reduce in reactive power which is applied to a load in parallel. Monitor displays the current, voltage, energy, power factor etc.

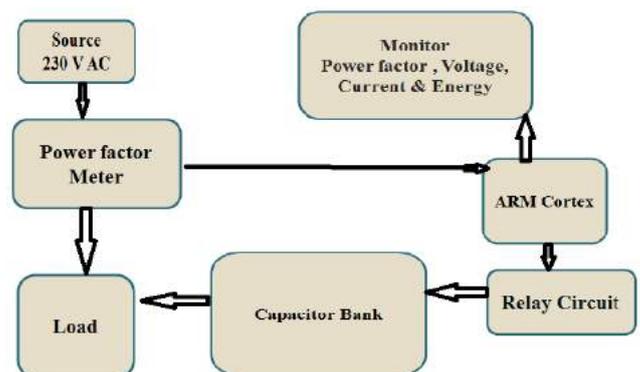


Figure 2

As we see in figure 2 the 230V AC supply going towards load through Power Factor Meter. Due to Reactive Power (KVAR) in load the power factor get lower, this information fed to ARM by Power Factor Meter. ARM first display the information about power factor on monitor. ARM calibrates the desire power factor by using Capacitor Bank. ARM is giving instruction to Relay Circuit, relay switches the capacitor which connected to the load and it can compensate the reactive power in the load. So this

capacitors helps to improve the lowering power factor of the system successfully.

V. USES

The power factor correction it can be used in real time application in industries home appliances anywhere because mostly electrical parts contains inductive loads so there is chances of reduction in power factor . So improvement is necessary for effective utilisation of electricity without losses we have to use this method.

VI. CONCLUSION

As we see in this proposed solution what are the necessities and causes of power factor reduction, so power factor have to improve because it directly affects system efficiency. Power factor correction drives the system efficiently with low losses and hence its better solution in cost wise. Furthermore we are trying to make this solution more accuracy and compact user friendly.

Acknowledgment

I would like to express sincere gratitude and appreciation to all those who gave me the possibility to complete this paper. A special thanks to my Project Guide Dr. (Mr.) Pramod Patil, Whose help, stimulating suggestions and encouragement, helped to coordinate project especially in writing this paper. Words often fail to pay one's gratitude oneself, still we would like to convey sincere thanks to our H.O.D Prof. (Mr.) Sanjeev Sharma , without whose encouragement and guidance this project would not have materialized.

REFERENCES

- [1] P. N. Enjeti and R. Martinez, "A high performance single phase rectifier with input power factor correction," IEEE Trans. Power Electron., vol. 11, No. 2, Mar. 2003, pp. 311-317
- [2] A. Fernandez, J. Sebastian, M. M. Hernando, P. Villegas, and J. Garcia, "Helpful hints to select a power-factor-correction solution for low- and medium-power single-phase power supplies," IEEE Trans. Ind. Electron., vol. 52, no. 1, pp. 46-55, Feb. 2005.
- [3] A. Prodic, "Compensator design and stability assessment for fast voltage loops of power factor correction rectifiers," IEEE Trans. Power Electron., vol. 22, no. 5, pp. 1719-1730, Sep. 2007.
- [4] H.Y. Kanaan and K. Al-Haddad, "Averaged Model Based Control of a Sheppard-Taylor PFC with Nonlinearity Compensation", inproc. CCECE 2007, 22-26 April 2007, pp. 1006-1009
- [5] D. G. Lamar, A. Fernandez, M. Arias, M. Rodriguez, J. Sebastian, and M. M. Hernando, "A unity power factor correction preregulator with fast dynamic response based on a low-cost microcontroller," IEEE Trans. Power Electron., vol. 23, no. 2, pp. 635-642, Mar. 2008
- [6] D. D.-C. Lu, H. H.-C. Lu, and V. Pjevalica, "A single-stage AC/DC converter with high power factor, regulated bus

voltage, and output voltage," IEEE Trans. Power Electron., vol. 23, no. 1, pp. 218-228, Jan. 2008.

- [7] D.G. Lamar, J. Sebastian, A. Rodriguez, M. RodriguezGonzalez, and M. M. Hernando, "A very simple control strategy for power factor correctors driving high-brightness LEDs," IEEE Trans. Power Electron. vol. 24, no. 8, pp. 2032-2042, Aug. 2009
- [8] D.G.Lamar, J. Sebastian, M. Arias, and A. Fernandez, "On the limit of the output capacitor reduction in power-factor correctors by distorting the line input current," IEEE Trans. Power Electron., vol. 27, no. 3, pp. 1168-1176, Mar. 2012.
- [9] ARM® Cortex™-M3 Stellaris Guru Development Kit Manual, Centre for Electronics Design and Technology, NetajiSubhas Institute of Technology.
- [10] F. Corrêa Alegria, A. Cruz Serra, « Gaussian Jitter-Induced Bias of Sine Wave. Amplitude Estimation Using Three-Parameter Sine Fitting », IEEE Transactions on Instrumentation and Measurement, vol.59, No. 9 pp.2328-2333, September 2010.

Review on AES -512 Algorithm for Communication Network

Ankit Dandekar

*Research Scholar, Department of Electronics and
Communication Engineering,
AbhaGaikwadPatil College of Engineering
Nagpur, India
E-mail: dandekar.ankit@gmail.com
Contact No.: +91-9021376326*

SagarPradhan

*Assistant Professor, Department of Electronics and
Communication Engineering,
AbhaGaikwadPatil College of Engineering
Nagpur, India
E-mail: sp8728@outlook.com
Contact No.: +91-8888898596*

Abstract—In computer networks increasing need of data protection led to the development of several cryptographic algorithms, hence it is critically important for sending data securely over a transmission link in many applications. Since for the declaration, Advance Encryption Standard (AES) has been subject to different Differential fault analysis (DFA) attacks and many of these attacks targets the AES with 128-bit key. DFA finds the key of a block cipher using differential information between correct and faulty cipher texts obtained by inducing faults during the computation of cipher texts. Among many ciphers, AES is the main target of DFA due to its popularity. This paper consists of an updated version of the AES algorithm with efficient utilization of resources such as memory and processor. The new algorithm AES- 512 consists of input block of 512 bit and key 512 bit. Due to this outline it becomes more resistant to linear and differential cryptanalysis which provides high security and throughput by consuming less memory and processor.

Keywords—*Differential Fault Analysis (DFA), AES- 512*

I. INTRODUCTION

Cryptography allows us to carry over the confidence found in the physical world to the electronic world. Since the amount of sensitive data being transmitted over an open environment the importance of cryptography is constantly increasing. The more information that is transmitted in computer-readable form, the more vulnerable it becomes to automated spying. Encryption is usually done just before sending data. To utilize the channel resources completely encryption algorithm should have a speed at least equivalent or same to data transmission speed. It is a challenging task to achieve high throughput for encryption algorithm for a communication channel of high data rate. We can easily find cryptographic hardware devices such as smart cards everywhere in our daily lives from

banking cards to subscriber identity module (SIM) cards for global system for mobile (GSM) communications.

The main reasons why these cryptographic hardware devices are widely used is that they are believed to be tamper-resistant. This is why they host the implementation of many

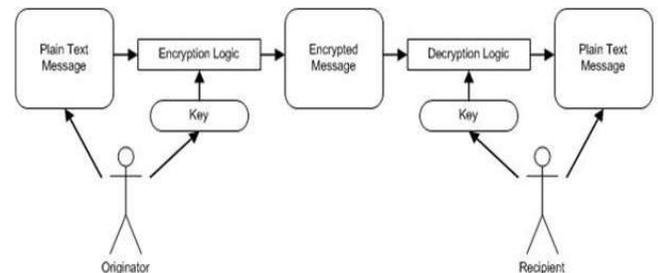


Fig. 1. Simple model for cryptographic algorithms.

cryptographic protocols. However, recent development of physical attacks shows that a naive implementation of cryptographic protocols does not provide security anymore. In practice, algorithms have to be implemented on real physical devices that are vulnerable to side-channel attacks like timing attacks, power attacks or electromagnetic attacks and fault attacks.

DFA is one of the fault attacks used to break block ciphers using differential information between correct and faulty cipher texts. An attacker gets faulty cipher texts by giving external impact on a device with voltage variation, glitch, and laser. The first DFA presented by Biham and Shamir in 1997 targeted DES. Afterward many people tried to break several cryptosystems such as Triple-DES and MacGuffin. DFA on AES can be split into two categories depending on the fault location: the DFA on the State and the DFA on the Key Schedule.

Furthermore, research on DFA has been diversified into several directions: reducing the number of required faults, changing fault models (from one-byte fault model to multi-byte fault model and vice versa), extending to AES-192 and AES-256, and exploiting faults induced at an earlier round. The first direction has been most actively researched because the attacker can perform the attack more easily as the required number of faults decreases. Piret and Quisquater showed that two faults induced on the AES State are sufficient to find the AES-128 key in a one-byte fault model.

TABLE I. NUMBER OF ROUNDS

Version	Number of Rounds
AES-128	10
AES-192	12
AES-256	14
AES-512	22

II. LITERATURE SURVEY

[1]. The paper presents that DFA finds the key of a block cipher using differential information between correct and faulty cipher texts obtained by inducing faults during the computation of cipher texts

[2]. The paper presents that presented clockwise collision analysis on non-protected AES hardware implementation

[3]. The paper shows comparison with published AES cipher implementations on general purpose processors, design has 3.5-15.6 times higher throughput per unit of chip area and 8.2-18.1 times higher energy efficiency

[4]. The paper presents the hardware implementation of AES algorithm using Xilinx-virtex5 Field Programmable Gate Array (FPGA).

III. PRESENT SYSTEM

Previously many hardware implementation were proposed and was implemented they are 128,192,256 bit. There various implementation for AES support the fact that different application required different implementation for the same algorithm. Some application has strict area requirement and a compact AES implementation will be very useful to provide security as in the some embedded system cases. On the other side, some application highly needed the most level of security that can be obtained without carrying about the area /time limitation.

The proposed method has several advantages

- 1) To avoid the attacker.
- 2) Secrecy of the data should be maintained.
- 3) The original secret data can be retrieved in totality.
- 4) Tremendous increase in throughput.

- 5) Reducing computation time.

The main problems that arise in existing encryption process are with respect to time it takes for computation and security level. This problem that arises in communication network is overcome by choosing those ciphers which preferably takes lesser amount of computational time so that speed is increased with better security.

IV. SYSTEM METHODOLOGY

AES can encrypt and decrypt 512-bit blocks with 128, 192 or 256-bit keys. The intermediate computation result of AES, called state, is usually represented by a 4*4 matrix, where each cell represents a byte. In encryption algorithm each round function is composed of four transformations except the last round:

- Sub Bytes
- Shift Rows
- Mix Columns
- AddRoundKey

The last round is lacking MixColumns. The first nine rounds of the decryption algorithm are governed by the following four stages:

- Inverse Shift rows
- Inverse Substitute Bytes
- Add round key
- Inverse Mix columns

Again the tenth round Inverse Mix columns stage is not included. The Overall flow of the encryption and encryption algorithm of the AES algorithm is show in Figure 2.

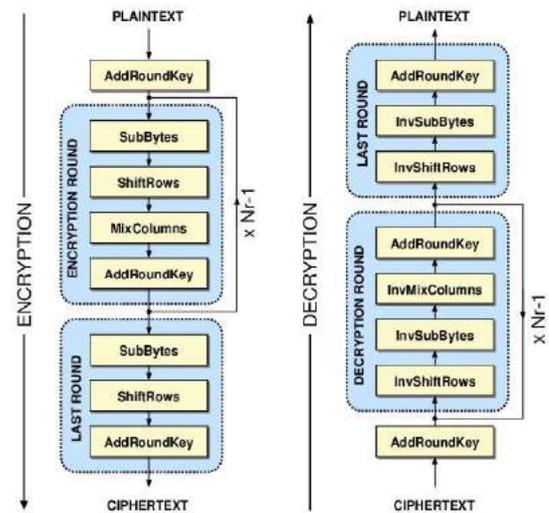


Fig. 2. Design flow of AES Algorithm for Encryption and Decryption Process.

Therefore, we expect that the key scheduling process as well as encryption process should be protected against fault

attacks and the larger key size make the algorithm more secure, and the larger input block increases the throughput.

Title of paper	Name of Author	Name of Journal /Year/ISSN No./Volume Number	Proposed Concept and Details
	Sanap		

REFERENCES

V. REVIEW SCRUTINY

TABLE II. REVIEW FROM VARIOUS RESEARCHERS

Title of paper	Name of Author	Name of Journal /Year/ISSN No./Volume Number	Proposed Concept and Details
Improved Differential Fault Analysis on AES Key Schedule	Chong Hee Kim	IEEE Transactions On Information Forensics And Security, Vol. 7, No. 1, February 2012	This paper deals with DFA on AES Key Schedule. Here it introduce new attacks that find the AES-128 key with two faults in a one-byte fault model without exhaustive search and the AES-192 and the AES-256 keys with six and four faults, respectively.
Fault Rate Analysis: Breaking Masked AES Hardware Implementations Efficiently	An Wang, Man Chen, Zongyue Wang and Xiaoyun Wang	IEEE Transactions On Circuits And Systems, 2013 IEEE.	We have proposed a new side-channel collision attack on masked AES based on the fault rate when injecting a clockglitch into the S-box circuit.
AES Algorithm Using 512 Bit Key Implementation for Secure Communication	Rishabh Jain, Rahul Jejurkar, Shrikrishna Chopade, Someshwar Vaidya, Mahesh	International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.	The paper consists of a new version of the advanced encryption standard algorithm with efficient utilization of resources such as processor and memory.

- [1] Chong Hee Kim, "Improved Differential Fault Analysis on AES Key Schedule" IEEE Transactions On Information Forensics And Security, Vol. 7, No. 1, February 2012
- [2] An Wang, Man Chen, Zongyue Wang and Xiaoyun Wang "Fault Rate Analysis: Breaking Masked AES Hardware Implementations Efficiently" IEEE Transactions On Circuits And Systems, 2013 IEEE.
- [3] M.Sambasiva Reddy, Mr. Y. Amar Babu, "Evaluation Of Microblaze and Implementation Of AES Algorithm using Spartan-3E" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013.
- [4] Rishabh Jain, Rahul Jejurkar, Shrikrishna Chopade, Someshwar Vaidya, Mahesh Sanap "AES Algorithm Using 512 Bit Key Implementation for Secure Communication" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.
- [5] S.Radhika, A.ChandraSekar , "AES Algorithm Using 512 Bit Key Implemented For Secure Communication", GJCST, Vol. 10 ,2010M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
- [6] Joan Daemen and Vincent Rijmen, "A Specification for Rijndael, the AES Algorithm", Dr. Brian Gladman, v3.1, 2001.
- [7] J. Daemen and V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard", 2009.
- [8] Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar "FPGA Implementation of AES Encryption and Decryption" International Conference on Control, Automation, Communication and Energy conservation -2009.
- [9] National Institute of Standards and Technology, "Federal Information Processing Standard Publication 197, the Advanced Encryption Standard (AES)," Nov. 2001.
- [10] AbidalrahmanMoh'd, Yaser Jaraweh, "AES-512: 512-Bit Advanced Encryption Standard Algorithm Design and Evaluation" International Conference on Information Assurance and Security (IAS) ,2011.
- [11] Sagar Paddhan, Mrs. Padma Lohiya, Sudhir N. Shelke, "AES-256 Encryption for Secured Communication".



Review on a Real Time Design and Implementation of Walking Quadruped Robot for Environmental Monitoring

Ritesh Waghe

*PG Student Department of ECE
Abha Gaikwad-Patil College of Engineering
Nagpur, India
riteshwaghe@gmail.com
Contact number: - +91 7588425498*

Rahul Godghate

*Ass. Professor Department of ECE
Abha Gaikwad-Patil College of Engineering
Nagpur, India
rahul.godghate@gmail.com
Contact number: - +91 8554986452*

Abstract—Four-legged robots also referred to as quadruped or a quadpods, can have very complex locomotion patterns and it provide the means of moving on surface where wheeled robots might fail. This conceptual shows usage of different creeping walks to accomplish synchronized development of the robot. The objective of this project is to develop a reliable platform that enables the implementation of stable and fast static/dynamic walking on even or uneven terrain. This also consisting of a different types of sensors embedded on it for detecting a real time status of the environmental condition and transmit it to the base station using wireless module.

Keywords—quadruped, locomotion, terrain, gaits

I. INTRODUCTION

In many cases, there is a requirement for mobile platforms that can move in areas with difficult landscape conditions where wheeled vehicles can't travel. Samples of such situations can be found in search and salvage task, and in addition in conveying payloads. Not at all like wheeled robots, walking robots are described by great portability in unpleasant territory. The primary objective of this paper is to show an inventive, modular and reasonable design of a four-legged robot for environmental research purposes.

The objective is to create a cheap legged platform, which allows research and testing of walking chassises and monitoring environmental conditions. The robot should either be driven from the base station or remote location that should send all available data from sensors, which will be displayed on the computer in the user interface program. It is also important to create and program a system into the microcontroller unit (MCU) of the robot, which would have the capacity to control the servomotors and sensors.

A. Why legged robot ?

Today's era is of robotics. One of the most important part of a robot is its chassis. There are several basic robot types: wheeled, tracked and legged robot. Wheeled robots are fast, but not suitable for rough area. Tracked robots are slower, but more suitable to rugged area. Legged robots are slow, much difficult to control but extremely powerful in rough area. Legged robots are capable to cross large holes and can operate even after losing a leg. Many researches were performed in this field in past few years, because of its large potential. Legged chassises are especially ideal for space missions. There are also several projects in military research.

Legs have unmistakable points of interest over wheels. The biggest advantage is in transvers ability and proficiency. Legged robot has a unique ability to

- Isolate their body from territory abnormalities
- Avoid undesirable foothold
- Regulate their stability
- Achieve energy efficiency

These advantages are very desirable in modern robotics, and therefore a lot of research is being put into creating robots that can walk.

II. CHARACTERISTICS OF LEGGED ROBOT

This part is focuses on several characteristics of walking robots. Some classifications of walking robots and most common walking gaits are described

A. Classification of walking robot

There are many ways to define walking robots

- By a body shape

- Number of legs
- Number of degrees of freedom per leg
- Locomotion technique.

To achieve many different configurations various options can be combined. By body shape they can be classified into two categories: Mammal and Spider.

At least two degrees of freedom are needed to construct a walking robot – first for lifting the leg, second for rotating it. Nevertheless, for a good functioning robot there should be three degrees of freedom, because the legs move along a circle and the forward movement of the body causes slipping between the foot and the surface, which can be compensated by third joint.

Walking chassis movement can be divided into statically stable and dynamically stable. Static stability represents the ability of the chassis that can remain in a stable position in every moment of movement. Static stability is typical for quadruped that is always stable during its movement. Dynamically stable chassis are sometimes out of balance – balancing or falling. This is common for two-legged robots.

B. Walking gaits

Walking gait refers to the locomotion achieved through the movement of robot legs. Compared to human gait, the legged chassis usually has more than two legs. Therefore, the locomotion of a robot is much more complicated. There are several basic gaits, such as trot, creep

Theoretical number of different gaits N can be calculated using Equation 1. Not all of them are usable for effective locomotion.

$$N = (2K-1)! \quad (1)$$

Where K is the number of the legs of the robot. For quadruped robot it is $7! = 5040$ possibilities of locomotion. The number is quite large, because this equation calculates all possible motions, like motion up and down, which of course doesn't lead to an effective movement.

III. LITERATURE SURVEY

Examination of walking machines started in the nineteenth century. One of the first models showed up around the year 1870 [1]. For 80-90 years, endeavors were made to build walking machines based on different kinematic chains that were supposed to generate a desired motion profile during operation. During those years, numerous models were proposed, yet the execution of a large portion of these machines was constrained by general cyclic walking forms and the inability to adjust a walking pattern to the landscape. In the late 1950s, it turned out to be clear that machines ought not simply be based on kinematic mechanisms that provide cyclic movements, and that there was a need to integrate planning and control systems. The first robot to move independently with computerized control and electric propulsion was built in 1966 by McGhee and Frank [2]. The main task of the robot's computer was to unravel the kinematic equations involved and to control the electric motors that drove the legs, such that the robot could go forward while maintaining equilibrium constraints. Since then, and following the advance of control technique technologies,

computing resources and motion actuators, many different robots with varied abilities have been built. Examples of these abilities include running [3], walking over rough terrain, jumping over obstacles [4], climbing [5, 6] and more

Robots have wide history of being used following the time when industrialization. [7] There has been and steadily developing improvement in the field which noted in the few records.

When in 1954 George C. Devol filed a U.S. patent for a programmable system for exchanging the article between distinctive parts of a manufacturing plant, he composed: "The present invention makes available for the first time a more or less general purpose machine that has universal application to a vast diversity of application where cyclic control is desired."

In 1967-68 the initially wheeled walking machine utilizing vision and different sensors, were accounted for. In 1974, the first servomotor impelled and microcomputer controlled robot were monetarily dispatched and they were utilized by NASA to gather tests from the surface of Mars. In 1981, a microprocessor based pneumatically worked pick and place Robot was indigenously created by the creator S.R. DEB in the Production Engineering Department at Jadavpur University. In 1984, Bhabha Atomic Research Central has built up a 6-axes multipurpose Robot, having weight around 300kg and can move an end-of-arm, heap of 10kg, including that of end effector.

Today, there are a substantial number of active research programs in the field of legged locomotion [7–15]. Apart from designing and building the robot itself, the main challenges are the planning and implementation of the legs' motions in generate a walking sequence, namely, how to plan the steps of the robot so that it moves in a desirable way while maintaining equilibrium constraints (quasi-static walking) or else maintaining the stability of the robot (dynamic walking)

At present, there are number of lab-scale quadruped robots being utilized as a part of exploration, for example, LittleDog from Boston Dynamics, StarLETH and ALoF from ETH, TITAN-IX, MRWALLSPECT III, the "bug like robot" created at Technion, AiDIN-III from Sungkyunkwan University (SKKU), and others. These models have complex mechanical designs, such as custom-made joints and structures, non-uniform motors and custom electronics. These models are specifically designed with powerful processing units or built-in sensors. The main advantage of the design presented in this paper is that it can be built from off-the-shelf products. Therefore, it can be used immediately in a simple and cost-effective manner. In addition, the proposed robot is based on open-source code and hardware, thus enabling future improvements. Such improvements might include sensor capabilities, control circles and the mechanical structure. The combination of the mentioned design features makes the robot unique and innovative and leaves it optimized for research purposes.

IV. RELATED WORK

There are several companies, which are producing quadpod models and platforms. These companies offer a variety of

hobby and research level robot kits and parts. They come in several types of quad pod that differ in the body shape and leg construction. Numerous robots accompany programming, which gives control of servomotors utilizing inverse kinematics and making custom gaits.

Although several solutions already exist and have great potential, each one of them has some disadvantage. The first one is price, which is quite high. Another disadvantage is equipment of the robots. Many of the robots have limited expansion options, like missing foot sensors, which are difficult to install later, or servomotor type with insufficient power or features. Also the batteries are often built in the body and it is difficult or even impossible to remove them.

REFERENCES

- [1] E. Lucas. Huitieme recreation-la machine a marcher. *Recreat. Math* 4, pages 198–204, 1894.
- [2] R. B. Mcghee and A. A. Frank. On the stability properties of quadruped creeping gaits. *Mathematical Biosciences*, 3(1-2):331–351, August 1968.
- [3] F. Iida, G. Gomez, and R. Pfeifer. Exploiting body dynamics for controlling a running quadruped robot. In *Advanced Robotics, 2005. ICAR'05. Proceedings., 12th International Conference on*, pages 229 – 235, 2005.
- [4] F. Kikuchi, Y. Ota, and S. Hirose. Basic performance experiments for jumping quadruped. In *Intelligent Robots and Systems, 2003. (IROS 2003). Proceedings. 2003 IEEE/RSJ International Conference on*, volume 4, pages 3378 – 3383 vol.3, oct. 2003.
- [5] A. Shapiro, E. Rimon, and Shoval S. A foothold selection algorithm for spider robot locomotion in planar tunnel environments. *The International Journal of Robotics Research*, 24(10):823–844, 2005.
- [6] A. Sintov, T. Avramovich, and A. Shapiro. Design and motion planning of an autonomous climbing robot with claws. *Robotics and Autonomous Systems*, 59(11):1008 – 1019, 2011Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” *IEEE Transl. J. Magn. Japan*, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
- [7] M. Hutter, C. D. Remy, M. A. Hoepflinger, and R. Siegwart, Efficient and Versatile Locomotion with Highly Compliant Legs, *IEEE/ASME Transactions on Mechatronics*, Vol. 18, No. 2, April 2013, 449-458
- [8] M. Hutter, H. Sommer, C. Gehring, M. Hoepflinger, M. Bloesch, and R. Siegwart, Quadrupedal locomotion using hierarchical operational space control, *The International Journal of Robotics Research (IJRR)*, vol. 33, no. 8, pp. 1062–1077, May 2014
- [9] G. C. Haynes, Alex Khripin, Goran Lynch, Jon Amory, Aaron Saunders, Alfred A. Rizzi, and D. E. Koditschek ,Rapid Pole Climbing with a Quadrupedal Robot, *IEEE International Conference on Robotics and Automation*. May 2009
- [10] C. Remy, O. Baur, M. Latta, A. Lauber, M. Hutter, M. Hoepflinger, C. Pradalier, R. Siegwart, Walking and crawling with ALoF: a robot for autonomous locomotion on four legs, *Industrial Robot: An International Journal*, Vol. 38, No. 3, 2011, 264-268.
- [11] Yam Geva, Amir Shapiro, A Novel Design of a Quadruped Robot for Research Purposes Robot for Research Purposes, *International Journal of Advanced Robotic Systems*
- [12] Sakagami, Y., Watanabe, R., Aoyama, C., Matsunaga, S., Higaki, N. and Fujimura, K. The intelligent ASIMO: system overview and integration. In *Proc. of IROS, 2002*, 2478- 2483.
- [13] Hirose, S., Fukuda, Y., Yoneda, K., Nagakubo, A., Tsukagoshi, H., Arikawa, K., Endo, G., Doi T. and Hodoshima, R. Quadruped walking robots at tokyo institute of technology. *IEEE Robotics & Automation Magazine*, 2009, 16(2), 104-114.
- [14] Pratt, J. Exploiting inherent robustness and natural dynamics in the control of bipedal walking robots. *Dissertation, Massachusetts Institute of Technology*, 2000.
- [15] Thrun, S. Toward robotic cars. *Communications of the ACM*, 2010, 53(4), 99-106.

Design and Simulation of Low Power and Area Efficient 32 Bit Multiplier

Sonali J. Rewatkar
Research Scholar

¹Electronics and Communication
Engineering

AbhaGaikwadPatil College of
Engineering, Nagpur, India
sonalirwtkr@gmail.com

SagarGhormade

Guide; Assistant Professor
Electronics and Communication
Engineering

AbhaGaikwadPatil College of
Engineering, Nagpur, India
hod.ece@agpce.com

SagarPradhan

M.Tech Coordinator
Electronics and Communication
Engineering

AbhaGaikwadPatil College of
Engineering, Nagpur, India
sp.ece@agpce.com

ABSTRACT: In majority of the digital and high performance systems like digital signal processors and microprocessors, multiplier acts as one of the important hardware unit. Speed of a system is actually judged by how a faster an arithmetic operations are performed within the structure for which mostly multiplication should be carried out at a faster rate which thus helps in improving the performance of the system. If you increase the speed then the area also increases likewise. Multipliers are one of the most significant building blocks in processors. Multipliers are of great importance in today's Digital Signal processing applications like DFT, IDFT, FFT, IFFT and ALU in Microprocessor. Actually, the two high speed multipliers, Modified booth multiplier (MBM) as well as the Wallace tree multiplier are hybridized with Carry select adder (CSA) and then they formed a hybridized multiplier which delivers high speed computation and here power consumption is low. Wallace tree multiplier is accompanied for fast addition and then finally CSA is used for final accumulation. This hybrid multiplier actually gives better results considering factors such as speed and power than the conventional designs.

This work find out the performance of the proposed designs considering the terms such as delay, area, power and their products by hand with logical effort and through custom design.

Keywords-Carry select adder, Wallace Tree, Booth Encoder, Unsigned multiplier, Carry Save Adder

I. INTRODUCTION

Most of the applications systems which are based on DSP need extremely fast processing of a large amount of digital data. The multiplier is an important element of the digital signal processing such as filtering and convolution. Multipliers are among one of the fundamental components of many digital systems and, hence, their power dissipation and speed are of great concern. For portable applications where the power consumption is the most important parameter, one should try to reduce the power dissipation as much as possible. It is the best way to reduce the dynamic power dissipation, so main intention of this paper is to minimize the total switching activity, i.e., the total number of signal transitions of the system. Continuous progress of microelectronic technologies actually make better use of energy, encode data in a more effective manner, transmit information more reliable, etc. Particularly, many of these technologies address low-power consumption to meet the needs of various portable applications. In these application systems, a multiplier is a most fundamental arithmetic unit and it is widely used in circuits.

II. SYSTEM ARCHITECTURE

The multiplier can be divided into three stages:

1. Partial products generation stage
2. Partial products addition stage

3. Final addition stage

By reducing the number of partial products the speed of multiplication can be increased. Lots of high-performance algorithms and architectures have been proposed in order to accelerate multiplication. Various multiplication algorithms like Booth, Modified Booth, Braun, and Baugh-Wooley have been proposed. The modified Booth algorithm actually reduces the number of partial products to be generated and thus is known as the fastest multiplication algorithm.

Wallace Tree Carry Save Adder structures have been used to add the partial products in reduced time. Our aim is to reduce computation time by using Booth's algorithm for multiplication and to reduce chip area by using Carry Save Adders arranged in a Wallace tree structure. The figure below describes about the Wallace Booth multiplier which has got following steps, where the multiplier and multiplicand is given to the booth encoder which thus produces the partial products followed by the Wallace tree structure which bringth down number of branches in the Wallace tree. After the reduction which is done by Wallace tree the final stageeventually arrives giving the final products for the multiplier.

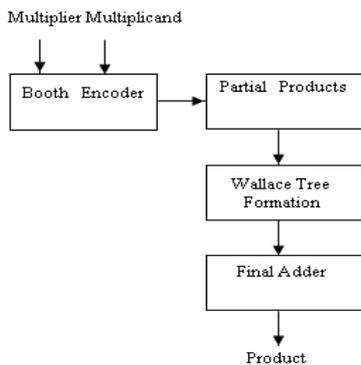


Fig1: Wallace Booth multiplier

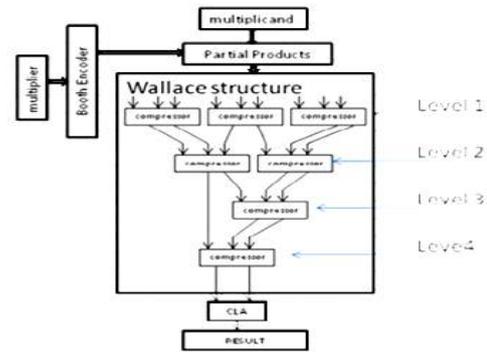
III. METHODOLOGY

Wallace multiplier

A Wallace tree is an efficient hardware implementation of a digital circuit that actually multiplies two integersWallace tree is known for their optimal computationtime, when adding multiple operands to two outputs using3:2 or 4:2 compressors or both. Wallace tree actually guarantees thelowest overall delay Fig2 shows nine

Fig. 2: Wallace tree structure

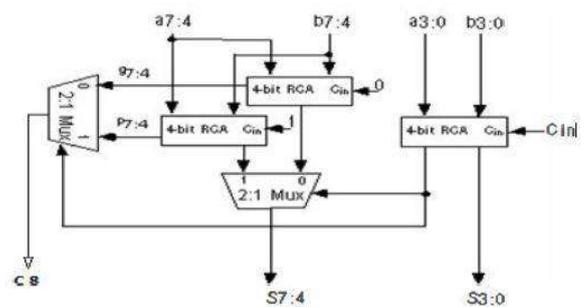
operands Wallacestructure, where 3:2 compressors compress the data havingthree multi-bit inputs and two multi-bit outputs.



4:2compressors compress the data having four multi-bit inputsand two multi-bit outputs. Using both compressor, No. oflevels has been bring down that also causes improving the speed of multiplier.

TheWallacetreehasthreesteps:

1. Multiply (that is AND) each bit of one of the arguments, by each bit of the other, yielding
2. Depending on position of the multiplied bits,the wires carry different weights, for example wire of bit carrying result of is 32 (see explanation of weightsbelow).
3. **Fig3: Carry select adder**
4. Reduce the number of partial products to two by layers of full and half adders.
5. Group the wires in two numbers, and add



them with conventional adder.

Carry select adder

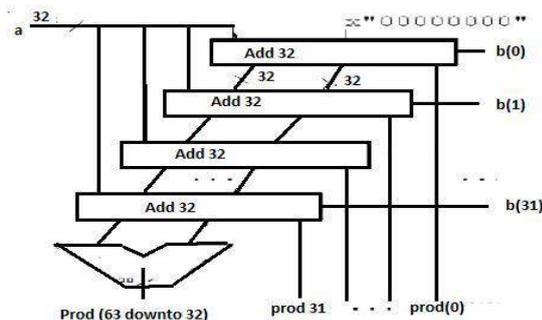
Usually the CSLA have the two ripple carry adder stages and multiplexer. Carry select adder selects the correct result using multiplexer

with single stage or multiple stage. For two stages of ripple carry adders we have got the two outputs (2 sums, 2 carry's). The multiplexer will select the correct result and speed will be high when compared with the different adders.

Unsigned Multiplier

Fig4: Unsigned Multiplier

The multiplier is one of the hardware and fundamental key block in Digital signal processing



techniques. The multiplier involves generation of partial products and summation. The n-bit multiplier multiplies with the

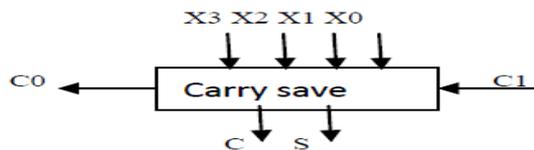
n-bit multiplier and it gives the final product term is a 2n bit value. The two 32 bit unsigned multipliers multiplication output will be shown in above Fig4.

Carry save Adder

Wallace tree increases the accumulation of the partial products. The speed, area and power consumption of the multipliers will be directly

Fig5: Carry save adder

proportion to the efficiency of the compressor. The structure is made of carry save adders. The carry save adders to decrease the number of partial products and sum rows. Compressors are arithmetic



components, analogous in principle to parallel adders. The 4:2 compressor shown in Fig.5 has 4 input bits and produces 2 sum output bits (out0 and out1), it

also has a carry-in (cin) and a carry-out (cout) bit (thus, the total number of input/output bits are 5 and 3).

Booth Encoder

Booths algorithm includes encoding of multiplier bits and partial product generation. Different modified booths algorithms have been proposed according to how many number of bits are used to encode multiplier. Modified booth algorithm reduces the number of partial products. Radix 2, radix 4, radix 8, radix 16, radix 32 are the different modified booth algorithms. NxN bit multiplication involves N partial products but modified Radix 2r produces N/r partial .In the proposed modified Radix -4 Booth Algorithm, multiplier has been divided in groups of 3 bits and each group of 3 bits have been taken into consideration according to modified Booth Algorithm for generation of partial products 0, ±1A, ±2A. In first group, first bit is taken as zero and other bits are least significant two bit of multiplier operand. In second group, first bit is most significant bit of first group and other bits are next two bit of multiplier operand. In third group, first bit is most significant bit of second group and other bits are next two bit of multiplier operand. This process is carried on. Partial product is generated using multiplicand operand A. For n bit multiplier there is n/2 or [n/2 + 1] groups and partial products .for 16X16 bit multiplication 8 partial products are generated. So it reduces the number of partial products in comparison to Booth algorithm (radix-2) improves the computational efficiency of multiplier, reduce the calculated delay.

y_i	y_{i-1}	z_{i-i}	Multiplier Value	Situation
0	0	0	0	String of 0s
0	1	1	+1	End of string of 1s
1	0	1	-1	Begin string of 1s
1	1	0	0	String of 1s

Fig6: Booth recoding table for Radix -2

Fig7: Comparison of power consumption among various multipliers

Above figure shows the various multipliers and their power consumption. Thus it is clear from the figure that Wallace tree multiplier structure shows far better performance results as compared to other techniques.

RESULTS

The figure below shows the result of proposed 16 bit carry select adder.

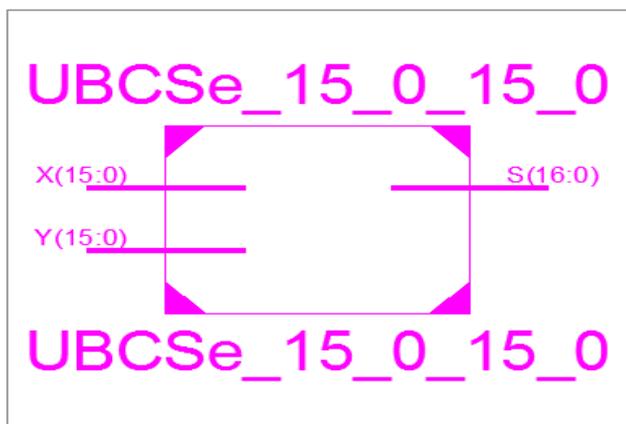


Figure 8 Top level entity of 16 BIT Carry select adder.

Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	20	768	2%
Number of 4 input LUTs	37	1536	2%
Number of bonded IOBs	49	124	39%

Figure 9 Device Utilization Summary

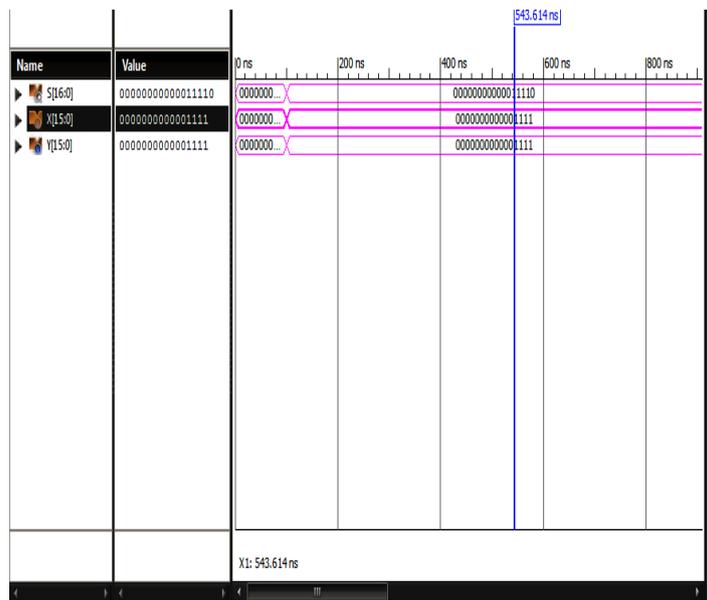


Figure 10.simulation result of CSA.

IV. CONCLUSION

Thus we designed the efficient multiplier with wallance tree with booth encoder. Out of thetree based reduction methodologies the reduction technique of wallance multiplier is based on minimum weight value actually more efficient than the array and serial multiplier.

V. REFERENCES

[1] Low-Power and area-efficient carry-select AdderB.Ramkumar and H.M. Kittur, *IEEE Trans. Very LargScaleIntegr. (VLSI) Syst.*, vol. 20, no. 2,pp. 371–375, Feb. 2012.

[2] Low-Power and high speed computation using hybridized Multiplier UvarajSubramaniam, SrinivasanAlavandar, *IEEE* 31661, July 4-6, 2013.

[3] Wallace Tree Multiplier Designs: A Performance Comparison Review, HimanshuBansal, K. G. Sharma, Tripti Sharma, *Innovative Systems Design and Engineering* ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online) Vol.5, No.5, 2014.

[4] Modified Wallace Tree Multiplier using Efficient Square Root Carry Select Adder,Paradhasaradhi, D. Prashanthi, M. Vivek, N. Green *Computing Communication and Electrical Engineering (ICGCCEE)*, 2014 International Conference.

[5] KulvirSingh ,Dilip Kumar “Modified Booth Multiplier with Carry Select Adder using 3-stage Pipelining Technique” *International Journal of Computer Applications* (0975 – 8887) Volume 44– No14, April 2012

[6] C. S. Wallace, “A Suggestion for a Fast Multiplier”, *Electronic Computers*, *IEEE Transactions*, vol.13, Page(s): 14-17, Feb. 1964

Design of Asynchronous Viterbi Decoder using Hybrid Register Exchange Method for Low Power Applications: A Review

Nita S. Kalaskar

Dept. of Electronics and Communications

Tulsiramji Gaikwad-Patil College of

Engineering & Technology

Nagpur, India

kalaskarnita@gmail.com, 9579872319

Abstract- This paper describe the design of viterbi decoder using various methods. Hybrid Register (HREM) exchange method which is the combination of design traceback(TB) & register exchange method (REM) exchange method which reduces further the switching activity and power. Power dissipation is analyzed for the Hybrid Register Exchange, REM method and TB method. The new Register Exchange Method shows an average power reduction of 45 percent.

Keywords— Viterbi decoder, HREM, REM, Traceback

1. INTRODUCTION

Now days with emerging trends and technology in wireless communication system it is necessary to reduce the power requirement. Viterbi decoder play an important role forward error correction and error detection. The Viterbi Algorithm has been widely used in digital communication and signal processing, was introduced in 1967 by Andrew J Viterbi as a method of decoding convolutional codes. By using Viterbi decoder we can find out mostly likely sequence at receiver side by following the procedure for design of decoder.

In Mobile station baseband modem, the Viterbi decoder consumes more than one-third of the chip area and the power dissipation of the baseband modem Therefore, a low-power implementation of the Viterbi decoder is a significant practical matter. Power efficiency becomes much less than 1%. If it is assume that the power efficiency can be increased to over 50%, the effective talk-time could be more than 250 h. Therefore, there is considerable margin in the power dissipation of the handset, especially in the power-controlled CDMA system. The approach we will adopt in the Viterbi design is to use a self-timed (or Asynchronous) timing strategy, because it saves power through not having to generate or distribute a global clock, instead, timing between blocks is performed by local handshake signals . This enables an asynchronous system to only consume power when doing useful work and to have an idle power of near zero. Furthermore, there is an inherent advantage to asynchronous

systems in that a system can switch almost instantaneously between the idle state and maximum activity.

There are two well-known methods for Viterbi decoder for survivor path storage and decoding, the Traceback method (TBM) and Register Exchange method (REM). In trace-back method, memory requirement is high. TBM is the preferred method used in Viterbi decoders having large constraint length and high performance. However, the TBM has drawbacks, which requires last-in-first-out (LIFO) buffer and has to use multiple read operations for high speed operation. This multiple operation results in complex control logic. The REM is logically simple, but it will consume large power and area, due to huge switching activity. The problem of switching activity of Viterbi decoder can be reduced by combining TB and REM that is Hybrid Register Exchange Method (HREM).

2. CONVOLUTIONAL ENCODER

Fig1 shows the convolutional encoder (3, 1, 2) with code rate $r=1/2$ i.e. the system encodes 1 input bit to 2 output bits constraint length K of 3 and number of memory element m is 2 (It consist of 2^m ($m=2$) shift stages, and modulo-2 adders ($n=2$)) as shown in fig1

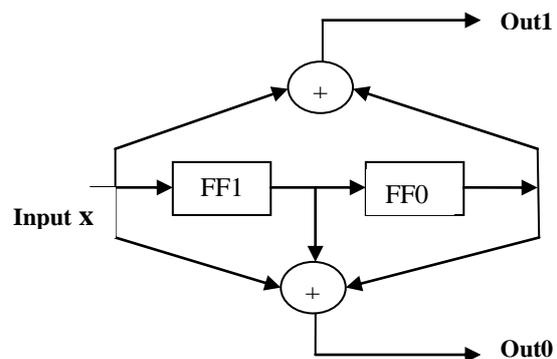


Figure 1 Block diagram of Convolutional Encoder(K=3, k=1,n=2)

In convolutional encoder input bit enter the shift register by one bit at a time. In order to encode bit x from the input stream, this encoder creates two bits, namely Out0 and Out1. The encoding bits are produced from the following equations:

$$\text{Out0} = \text{Input} \oplus \text{FF1} \oplus \text{FF0} \quad (1)$$

$$\text{Out1} = \text{Input} \oplus \text{FF0} \quad (2)$$

3. VITERBI DECODER

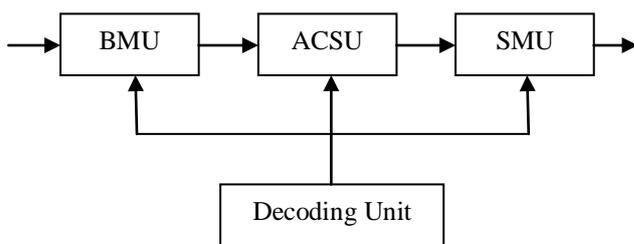


Figure 2. Block Diagram of Viterbi decoder

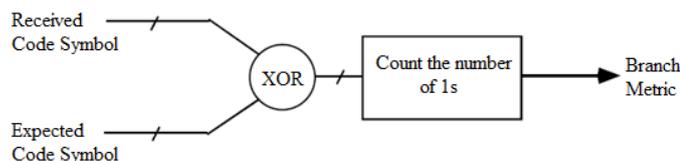
Fig 2 shows Viterbi decoder consists of three basic computation units. Viterbi decoders are used to decode data which is encoded using convolutional encoders and transmitted over noisy channels.

3.1 Branch Metric Unit (BMU)

This unit computes the branch metric of each transition, which is a hamming distance between the received symbol and expected symbol. It also counts the number of differing bits.

3.2 The Add-compare-select unit(ACSU)

The Add-compare-select unit is a collection of ACS units. For a single state, an ACS unit receives two branch metric and two path metrics. It adds each incoming branch metric to the corresponding path metric and compares the two results to select a smaller one. The path metric of the state is updated with the selected one.



3.3 Survivor Memory Unit

The Survivor Memory Unit (SMU), which stores the decisions of survivor path. The Survivor Memory Unit receives decision bits from the ACS unit and compare received decision bits for each node in trellis.

4. DECODING METHODS

4.1 Traceback Method

Trace Back Method, a trace back module is placed in the decoder which is connected by the ACS unit. Traceback memory stores the history of decision bits from ACS operation. This memory is a two dimensional circular buffer, with rows and columns. The number of rows is equal to the number of states $N = 2^{K-1}$ where K is the constraint length. Each column stores the results of N comparisons corresponding to incoming coded bits at each time interval. In this method decoding is performed by transition from the present state and previous state and finding the input that caused that transition from the previous state to this present state.

4.2 Register Exchange Method

In this method a register is assigned to each state. Each register contains the information of the survivor path bit throughout the trellis. The register keeps information of the partially decoded output sequence of decoder along the path. The register exchange method there is no need of traceback because the register present at the final state contains the decoded output sequence. This method approach to complex hardware and high switching activity due to the need of the copying the contents of all the registers from one state to another state.

4.3 Hybrid Register Exchange Method

This method is combination of register exchange method and traceback method hence the name Hybrid register exchange method. This method reduces the switching activity and power. In HREM instead of processing single bit in a cycle, now two bits are decoded, which reduces the switching activity to half as compared to REM. In this method we are using a property of trellis. Initial state can be first find traced back through an m cycle. Then contents of initial state transfer to current state and the next m bits of the register is the m bits of current state itself.

5. Asynchronous Viterbi Decoder

Asynchronous circuits are consist of blocks that communicate to each other by using handshaking protocol via asynchronous channels, to carry out the required synchronous operation for communication and sequencing. In Asynchronous communication channel there are bundle of wires and a protocol to communicate between the data and blocks. Asynchronous channels has two types of encoding scheme are single rail encoding and dual-rail encoding. Single rail encoding is that if the encoding scheme uses one wire per bit to transmit the data and a request line to identify when the

data is valid. Then channel is called a bundled-data channel. Alternatively, in dual-rail encoding the data is sent by using two wires for each bit of information.

There are different types of asynchronous methods are use some of them given below:

Quasi Delay Insensitive (QDI): In digital logic design, Quasi Delay-Insensitive (QDI) circuits are a class of almost delay-insensitive asynchronous circuits which are invariant to the delays of any of the circuit's wires or elements, except to assume that certain fanouts are isochronic. Isochronic forks allow signals to reach two destinations with negligible difference in delay.

4-Phase Handshaking Protocol: In this type of protocol, the request and acknowledge wires use normal Boolean levels to encode information.

Current Sensing Completion Detection (CSCD) technique: The goal of this method is to detect a predefined current threshold and generate a signal as soon as the transient-current flow is above this threshold level.

CONCLUSION

As we see different methods for power reduction but some methods have drawbacks such as in traceback method memory requirement is more. In Register exchange method we are assign register to each state and copying contents of one register to another register increases switching activity and power consumption. To overcome these problem our main objective is to design asynchronous viterbi decoder using hybrid register exchange method for low power application. HREM reduces the switching activity to better extend.

REFERENCES

- [1] Amruta J. Mandwale, Altaf O. Mulani, "Different Approaches For Implementation of Viterbi decoder on reconfigurable platform", Pervasive Computing (ICPC), Pune, India-1-4799-6272-3/15/\$31.00(c)2015 IEEE
- [2] Narayan V. Sugur, Saroja V. Siddamal, "Design and Implementation of High Throughput and Area Efficient Hard Decision Viterbi Decoder in 65nm Technology", VLSI Design and 2014 13th International Conference on Embedded Systems, 2014 27th International Conference, 5-9 Jan. 2014, Mumbai, India. 1063-9667/14 \$31.00 © 2014 IEEE DOI 10.1109/VLSID.2014.67
- [3] Surekha Tadse, "Asynchronous Viterbi Decoder for Low Power Consumption: A Technical Review," *Inventi Rapid: Telecom* Vol. 2014, Issue 1 [ISSN 2278-6341], 13 October 2013.
- [4] T. kalavati Devi and C Venkatesh, "Design of Low Power Viterbi Decoder using Asynchronous Techniques", *International Journal of Advances in Engineering & Technology*, Vol 4, Issue 1, pp. 561-570, July 2012.
- [5] S. L. Haridas, N. K. Choudhari, "Very Low Power Viterbi Decoder Employing Minimum Transition and Exchange-less Algorithms for Multimedia Mobile Communication", *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 2, No. 12, 2011.
- [6] Mohamed Kawokgy, C. André, T. Salama, "Low Power Asynchronous Viterbi Decoder for Wireless Applications," *International Symposium on low power Electronics and Design (ISPELD)* 2004.
- [7] "A Low power Viterbi Decoder Design for wireless communication Application", Samirkumar Ranpara, Dong Sam Ha, IEEE 1999.
- [8] A. J. Viterbi, J.K. Omura, "Principals of digital communication", McGraHill, Inc, 1979.
- [9] "A Viterbi Algorithm with soft decision outputs and its application", Joachim Hagenauer, Peter Hoeher, IEEE 1989.
- [10] Viterbi, A. J., "A personal history of the Viterbi algorithm," *signal Processing Magazine, IEEE*, Volume 23, Issue 4, July 2006, pp. 120-142.
- [11] Sunil P Joshi and Roy Paily. Low Power Viterbi Decoder by Modified ACSU architecture and Clock Gating Method. IEEE, 499-503, 2011.

- [12] M Santhi, G Lakshminarayanan, R Sundaram, N Balachander. Synchronous pipelined two-stage radix-4 200mbps MBOFDM UWB viterbi decoder on FPGA. IEEE, 468-471, 2009
- [13] Chien-Ching Lin, Yen-Hsu Shih, Hsie-Chia Chang and Chen-Yi Lee. Design of a Power-Reduction Viterbi Decoder for WLAN Applications. *IEEE Transactions on Circuits and Systems*, 52(6):1148-1156, 2005.
- [14] Dong-Sun Kim, Seung-Yerl Lee, Kyu-Yeul Wang, Jong-Hee Hwang and Duck-Jin Chung. Power Efficient Viterbi Decoder based on Pre-computation Technique for Portable Digital Multimedia Broadcasting Receiver. *IEEE Transactions on Consumer Electronics*, 53(2):350-356, 2007.
- [15] Dalia A F, El-Dib and Mohamed I Elmasry. Low-power register exchange viterbi decoder For high-speed wireless communications. *IEEE*, 5:V737-V740, 2002.
- [16] Wing-Kin Chan, Chiu-Sing Choy, Cheong-Fat Chan and Kong-Pang Pun. An asynchronous SOVA decoder for wireless communication Applications. *IEEE*, 2(ID):517-20, 2004.
- [17] Mohamed Kawokgy, C Andre, T Salama. A Low-Power CSCD Asynchronous Viterbi Decoder for Wireless Applications. *International Symposium on low power Electronics and Design (ISPELD)*. Portland, Oregon USA, 363-366, 2007.
- [18] Xuguang Guan, Duan Zhou, Dan Wang, Yintang Yang, Zhangming Zhu. A Case Study on Fully Asynchronous ACS Module of Low-power Viterbi Decoder for Digital Wireless Communication Applications. *International conference on Computational Intelligence and Natural Computing*. IEEE, 426 - 429, 2009.
- [19] Kang and A. N. Willson Jr., "Low-power Viterbi decoder for CDMA Mobile Terminals," *IEEE Journal of Solid-State Circuits*. Vol. 33, no. 3, pp. 473-82, March 1998.
- [20] J.A. Ryu, S.C. Kim, J.D. Cho, H.W. Park and Y.H. Chang, Lower Power Viterbi decoder Architecture with a new clock-gating trace-back unit," *Proc. 6th International Conference on VLSI and CAD*, Oct. 1999, pp. 297-300.



Improvement in Embedded Attendance System

Ashwini C. Ingle
E&TC Department
Polytechnic Akola, India
ashwiniingle28@gmail.com

Priyanka N. Alone
E&TC Department Bhonsla
Bhonsla Polytechnic Akola, India
alonepriyanka4@gmail.com

Abstract- Maintaining the attendance is very important in all the institutes for checking the performance of employees. Every institute has its own method in this regard. Some are taking attendance manually using the old paper or file based approach and some have adopted methods of automatic attendance using some biometric techniques. An attendance recording system's basic function is to keep a record of the time at which the employees of a particular firm report to work and leave from work. It is one of the most widely used event recording application in the industry today. A track of employee attendance is a must for payroll generation. The traditional method of maintaining an attendance register makes the job very tedious and prone to human errors. The collection and processing of data of employee. Attendance which may include leaves, half working days, overtime etc. and using it to generate the payroll manually consumes important man hours, which in turn could be used to increase productivity and in turn profitably of the firm. In case of an error, even more time will be used to detect and rectify it, if the process is manual. The whole process will be simplified to great extent.

Keywords- *RFID, biometrics, student's attendance, fingerprint recognize.*

I. INTRODUCTION

Now-a-days, there are lots of colleges and Universities around the world and some of them consist of students up to thousands or more. To

handle a large number of students may be a problem especially to get the attendance of the students. The manual process is that whenever a lecturer comes to class, he came with register and manually takes attendance by calling roll numbers. This manual process has some flaws because in case where students can cheat by saying attendance of their friends, another problem is that the lecturer had to take care of the register and enter the attendance into the log (or) data-base, calculate the attendance percentage. This would be a big problem in the colleges and Universities.

The suitable solution for this problem is by designing a system that will record attendance automatically. RFID system is used to record the numbers of student's attendance automatically. The ID cards of the students is embedded with RFID tag which is read by a reader. This RFID system is interfaced to a database through a computer or some electronic circuits. This method is more effective to prevent problem encountered when getting attendance manually components that the RFID technology consists are RFID Reader and RFID Tag. RFID is a nascent technology, deeply rooted by its early developments in using radar 1 as a harbinger of adversary planes during World War II. A plethora of

industries have leveraged the benefits of RFID technology for enhancements in sectors like military, sports, security, airline, animal farms, healthcare and other areas.

Industry specific key applications of this technology Include vehicle tracking, automated inventory management, animal monitoring, secure store checkouts, Supply chain management, and automatic payment, sport timing technologies, the distinctive components of RFID technology and focuses on its core competencies: scalability and security. It will be then supplemented by a detailed synopsis of an investigation conducted to test the feasibility and practicality of RFID technology.

RFID can be used in many applications. A tag can be affixed to any object and used to track and manage inventory, assets, people, etc. For example, it can be affixed to cars, computer equipment, books, mobile phones, etc. The Healthcare industry has used RFID to reduce counting, looking for things and auditing items. Many financial institutions use RFID to track key assets and automate compliance.

II. SYSTEM OVERVIEW

Biometric technologies enable automatic personal recognition based on physiological or behavioural characteristics (Prabakar, 2003). Biometric is defined as the "automated identification or verification of human identity through the measurement of repeatable physiological and behavioural characteristics" (Association of Biometric, 2004).

Different types of biometric techniques are shown in

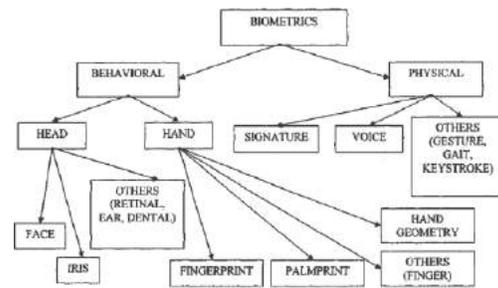


Fig. 1 Biometrics Techniques The absence of an automated time and attendance system, [2] companies lose productivity, overpay employees, and become distracted by the manual tasks of time and attendance.

The Attendance recording in educational institutions is an imperative task. [3] Most present systems provide database management but still involve laborious manual data entry procedures. The design presented offers a twofold solution to the problem. It relieves from handling paper records of attendance taken in the class by providing firsthand entry into a portable gadget built around the AVR ATmega8 microcontroller. The attendance entered is firstly stored in the microcontroller's EEPROM from where it is transferred to application software residing on a computer through the serial port. This application stores the attendance data in a database and also displays requested information extracted from them.

METHODOLOGY

The proposed system provides solution to lecture attendance problems through the use of attendance Management software that is interfaced to a fingerprint device. The student bio-data (Matriculation number, Name, Gender and Date of Birth) and the fingerprint is enrolled first into the database.

This section describes the software algorithm for the system.

The algorithm consists of the following steps

- Image acquisition
- Noise removal
- Face detection
- Face recognition
- Attendance

In the first step, image is captured from the CCTV camera. There are illumination effects in the captured image because of different lighting conditions and some noise which is to be removed before going to the next

III.SYSTEM DESIGN

A commercial system based on RFID for attendance management for schools and colleges. The system can send SMS and email alert to parents/guardians of the students automatically. The student will register at the gate by touching RFID device with their RFID tag and send the data to BISAM server in the school. The server will process the attendance data and send an SMS to the parents/guardians of the absentee student through BISAM SMS gateway server. The system also has Time Manager Software for managing employees' attendance and HR related functionalities. The problem in this research is there is verification is not done. So proxy attendance may be marked. [7]

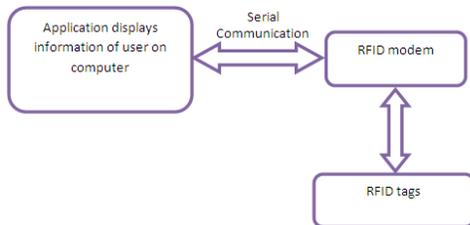


Fig. 2 Functioning of the System

In [22] RFID reader was designed with microcontroller, transceiver chip, serial communication IC, LCD, USB

interface, power supply module, etc as components. When a staff member touches the reader with their card the data is sent to PC manager application which will validate the data and extract information like staff ID and access time into the data. Is sent to PC manager application which will validate the data and extract information like staff ID and access time into the database. Again same problem as above system is being faced by this research.

IV.Hardware Architecture

The attendance system has been more hardware like RFID, finger print, Biometric etc

The hardware to be used can be divided into two categories – fingerprint scanner which captures the image and personal computer which: houses the database, runs the comparison algorithm and simulates the application function. The fingerprint scanner is connected to the computer via its USB interface. Basically this work does not involve the development of hardware.



Figure 3: Fingerprint Device.

Using the Secugen Fingerprint Reader, the Grainger Software Development Kit (SDK) toolbox provided by the Griaule (will explain the detail) can be used as an interface between the fingerprint reader and the attendance software.

RFID TAG

A radio-frequency identification system uses tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response.

RFID tags can be passive, active or battery-assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery-assisted passive (BAP) has a small battery on board and is activated when in the presence of an RFID reader. A passive tag is cheaper and smaller because it has no battery; instead, the tag uses the radio energy transmitted by the reader. However, to operate a passive tag, it must be illuminated with a power level roughly a thousand times stronger than for signal transmission. That makes a difference in interference and in exposure to radiation.

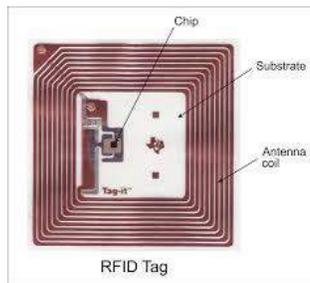


Fig 4. RFID Tag

Shows the RFID reader transmits an encoded radio signal to interrogate the tag. The RFID tag receives the message and then responds with its identification and other information.

FINGER PRINT

Biometric time and presence system is one of the most effective solicitations of biometric technology. Impression Recognition is an established field today,

but still identifying individual from a set of enrolled fingerprints is a time

Taking process. Most fingerprint-based biometric systems store the finger point's template of a user in the database has been usually assumed that the minutiae pattern of a user does not reveal any information about the original

Fingerprint. This belief has now been shown to be false; several algorithms have been proposed that can renovate fingerprint images from minutiae templates. are construct the segment image, which is then converted.

COMPARISON WITH MANUAL ATTENDANCE

The manual attendance system average execution time for eighty (80) students is approximately 17.83 seconds as against 3.79 seconds for the this automatic attendance management system using fingerprint identification. Reports generation for the attendance system takes approximately 30s. The table is a 25 student sample out of the 80 tests conducted. It can be shown in the graph below and thus, it can be seen that the automatic attendance management system using fingerprint authentication is better and faster than the use sheets of paper.

CONCLUSION

Thus I would like to conclude that automatic embedded attendance system is a system where we conduct the attendance with the help of RFID, Biometrics, and Fingerprint Recognition. Etc this report presents an analysis of different technologies which are used for attendance making system.

Traditionally student attendance is taken by professor and it will waste too much time of lecture. Too much proxy attendance can be recorded in manual system. This can be replaced with computerized system. RFID and WhatsApp based will take auto attendance for all the students entered in the class which will remove the time loss of professor. On the other hand Face Recognition will verify the student which will remove the proxy attendance.

REFERENCE

- [1] Newman-Ford, L.E., Fitzgibbon, K., Lloyds, S. & Thomas, S.L., "A Large-Scale Investigation into the Relationship between Attendance and Attainment: A Study Using an Innovative, Electronic Attendance Monitoring System", *Studies in Higher Education*, 33(6), pp. 699-717, 2000
- [2] Marr, Liz & Lancaster, Guy, "Attendance System", *Learning and Teaching in Action*, 4 (1), pp. 21-26, 2001.
- [3] Mazza, R. & Dimitrova, V., "Visualising student tracking data to support instructors in web-based distance education", *Proceedings of the 13th International World Wide Web Conference on Alternate Track Papers & Posters Press*, pp.154-161, New York: USA, 2002.
- [4] Mehmet Kizildag, Erden Basar, Murude Celikag, Emine Atasoylu and Sayedali Mousavi, "An Automated Attendance Monitoring and Registration System for EMU's SPIKE Seminar Series", *Proceedings in Academia.edu*. 2003
- [5] RESEARCH NOTE, AUTOMATING TIME AND ATTENDANCE: LOW HANGING ROI, *Proceeding in Nucleus Research*, January 2004
- [6] S. K. Jain, U. Joshi, and B. K. Sharma, "Attendance Management System," *Masters Project Report*, Rajasthan Technical University, Kota, June 2004
- [7] Seifedine Kadry* and Mohamad Smaili, "Wireless attendance management system based on iris Recognition", *Scientific Research and Essays* Vol. 5(12), pp. 1428-1435, 18 June, 2010, ISSN 1992-2248. 2005
- [8] Vishal Bhalla, Tapodhan Singla, Ankit Gahlot and Vijay Gupta, "Bluetooth Based Attendance Management System", *International Journal of Innovations in Engineering and Technology (IJJET)* Vol. 3 Issue 1 October 2011 ISSN: 2319 – 1058. 2006
- [9] Josphineleela.R and Dr.M.Ramakrishnan, "An Efficient Automatic Attendance System Using Fingerprint Reconstruction Technique", *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 10, No. 3, April 2006

Satellite Image Segmentation Soft Computing Techniques: A Survey

Niraj K. Nagrale¹, Vishakha Nagrale²

Rajiv Gandhi college of Engineering, Research and Technology, Chandrapur
¹ n_niroo@rediffmail.com, ² vishakha_bansod@rediffmail.com

Abstract—The term image segmentation refers to the partition of an image into a set of regions that cover it. The goal in many tasks is for the regions to represent meaningful areas of the image, such as the crops, urban areas, and forests of a satellite image. Soft computing is an emerging field that consists of complementary elements of fuzzy logic, neural networks and Genetic algorithms. Soft computing deals with approximate models and gives solution to complex problems. In this paper, the main aim is to survey the various soft computing approaches i.e. fuzzy clustering and relevance vector machine (RVM) for satellite image segmentation.

Keywords- *Image segmentation, soft computing, satellite image, RVM, fuzzy c-means (FCM)*

I. INTRODUCTION

Digital image processing is application of various algorithms on the image to improve the quality of the image by removing noise & other unwanted pixels and also to obtain more information on the image. Among the various image processing techniques image segmentation is very crucial step to analyze the given image. This paper mainly focuses on this method, the various methods followed and few algorithms that are widely used. An attempt is made to provide the comparison on these methods by taking test images. The images are operated using MATLAB software.

Image segmentation is a mid-level processing technique used to analyze the image and can be defined as a processing technique used to classify or cluster an image into several disjoint parts by grouping the pixels to form a region of homogeneity based on the pixel characteristics like gray level, color, texture, intensity and other features. The main purpose of the segmentation process is to get more information in the region of interest in an image which helps in annotation of the object scene. Image segmentation aims at domain-independent partition of the image into a set of visually distinct and homogeneous regions

with respect to certain properties. The main goal of segmentation is to clearly differentiate the object and the background in an image. Satellite images are one of the most powerful and important tools used by the meteorologist. They are essentially the eyes in the sky. These images reassure forecasters to the behavior of the atmosphere as they give a clear, concise, and accurate representation of how events are unfolding. Forecasting the weather and conducting research would be extremely difficult without satellites. Data taken at stations around the country is limited in its representations of atmospheric motion. It is still possible to get a good analysis from the data, but because the stations are separated by hundreds of miles significant features can be missed. Satellite images aid in showing what cannot be measured or seen. In addition the satellite images are viewed as truth. There is no chance for error. Satellite images provide data that can be interpreted "first-hand".

Satellites images give a good representation of what is happening at every point in the world, especially over oceans where large gaps in data occur. Data can only be taken at certain points around the world, though, without this data, forecasting would be just as difficult as not having satellites. It is essential to have both. Having the two together gives a much better understanding as to how the atmosphere is behaving and greatly improves forecasting accuracy.

There are two types of satellites that orbit the Earth, polar and geostationary. Geostationary Operational Environmental Satellites (GOES) remain above a fixed location on the Earth's surface, approximately 22,500 km above the equator. Because the satellites rotate with the Earth, they always view the same portion of the globe. The polar orbiting satellites, in contrast, orbit at much lower elevations (800-900 km). Their path is

2,400 km wide centered at the orbit path. The polar satellites observe a new path on each orbit. Polar satellites are not as useful to operational meteorologists because they do not continuously view the same area. Geostationary satellites allow meteorologists to view the weather as it develops since they view the same area continuously.

Satellite Images are of three types: A. Visible Image Visible satellite pictures can only be viewed during the day, since clouds reflect the light from the sun. On these images, clouds show up as white, the ground is normally grey, and water is dark. In winter, snow-covered ground will be white, which can make distinguishing clouds more difficult. To help differentiate between clouds and snow, looping pictures can be helpful; clouds will move while the snow won't. Snow-covered ground can also be identified by looking for terrain features, such as rivers or lakes. Rivers will remain dark in the imagery as long as they are not frozen. If the rivers are not visible, they are probably covered with clouds. Visible imagery is also very useful for seeing thunderstorm clouds building. Satellite will see the developing thunderstorms in their earliest stages, before they are detected on radar. B. Infrared Image Infrared satellite pictures show clouds in both day and night. Instead of using sunlight to reflect off of clouds, the clouds are identified by satellite sensors that measure heat radiating off of them. The sensors also measure heat radiating off the surface of the earth. Clouds will be colder than land and water, so they are easily identified. Infrared imagery is useful for determining thunderstorm intensity. Strong to severe thunderstorms will normally have cold tops. Infrared imagery can also be used for identifying fog and low clouds. The fog product combines two different infrared channels to see fog and low clouds at night, which show up as dark areas on the imagery. C. Water Vapor Image Water vapor satellite pictures indicate how much moisture is present in the upper atmosphere (approximately from 15,000 ft to 30,000 ft). The highest humidities will be the whitest areas while dry regions will be dark. Water vapor imagery is useful for indicating where heavy rain is possible. Thunderstorms can also erupt under the high moisture plumes. [1]

II. SEGMENTATION APPROACHES

Segmentation can be considered the first step and key issue recognition, scene understanding and image understating. Applications range from industrial quality control to medicine, robot navigation, geophysical exploration, remote sensing, and military applications. In all these areas, the quality of the final result depends largely on the quality of the segmentation. During the past

years, many image segmentation techniques have been developed and different classification schemes for these techniques have been proposed.

A. *Thresholding segmentation:*

This method consists in comparing the measure associated to each pixel to one or some threshold in order to determine the class which the pixel belongs to. The attribute is generally the grey level, although color or a simple texture descriptor can also be used. Threshold may be applied globally across the image (static threshold) or may be applied locally so that the threshold varies dynamically across the image. Several algorithms have been proposed for thresholding segmentation of satellite images, proposing thus an automatic selection of an adequate threshold for different satellite image class[2].

B. *Edge segmentation:*

Edges segmentation is a particularly simple and effective means for increasing geometric detail in an image. It is performed by first detecting edges and then either adding these back into the original image to increase contrast in the vicinity of an edge, or highlighting edges using saturated (black, white or color) overlays on borders. Indeed, edges in images are areas with strong intensity contrasts – a jump in intensity from one pixel to the next. Edge detecting an image significantly reduces the amount of data and filters out useless information, while preserving the important structural properties in an image. The fundamental importance of line and edge information in satellite images has been recognized. Indeed, local features, such as lines and edges, can describe the structure of a scene relatively independently on the illumination. Image segmentation techniques based on edge have long been in use. Although a variety of methods of edge detection have been suggested, and may be grouped into two categories: derivative methods and optimal filtering method [2].

C. *Region segmentation:*

Another way of extracting and representing information from an image is to group pixels together into regions of similarity. One would group pixels together according to the rate of change of their intensity over a region. In fact, the regions formation can be realized in two different ways: (i) split and/or merge process founded on some global criteria, (ii) a points aggregation procedure based on some local similarity criteria. Due to the global level of the analysis, in a split and merge process the local information is not considered. On the other hand, a point's aggregation to a region needs to take into account some global information of the region, as well as

some local information relative to the pixel. For this reason, the region extraction through point's aggregation approach has been retained [2].

III. SOFT COMPUTING SEGMENTATION APPROACH

A. FuzzyClustering

Soft or Fuzzy clustering technique classify pixel values with great extent of accuracy & it is basically suitable for decision oriented applications like tissue classification & tumor detection etc. Fuzzy clustering divides the input pixels into clusters or groups on the basis of some similarity criterion, such that similar pixels belong to same cluster. Similarity criterion used can be distance, connectivity, intensity. The resulting partition improves the understanding of human beings & helps in a more informed decision making. The advantage of fuzzy system is that they are easy to understand, as the membership function partition the data-space properly [8]. Fuzzy clustering algorithms include FCM (fuzzy C means) algorithm, GK (Gustafson-Kessel), GMD (Gaussian mixture decomposition), FCV (Fuzzy C varieties), AFC (Adaptive Fuzzy Clustering) algorithm and etc. The FCM is the most accepted method since it can preserve much more information than other approaches. Fuzzy c-means algorithm (FCM) is most popular objective function based fuzzy clustering algorithm.

FCM algorithm the procedure is as follows:

- (i) Initially the number of clusters c ($2 \leq c < n$), m , U are specified by user.
- (ii) All the user-defined parameters are defined, run the algorithm.
- (iii) The validity index measures the compactness of the output cluster is measured. Validity index measures like Partition Coefficient, Partition Entropy, etc are used to measure the fitness of the outcome.
- (iv) If the calculated index is satisfactory, then it moves to next step or the parameters are changed and process is repeated.
- (v) Least Square Estimation (LSE) is calculated. This error should be minimum.
- (vi) Finally the outputs obtained for various inputs are compared and plotted.

The selection of initial cluster center is directly related to the performance of the algorithm. If cluster center is close to actual center, then the algorithm converges quickly. This also reduces the processing time[3].

B. Support Vector Machine (SVM) Ensemble Fuzzy Clustering

Support vector machine ensemble is a classification method which includes two procedures: Firstly, it gives the sub-forecasts of a new sample using sub-SVM classifiers that can be obtained by various ways, and then, combines these sub-forecasts to decide the final class. Theoretically, compared with the single SVM, the SVM ensemble method has better classification accuracy. Supposing there are n sub-classifiers and a sample to be classified, it is obvious that the SVM ensemble has the same classification ability if all sub classifiers are equal; else if they are different and uncorrelated then the SVM ensemble outperforms the individuals. Actually, the theory is also suit to any other learning mechanism (strictly, weak learning mechanism). Since ensemble learning method behaves remarkably well, it has been a hot topic in academic circles in recent years.[4]

Selective SVM ensemble approach using fuzzy clustering algorithm which is realized in three steps: firstly, train a number of SVMs from the training set with Bootstrap, then, obtain the selected SVMs using clustering algorithm to select objects near to each clustering center, finally, construct the ensemble with the selected SVMs through voting. The group number of clustering is that having highest testing precision. The algorithm can be described as following:[4]

Input : training set S , testing set T , parameters of SVM, such as kernel function, penalty coefficient, etc ;

Initialization : set the number of training samples $n=N, i=1, j=1$;

Step1 if $i \leq N$ then Establish sub-set S_i with Bootstrap algorithm; Train SVM $_i$; Let $i=i+1$; Else Goto Step 2 ;

Step2 if $j \leq N$ then Execute the FCM algorithm to cluster the SVMs into j groups based on the differences of the classification results by the SVMs; Choose one SVM which is nearest to the group center from each group to obtain j SVMs for constructing the ensemble; Construct the ensemble $_j$ by voting; Calculate the classification rate R_j of the ensemble $_j$; Let $j=j+1$; Else End

Output : Choose the ensemble with biggest R_j as the selected ensemble, j denotes the number of SVMs.

C. Relevant vector machine

SVM is methodology for regression and classification that has attracted considerable interest. It is a constructive learning procedure rooted in statistical learning theory, which is based on the principle of structural risk minimization. It aims to minimizing the bound on the generalization error (i.e., the error made by the learning machine on data unseen during training) rather than minimizing the empirical error such as the mean square error over the data set. This results in good generalization capability and an SVM tends to perform well when applied to data outside the training set[5].

As RVM is not multi class classifier. So to classify image using RVM tree structure is used. In tree structure first of all samples are classified into two classes as pixels of one cluster in one class and remaining other pixels in second class. And following the same procedure all points of an image are classified. After feature extraction to reduce dimension principal component analysis is used. It is one of the most popular techniques for dimension reduction. SVM the support vectors are typically formed by "borderline", difficult-to-classify samples in the training set, which are located near the decision boundary of the classifier; in contrast, for RVM the relevance vectors are formed by samples appearing to be more representative of the two classes, which are located away from the decision boundary of the classifier. Compared to SVM, RVM is found to be advantageous on several aspects including: 1) The RVM decision function can be much sparser than the SVM classifier, i.e., the number of relevance vectors can be much smaller than that of support vectors; 2) RVM does not need the tuning of a regularization parameter (C) as in SVM during the training phase. As a drawback, however, the training phase of RVM typically involves a highly nonlinear optimization process.

The relevance vector machine (RVM) technique has been applied in many different areas of pattern recognition, including communication channel equalization, head model retrieval, feature optimization, functional neuroimages analysis and facial expressions recognition. The main difficulties of RVM when applied to large data sets (such as images) are that the computations required for the posterior statistics in equation (14) can be prohibitive. In what follows we first introduce a methodology to ameliorate this problem.

When the training points are uniform samples of a signal (e.g., the pixels of an image) and the kernel is symmetric, the RVM for the single kernel case can be written using a convolution [5].

First of all for an input image we will evaluate optimal number of clusters using Davies-Bouldin index. The Davies-Bouldin index is based on ratio of within cluster distance and between cluster distances. In other words it is based on the ratio of inter and intra cluster distance. The equation used is as follows:

$$\text{intra} = \sum_{i=1}^K \sum_{x \in C} \|x - z_i\|^2$$

where N denotes number of pixels in n image and K is the number of clusters and z_i is the cluster center of respective cluster.

The inter cluster is calculated as the distance between cluster centers and take the minimum of them.

$$\text{inter} = \min (\|z_i - z_j\|)^2$$

where $i=1,2,\dots,K-1$ and $j=i+1,\dots,K$ then we take ratio of these measures

$$\text{validity} = \text{intra} / \text{inter}$$

We choose an upper limit let K_{\max} for the number cluster and then we calculate validity measure for each of them. The minimum value of Davies-Bouldin index gives optimal clustering and maximum value represent worst case. After evaluating optimal number of clusters for image i.e. K we will pass this image along with calculated K in fuzzy clustering algorithm such as FCM, DeFC, MoDEFC. Then by using different clustering solutions obtained from clustering algorithm RVM is trained. For this some percentage of points are selected as training points from each clusters based on their distance from cluster centers, these points can be considered as high confidence points and the remaining low confidence points of image are classified on the basis of trained RVM classifier. Since clustering is unsupervised learning method, we are using result of unsupervised learning classifier to train supervised learning classifier that is RVM.

For this purpose we are choosing some percentage of points to train RVM classifier. As mentioned training of RVM is slower as compared to SVM. Relevance Vector Machine takes $O(N^3)$ time. Functional form of both RVM and SVM is identical but RVM does probabilistic classification. In RVM we need to maximize this equation:

$$\ln P(\alpha, \beta) = \sum_{i=1}^N \ln \beta - E(t) - 2 \ln \Gamma(\cdot) - 2 \ln (2^{\cdot}) +$$

With respect to hyper parameters α and β . The original algorithm for RVM is for linear classifier. RVM belongs to the family of linear classifier. Despite this it does not mean that non linear data cannot be classified, non linear classifier can be created by using kernel trick. Kernel functions are used to classify non linear data. Kernel function projects data to higher dimension space so that it can be linearly classified. Since the classifier is a hyper plane in high dimension space it may be non linear in the original input space. Different types of kernels are there which are used to project data in higher dimension space so that can be linearly classified. Some commonly used kernels are:

- Polynomial Homogeneous Kernel

$$K(x_i, x_j) = (x_i \cdot x_j)^d$$

- Polynomial Inhomogeneous Kernel

$$K(x_i, x_j) = (x_i \cdot x_j + 1)^d$$

As RVM is not multi class classifier. So to classify image using RVM tree structure is used. In tree structure first of all samples are classified into two classes as pixels of one cluster in one class and remaining other pixels in second class. And following the same procedure all points of an image are classified. After feature extraction to reduce dimension principal component analysis is used. It is one of the most popular techniques for dimension reduction. Other techniques for dimension reduction such as linear discriminant analysis (LDA), canonical correlation analysis (CCA) can also be used. By computing covariance, mean and eigen values it reduces dimensions. After classifying all points using trained RVM classifier Cluster based Similarity partition algorithm (CSPA) is used to ensemble solutions from different clustering algorithm. CSPA is used in situation where it is desired to find a single clustering solution from number of different clustering solutions. CSPA works by calculating that by how many clustering algorithm data points are placed in same cluster. Its main task to calculate similarity between two data points which is done by analyzing that number of clustering algorithm are placing these two data points in same cluster. More clustering algorithm placing these points in same cluster more similar are these two data points.

IV. CONCLUSION

In this survey, an overview of different segmentation methods and classification are studied, an overview of all related satellite image segmentation techniques has been presented in this paper. Fuzzy clustering method which is widely

used for images is powerful unsupervised clustering method. RVM is found to be advantageous on several aspects. RVM decision function can be much sparser than the SVM classifier, i.e., the number of relevance vectors can be much smaller than that of support vectors.

REFERENCES

- [1] Jay Narayan Thakre, Divakar Singh, "A Survey on Knowledge Discovery from the Satellite Image Using Association Rule Mining" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013
- [2] Ahmed REKIK, Mourad Zribi, Ahmed Ben Hamida, Mohammed Benjelloun, "Review of satellite image segmentation for an optimal fusion system based on the edge and region approaches" IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.10, October 2007.
- [3] Preeti, Kompal Ahuja, "A Survey on Image Segmentation Using Clustering Technique", International Journal for research in Applied science and Engg. Technology, Volume 2, Issue 5, May 2014.
- [4] Hengnian Qi, Meili Huang, "Research on SVM Ensemble and Its Application to Remote Sensing Classification", www.atlantis-press.com.
- [5] Dimitris G. Tzikas, Liyang Wei, Aristidis Likas, Yongyi Yang, and Nikolas P. Galatsanos, "A Tutorial of Relevance Vector machine for Regression and Classification With Application",
- [6] Harsh Pareek, "Satellite Image Segmentation Using RVM and Fuzzy Clustering,



Shape Classification Using Regional and Global Descriptors

Meetal Kalantri

Department of ECE,
Tulsiramji Gaikwad-Patil College of
Engineering & Technology
Nagpur, India

Rahul Dhature

Department of ECE,
Tulsiramji Gaikwad-Patil College of
Engineering & Technology
Nagpur, India

Amit Fulsunge

Department of ECE,
Tulsiramji Gaikwad-Patil College of
Engineering & Technology
Nagpur, India

Abstract— In this paper three novel hybrid regional descriptor are used for shape classification. The three descriptors are regional skeleton descriptor (RSD), regional area descriptor (RAD) and tangent function (TF). The RAD and RSD are defined by shape's skeleton as a primitive descriptor. The tangent function is generated from the contour by finding the important landmark points and gathering regional information about them. In the matching stage, optimal path searching algorithm is defined in the setting as distance measure function. These shape descriptors are tested on common datasets and the results are analyzed and compared with state of the art methods. The experimental results show that, our results are satisfactory as compared to others.

Keywords— RAD, RSD, Tangent Function, skeleton, optimal path searching

I. INTRODUCTION

The shape of an object is affected by various factors. The variation of shape with protusion. Occlusion, affine deformation and noise are called non-rigid transforms[1][2]. The good representation should be scale, transition and rotation invariant and be robust to non-rigid transform.

The procedure to find good features which can represent shape and similarity measure for classification is called shape classification. Many descriptors have been proposed, which can be categorized as 1) contour based methods 2) Skeleton based methods 3) region based methods.

The boundaries of shapes are used in countour based method. The methods which uses contour based features are mostly efficient and can be easily implemented. But they are insensitive to boundaries. The countour based methods are Wavelet Decriptors [3]-[5] on boundary, Hidden Markov Models[6] etc.

The information inside the shape is used by region based method. The whole shape is considered as domain and is transformed to another domain for descriptor extraction. E.g. Radon transform. The landmark points on contour and descriptors are computed by gathering region information around those points.

Skeleton based methods uses topological information from the shape and forms shape descriptors based on it. Many methods fall into this category like Shock graph [7] etc. However skeleton is heavily affected by protrusion and occlusion. Also this category are requires to process alignment problems.

In this paper, we have proposed regional descriptor for shape classification, which includes three descriptors regional are descriptor(RAD), regional skeleton descriptor (RSD) and tangent function (TF). In next section, the framework of the proposed method and how the features are extracted from the shape are explained. We have also introduced the dynamic algorithm for classification and how the distance generated dissimilarity in Section III. The experimental results from the proposed method which are done on widely used datasets are explained in Section IV. Analyzing of the results and the comparison with other methods are done in this section. Finally, conclusions are made in Section V.

II. EXTRACTION OF SHAPE DESCRIPTORS

Our work shares similar framework with the Ling's Inner-distance [8], Belongie's Shape Context [9] and Alajlan's Triangle-Area Representation [10]. We begin with extraction of features on local points and gathering surrounding shape information. A dynamic algorithm based Optimal Path Searching (OPS) is used to find local point's correspondences and measure total distance of two shapes. Finally, the shape is classified into the category having minimum distance. In previous work, local points were used, whereas in our method local regions are used. In our proposed approach, we have defined three descriptors: 1) regional area descriptor (RAD) and 2) regional skeleton descriptor (RSD), which uses the skeletons and contours and can called as skeleton based and contour based hybrid descriptors. And 3) Tangent Function, which falls into contour based category, collects the significant points from the contour according to some rules. It is assumed that the shapes are well segmented and considered as solid plate, like other shape classification methods.

A. Regional Skeleton Descriptor

The most useful primitive shape descriptor for representing as shape is the skeleton. But matching of two skeleton is too tough because the skeleton is the representation of the topological structure of the shape and as the shape changes, the topological structure changes. Hence, in our proposed approach, we have tried to take advantages of skeleton which is effective in topological structure and have tried avoiding the disadvantages of it, and we proposed the shape descriptor viz. Regional skeleton descriptor.

The RSD defines the local part of shape by calculating the perimeter of the area from the skeleton to the segment of the contour. Following the procedure given below, the regional skeleton features are extracted from the specific local region:

- 1) A graph of multiple base points, which are distributed along the contour, equally, is built.
- 2) The skeleton of the shape is found out and the point in skeleton must have radius of it maximum disk from the contour.
- 3) To find the closest points on skeleton from each point, skeleton is searched and accordingly, Euclidean distance is calculated between them.
- 4) Using depth priority search (*DPS*) algorithm, for each pair of consecutive base points, the corresponding closest points distance on skeleton is calculated by finding out the path length on skeleton.
- 5) The regional skeleton descriptor is obtained by adding up distances from 3) and 4).

Geometrically, this descriptor defines that how much area the part of contour between two points is included in the shape. Given two base points p_1 and p_2 , and their closest points on skeleton sp_1 and sp_2 , the *RSD* of the region between these points can be mathematically defined as:

$$RSD(p_1, p_2) = D(p_1, sp_1) + D(p_2, sp_2) + length(DPS(p_1, p_2)) \quad (1)$$

where *DPS* (,) is depth priority search function which returns a discrete path . Let *O* be the global descriptor and it is organized into a vector as follows, supposing that we have *N* base points,

$$RSD(O) = \{RSD(p_1, p_2), RSD(p_2, p_3), \dots, RSD(p_{N-1}, p_N), RSD(p_N, p_1)\} \quad (2)$$

B. Regional Area Descriptor

Though RSD can be used for representation of shape, but it solely is not enough to justify distance between shapes. Fig. 1 is a very clear counter-

example of the two local shape descriptors shown as below:

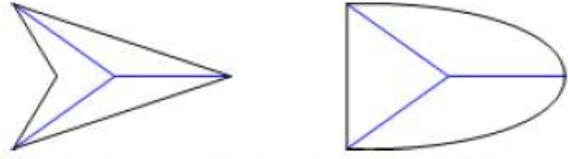


Fig. 1. Two simple different shapes have same skeleton.

Therefore, the regional area descriptor is generated by the same procedure as *RSD* that is based on local part. The Regional Area Descriptor (*RAD*) adds the maximal radii information on the skeleton segment which corresponds to the segment of contour, which is nearly equal to the quantity of area of local region. It could be expressed in mathematical form as:

$$RAD(O) = \{RAD(p_1, p_2), RAD(p_2, p_3), \dots, RAD(p_{N-1}, p_N), RAD(p_N, p_1)\} \quad (3)$$

where

$$RAD(sp_i, sp_{i(mod.N)+1}) = \sum_{j=1}^{length(sp_i, sp_{i(mod.N)+1})} radius(p_j) \quad p_j \in [sp_i, sp_{i(mod.N)+1}]$$

C. Tangent Function

A very important primitive descriptor for a shape which can be used as complementary descriptor along with the skeleton based descriptors is contour, which is show in Fig. 2.



Fig. 2. Two simple shapes may have same skeleton and same size of local area.

A segmented shape, generally, contains some noise which affects its shape descriptors to some extent and cause high computational cost. The insignificant information on the boundary noise and should be removed and those important points on the large turning corners should be preserved. We have used the turning angles and considered that other two shape descriptors will compensate the loss of information in the segment on simplified contour in the whole system. For simplifying it: we replace two consecutive line segments on the contour with one line segment which will join their endpoints, if joint 'condition' of two line segments that are consecutive is lower than a pre-defined threshold. The joint 'condition' is a function which is defined to compute that how much the two consecutive line segments and their angle is contributing to the whole shape. And our approach reduces each and every shape to a minimum fixed number of points.

We first define the relevance function [11], [12], to achieve this:

$$K(s_1, s_2) = \frac{\beta(s_1, s_2) \cdot L(s_1) \cdot L(s_2)}{L(s_1) + L(s_2)} \quad (4)$$

The relevance function which is defined on two consecutive vectors and gives a value which represents how important the triangle consist of s_1 and s_2 contributes to the whole shape. The higher value of $K(s_1, s_2)$, the more significant. The two vectors that connects the endpoints, are to be replaced, and number of points is more than the pre constant which is predefined and if there is an i , such that it is minimum. By applying such operation iteratively, the shape boundary is traversed until number of points gets equal to our pre-defined value.

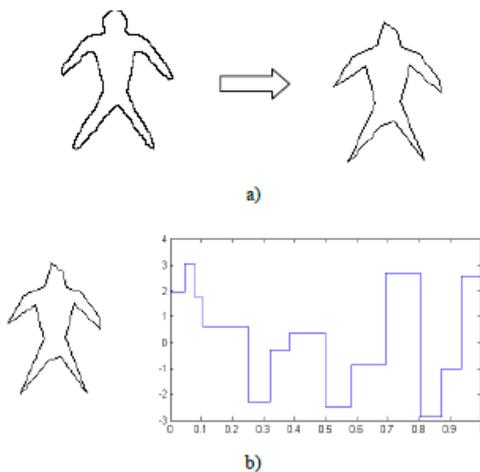


Fig. 3. a) An image boundary and corresponding simplified one. b) A simplified boundary and its tangent function.

After simplification, as Shown in Fig. 3, a simplified shape is generated which has less noise and preserves shape information as well. The tangent function (TF), also called a turning function is as shown in Fig. 4 which is a multi-valued function defined $T(C) : [0,1] \rightarrow [-\pi, \pi]$ by $T(C)(s) = C'_-(s)$ and $T(C)(s) = C'_+(s)$, where $T(C)(s) = C'_-(s)$ and $T(C)(s) = C'_+(s)$ are left and right derivatives of C . The value of $T(p)$, p is a point on C , is angle between the line segment vector and a reference vector. The tangent function $T(C)(s)$ specifies wherever there is turning on the contour, decreasing with right turns and increasing with left turns is used as a shape descriptor. To achieve rotation invariance, we pick up the pixel which is farthest from centroid in the shape to start simplification.

D. Rotation, Scale, Transition Invariance

The proposed descriptors can achieve *RST* invariance. Firstly, the transition invariant can be naturally satisfied. After the contour and skeleton are extracted, our descriptors have nothing to do with the position of the shape. As for rotation invariant, our descriptors are arranged in vector form in which the local features are kept in clock-wised form. Therefore, the invariant property can easily solved by a circular shift on the

vector in matching. Finally, by normalizing the global vector or the vectors divided by the sum of local features, the scale invariant can be achieved.

III. CLASSIFICATION AND DISTANCE MEASURE

The Optimal Path Searching (*OPS*), which is extended from dynamic algorithm, was used in our matching stage. The most important advantage of *OPS* is that it can handle two descriptor vectors with different dimensions. The local point on one shape is not necessary matched to a fixed point on another shape, but could be matched to the neighbors of a point on the other shape. This is useful in handling deformed shapes which global similarity is exist while some significant differences on local parts. The total distance of two shapes is computed during *OPS* as cost of the optimal path to obtain the optimal path, searching all the possible paths is a conventional approach. However, the time and space complexities are prohibitive. To solve this problem, we adopt the dynamic programming algorithms based on Bellman's principle to reduce the time and computational cost. In other words, the Bellman's principle tells us that the concatenation of its two optimal sub-paths will be considered as the optimal path. Therefore, to search the optimal path, we could cast the problem into searching its two optimal sub-paths. The proposed descriptors have different capability in classifying shapes because of different natures and different origins. A combination might be a good idea to take all use their advantages. In order to avoid complicated combination of distance measures, we use a simple linear combination of the distances from three shape descriptors.

IV. EXPERIMENTAL RESULTS

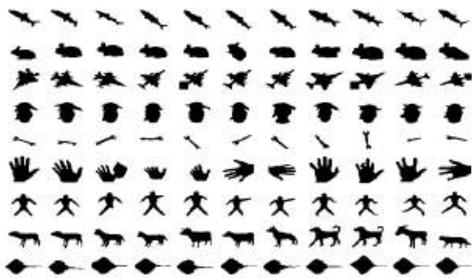
A. Classification

Our classification employed the traditional distance measure based approach which determined by the minimal distance between sample shape and shapes in the dataset. The distance is the dissimilarity of two shape and distance functions are usually defined for the feature that proposed. The distance measure function takes in two descriptors vectors from a pair of shapes respectively and calculates dissimilarity. The larger is the output distance, the less similar are the two shapes. Every shape in dataset is labeled with a known class. A sample from dataset is to be matched with every shape in the same dataset except for itself and the distances are also calculated. We find out the shape in dataset with minimal distance and consider the sample and *this* retrieved shape are in the same class.

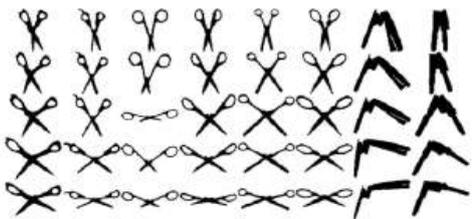
B. Datasets for Experiments

In order to evaluate which approach is better in this field, some standardized databases and benchmarks for experiment are designed. Many databases are designed for different kinds of methods, owing that different methods may have different assumptions on shapes. A commonly used database is 99shapes, by Kimia *et al.* It contains ninety nine planar shapes which classified into nine classes, with eleven shapes in each. Shapes in the same class are in different variant form, including occluded, noised, rotated, etc. Other databases including MPEG-7 Shape Dataset [5], Articulated Dataset,

Swedish Leaf Dataset and Brown Dataset are used to have further experiments. Similar to [13], Precision and Recall is used for benchmark for the reason of fair comparisons.



(a)



(b)

Fig. 4. Common used test material (a) Image dataset of 99 testing shapes provided by Kimia *et al.* (b) Image dataset of articulated testing shapes.

C. Results and Discussion

Table I shows the optimal result from test on 99shape dataset. The numbers of points we sampled from the shapes are 50, 50 and 25 for *RSD*, *RAD* and *TF* respectively.

TABLE I: RETRIEVAL RESULT OF COMBINED DESCRIPTORS ON 99 SHAPE DATASET FOR EACH CLASS

Rank	1 st	2 nd	3 rd	4 th	5 th	6 th	7 th	8 th	9 th	10 th
Quadrupeds	11	11	11	11	8	8	6	5	6	3
Humans	11	11	11	11	11	11	11	11	11	10
Airplanes	11	11	8	5	6	6	2	4	4	2
Grebes	11	11	11	11	10	11	10	8	10	3
Fish	11	11	11	11	10	11	10	7	6	5
Hands	11	11	11	11	9	8	6	8	4	1
Rays	11	11	10	11	11	11	9	7	5	3
Rabbits	11	11	11	10	10	10	11	5	8	5
Wrenches	11	11	11	11	11	11	11	11	11	11

For the articulated dataset, 45, 35 and 45 points are sample for *RSD*, *RAD* and *TF*. Retrieval result on articulated dataset was presented in Table I. We have noticed that result on 99shape from *RAD* is slightly better than *RSD*, while on articulated dataset *RSD* performs slightly better than *RAD*. During the above experiment, we tried to normalize the descriptors and found that experiment on 99 shapes received little influence from normalization while result from articulated dataset has some improvement.

TABLE II: COMPARISON OF RESULTS OF 99 SHAPE DATASET WITH SHAPE CONTEXT [16]

Method	Shape context	Ours
1 st	97	99
2 nd	91	99
3 rd	88	95
4 th	85	93
5 th	84	85
6 th	77	87
7 th	75	74
8 th	66	68
9 th	56	63
10 th	37	45

TABLE III: COMPARISON OF RESULTS OF ARTICULATED DATASET WITH STATE-OF-THE-ART

Descriptor	1 st	2 nd	3 rd	4 th
L_2 (baseline)	25	15	12	10
SC + DP[16]	20	10	11	5
MDS + SC + DP[16]	36	26	17	15
Contour Distance[10]	36	31	28	23
Center of mass-based[10]	25	12	9	11
Our method	39	36	30	22

From the Table I, our algorithm has a almost 100% correct classified rate for Human and Wrench. We noticed that the Airplanes class is of the lowest correct rate except for the top 3 ranks. And the hit rate declined rapidly which make it singled out from the Table I. The matching distance in this class is carefully investigated and the distance revealed that our descriptors have difficulties in classifying sampled with a large part of protrusion in proportion to its main part. Another reason leads to the low correct rate in Airplanes class is the different numbers of sharp protrusions in different samples in same class and the numbers are various. Since the sharp protrusions influence the branches in skeleton, different numbers of protrusion affect the skeletons' stability within the class and diversify the descriptors of this class.

Comparison with Shape Context is listed in Table II. Compared to Shape Context our proposed shape descriptors have the advantageous property of scale and rotation invariant. Our method enjoy a high hit rate from 1st to 5th rank however, unfortunately, it slightly falls behind from 6th to 10th rank.

A comparison of the results on articulated dataset with other state-of-the-art methods shows that our method is highly articulation insensitive. The articulated dataset is a challenging dataset for shape classification owing that most samples in the dataset are segmented from real images of same type of object, for instance, the scissors and samples in the same class are from the same object but with some degree of articulation at some branch points. Results data listed in Table III shows that the proposed method outperformed others on this dataset.

V. CONCLUSIONS

In this paper, we proposed hybrid regional and global descriptor for shape classification. By combining the descriptors, the drawbacks of each descriptor are overcome. In the matching stage, a dynamic programming based Optimal Path Searching is integrated into our method. The matching algorithm successfully handled the challenge of matching two different descriptors in different lengths. The proposed methods are tested on the widely used 99shape and articulated dataset. Experimental results are satisfactory. Data of result is presented in table form and compared to other the-state-of-art methods in literature as well.

ACKNOWLEDGEMENT

The authors would like to thank the referees for their valuable comments.

REFERENCES

- [1] L. Latecki, R. Lakämper, and U. Eckhardt, "Shape descriptors for non-rigid shapes with a single closed contour," in *Proc. IEEE Conference on Computer Vision and Pattern Recognition*, 2000, vol. 1, pp. 424-429.
- [2] T. Schoenemann and D. Cremers, "Matching non-rigidly deformable shapes across images: A globally optimal solution," in *Proc. IEEE Conference on Computer Vision and Pattern Recognition*, CVPR 2008, pp. 1-6.
- [3] D. Huang and G. Lu, "Review of shape representation and description techniques," *Pattern Recognition*, vol. 37, 2004.
- [4] Y. W. Chen and Y. Q. Chen, "Invariant description and retrieval of planar shapes using radon composite features," *IEEE Transactions on Signal Processing*, vol. 56, pp. 4762-4771, 2008.
- [5] W. I. Yao and C. M. Pun, "Invariant shape representation by radon and wavelet transforms for complex inner shapes," in *Proc. International Conference on Information and Automation*, 2009, pp. 1144-1149.
- [6] M. Bicego and V. Murino, "Investigating hidden markov models' capabilities in 2d shape classification," *IEEE Transactions on Pattern Analysis And Machine Intelligence*, vol. 26, pp. 281-286, Feb. 2004.
- [7] T. B. Sebastian, P. N. Klein, and B. B. Kimia, "Recognition of shapes by editing their shock graphs," *IEEE Transactions on Pattern Analysis And Machine Intelligence*, vol. 26, pp. 550-571, May 2004. [8] H. Ling and D. W. Jacobs, "Shape classification using the inner-distance," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, pp. 286-299, 2007.
- [9] S. Belongie, J. Malik, and J. Puzicha, "Shape matching and object recognition using shape contexts," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, pp. 509-522, 2002.
- [10] N. Alajlan, I. E. Rube, M. S. Kamel, and G. Freeman, "Shape retrieval using triangle-area representation and dynamic space warping," *Pattern Recognition*, vol. 40, pp. 1911-1920, 2007.
- [11] L. J. Latecki and R. Lakämper, "Convexity rule for shape decomposition based on discrete contour evolution," *Computer Vision and Image Understanding*, vol. 73, pp. 441-454, 1999.
- [12] L. J. Latecki and R. Lakämper, "Shape similarity measure based on correspondence of visual parts," *IEEE Transactions on Pattern Analysis And Machine Intelligence*, vol. 22, pp. 1185-1120, 2000.
- [13] D. Sharvit, J. Chan, H. Tek, and B. Kimia, "Symmetry-based indexing of image databases," *J. Vis. Commun. Image Represent*, vol. 12, 2004.



GSM BASED IRRIGATION SYSTEM CONTROL & MONITORING

Ketan Mishra¹, Deepak Kumar Sharma²

¹Design Engineer, Free Scale Semiconductor
Bangalore, Karnataka, India

²Assistant Professor, Department of Electronics Engineering
Tulsiramji Gaikwad-Patil College of Engineering and Technology,
Nagpur (M.S), India

¹ketanmse@gmail.com , ²deepaksharmatgpcet@gmail.com

Abstract- Agriculture is source of livelihood of majority Indians and has great impact on the economy of the country. In dry areas where there is shortage of water in case of inadequate rainfall, Irrigation becomes difficult. So, it needs to be automated for proper growth and productions are handled remotely for farmer safety.

In accordance to this we design a GSM based Irrigation System Control and monitoring this system will be very economical in terms of hardware cost, power consumption and call charges. The proposed control system works on two principles one is GSM Modem based sensor network and another is of 'packet switching' used by SMS controlled devices. Hence it can be seen that in India the process of automation is very much needed to be spread as to achieve good cultivation providing a cheaper approach to the 'COMMON MAN'.

Keywords- GSM Modem, irrigation, packet switching, control monitoring, automation.

I.INTRODUCTION

The purpose of this project is to monitor and control the water flow to an irrigation system using Mobile Phone. This can be achieved by the use of soil moisture sensor, which senses the water content in the soil. This sensor output is given to a Microcontroller based control system for further data processing.

II.LITERATURE REVIEW

International Conference on Communication Systems and Network Technologies 2011-2012, has provided the need of remote automation of irrigation. As seen in the recent Monsoon the average rainfall has considerably reduced in India thus, leading to various adverse effect on the farmer's and leading to increase of burden leading to high inflation in economic standards hence a proper mix of technology with Agriculture will provide a new look to the Indian Irrigation system with a proper automated irrigation system [2] which can be controlled by the farmer anywhere in India [3].

A Microcontroller is a single chip inbuilt with advance functions [2][8] with the use of various Sensors providing the circuit user friendly and very much in accordance with 'packet data transfer' from GSM Modem 1 in User side to the GSM Modem 2 in the Field interfaced with simple programming logic with hardware providing simple codes to the User to whether Switch ON/OFF the pump.

III. BLOCK –DIAGRAM

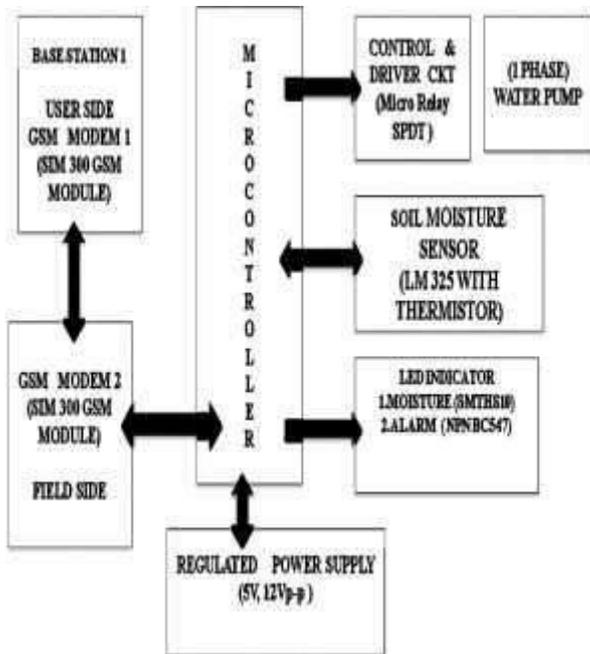


Fig 1: Block Diagram in respect to User Side and Field Side

Base Station Unit works as the main unit for the User side and it is connected to the Microcontroller [7] for receiving the message for functioning of the water pump in ON/OFF state and thus the GSM MODEM 2 provides the Filed side synchronization with the Microcontroller as well as the Soil Moisture Sensor which acts as Transducer [4] for the working of the sensor producing the indication on the LED indicator. Moreover, it often happens that the Pump goes out of order for that has to be achieved by an error message to the User side however the LED indicator will also provide a Light indication [3] alarm for manual working and correction of the pump as it would have been damaged.

IV. DISRIPTION

To operate the sensor message is sent by the Base Station Unit (User/Farmer) GSM Modem1 should send a message to the GSM modem 2 in references to that of the soil moisture sensor. As we get the feedback of motor status i.e., ON/OFF in form of simple message from GSM modem 2 present at the motor end.

V.METHODOLOGY

The major building blocks of this project is the Microcontroller based control system [7] with regulated power supply. Soil moisture sensor for providing the proper sensing of soil moisture [2] and its level which is attached to the GSM modem 2 attached to Microcontroller [5] for remote communication [4].Controlling the electrical Water motor (pump) with Hardware and Software interface of Embedded C is provided [6]

to the Control and Driver Circuitry which provides indication LED Indicators for moisture and Alarm based operations [4].

VI.APPLICATIONS

1. As GSM IRRIGATION system control and monitoring finds applications in various fields as: It can be used as controlling of elevators in multistoried buildings
2. It can be used for controlling the temperature coefficients in case of blast furnace and boilers
3. It can be used for household water inlet flow controlling incase of timely storage of water in tanks.
4. It can be used for domestic plant irrigation in gardens thus saves considerable amount of water and provides good plant growth.
5. It can provide monitoring of large water wells situated in remote locations.

VII. WORKING & RESULT

User sends the message through phone to the gsm module. That message is captured by gsm module and sends the message to the microcontroller. Here we are writing the program using the string command that accepts the strings as commands directly. If the command is 'help' then gsm understands that user is ready to use the gsm. It stores the number and ready to communicate with that number.

Then it sends a message that "irrigation project is ready to use" Later if the user wants to on the pump. He sends the command 'on' then that message is sent to the microcontroller. Microcontroller checks the output of soil moisture sensor.

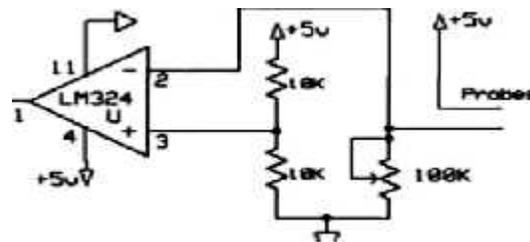


Fig 2: LM324 Soil Moisture Sensor

even people whose life styles are very far to this well known term technology. So it is our responsibility to design few reliable systems which can be even efficiently is used by those people. This basic idea gave birth to GSM Based Irrigation System Control and Monitoring. Here the automation is done and divided into User Side and Field Side using Microcontroller based Technology in reference to widely used GSM.

REFERENCES

- [1] Neetesh Purohi, Pritish Varadwaj, Sanjiv Tokekar "Reliability Analysis of Wireless Sensor Network" IEEE INTERNATIONAL CONFERENCE ON NATURAL LANGUAGE PROCESSING 2008.
- [2] Wall RW, King BA (2004). *Incorporating plug and play technology into measuring and control systems of irrigation management.*
- [3] Meron M, Assaf R, Bravdo B, Wallach R, Hallel R, Levin A , Dahan I (1995). *Soil sensor actuated micro irrigation of apples. In: Proceedings of the 5th International Micro irrigation Congress, pp.486- 491.*
- [4] Perry CD, Dukes MD, Harrison KA (2004). *Effects of Variable rate sprinkle cycling on irrigation uniformity.* Annual International Meeting, p.041117.
- [5] *GSM and UMTS: the creation of global mobile communication* by Fried helm Hillenbrand.
- [6] *GSM: Cellular Network, Subscriber Identity Module* by Frederic P. Miller, Agnes F. Van dome.
- [7] *The PIC microcontroller* by John Morton.

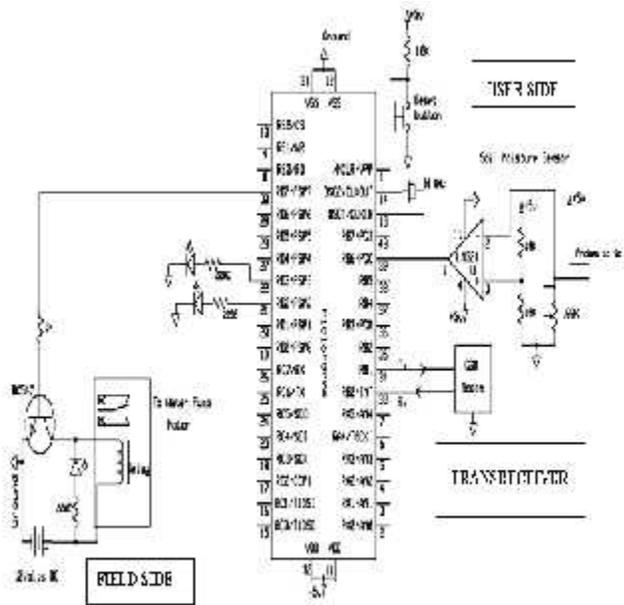


Fig 3: Simulation of Working



Fig 4: Picture of Project Working



Fig 5: SIM 300 GSM MODULES

VIII. CONCLUSION

As the technology is running with time, it is completely occupied the life style of human beings. Even though there is such an importance of technology in our routine life there are



Spin Valve Transistor

Bapan Maiti¹, Deepak Kumar Sharma²

¹Design Engineer, Semiconductor Electronics Pvt. Ltd.,
Delhi, 110006, India

²Assistant Professor, Department of Electronics Engineering
Tulsiramji Gaikwad-Patil College of Engineering and Technology,
Nagpur (M.S), India

¹bapanmfs@gmail.com, ²deepaksharmatgpcet@gmail.com

Abstract-As this universe is concentrated with electrons and its nature plays an important role in the energy distribution. In our conventional electronic devices we use semi conducting materials for logical operation and magnetic materials for storage, but spintronics uses magnetic materials for both purposes.

As referred as Spin Valve Transistor is different from conventional transistor. In terms for conduction we use spin polarization of electrons. Only electrons with correct spin polarization can travel successfully through the device. These transistors are used in data storage, signal processing, automation and robotics with less power consumption and results in less heat. This also finds its application in Quantum computing, in which we use Qubits instead of bits.

Key words- Spin Valve Transistor, Qubits, Quantum

I. INTRODUCTION

Two experiments in 1920's suggested spin as an additional property of the electron. One was the closely spaced splitting of Hydrogen spectra lines, called fine structure. The other was Stern-Gerlach experiment, which in 1922 that a beam of silver atoms directed through an inhomogeneous magnetic field would be forced in to two beams. These pointed towards magnetism associated with the electrons. Spin is the root cause of magnetism that makes an electron tiny magnet. Magnetism is already been exploited in recording devices. Where data is recorded and stored as tiny areas of magnetized iron or chromium oxide. To access that information the head detects the minute changes in magnetic field. This induces corresponding changes in the head's electrical resistance – a phenomenon called **Magneto Resistance**.

II. LITERATURE REVIEW

Spintronics came into light by the advent of Giant Magneto Resistance (GMR) in 1988. GMR is 200 times stronger than ordinary Magneto Resistance. It results from subtle electron – spin effects in ultra multilayer of magnetic materials that cause a huge change in electrical resistance. The literary aspect of it shows the discovery of Spin Valve Transistor (GMR in magnetic multilayers) has led to a large number of studies on GMR systems. Usually resistance of multilayer is measured with the Current in Plane (CIP). For instance, Read back magnetic

heads uses this property. But this suffers from several drawbacks such as; shunting and channeling, particularly for uncoupled multilayer and for thick spaced layers diminish the CIP magneto resistance. Diffusive surface scattering reduces the magneto resistance for sandwiches and thin multilayer's.

The use of Micro fabrication techniques for CPP measurements, from 4.2 to 300k was first shown for Fe/Cr multilayer's, where the multilayer's were etched into micro pillars to obtain a relatively large resistance (a few milli ohms). These types of measurements have confirmed the larger MR for the CPP configuration, but they suffer from general complexity of realization and measurement techniques. Experiments using electro deposited nano wires showed CPP MR up to 15% at room temperature; such multilayers find an application in Spin Valve Transistors.

III. PRINCIPAL AND CONSTRUCTION

A spin valve multilayer serves as a base region of an n silicon metal base transistor structure. Metal base transistors have been proposed for ultrahigh frequency operations because of 1. Negligible base transport time. 2. Low base resistance, but low gain prospects have limited their emergence. The first evidence of a spin valve effect for hot electrons in Co/Cu multilayers is the spin valve transistor.

In spin valve transistor (SVT) electrons are injected in to metallic base across a Schottky barrier (Emitter side) pass through the spin valve and reach the opposite side (Collector side) of transistor. When these injected electrons traverse the metallic base electrons are above Fermi level, hence hot electron magneto transport should be considered in Spin Valve Transistor (SVT). For the preparations of transistor we apply direct bonding, both to obtain device quality semiconductor material for the emitter and to allow room temperature processes.

Here metal parts were laid down directly on to the doped Silicon base layer, which resulted in the information of metal silicides at the interface. These degrade device performance due to the large depolarizing effect they have on the flow of spin polarized charge carriers through the interface which severely reduces the magnetic sensitivity of devices.

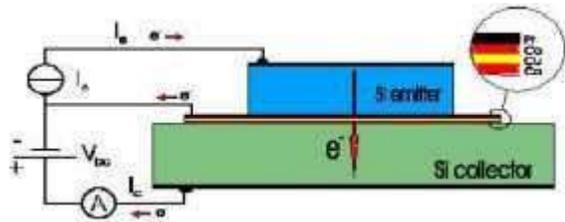


Figure 1. Spin valve Transistor construction

IV. WORKING

The collector barrier height about 0.7eV while the emitter barrier height is 0.6eV. The emitter and collector Schottky barrier are in forward and reverse bias respectively as illustrated by the CB configuration in Fig. 1. The emitter bias accelerates the electrons towards the emitter barrier, after which they constitute the hot “Ballistic” electrons in the base. The probability of passing the collector barrier is limited by the collisions in the base which effect their energy and trajectory by optical phonon scattering in the semiconductor and by quantum mechanical reflections at the base collector interface. For a base transistor with a single metal base film, this can be expressed by the CB current transfer ratio r current gain. The energy band diagram of the bonded Co/Cu f spin valve transistor is shown below.

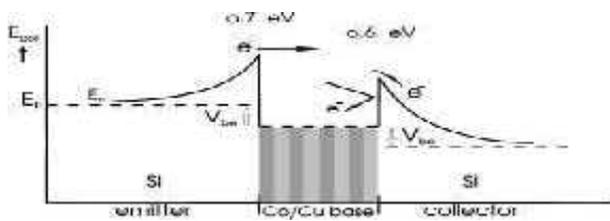


Figure 2. Energy Band Diagram

$$\alpha_o = (J_c - J_{leak}) / J_e = \alpha_c \alpha_e \alpha_{qm} e^{-w/\lambda}$$

Where

α_e = emitter efficiency

α_c = collector efficiency

α_{qm} = quantum mechanical transmission

W = base width

And λ is the hot electron mean free path (MFP), in the base. The factor $e-w/\lambda$ represents the probability of transmission of the hot electrons through the base. J_c is the total collector current, J_{leak} the collector leakage current, determined by the reverse biased collector Schottky barrier and J_e is the injected emitter current. The ascend of electrons depend among others, on the type and quality of the semi conductors. In the SVT under consideration, the thickness of the individual layers (Co/Cu) is much smaller than the spin-slip diffusion length.

V. CHARACTERISTIC APPROACH

A. Magnetic sensitivity

The barrier height of collector and emitter as determined at room temperature by the current voltage method are 0.7 and 0.6 eV. Because of the low barrier heights and large area of the collector the leakage current is quiet large (30 μ A) and exceeds the magneto current for an injection current of 100mA. Magneto current measurements have been performed at 77 K reducing the leakage current to acceptable values, magneto current measurements have been performed with the CB setup of fig.1, $I_b = 0V$. The collector current I_c Vs the applied magnetic field is plotted in fig. 3 as large current change with field is observed, with typical GMR characteristics of a second peak Co/Cu multilayer, such as saturation field and hysteresis. The corresponding CIP-MR value of implemented multilayer was only 3% in 10K Oe. The large values of MC (%) and J indicate a short $\lambda \uparrow$ (\downarrow) (of order of 0.5 to 1 nm): however bulk MFP will require further measurements.

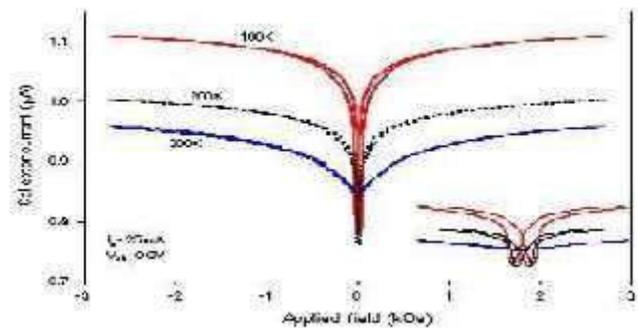


Figure 3. Magnetic sensitivity of collector current at different temperatures

B. Temperature effects

Transport property of hot electron is not fully understood at very low energy regime at finite temperatures. So, It is necessary to probe the temperature dependence of the hot electron transport property in relation to the SVT. The collector current across the spin valve changes its relative orientation of magnetic movements at finite temperature. Surprisingly the collector current showed

different behaviors depending on the relative spin orientation in Ferro Magnetic layers. The parallel collector current is increasing up to 200 K and decreasing after that, while anti-parallel collector current is increasing up to room temperature. Actually in ordinary metals, the scattering strength increases with temperature T. This implies that any thermally induced scattering process enhances the total scattering. As a result measured current should be decreased, but it is happening so, increasing of collector current with temperature T may not be related to the ordinary scattering events in the metallic base. Two different mechanisms are suggested. One of them is spatial distribution of Schottky barrier diode. This may explain the behaviors of both parallel and ant parallel collector current up to 200K because thermal energy contributes overcome the Schottky barrier height at Collector side with the increasing temperature T. This mechanism not related to any dependent property but only for the absolute magnitude of both parallel and ant parallel collector current. Therefore, physicist attributes the measured temperature dependence of magneto current to this spin mixing effect.

Basically spin mixing is spin flip process by thermal spin wave emission or absorption at finite temperatures. For example majority (minority) electrons can flip its spin by absorbing (emitting) thermal spin wave and then goes into spin down (up) channel.

VI. APPLICATIONS

Spin transistors have huge potential for incorporation in stable, high sensitivity magnetic field sensors for automotive, robotic, mechanical engg. & data storage applications. This may also be used as Magnetically Controlled Parametric Amplifiers & Mixers, as magnetic signal processors, for control of brush less DC motors & as Magnetic Logic elements. In log applications they have the advantage over conventional semiconductor chips that they do not require power to maintain their memory slate. It finds its application towards Quantum Computer, a new trend in computing. Here we use Qubits instead of bits. Qubit also represents only 1 & 0 but here they show superposition these classical states. But it is in pioneering stage.

There are major efforts ongoing at Honeywell, IBM, Motorola in developing RAM based on spin valves and metal tunnel junctions such devices called MRAM have demonstrated faster speed, high density low power consumption, non volatility and radiation harness they are promising replacements for the Semi Conducting RAM currently used.

VII. ADVANTAGES

Traditional transistors use on & off charge currents to create bits – the binary 0&1 of Computer information. Quantum spin field effect transistor will use up & down spin states to generate the same binary data.

1. A currently logic is usually carried out using conventional electrons, while spin is used for memory. Spintronics will combine

both.

2. In most Semi Conducting transistors the relative proportion of the up & down carries types are equal. If Ferro Magnetic material is used as the carrier source then the ratio can be deliberately skewed in one direction.

3. Amplification and / or switching properties of the Device can be controlled by the external magnetic field applied to the device.

4. One of the problems of charge current electrons is that we pack more devices together, the chip heats up. Spin current releases heat but it is rather less.

VIII. CONCLUSION

Now it is clear that, Spin valve transistor is more versatile and more robust but it needs further fabrication methods to improve magnetic sensitivity of collector current. The greatest hurdle for spintronic engineers may be controlling all that spin. To do it on a single transistor is already feasible while to do it on a whole circuit will require some clever ideas. However the key question will be whether any potential benefit of such technology will be worth the production cost. Spin valve transistors and other spin devices will become affordable by using common metals.

REFERENCES

- [1] *Perpendicular hot electron spin-valve effect in a new magnetic field sensor: The spin-valve transistor* D.J. Monsma, J.C. Lodder, Th.J.A. Popma and B. Dieny Phys. Rev. Lett. 74, 5260 (1995).
- [2] *Temperature dependence of magneto current in spin-valve Transistor: a phenomenological study* Jisang Hong, P.S. Anil Kumar
- [3] *Spintronics: A Spin-Based Electronics Vision for the Future-* S. A. Wolf, D. D. Awschalom, R. A. Buhrman, J. M. Daughton, S. von Molna, M. L. Roukes, A. Y. Chtchelkanova, D. M. Treger.
- [4] *Spin-valve transistor formed on GaAs [001] substrate* Magnetism Conference, 2002. INTERMAG Europe 2002. Digest of Technical Papers. 2002 IEEE International Date of Conference: 2002 Author's Mizushima, K. Corp. Res. Dev. Center, Toshiba Corp., Kawasaki R.
- [5] *Current fluctuations in non-collinear single-electron of Spin Valve Transistor-* dated 5th June 2012 Stephan Lindebaum and Jürgen König Theoretical Physics, University of Duisburg-Essen and CENIDE, Duisburg, Germany.



Review on Automatic RBC's and WBC's Counting by Using Circular Hough Transform and K-Mean Clustering Algorithm

Sneha Chauhan

*PG student dept. of ECE
Abha Gaikwad-Patil College of Engineering
Nagpur, India
snehachauhan2011@gmail.com*

Deepak Bhoyar

*Assistant Professor dept. of ECE
Abha Gaikwad-Patil College of Engineering
Nagpur, India
deepakbhoyar@gmail.com*

Abstract—Blood cell analysis is important for all human beings, because there are WBCs, RBCs, and Platelets in human blood, White blood cell count gives the important information about our blood and diseases related to blood that help diagnosis many of the patient's sickness. This project work presents an adaptive approach for extracting, detecting and WBC counting in microscopic blood sample images. The measure of WBC and RBC Cells are very important for the doctor to diagnose various diseases such as anemia, leukemia etc. So, precise counting of blood cells plays very important role. In hospital laboratories the old conventional method used which involves manual counting of blood cells using a device called Haemocytometer. But due to this, process is extremely monotonous, time consuming, and leads to inaccurate results. Even the hardware solutions such as the Automated Hematology Counter exists, they are very expensive machines and unaffordable in each and every hospital laboratory. In order to overcome these problems, this project presents an image processing technique to counting and detecting the number of red blood & white blood cells in the blood sample image using circular Hough transform and k-means clustering technique. The use of image processing technique to helps in improving the effectiveness of the analysis in term of accuracy and time consumption.

Keywords: *WBC, RBC, Automated Hematology Counter, circular Hough transform, k-means clustering technique*

I. INTRODUCTION

In medical analysis blood cell count plays very vital role for blood cell count. Variations in the count of blood cells cause many diseases in the human body. For overall health diagnosis and health assessment of many human disorders complete blood count is required. Abnormal increment or decrement in cell count indicates that the person has many indispensable medical condition. In which the Complete Blood Count (CBC) is a blood test, extensively used to check various disorders such as allergies, infections, problems with clotting, anemia, leukemia etc. In order to perform CBC test, firstly the blood film is imaged and then stained with a transmission light microscope. Here the analysis of the blood sample is done manually to count number of blood cells and also to identify

and to judge disorders in blood samples through a microscope. But it is a very time consuming process and undesirable human error. In essence, the goal behind of this paper is to develop and to validate the required image processing steps to count blood cells on blood smear slides. Recently aims to provide the current work of mitigate problems posed by different conditions such as noisy and degraded images; detect the overlapping of cells to differentiate RBCs and WBCs which are present in a blood smear slide counting RBCs and WBCs.

II. CELLULAR ELEMENTS OF BLOOD

A. White blood cells or leukocytes

White blood cells are an important part of the body's immune system. They protect against certain type of the bacteria, viruses, cancer cells, infectious diseases. The density of the leukocytes in the blood is 5000-7000 /mm³. In 5 different types Leukocytes are categorized. They are Neutrophil, Eosinophil, Basophil, Monocyte, and Lymphocyte. This type of Low WBC counts may indicate that a person is in risk of infection. The high WBC counting might indicate an existing infection, tissue damage and leukemia.

B. Red blood cells

Red blood cells, also known as Erythrocyte are the most numerous and important blood cells in the human body. Main function of RBCs is to carry oxygen to the cells in the body. They are small and minute disc shaped cells and contain a protein called hemoglobin by which it will found in red color to blood. Decrease in level of RBC's and WBC's may cause severe diseases including anemia, and leukemia.

C. Platelets

A platelet is a cell fragment that circulates in all the human blood. A low platelet count can cause in human body a person to bleed without their blood clotting. A high platelet count can

be increase the risk of thrombosis like(blood clots inside blood vessels), which stops blood from flowing properly.

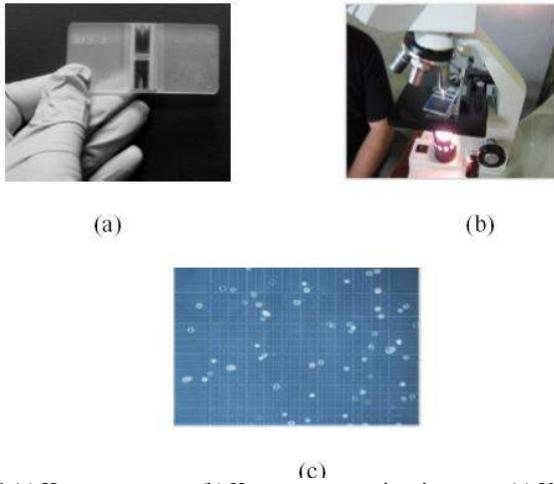


Fig. 1 (a) Haemocytometer (b) Haemocytometer in microscope (c) View of haemocytometer slide through the microscope

III. CURRENT METHODS FOR BLOOD CELL COUNTING

TheHaemocytometer is a conventional device used to count blood cells. It consists of avery thick glass microscope slide with a rectangular indentation by creating a chamber of certain dimensions. This type of chamber is etched with a grid of perpendicular lines in this. It is possible to count the chamber of cells in a specific volume of liquid fluid, and to calculate the concentration of cells in the fluid. To count blood cell, physician will be view haemocytometer through a recently used microscope and count blood cells using hand tally counter.

IV. PRESENT SYSTEM IN USE:

At present there are many manual methods for detecting blood samples like microscope by using Haemocytometer but overlapping of blood cells is a very major problem. In todays available equipment there is found overlapping of blood sample but by this software based method it is to be overcome easily.

- Manual counting task is time-consuming and laborious
- In blood cells the counting overlapping is a major problem
- Difficult to get consistent results from visual inspection

Work is based on counting blood cells from different blood sample images which found in it, it is important for every human being to know about their blood cells at low cost and by saving their time with accuracy.

V. PROBLEMS IN THE EXISTING SYSTEM

Image processing is used to modify the Images to improve the image quality. Hence, it can be analyzed in many applications such as in the result accuracy and time consuming. The major steps in image analysis are preprocessing, image segmentation, feature extraction and counting. The most important and challenging step is image segmentation because the feature extraction and counting depends on the correct segmentation of RBC and WBC. Besides that, the uncertainties inherent in the microscope image to identify whether it is a foreign bodies or cell such as dust can interfere in the image analysis process.

- Manual counting task is very time-consuming and laborious
- Counting overlapping blood cells is a major problem
- Difficult to get consistent results from visual inspection

Table I:Normal RBC and WBC in human body:

Blood cell types	Gender	
	Male	Women
RBC	4.5 - 6.0 million/microliter	4.0 - 5.0 million/microliter
WBC	4.5 - 11 thousand/microliter	4.5 - 11 thousand/ microliter
Platelet	150 - 450 thousand/microliter	150 - 450 thousand/microliter

VI. METHODOLOGY:

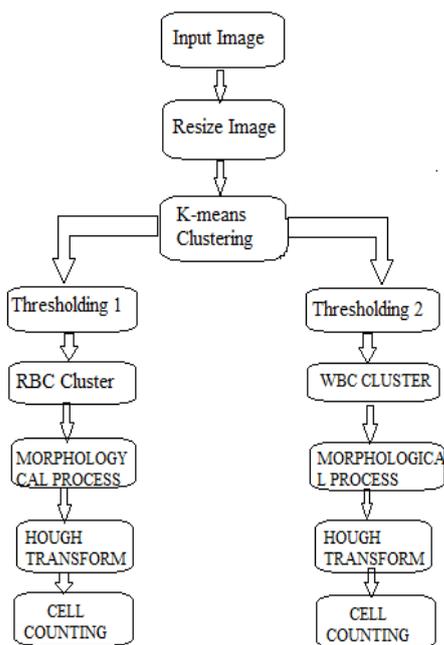


Fig 2. General Methodology for the proposed Method

A. Input Image

The digital microscope is interfaced to a computer and the microscopic images are obtained as digital images.

B. Resize Image

For better segmentation of the blood cells, the obtained image has to be enhanced.

- Green Plane Extraction: The green plane is extracted from a human imported blood cell image. The other planes such as blue and red are not considered because they contain less information about the image.
- Contrast Adjustment: To enhance the image, its available contrast is adjusted by altering its histogram. The image's histogram is equalized.

C. Image Segmentation

By image segmentation, it involves selecting only the region of interest in the image. Here only the blood cells are selected, because they are the important areas of interest. When circular Hough transform is applied, not much of the image segmentation is needed because the applied transform only looks for the circular objects in the image.

D. Detection of Blood Cells

The circular Hough transform is mostly applied to the contrast adjusted image. This transform searches for the blood cells in the image and then to detects them for better result. The function "draw circle" draws circles around the detected cells. Even the overlapped circles are detected.

E. Counting of Blood Cells

Counting the number of cells drawn gives the total number of blood cells in the image.

REFERENCES

- 1) Venkatalakshmi.B, Thilagavathi.K "Automatic Red Blood Cell Counting Using Hough Transform" in Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013) in 2013.
- 2) S.Kareem, R.C.S Morling and I.Kale "A Novel Method to Count the Red Blood Cells in Thin Blood Films" in 978-1-4244-9474-3/11/ IEEE in 2011
- 3) JameelaAli, Abdul Rahim Ahmad, Loay E. George, Chen Soong Der, ShernaAziz, "Red Blood Cell Recognition using Geometrical Features" in IJCSI International Journal of Computer Science Issues, Vol. 10, Issue, 1 in January 2013.
- 4) Ms. Minal D. Joshi, Prof. Atul H. Karode, Prof. S.R.Suralkar, "White Blood Cells Segmentation and Classification to Detect Acute Leukemia" in International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, ISSN 2278-6856 in May – June 2013.
- 5) Naveed Abbas, Prof. Dr. DzulkifliMohamad in "Microscopic RGB color images enhancement for blood cells segmentation in ycbcr color space for k-means clustering" in Journal of Theoretical and Applied Information Technology, Vol. 55 No.1 10th september 2013.
- 6) Gaganjit Singh, Swarnalatha P., Tripathy B.K., SwethaKakani "Convex Hull based WBC Computation for Leukaemia Detection" in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 5 in 2013.
- 7) A.Shanmugam "WBC Image Segmentation and Classification Using RVM" in Applied Mathematical Sciences, Vol. 8, 2014, no. 45, 2227 -2237 Hikari Ltd in 2014.
- 8) C. Allayous, S. Regis, A. Bruel, D. Schoevaert, R. Emilion and T. Marianne-Pepin, "Velocity Allowed Red Blood Cell Classification" in 10th International IFAC Symposium on Computer Applications in Biotechnology in June 4-6, 2007.
- 9) J. M. Sharif, M. F. Miswan, M. A. Ngadi, MdSahHj, MuhammadMahadi bin Abdul Jamil, "Red Blood Cell Segmentation Using Masking and Watershed Algorithm: A Preliminary Study" in International Conference on Biomedical Engineering (ICoBE) in 27-28 February 2012.
- 10) SiyuGuo, Tony Pridmore, Yaguang Kong, Xufang Zhang "An improved Hough transform voting scheme utilizing surround suppression" in Pattern Recognition Letters 30 (2009) 1241–1252 in 2009.
- 11) Harsh Kapadia1, Alpesh Patel "APPLICATION OF HOUGH TRANSFORM AND SUB-PIXEL EDGE DETECTION IN 1-D BARCODE SCANNING" in International Journal of Advanced
- 12) Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 6 in JUNE-2013.
- 13) Vinodv.Kimbahune, Mr. Nelesh j.Uke, "Blood Cell Image Segmentation and Counting" in International Journal of Engineering Science and Technology (IJEST) ISSN : 0975-5462 Vol. 3 No. 3 in march 2011.
- 14) Michael R. Pinsky, Laurentbrochard and JordiMancebo " Applied Physiology in intensive care medicine" springer 229-238 2007
- 15) Dondrop AM, Angus BJ, Chotivanich K., Silamut K., Ruangveerayuth R, Harderman MR, Kager PA, Vreeken J, White NJ. "Red Cell deformability as a predictor of anemia in severe falciparum malaria" AM J Trop Med Hyg 60: 733-744,1



A Review of Improved Vertical Handover in Wireless Network

Prashant G. Bangade

Department of Electronics & Communication

G. H. R. A. E. T.

Nagpur, Maharashtra.

prashants.bangade@gmail.com

Abstract— In traditional vertical handover for individual user, is aware of the decision made by the other users which helps the user to make the choice accordingly. Hence there is a need of acquiring a network selection method which will resolve the problem of network congestion in group vertical handoff. Here Nash equilibrium concept will be used for group of users to achieve the best network selection in Heterogeneous wireless network. For the network selection various network parameters will be taken into consideration for determining the need of handoff. This will reduce the network congestion problem in case of group handover. The result will be obtained and analyzed with the help of simulation tool Network Simulation 2.

Keywords—Vertical Handoff, Nash Equilibrium, 4G and LTE network.

I. Introduction

A heterogeneous wireless network is a network connecting computers and new more devices with different operating systems or protocols. In Wireless heterogeneous Network there are various networks like WIFI, GPRS, WIMAX, UTMS, and WLAN Networks.

- The main benefits of Heterogeneous are enriched capacity and guaranteed spot-free coverage.
- high-speed, high-capacity communications
- This is especially popular in densely-populated areas and business districts that want to provide consistent communication services.

Need of Handoff:

When the mobile travels from one area to another area it might be possible that the coverage of that node or mobile may get loss so it is very much necessary to keep call active or not to break the connection. This is possible because of handoff techniques.

When all the mobile comes to the area of multi-access network then the group of such mobile search for the best network at the same time in the same region this processor is called the group prediction, then the network congestion and degradation occurs and, how to improve such type of congestion thus we have described in this paper using the

various parameters. Previously the network selection is done on the only RSSI and QoS parameter but this parameter gives a rough approximation about the network state, thus even if the network is unable to handle the handoff request then too handoff occurs their by reducing the network efficiency and also the number of successful handoff per unit time.

In this paper we propose the fully decentralize algorithm for network selection i.e. base station doesn't have an authority to select the best network this is done on individual basis that the user mobile take the decision to choose the best network using the various parameter that will define in this paper.

II. Review Of Related Work

In literature, unusual vertical handover algorithms be compared and discussed in wherever their schemes are founded on a universal hypothesis to facilitate the mobiles are coming individually along with these schemes are projected to select the utmost network for every mobile. Though in GHVO circumstances, these VHO schemes may perhaps system performance degradation for instance incompetent resource exploitation, bigger transmission delay and stumpy network accessibility bandwidth, since during these schemes, the existing mobile makes his verdict without the knowledge of the further mobiles decisions. To reduce the network congestion and degradation we use the Nash theory algorithm [1].

The mobiles in this state do not require perceptive the traffic and decisions of every mobiles as happen, only the traffic of mobile they want to know and take the decision [2]. Essentially every mobile does not require a bundle of information like traffic load and strategy of new mobiles to modernize its judgment. What it wants is simply to distinguish his effectiveness depending on the other mobiles trial [5]. The originality in this paper is that it examines the stochastic condition in which mobiles appear concurrently in group, and they do not require to be acquainted with several in succession about the other mobiles in their crowd. Therefore, it propose a completely decentralized algorithm [6] by no information

broadcasted by means of the base station for network choice based on congestion game to tenacity the trouble of network blocking in GVHO circumstances. By using the above decisions, when the mobile has not got the proper handoff and choose the bad network we propose some more parameters. As we know that these generations like to use the faster network hence propose to use the handoff between 4G and LTE networks.

III. Vertical Handoff Technique

In this approach, the accessible fuzzy advance and the projected approach is Classical approach to vertical handoff decision. This is best method of vertical Handoff. In this method, the verdict to handoff is based on RSS, whenever the mobile user approaches the cell edge. The RSS in a mobile radio channel shows to facilitate the received signal power decreases logarithmically by means of expanse between a transmitter and receiver. The average power received (P_r) at a space (d) from the transmitting antenna is given by,

$$P_r = P_0(d/d_0)^{-n} \quad (1)$$

$$P_r = P_0 - [10 \times n \times \log(d/d_0)] \quad (2)$$

Where n is the course loss model, P_r is the standard received power at a distance d from the transmitting antenna, P_0 is the power transmitted. To maintain a tolerable voice quality at the BS receiver, the handoff threshold is reserved vaguely above minimum usable signal. The delta (D) is given as

$$d = P_r \text{ handoff} - P_r \text{ minimum usable} \quad (3)$$

Where $P_r \text{ handoff}$ is the avg. power received at a distance d and $P_r \text{ minimum usable}$ is the min. power.

d is neither too large nor so small.

In this paper we are improving the handoff efficiency of the network without call drop so we are using the various parameters as discussed below:

A. BANDWIDTH

Bandwidth is used to define the range of frequency. For defining the range of frequency there will be upper and lower frequencies in the sets. To provide faultless handoff for Quality of service (QoS) in wireless area, there is a want to control bandwidth constraint of mobile node during progress. Capacity of node is defined as bandwidth, higher the bandwidth lower the call drop and reduce the call blocking ; hence advanced throughput .Bandwidth managing should be an vital part of several of the handoff technique. So we define the bandwidth of LTE network much less than the 4G network.

B. HANDOFF LATENCY

Handover of calls among two BS is encountered normally and the delay can arise during the process of handoffs. This hindrance is called as handoff latency. A good quality handoff verdict model should judge Handoff latency factor along with the handoff latency should be minimized. Various projected handoff decision models have tried to reduce the handoff

latency by incorporating this aspect in their handoff assessment models. Handoff Latencies influence the service worth of numerous applications of mobile phone users. It is essential to consider handoff latency even as crafty any handoff procedure.

C. RECEIVED SIGNAL STRENGTH

The recital of a wireless network correlation depends in piece on signal strength. RSS depicts the power there in a received signal. A signal must be strong as much as necessary among base station and mobile unit to keep signal eminence at receiver. The RSS ought to not be below certain threshold during a network handoff. VHO includes three chronological steps as discussed prior in this paper, specifically handoff initiation, handoff decision and handoff carrying out. Handoff commencement is concerned with values of RSS.

D. NETWORK CAPACITY

A multi criterion algorithm for handoff should as well judge the network cost feature. The cost is to be minimized in VHO in wireless networks. The novel call arrival rates and handoff call advent rates can be analyzed by means of cost function. New Generation heterogeneous networks can come together their respective advantages on coverage and data rates, present a high Quality of Service (QoS) to mobile users. During such situation multi-interface terminals should faultlessly switch from one to other network in order to obtain improved performance or else at least to maintain a incessant wireless connection. Hence, network choice cost is important in handoff decisions. Hence we used to define the network of different capability to which the handoff is doing.

IV. Theoratic Game Model

We relate a group of mobiles so as to arrive scheduled the same instance to a zone enclosed by two technologies (4G, LTE). Let N shows the total quantity of mobiles in group. We describe by n_1 (respectively n_2) the number of mobiles linked to system 1 (respectively 2). On behalf of every mobile, we regard as that the utility function is the same to the throughput professed by the each mobile. The throughput is gritty by the number of mobiles with physical rate individual used by the technology selected. We presume also that the mobiles choose the same technology will receive the related throughput. This shows that the utility function of any mobile depends merely taking place the number of user in the system. This type of non-obliging game is a symmetric congestion game. This kind of game for eternity admits at least one untainted Nash Equilibrium during when every mobile considers its selected strategy near be the best under the certain choices of other mobiles. Thus at Nash equilibrium, no user will yield as of deviating its approach unilaterally.

Let U_i exist the utility function of a user associated to the system. Since the game is symmetric, a Nash equilibrium (NE) (n_1^*, n_2^*) is shown by the below conditions:

- $U_1(n_1^*) \geq U_2(n_2^* + 1)$

$$\bullet U2(n2^*) \geq U1(n1^* + 1)$$

1. Model

We have shown here the game scenario:

- 1) $A = (1, \dots, m)$ is the rest of available networks in outstate, we consider the coexistence among LTE and 4G systems ($m=2$).
- 2) $B = (1, \dots, n)$ is the rest of mobiles. Each mobile has to choose one system network amongst the two accessible networks.
- 3) $X[q]$ move toward of mobile q .
 $X[q] = 1$ if mobile q chooses LTE.
 $X[q] = 2$ if mobile q chooses 4G.
- 4) n_w^t is the number of players that choose LTE at time t .
- 5) n_h^t is the number of players that choose 4G at time t .
- 6) U_{tw} the utility perceived by each user in LTE at time t .
- 7) U_{th} the utility perceived by each user in 4G at time t .

2. The function utility

The observation shows the entire number of mobiles in every set and their allocation in both networks (LTE AND 4G) after meeting to Nash equilibrium. As we compare the parameters of both the network, they don't have the identical decisions (a part of the mobiles choose LTE and the rest choose 4G. This procedure solves the problem of network congestion. The capacity of 4G is greater than the capacity of LTE, a greatest part of mobiles is moved out to the 4G while there are more numbers of mobiles that appear at the matching time. This is due to the force of LTE which is the fact that technology is firstly intended for a lot of mobiles, while 4G is the high speed network. We try to compare the result we have achieved with the Traditional Vertical Handover Algorithm which is

based on the parameters to take decisions. In Vertical handoff several approaches Mobile is receiving signal from several Base station,

Begin

If ($B_w \geq B_h$)

Mobile switch to LTE network

Else

Mobile switch to 4G network

EndIf

If ($rss_1 \geq rss_2$)

Mobile switch to LTE network

Else

Mobile switch to 4G network

EndIf

If ($Qos_1 \geq Qos_2$)

Mobile switch to LTE network

Else

Mobile switch to 4G network

EndIf

End

Hence choosing the best network (4G presents the highest accessible network) by all mobiles due to individual selection at the same time that leads to considerably degradation of mobiles performance. We assume that after convergence to Nash equilibrium is declining in both networks, when additional mobiles are added to the group, but the performance achieved is superior than that achieved by the individuality approach, and hence it is the greatest because mobiles choose different networks based on every others decisions. This results in solving the trouble of network problems due to the throughput apparent in Nash equilibrium which cannot be improved by varying strategies of every user. And the capacity of 4G is greater than the capacity of LTE.

v. Conclusion

We have studied the problem with regard to network choice for GVHO circumstances when several mobile nodes require to handover at the same time. As each mobile node resolve tend to select individually the best network without charming into consideration the other nodes decisions, it is liable that individual selection occurs degradation and network congestion of user function. In this paper the is a prophecy done by all mobile in the grouping that helps them to achieve Nash equilibrium without any single information broadcasted by the BS and comparing the parameters so that the mobile use the best network. This results in solving the trouble of network congestion and performance degradation.

References

- [1] Abdellaziz Walid, Mohamed El Kamili, Abdellatif Kobbane, Abdelfettah Mabrouk, Essaid Sabir, Mohammed El Koutbi, "A Decentralized Network Selection Algorithm for Group Vertical Handover in Heterogeneous Networks": 978-1-4799-3083-8/14/©2014IEEE.
- [2] Sui Bo and Li Lin, Dan Feng, "The Multi-attribute Vertical Handoff Algorithm Based on Node Mobility" 978-1-4799-3279-5 /142014 IEEE.
- [3] R. Kumar and B. Singh, "Comparison of vertical handover mechanisms using generic QoS trigger for next generation network. International Journal of Next-Generation Networks", AIRCCSE, and DOI: 10.5121/ijngn.2010.
- [4] M. Ibrahim, K. Khawam, and S. Tohme, "Congestion games for distributed radio access selection in broadband networks", in Proceedings of IEEE Globecom, Miami, FL, December 2010.
- [5] X. Cai, and F. Liu, "Network Selection for Group Handover in Multi-Access Networks", ICC 08, pp.2164 - 2168, May. 2008
- [6] P.S. Sastry, V.V. Phansalkar, and M.A.L.Thathachar, "Decentralized learning of Nash equilibria in multi-person stochastic games with incomplete information" IEEE Transactions on Systems, Man and Cybernetics, 24(5):769 - 777, May 1994.



The dynamic traffic signal timing control for efficient transportation system

Bhakti Ganesh Kulkarni

Department of electronics and telecommunication,
Pimpri Chinchwad College of Engineering,
Maharashtra,India

Swapna Dhananjay Kulkarni

Department of electronics and telecommunication,
Pimpri Chinchwad College of Engineering,
Maharashtra,India.

Prof.A.M.Ekbote

Department of electronics and telecommunication,
Pimpri Chinchwad College of Engineering,
Maharashtra,India.

Abstract—Traffic management is very difficult task today. In urban areas traffic congestion is very serious problem. It leads to fuel wastage, irritation of vehicle driver time delay in reaching the destination. The existing system uses predetermined traffic light sequence with fixed signal cycle timing.

In this paper we have used strategy of making traffic signal timing dynamically controlled for real time system. The methodology we have used is radio frequency identification RFID technology for achieving low cost and efficient transportation system.

Keywords—Traffic management, Low cost, Efficient transportation system

INTRODUCTION

In urban areas congestion in traffic network is a daily occurrence. Due to high cost building new roads is not an option, there are some geographical as well as environmental limitations. Traditional traffic controls are not efficient to control growing traffic demand. Thus a new technology called as is developed. In this paper we will study traffic signal control systems which will reduce congestion effects and it will make the transportation system efficient.

In conventional method there is fixed signal setting i.e. the time slots for each state (e.g. a red light) is fixed.[2] The signal works in cycle. The cycle time is calculated from observations of traffic volume in particular period. Thus there is no provision to adapt the rapid changes due to various traffic incidents.

The efficient way to solve traffic congestion problem is using dynamic traffic signal control system. In this system time slot for each state is calculated according to traffic volume is real time. Hence it is more efficient way to solve traffic problem. It saves fuel, money and time.

PREVIOUS APPROACH

Most of the present intelligent traffic lights are sensor based with a certain algorithm that controls the switching operation of the system This approach considers the traffic to be moving smoothly and hence does not require any management or monitoring of traffic conditions. When some unpredictable situation develops, or when congestion occurs, there is no proper way of dealing with such development. The sensor based traffic light control on the other hand may require sensors that operate with a line of sight detection, which may present difficulty in detecting vehicles that pass through blind spots detection range. A more elaborate approach has been introduced to overcome these problems. It employs real-time traffic flow with low cost and using RFID technology.

METHODOLOGY

In this system, We are monitoring and displaying 3 main things in signal unit display viz Length of traffic ,Amount of cars,Signal time.we are monitoring and controlling these things because of same latitude and longitude we can talk about length of traffic and amount of cars in a single road.

Microcontroller, RF transceiver, data display unit, power supply unit are key elements of the system. Microcontroller is used for calculation of signal timing depending upon information received from corresponding RFID unit.[3]RF transceiver module is used for wireless data communication. Data display unit is used for displaying and information like calculated signal timing and number of vehicles.

These basic elements are used in various combinations to form three main units viz Signal unit, Roadside unit, Vehicle unit.

[1]Roadside unit initializes RF transceiver module and checks for each consequent unique vehicle ID by transmitting RF signal and then it waits for sometime (few milliseconds) for vehicle response. If vehicle responds it increases count and if no response comes then it sends net unique ID.In this fashion total number of vehicles on one side of intersection is counted. this count is sent to signal unit.

Signal unit receives count from roadside unit ,processes it and calculates dynamic signal time depending on count.then it displays signal time for vehicles.

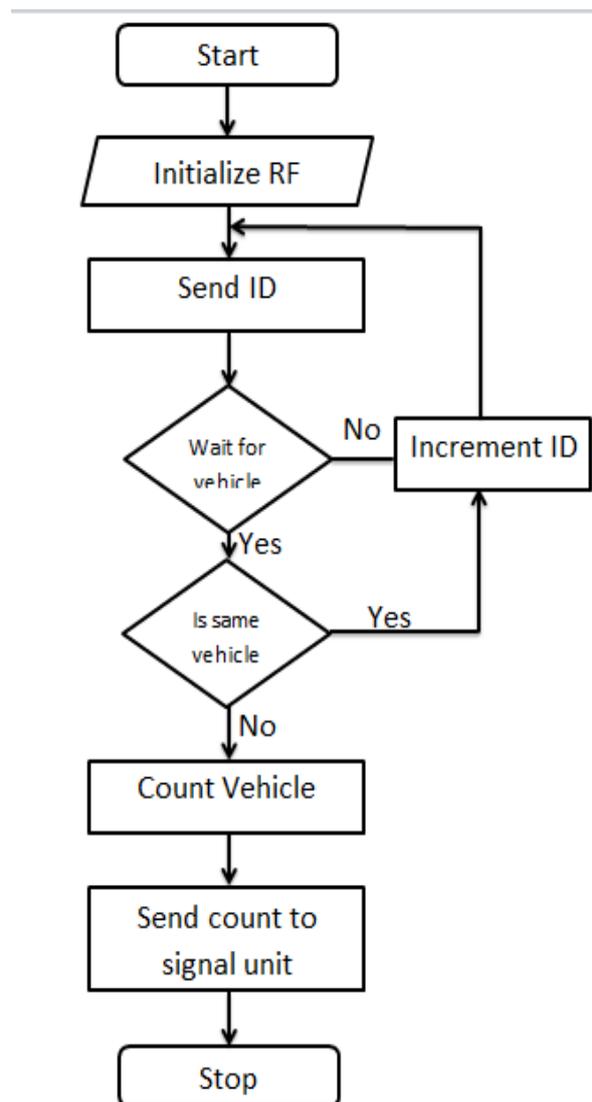
Each vehicle unit has unique ID stored in its memory.When unique ID transmitted by roadside unit matches with ID which is stored in memory then this unit sends acknowledgement to roadside unit.

COMUNICATION PROTOCOL

The communication between microcontroller and RF transceiver module is done by Serial peripheral interface SPI protocol. Serial Peripheral Interfacing is one of the most used serial communication protocols, and very simple to use

Wired transmission of data (though the first preference is mostly USART, but SPI can be used when we are using multiple slave or master systems, as addressing is much simpler in SPI). Wireless transmissions through Zigbee, 2.4GHz

FLOWCHART



CONCLUSION

In this paper simple RFID technology is used to dynamically control traffic signal timing which is based on calculating number of vehicles present on corresponding side of intersection. One of the leading technology in this issue is Digital signal Processing which requires complex processing which takes time and also increases cost of the system. Moreover environmental factors affect image quality.Instead RFID is fast, low cost and solution to manage the traffic congestion.

ACKNOWLEDGMENT

We would like to thank Prof. Angha Ekbote for her special guidance. The authors would like to thank Mr. Milind Potdar, Mr. Nitin Swami for technical guidance and very helpful discussions.

REFERENCES

- [1] A Differential Game Modeling Approach to Dynamic Traffic Assignment and Traffic Signal Control by Li Zhenlong.
- [2] Real-time Traffic Signal Control with Dynamic Evolutionary Computation
Kai Zeng, Yue-Jiao Gong (Corresponding Author) and Jun Zhang.
- [3] AN INTELLIGENT TRAFFIC CONTROL SYSTEM USING RFID by Anuran Chattaraj, Saumya Bansal, and Anirudhha Chandra.
- [4] IoT-RFID Testbed for Supporting Traffic Light Control N. Choosri, Y. Park, S. Grudpan, P. Chuarjedton, and A. Ongvisesphaiboon.
- [5] Eco-Sign: A Load-Based Traffic Light Control System for Environmental Protection with Vehicular Communications by Lien-Wu Chen Pranay Sharma Yu-Chee Tseng.
- [6] Chong hua Li "Automatic Vehicle Identification System based on RFID", Anti Counterfeiting Security and Identification in Communication (ASID), 2010, pp 281-284.
- [7] A. Chattaraj, S. Chakrabarti, S. Bansal, S. Halder and A. Chandra "An Intelligent Traffic Control System using RFID", IEEE Potentials, vol. 28, no. 3, May-Jun. 2009, pp. 40-43.
- [8] Faisal A. Al-Nasser, Hosam Rowaihy "Simulation of Dynamic Traffic control system based on Wireless sensor network", IEEE Symposium on Computers & Informatics 2011, pp 40-45.
- [9] Lejiang Guo, Wei Fang, Guoshi Wang "Intelligent traffic management system based on WSN and RFID" International Conference on Computer and Communication Technologies in Agriculture Engineering 2010, pp 111-114
- [10] Y. Oh and C. Lee, "The decision of the optimal shape of inductive loop detector for real-time signal control," *J. Transp. Res. Soc. Korea*, vol. 13, no. 3, pp. 67-86, 1995.
- [11] M. Rossetti et al., "A DYNAMIC DATA-DRIVEN APPROACH FOR RAIL TRANSPORT SYSTEM SIMULATION," in Winter Simulation Conference, Austin, Texas, 2009.
- [12] M. P. Hunter, et al., "An investigation of real-time dynamic data driven transportation simulation," presented at the Proceedings of the 38th conference on Winter simulation, Monterey, California, 2006



FPGA IMPLEMENTATION OF MAC UNIT USING VEDIC MULTIPLIER

SYED NIGHAT

*Deptt Of Electronics & Comm Engg
Anjuman College Of Engg &Tech
Nagpur, India
nighatsyed786@gmail.com*

PROF.M.NASIRUDDIN

*Asstt Prof Deptt Of Electronics &Telecomm Engg
Anjuman College Of Engg & Tech
Nagpur, India
mn151819@gmail.com*

Abstract—

Implementation of MAC unit is essential for any ALU or microprocessor based application specific integrated circuit. Thus implementing such a circuit with either high speed or low power is very essential for the proper operation of the MAC unit. The MAC unit implemented has slower speed due to inefficient implementation of the multiplier. Ancient Indian mathematics proposed a Vedic technique which allows us to implement the Vedic based multiplier on hardware. This multiplier is not only hardware friendly but also improves the speed of operation of the MAC unit. If a MAC unit is used N times in a microprocessor based system and we are able to speed up the multiplier by a factor of K then the overall speed improvement during the given time is NK. In the previous papers the MAC unit implemented has slower speed due to inefficient implementation of the multiplier. The Vedic multiplier is not only hardware friendly but also improves the speed of operation of the MAC unit. Instead of simple Vedic multiplier, in this paper we will be using a parallel or pipelined Vedic multiplier which will give faster outputs than the previous papers.

Keywords—MAC, Vedic Multiplier, Vedic mathematics, high speed and low power, Urdhava Tiryakbhyam Sutra, pipeline.

I. INTRODUCTION

Due to fast growth of transferable electronic systems like laptop, calculator and mobile etc., and the low power devices has become extremely essential in today's community. The Low power and high throughput circuitry design are playing the challenging role in VLSI designing for real-time signal processing. A high speed and high throughput MAC unit is always a key to attain a high level performance in digital signal processing system. The main motivation of this work is to explore different pipelined multiplier and accumulator structure and circuit design techniques which are suitable for implementing high output in signal processing algorithms and at the same time achieve low power consumption. A regular MAC unit contains of multipliers and accumulators that have

the sum of the previous consecutive products. In this paper a high performance and a high throughput MAC unit with Vedic multiplier and pipe lined accumulator is proposed. Digital signal processors (DSPs) are very essential in different engineering disciplines and the speed of the DSPs is determined by the speed of its MAC Unit. Fast multiplication is very important for convolution, Fourier transforms etc. A fast method for multiplication based on ancient Indian Vedic mathematics is proposed in this paper. Out of the 16 sutras of Vedic mathematics the Urdhva Triyakbhyam Sutra implemented because this sutra is applicable to all cases of algorithm for $n \times n$ bit numbers and gives minimum delay for multiplication of all types of numbers. It enables parallel generation of partial products and eliminates unwanted multiplication steps. Instead, we focus on bringing high performance with new levels of reuse and portability for the logic designer. We have modeled our architectures in VHDL and analyze achievable performance within a real life application as it is being increasingly used for variety of computationally demanding. The function of the MAC unit is given by the following equation $F = \sum A_i \times B_i$.

The paper is organized as follows. Section II presents the Basic operation and design of MAC architecture. Vedic Multiplier and Comparative result described at Section III and IV respectively and Section V shows the conclusion of the work.

II. MAC ARCHITCTURE

The multiplication and accumulation is the main computational kernel in Digital Signal Processing architectures. The MAC unit determines the speed of overall System as it is always lies in the critical path. To develop high Speed MAC unit essential for real time DSP application. In Order to improve the speed of the MAC unit there are two Major factors that need to be considered. The first one is the

Fast multiplication network and the second one is the Accumulation. Both of these stages require addition of large Operands that involve long paths for carry propagation. In Recent MAC accumulation and addition are merging to save The time and power. The MAC unit basically do the Multiplication of two Numbers multiplier and multiplicand and add that product in result stored in the accumulator. For high speed MAC unit, faster adder and multiplier circuits are Required. Figure 1 shows the MAC unit architecture A basic MAC unit can be divided into two main blocks.

1. Multiplier
2. Accumulator

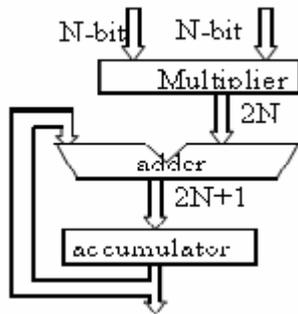


Fig. 1. MAC unit basic structure

The design of MAC unit architecture from Figure 1 shows that the design consists of multiplier, accumulator using carry look Ahead adder (CLA). In this paper, Vedic multiplier and carry Look adder, and full pipelined accumulator are used to high Performance MAC unit design. Vedic multiplier is used to Multiply the two N-bit number. Given multiplier also reduces Power consumption of the MAC unit. The inputs for the MAC Are fetched from memory location and fed to Vedic multiplier block of the MAC which will perform multiplication and give the result to adder which will accumulate the result and then will store the result into a memory location. This entire process is to be achieved in a single clock cycle [2].

III. VEDIC MULTIPLIER

The use of Vedic mathematics lies in the fact that it reduces the typical calculations in conventional mathematics to very Simple one. This is so because the Vedic mathematics are accepted to be based on the natural principles on which the Human mind works. The proposed Vedic multiplier is based on the Vedic multiplication Sutras or formulae. These methods Have been traditionally used for the multiplication of two numbers in the decimal number system. In this paper we apply The same ideas to the binary number system to make the proposed algorithm compatible with the digital hardware. Vedic multiplication based on *URDHVA TIRYAKBHYAM SUTRA* algorithms discussed below.

URDHVA TIRYAKBHYAM SUTRA

Urdhva Tiryakbhyam is a Sanskrit term which means “Vertically and crosswise” of ancient Indian Vedic Mathematics. Urdhva Tiryakbhyam Sutra is a general Multiplication formula applicable to all cases of Multiplication. The idea here is based on a concept which results in the generation of all partial products along with the concurrent addition of these partial products in parallel. The parallelism in generation of partial products and their summation is obtained using Urdhva Tiryakbhyam explained in Figure blow. Since there is a parallel generation of the partial products and their sums the processor becomes independent of the clock frequency. Thus the multiplier will need the same amount of time to calculate the product and hence is independent of the clock frequency. The Vedic multiplier has the advantage that as the number of bits increases, gate delay and area increases very slowly as compared to other multipliers, thereby making it time, space and power efficient. To illustrate this multiplication scheme, let us consider the multiplication of two decimal numbers (325 * 738). Line diagram for the multiplication is shown in Figure 2. Initially the LSB digits on the both sides of the line are multiplied and added with the carry from the previous step. This generates one of the bits of the result and a carry. This carry is added in the next step and the process goes on likewise. If more than one line are there in one step, all the results are added to the previous carry. In each step, least significant bit act as the result digit and all other digits act as carry for the next step. Initially the carry is taken to be zero.

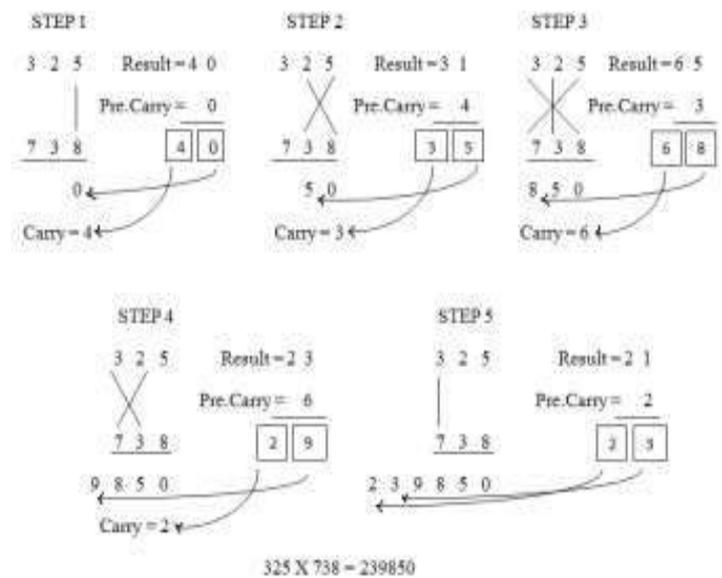


Fig. 2. Multiplication of two decimal numbers by Urdhva Tiryakbhyam

Firstly, least significant bits are multiplied which gives the Least significant bit of the product (vertical). Then, the LSB of The multiplicand is multiplied with the next higher bit of the Multiplier and added with the product of LSB of multiplier and next higher bit of the multiplicand (crosswise). The sum

gives second bit of the product and the carry is added in the output of next stage sum obtained by the crosswise and vertical multiplication and addition of three bits of the two numbers from least significant position. Next, all the four bits are processed with crosswise multiplication and addition to give the sum and carry. The sum is the corresponding bit of the product and the carry is again added to the next stage Multiplication and addition of three bits except the LSB. The Same operation continues until the multiplication of the two MSBs to give the MSB of the product

IV. COMPARATIVE RESULTS OF PROPOSED VEDIC MULTIPLIER FOR MAC UNIT

To show the efficiency of proposed Vedic multiplier for MAC unit, it has been implemented and compared with other popular multiplier structures based on different multiplication algorithms on the same platform of target FPGA, which has been used to implement these popular multiplier structures. Comparison tables are shown below:-

In the following given table which target FPGA has been used belongs to Virtex 2P (family), XC2VP2 (device), FG 256 (Package), -7 (speed grade).

Table 1: Comparative table

Maximum Combinational Path Delay (in ns) for different multipliers at eight bit level						
Karatsuba [19]	Vedic Karatsuba [19]	Modified Booth-Wallace [21]	Vedic with partitioning [21]	Conventional Vedic [19]	Vedic with CSA [12]	Vedic multiplier [4]
31.029	18.695	15.815	15.685	15.418	13.07	11.886

In the following given table which target FPGA has been used belongs to Spartan 3 (family), XC3S50 (device), PQ 208 (Package), -4 (speed grade).

Table 2: Comparative table

Maximum Combinational Path Delay (in ns) for different multipliers at eight bit level			
Array [13]	Booth [13]	Conventional Vedic [13]	Vedic multiplier [4]
32.01	29.549	24.16	19.467

In the following given table the target FPGA used belongs to Virtex 2P (family), XC2VP2 (device), FG 256 (Package), -7 (speed grade).

Table 3: Comparative table

Maximum Combinational Path Delay (in ns) for different multipliers at different bit levels							
N bit level multiplier	Karatsuba [19]	Vedic Karatsuba [19]	Modified Booth-Wallace [21]	Vedic with partitioning [21]	Conventional Vedic [21]	Vedic with CSA [12]	Vedic Multiplier [4]
4-Bit	---	---	---	---	---	8.405	8.387
8-Bit	31.029	18.695	15.815	15.685	15.418	13.070	11.886
16-Bit	46.811	27.81	36.071	23.063	22.604	18.580	15.718
32-Bit	82.834	49.864	---	---	35.76	---	20.574

In the following given table the target FPGA used belongs to Spartan 3 (family), XC3S50 (device), PQ 208(Package),-4(speed grade).

Table 4: Comparative table

Maximum Combinational Path Delay (in ns) for different multipliers at different bit levels				
N bit level multiplier	Array [13]	Booth [13]	Conventional Vedic [13]	Vedic Multiplier [4]
8-Bit	32.01	29.549	24.16	19.467
16-Bit	60.928	70.809	36.563	29.012

By implementing the proposed Vedic multiplier for MAC unit on the same reconfigurable hardware as given make the platform (hardware) independent algorithmic technique and approach based comparison. So by this it can be concluded that the algorithm and approach which has been proposed to design MAC unit using proposed Vedic multiplier, in this research work, is better in comparison to the other popular algorithms.

V. CONCLUSION

We have proposed a design for the NxN bit MAC Unit using a unique Vedic multiplier which provides better results with respect to the conventional MAC unit .This Proposed MAC Unit is very useful for designing the high speed digital signal processors. And thus the optimized designs can be made for FFT, FIR, IIR etc.

An improved version of the conventional MAC unit has been designed and implemented in FPGA. This design can be used in Digital Signal Processors and in devices where power and area are major constraints. In the future, the delay can be further reduced by Introducing a pipelined architecture in the multiplier design.

References

1.Abdelgawad, A.; Sch. of Eng. & Technol., Central Michigan Univ., Mount Pleasant, MI, USA, "Low power multiply accumulate unit (MAC) for future

Wireless Sensor Networks ",Sensors Applications Symposium (SAS), 2013 IEEE.

2. Jagadeesh, P. ; VIT University, Vellore, India ; Ravi, S. ; Mallikarjun, Kittur Harish , "*Design of high performance 64 bit MAC unit* ", Circuits, Power and Computing Technologies (ICCPCT), 2013.

3. K.Kalaiselvi, H. Mangalam, PhD., "*Area Efficient High Speed and Low Power MAC Unit* ", International Journal of Computer Applications (0975 – 8887) Volume 67– No.23, April 2013.

4. Abhishek Gupta, et.al. "Design of speed energy and power efficient reversible logic based vedic ALU for Digital Processors", NuiCONE, Nirma University International Conference (IEEE), 2013.

5. Deepak, S. ; Kailath, B.J.,"Optimized MAC unit design ", Electron Devices and Solid State Circuit (EDSSC), 2012 IEEE.

6. Umesh Akare, T. V. More, R. S. Lonkar, "*Performance Evaluation and Synthesis of Vedic Multiplier*", National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2012) Proceedings published by International Journal of Computer Applications® (IJCA)

7. waraj, R.M. ; Arun, K.K. ; Srinivas, R.K., "*Reversible implementation of novel multiply accumulate (MAC) unit* ", Communication, Information & Computing Technology (ICCICT), 2012.

8. Naveen Kumar, et.al., "*VLSI Architecture of Pipelined Booth Wallace MAC Unit* ", International Journal of Computer Applications (0975 – 8887) Volume 57– No.11, November 2012.

9. M.Jeevitha, R.Muthaiah, P.Swaminathan, "*Review Article: Efficient Multiplier Architecture in VLSI Design*" Journal of Theoretical and Applied Information Technology, vol. 38, no. 2, April 2012.

10. G.Ganesh Kumar, V.Charishma," *Design of High Speed Vedic Multiplier using Vedic Mathematics Techniques*", International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012 ISSN 2250-3153.

11.Kandimalla Rajaneesh, M.Bharathi, "A Novel High Performance Implementation of 64 bit MAC Unit and their Delay Comparison", Int.Journal of Engineering Research and Applications, Vol. 4, Issue 6(Version 6), June 2014.

12.Stephen D. Brown, and ZvonkoVranesic, McGraw Hill, June, 2007, Book.

13. Morris Mano, "*Digital circuits and systems*", Prentice-Hal, Last updated on-02/27/2011, 11:55, Book.

14. Wayne Wolf, "*Computer as components*",2nd edition, Book.

15.http://www.xilinx.com/support/documentation/data_sheets/ds312.pdf

16. <http://en.wikipedia.org/wiki/Verilog>



Novel Technique For Improving Image Deblurring Using Residual Whiteness Measures

Ruqaiya Begum

Dept. of electronic and communication engg
Anjuman college of engineering and technology
Nagpur, India
Ruqaiyaansari14@gmai.com

Prof.S.M Ali

Dept. of electronic and communication engg
Anjuman College of engineering and technology
Nagpur, India
ali_acet2003@yahoo.co.in

Abstract—When we use a camera to click a picture, we want the clicked image to be an exact representation of the scene that we see—but every image is more or less blurry. Thus, image deblurring is fundamental in making pictures sharp and useful. A digital image is made of picture elements called pixels. Each pixel is assigned an intensity, meant to characterize the color of a small rectangular segment of the scene. A small picture typically has around $2562 = 65536$ pixels while a high-resolution picture often has 5 to 10 million pixels. Some blurring always arises in the recording of a digital image, because it is unavoidable that scene information “spills over” to neighboring pixels. For example, the optical system in a camera lens may be out of focus, so that the incoming light is smeared out. The same problem arises, for example, in astronomical imaging where the incoming light in the telescope has been slightly bent by turbulence in the atmosphere. In these and similar situations, the expected result is that we record a blurred image.

In image deblurring, we want to recover the unique, sharp image by using a mathematical model of the blurring process. The issue is that some information on the lost details is present in the blurred image—but this information is “hidden” and can only be improved if we know the details of the blurring process. Unhappily there is no hope that we can recover the original image exactly! This is due to various unavoidable errors in the recorded image. The most important errors are approximation errors and fluctuations in the recording process when representing the image with a limited number of digits. The effect of this noise puts a limit on the size of the details that we can hope to recover in the reconstructed image, and the limit depends on both the noise and the blurring process. **Keywords**—component; formatting; style; styling; insert (key words)

I. INTRODUCTION

Image deblurring (ID) is a problem where the observed image is produced as the convolution of a sharp image with a blur filter, possibly along with some noise (assumed spectrally white and Gaussian). With applications in many areas (e.g. photography, surveillance, remote sensing, medical imaging, astronomy), research on ID can be split into *non-blind* ID (NBID), in which the blur filter is assumed familiar, and (real) *blind* ID (BID), in which both the image and the blur filter are

(totally or partly) are not familiar. Despite its narrower applicability, NBID is already a challenging problem to which a large amount of research has been (and still is) devoted, mainly due to the ill-conditioned nature of the blur operator: the observed image does not uniquely and stably determine the underlying original image [38]. If this problem is serious with a known blur, it is much worse if there is even a slight mismatch between the assumed blur and the true one. Most of the NBID methods overcome this difficulty through the use of an image regularizer, or prior, the weight of which has to be tuned or adapted. Most state-of-the-art regularizers exploit the sparsity of the high frequency/edge components of images; this is the rationale underlying wavelet/frame-based methods and total variation (TV) regularization. With application not only in ID, but also in other inverse problems, several optimization techniques have been proposed to handle scarcity-inducing regularizers.

In BID, even if the blur operator was not ill-conditioned, the problem would still be inherently ill-posed, since there is a vast number of solutions adaptable with the blurred image. In order to obtain reasonable results, most BID techniques restrict the class of blur filters, either in a hard way, through the use of parametric models, or in a soft way, through the use of priors/regularizers. In contrast, a recent BID method does not use prior knowledge about the blur, yet achieves state-of-the-art performance on a huge range of synthetic and real problems. That method is iterative and starts by supposing the main features of the image, using a large regularization weight, and gradually learns the image and filter details, by slowly decreasing the regularization parameter. From an optimization point of view, this can be seen as a continuation method designed to obtain a good local minimum of the underlying non-convex objective function.

The disadvantage of the technique is that it is not automatic but it requires manual stopping, which corresponds to choosing the final value of the regularization parameter. In fact, adjusting the regularization parameter and/or finding robust stopping criteria for iterative (blind or not) ID

algorithms is along standing, but still open, research area .A crucial issue in the regularization of ill-posed inverse problems is the choice of the regularization factor, a subject to which much work has been devoted. The *discrepancy principle* (DP) chooses the regularization factors that the variance of the residual equals that of the noise; the DP thus requires an accurate estimate of the noise variance and is known to yield over-regularized estimates. A recent extension of the DP uses not only the variance, but also other residual moments. Local residual information have also been used to obtain locally adaptive TV regularizes for NBID.

II. IMAGE DEBLURRING

ID can be split into *non-blind* ID (NBID), in which the blur filter is assumed familiar, and (real) *blind* ID (BID), in which both the image and the blur filter are (totally or partly) are not familiar.

A .Non-blind Deblurring

In NBID, h is assumed to be known and the cost function (2) is reduced with respect to x , given some of the regularization factor λ . Many optimization methods for ID decrease the cost function (2) iteratively compute the picture estimate at iteration $t + 1$ as a reason of the previous estimate x_t , the available data (y and h), and the regularization parameter λ :

$$x_{k+1} = f(x_k, y, h, \lambda). \quad (3)$$

Besides requiring a good estimate for the regularization parameter λ , these iterative approaches also need stopping criteria, which considerably influence the final results. For fairness, it should be mentioned that some high-tech methods don't fall in the category of methods mentioned in the previous paragraph. For example, the method proposed in[16] (arguably the method yielding the current best results) is iterative, but rather than look for a minimize of an objective function, it looks for equilibrium between two objective functions. Other NBID methods are not based on iterative minimization of objective functions.

B .Blind Deblurring

In BID, both the image and the filter are not familiar. A BID problem suffers from an obvious scarcity of data, since there are many pairs (x , h) that explain equally well the observed data y . Most BID methods circumvent this difficulty by adding to (2) a regularizer on the blur filter and, usually, by alternately estimating the image and the blur filter. A regularizer on the blur naturally involves a supplementary regularization parameter, also requiring alteration, while the alternating estimation of the image and the filter requires good initialization (since the underlying objective (2) is non-convex) and a good criterion to stop the iterative process.

III. PROBLEM FORMULATION

In the existing system the researchers have focused on estimation of parameters for blind and non blinded blurring

which causes inherent time delay in estimation of residual whiteness measures. Thus the system speed in reduced and overall system accuracy is compromised. Our approach will be to reduce the system time and improve the accuracy.

In our approach we will be integrating residual whiteness measures with genetic algorithm so that the speed of estimation is improved and also genetic algorithm finds the best possible solution of a particular problem so we will get the best deblurring results. Genetic algorithm works in the following steps

1. Generate population for all possible deblurring solutions.
2. For each iteration perform the following.
 - A) Find the fitness of each solution.
 - B) Fitness will be a function of delay time and SNR.
 - C) Find the mean fitness.
 - D) Remove all solutions which have fitness value lower than the mean fitness.
 - E) For all other solutions pass them to next iteration.
3. At the end of all iteration select the solution with best fitness.

IV.ALGORITHM

Picture editing consists of the processes of altering images, whether they are digital photographs, conventional photochemical photographs, or illustrations. Traditional analog image editing is known as photo retouching, using tools such as an airbrush to adapt photograph, or cutting illustration with any conventional art medium. Graphic software programs, which can be broadly grouped into vector graphics editors, raster graphics editors, and 3D modelers, are the primary tools with which a user may change, enhance, and transform images. Many image editing programs are also used to create computer art from scratch.

To achieve clear and bright images under dim lighting conditions is a challenging work. The brightness of the images can be determined by sensor sensitivity (ISO),exposure time and aperture. A higher ISO value, longer exposure time, and wider aperture setting increase the image brightness at the cost of image quality. A longer exposure time effectively ensures brightness of acquired image but leads to a higher probability of movement in both the scene and the camera while the shutter is open. Conversely, a higher ISO setting to obtain brighter image introduces more noise which is composed of time-independent and time-dependent components. The situation requires a higher ISO value implies a weak image signal and a relatively high level of time-independent noise which is inherent in the sensor. A shorter exposure time for compensating the high ISO results in time-dependent noise due to increased randomness of captured photons. In most cases, since the incoming light is insufficient in dark situations, both noise and blur a represent in the image.

- 1.To improve the speed of image deblurring.
- 2.To improve the SNR of deblurred image.

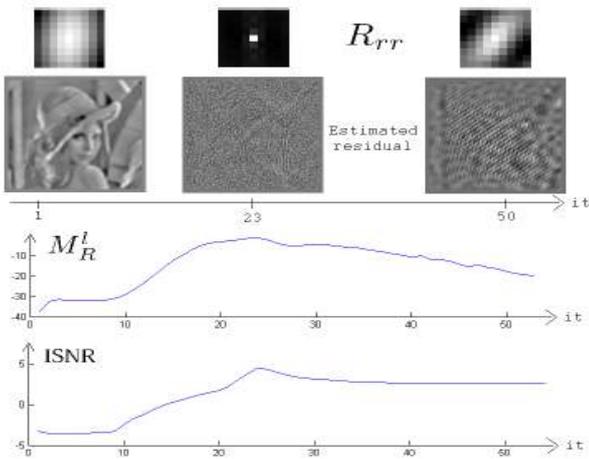


Fig. 2. Illustration of the proposed approach; results obtained with the *Lena* image, blurred with an out-of-focus blur and contaminated with noise at 30dB BSNR. Evolution along the iterations (from top to bottom) of: R_{rrr} , residual image r , whitening measure M_R , and $ISNR$.



Fig. 3. Real-life photos used in the experiments. (b), (c), and (d) are out of focus; (a), (e), (f), and (g) suffered motion blur.

V. CONCLUSIONS

We have suggested new technique that can be used to choose the regularization factor and to stop iterative blind and non-blind picture deblurring algorithms. Our suggestion is based on measures of the whiteness of the residual image. The technique is quite general and does not need any information about the type of convolution factor. The suggested method were aggravated by blind de-convolution complexity, and it is particularly well suitable to a new state-of-the-art method that

uses a *continuation* scheme based on the regularization parameter. On a huge range of synthetic experiments, we show that the best of the suggested criterion yield ISNR losses with the respect to the best ISNR of only 0.15dB, on average. The method was also compare with two other criterion, of the few that can be used in blind de-convolution complexity, showing to execute better in terms of SNR. Finally, test on more than a few real images, dishonored with a variety of out-of-focus and motion blurs, show that the proposed method yields visually good outcome. The proposed technique was shown to be also adequate for estimate both the regularization factor and the number of iteration of non blind deblurring algorithm.



Fig. 5. Results obtained with real blurred photos. From left to right, at each row: restored image at the “optimal” (visually selected) iteration, estimated blur filter at the “optimal” iteration, restored image at the iteration chosen using MIR , blur filter estimate at the iteration chosen using MIR

References

- [1] Mariana S. C. Almeida and M'ario A. T. Figueiredo, Fellow, “Parameter Estimation for Blind and Non-Blind Deblurring Using Residual Whiteness Measures” IEEE TRANSACTIONS ON IMAGE PROCESSING, 2013 (TO APPEAR) 1
- [2] M. Afonso, J. Bioucas-Dias, and M. Figueiredo, “Fast image recovery using variable splitting and constrained optimization,” IEEE Trans. Image Processing, vol. 19, pp. 2345–2356, 2010.
- [3] M. S. C. Almeida and L. B. Almeida, “Blind deblurring of natural images,” in IEEE Int. Conf. Acoustics, Speech, and Signal Processing ICASSP, 2008, pp. 1261–1264.
- [4] —, “Blind and semi-blind deblurring of natural images,” IEEE Trans. Image Processing, vol. 19, pp. 36–52, 2010.

- [5] M. S. C. Almeida and M. A. T. Figueiredo, "New stopping criteria for iterative blind image deblurring based on residual whiteness measures," in Proceedings of the IEEE Statistical Signal Processing Workshop (SSP), pp. 337–340, 2011.
- [6] B. Amizic, S. D. Babacan, R. Molina, and A. K. Katsaggelos, "Sparse Bayesian blind image deconvolution with parameter estimation," in European Signal Processing Conference, 2010.
- [7] S. D. Babacan, R. Molina, and A. K. Katsaggelos, "Variational Bayesian blind deconvolution using a total variation prior," IEEE Trans. Image Processing, vol. 18, pp. 12–26, 2009.
- [8] A. Beck and M. Teboulle, "A fast iterative shrinkage-thresholding algorithm for linear inverse problems," SIAM Journal on Imaging Sciences, vol. 2, pp. 183–202, 2009.
- [9] J. M. Bioucas-Dias and M. A. T. Figueiredo, "A new TwIST: Two-step iterative shrinkage/thresholding algorithms for image restoration," IEEE Trans. on Image Processing, vol. 16, pp. 2992 – 3004, 2007.
- [10] G. Box and G. Jenkins, Time Series, Forecasting, and Control. San Francisco, CA, USA: Holden-Day, 1970.
- [11] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," Foundations and Trends in Machine Learning, vol. 3, no. 1, pp. 1–122, 2011.
- [12] A. S. Carasso, "The APEX method in image sharpening and the use of low exponent L'evy stable laws," SIAM Journal of Applied Mathematics, vol. 63, pp. 593–618, 2003.
- [13] S.M.Ali, Dr. P.t. karule Noise Removal From Pathological Speech Signal, Its Framing And Windowing , Proc. of the Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering,seek digital library .2012,pp 118-12



Review of Compression and Denoising Speech Signal Using Cellular Automata Concept

Sharmeen Saba

Deptt. of Electronics & Telecomm. Engg.

A.C.E.T.

Nagpur, India.

Email: sharmeensaba@gmail.com

Prof. A.S.Khan

Deptt. of Electronics & Telecomm. Engg.

A.C.E.T.

Nagpur, India.

Email: acetsajjadsir@yahoo.co.in

Abstract—Cellular automata (CA) are made up as of a regular grid of cells, all of which can be in one of a finite set of states. At a particular instance the state of every cell is updated in parallel, and is determined as a function of the value in the neighborhood cell in the preceding time step, i.e. by a set of cell state transition rules. CA is discrete dynamical systems, furthermore their ease coupled by means of their complex behavior has made them popular for simulating complex systems. In the previous work, researchers have implemented cellular automata to remove noise from the input signal. But this method does not give the best results in real time noisy environments like airport. We planned to propose a hybrid cellular automata based system which consists of combination of LMS(Least Mean Squares) estimation applied to cellular automata for removing the noise.

By this approach we intend to reduce the noise from the input sound or speech signal and improve the signal to noise ratio, reducing the time of denoising the speech signal. A cellular automata takes large time as it analyses the system of speech both finegrain and coarse but we can apply coarse denoising based on LMS and finegrain denoising based on cellular automata. Thereby reducing the delay and improving the efficiency of denoising. By compressing the data using CA less storage space is required.

Keywords—Cellular Automata, LMS, Coarse denoising, Finegrain denoising

I. INTRODUCTION

Noise reduction of audio signals is a important challenge in speech enhancement, speech recognition and speech communication applications. In every realistic situations, the received speech waveform have a few form of noise component. This noise can be a consequence of the limited precision involved in coding the transmitted waveform (quantization noise), or due to the addition of acoustically coupled surrounding noise. Depending on the quantity and form of noise, the quality of the received waveform can vary as of being a little degraded to being irritating to listen to, and lastly to being entirely meaningless. The difficulty of removing the unwanted noise component from a received signal has been attracted many researchers.

II. RELATED WORK

A. Dual Channel Delay Speech Denoising Based on Underdetermined BSS

We reviewed the study of mixture of speech and Gaussian noise. A delay speech denoising method, which considers two received speeches with time delay, is proposed. The algorithm is based on underdetermined BSS method and applies time frequency sparsity. The noisy speeches are firstly divided the two parts by means of a threshold and then one part less than the threshold can be regard as noise. Speech signal will be separated from another part by time frequency mask. The separated speech is finally furthermore smoothed by a filter. This paper discusses the problem of the two delay speeches are corrupted by Gaussian white noise. We reviewed a delay speech denoising method using the blind source separation method. It is more practical than Dual speech denoising algorithm[1].

B. Cellular Automata and Chaotic Maps for Speech Signal Encryption

We reviewed the permutation process based on permutation key that generated from Game of Life matrix which is a simple cellular automaton, remarkable for its complex behavior. . The substitution performed with mask key that generated from one dimensional cubic and sine chaotic maps. The preliminary conditions and control parameters for chaotic maps are used as password for the sender and receiver. The outcome shows that the encryption system provides encryption speech signal of low residual intelligibility though preserves the good quality of the recovered speech signal. The system has a large key sensitivity because a small change in the secret key causes a large change in the encrypted signal[2].

C. Performance Comparison of STFT, WT, LMS and RLS Adaptive Algorithms in Denoising of Speech Signal

The performance of a particular technique depends on mean, variance and maximum amplitude of error. simultaneously the process time of signal and complexity of realistic implementation of circuits is also a measuring tool for performance of a technique. We reviewed the compared

performance among the short time Fourier transform (STFT), wavelet transform (WT), least mean square (LMS) and recursive least square (RLS) methods in cancellation of noise from a speech signal. The analysis of the paper provides us the way of selection of the best denoising technique based on the statistical parameters of the above four mentioned techniques[3].

D. Adaptive Noise Canceling for Speech Signals

We reviewed least mean-square (LMS) adaptive filtering approach for removing the deleterious effects of additive noise on the speech signal. Unlike the classical LMS adaptive filtering scheme, the proposed method is designed to cancel out the clean speech signal. This scheme takes benefit of the quasi-periodic nature of the speech signal to form an estimate of the clean speech signal at instance t from the value of the signal at instance t minus the estimated pitch period. For additive white noise distortion, preliminary tests indicate that the method improves the perceived speech quality and increases the signal-to-noise ratio (SNR) by 7 dB in a 0 dB environment. The method has also been revealed to partially remove the perceived granularity of CVSD coded speech signals and to lead to an improvement in the linear prediction analysis/synthesis of noisy speech [4].

D Audio and Speech Compression Using DCT and DWT Techniques

We reviewed “Audio and Speech Compression Using DCT and DWT Techniques”, in this there is a simple discrete wavelet transform & DCT based audio compression. It is implemented using MATLAB. Experimental results show that in general there is improvement in compression factor & signal to noise ratio with DWT based technique. Also Specific wavelets have varying effects on the speech signal being studied.[5]

III. OUR APPROACH

In the previous work, researchers have implemented cellular automata to eliminate noise from the input signal. But this method does not give the best results in real time noisy environments like airport. We planned to propose a hybrid cellular automata based system which consists of combination of LMS(Least Mean Squares) estimation applied to cellular automata for removing the noise. By this approach we intend to reduce the noise from the input sound or speech signal and improve the signal to noise ratio, reducing the time of denoising the speech signal. A cellular automata takes large time as it analyses the system of speech both fine grain and coarse but we can apply coarse denoising based on LMS and fine grain denoising based on cellular automata. Thereby reducing the delay and improving the efficiency of denoising. Also due to compressing the data using CA less storage space is required.

A. CELLULAR AUTOMATA

Because of simple arrangement of cellular automata (CA) to form complex behavior system, it has attracted many researchers from diverse areas. Cellular automata primarily announced by Ulam and Von Neumann in 1950’s and also discussed in the book of Wolfram ‘A New Kind of Science’

with the idea of obtaining models of biological self-reproduction.. In cellular automata state of a cell at the next time step is determined by the current states of a surrounding neighborhood of cells all along with its own state and is updated synchronously in discrete time steps. Cellular automaton is a discrete dynamical system. Space, time, and the states of the system are discrete. Each point in a regular spatial lattice, called a cell, can have any one of a finite number of states. The states of the cells in the lattice are updated according to a local rule. That is, the state of a cell at a given time depends only on its own state one time step previously, and the states of its nearby neighbors at the previous time step. All cells on the lattice are updated synchronously. Thus the state of the entire lattice advances in discrete time steps. Formally, a (bi-directional, deterministic) cellular automaton is a triplet

$$A = (S; N; \delta),$$

Where, S is a non-empty state set, N is the neighborhood system, and $\delta: SN \rightarrow S$ is the local transition function (rule). This function defines the rule of calculating the cell’s state at t +1 time step, given the states of the neighborhood cells at previous time step t[6].

B.LMS

An adaptive filter is a system with a linear filter that has a transfer function controlled by variable parameters and a means to adjust those parameters according to an optimization algorithm..Least mean squares (LMS) algorithms are a class of adaptive filter used to mimic a desired filter by finding the filter coefficients that relate to producing the least mean squares of the error signal (difference between the desired and the actual signal). It is a stochastic gradient descent method in that the filter is only adapted based on the error at the current time. The basic idea behind LMS filter is to approach the optimum filter weights

$$(R^{-1}P),$$

by updating the filter weights in a manner to converge to the optimum filter weight. The algorithm starts by assuming small weights (zero in most cases) and, at each step, by finding the gradient of the mean square error, the weights are updated. That is, if the MSE-gradient is positive, it implies, the error would keep increasing positively, if the same weight is used for further iterations, which means we need to reduce the weights. In the same way, if the gradient is negative, we need to increase the weights. So, the basic weight update equation is :

$$W_{n+1} = W_n - \mu \nabla \epsilon[n]$$

where ϵ represents the mean-square error. The negative sign indicates that, we need to change the weights in a direction opposite to that of the gradient slope. The mean-square error, as a function of filter weights is a quadratic function which means it has only one extreme, that minimizes the mean-square error, which is the optimal weight. The LMS thus approaches towards these optimal weights by ascending/descending down the mean-square-error vs. filter weight curve.

compressing the data using CA less storage space will be required.

IV. COMPARISION

METHODS	PERFORMANCE
DWT	For real time noise signals it is preferable
RLS	For non real time case it is preferable
STFT AND WT	STFT and WT transforms are suitable for denoising of a signal but in case of recovery of fading signals of wireless communication, adaptive algorithms are the best.
CELLULAR AUTOMATA	Suitable for real time noisy environment .We can apply coarse denoising based on LMS and fine grain denoising based on cellular automata. Thereby reducing the delay and improving the efficiency of denoising

V.CONCLUSION

By this approach we intend to reduce the noise from the input sound or speech signal and improve the signal to noise ratio, reducing the time of denoising the speech signal. Also due to

REFERENCES

[1] Kaipeng Li, Shenzhen Coship Electronics Co., Ltd., Gongxian Sun and Ming Xiao,Guangdong Provincial Key Laboratory of Petrochemical Equipment Fault Diagnosis “Dual Channel Delay Speech Denoising Based on Underdetermined BSS” in 2014 International Conference on Mechatronics and Control (ICMC) July 3 - 5, 2014, Jinzhou, China
 [2] Eman Hato “Cellular Automata and Chaotic Maps for Speech Signal Encryption” in International Journal of Applied Information Systems (IJ AIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 9 – No.3, June 2015 – www.ijais.org
 [3] Mahbulul Alam, Md. Imdadul Islam, and M. R. Amin “Performance Comparison of STFT, WT, LMS and RLS Adaptive Algorithms in Denoising of Speech Signal” in IACSIT International Journal of Engineering and Technology, Vol.3, No.3, June 2011
 [4] Marvin R. Sambur “Adaptive Noise Canceling for Speech Signals” in IEEE transactions on acoustics, speech, and signal processing, vol. assp-26, no.5,october1978
 [5] M. V. Patil1, Apoorva Gupta2, Ankita Varma3, Shikhar Salil4 “Audio and Speech Compression Using DCT and DWT Techniques” in International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 5, May 2013
 [6] Anand Prakash Shukla, et.al.,2014“ An Enhanced Cellular Automata based Scheme for Noise Filtering” International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.7, No.4 (2014), pp.231-242.
 [7] wikipedia

LINKING WIRELESS SENSOR NETWORKS WITH GLOBAL ENERGY BALANCE

ZEBASHEIKH

*Dept Of Electronics & Communication Engg
Anjuman College Of Engg & Tech
Nagpur, India
Zebasheikh456@gmail.com*

PROF.M.NASIRUDDIN

*Asstt. Prof.Dept Of Electronics & Telecommunication Engg
Anjuman College Of Engg & Tech
Nagpur ,India
mn151819@gmail.com*

Abstract—Extending network lifetime and sensor functionality is crucial for the successful utilization of wireless sensor networks (WSNs) in applications where replacing or charging energy storage units is impractical or not cost effective. In the previous work, the system of WSN was used for reducing the power consumption in the network .This allowed the network to improve its lifetime by using cluster head based algorithm .In cluster head based algorithm the system selects the nodes with the highest energy in the network and sends data via this node only .This allow the network to perform multiple communication in a given period of time and the lifetime is automatically improved. We propose a cluster of cluster head based algorithm where we will be selecting at least two nodes from each cluster to become the cluster and perform all communication via this cluster head. The main advantage of this protocol over the existing protocol is that this protocol has a backup of cluster head which when the current cluster head has lost enough energy, thereby further improving the lifetime of the network.

Keywords- *Energy balance, wireless sensor networks, cluster head based algorithm, clustering, energy efficient clustering, LEACH, network lifetime, energy efficient algorithms, energy efficient routing.*

I. INTRODUCTION

A Wireless Sensor Network is a spatially scattered autonomous sensor to monitor physical and environmental conditions, such as temperature, pressure and to cooperatively pass their data through a network to the main location.

Extending network lifetime and sensor functionality is important for the successful utilization of wireless sensor networks (WSNs) in implementations where changing or charging energy storage units (i.e. batteries) is impractical or not affordable. Different techniques were evolved to extend the lifetime of sensor networks, the most prominent approach is to balance the WSN communication in the network in order to exhaust energy at a similar time or rate. In such approach, routing decisions play an important role in selecting nominee paths in order to balance energy in the network.

The main objective of this paper is to introduce a new method for extending the network lifetime.

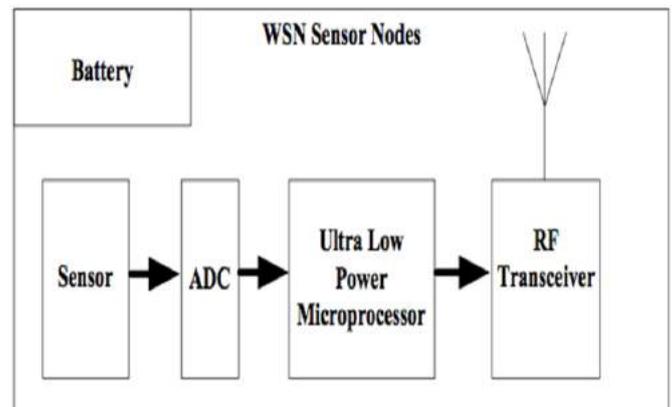


Fig 1. Block diagram of wireless sensor nodes.

With a view to achieve high energy efficiency and increase the network scalability, sensor nodes can be organized into clusters. The increased density of the network may lead to multiple neighbor sensors generating redundant data, thus aggregation of data can be used to eliminate the data redundancy and reduce the communication load. In periodical data gathering applications, methods promise to efficiently create the network since data collection and processing can be done. Among the sources of energy consumption in a sensor node, wireless data transmission is very important.

In a clustering organization, intra-cluster communication can be single hop or multi hop, as well as inter-cluster communication. However, the hot-spots issue arises when using the multichip forwarding model in inter-cluster communication. Because the cluster heads nearer to the data sink are burdened with heavy relay traffic, they will die much faster in comparison to the other cluster heads, reducing sensing coverage and causing network separation.

Although many protocols reduce energy consumption on forwarding paths to increase energy efficiency, they do not necessarily increase network lifetime due to the continuous many-to-one traffic pattern

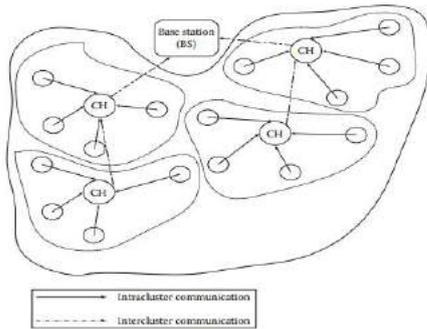


Fig 2 .DATA COMMUNICATION IN CLUSTER NETWORK

II. CHALLENGES OF WIRELESS SENSOR NETWORKS

In WSN sensor nodes have limited amount of processing power, communication bandwidth, and storage space. This gives rise to new and different challenges in data management and information processing methods, such as data aggregation need to be developed. Network lifetime is the main feature used for calculating the performance of any sensor network. A lifetime of the network is determined by the amount of residual energy of the system, hence main and most important problem in WSN is the efficient use of energy resources.

III Hierarchical Routing in WSNs

The main motive of hierarchical routing or cluster based routing is to efficiently manage the energy usage of sensor nodes by using them in multi-hop communication within a specialized cluster. Cluster formation is based on the energy storage of sensors and sensors proximity to the Cluster Head (CHs). Clustering plays a vital role for energy storage in WSNs. With the help clustering in WSNs, energy consumption, lifetime of the network can be improved. Because only cluster head node per cluster is required to operate routing task and the other sensor nodes just forward their data to cluster head. Clustering has major applications in high-density sensor networks, because it is much easier to manage a set of cluster group (cluster head) from each cluster as compared to managing whole sensor nodes. In WSNs the sensor nodes are dependent on resource which means they have limited energy, transmit power, memory, and computational complexities. Energy consumed by the sensors for communicating data from sensor nodes to the base station is the critical cause of energy degradation in sensor nodes systems.

IV. CLUSTER HEAD BASED ALGORITHM

Energy consumption is the most crucial design issue in WSNs. In order to solve the issue and prolong the network lifetime, energy resources of each node in wsn need to be effectively managed. With respect to energy efficiency, the best known

protocol are hierarchical in nature .Energy consumption can be reduced efficiently by using ‘clustering based hierarchical routing protocol.

In cluster head based algorithm the system selects the nodes with the highest energy in the network and sends data via this node only .This allow the network to perform multiple communication in a given period of time and the lifetime is automatically improved. We propose a cluster of cluster head based algorithm where we will be selecting at least two nodes from each cluster to become the cluster and perform all communication via this cluster head.

V. CLUSTER FORMATION

Sensor nodes typically use irreplaceable power with the limited capacity, the node’s capacity of computing, communicating, and storage is very limited, which requires WSN protocols need to conserve energy as the main objective of maximizing the network lifetime. An energy-efficient communication protocol LEACH, has been introduced which employs a hierarchical clustering done based on information received by the BS. The BS periodically changes both the cluster membership and the cluster-head (CH) to conserve energy. The Cluster Head collects and aggregates information from sensors in its own cluster and passes on information to the BS. By rotating the cluster-head randomly, energy consumption is expected to be uniformly distributed. However, LEACH possibly chooses too many cluster heads at a time or randomly selects the cluster heads far away from the BS without considering nodes’ residual energy. As a result, some cluster heads drain their energy early thus reducing the lifespan of WSN.

In each round of the cluster formation, network needs to follow the two steps to select cluster head and transfer the aggregated data. (i) Set-Up Phase, which is again subdivided in to Advertisement, Cluster Set-Up & Schedule Creation phases. (ii) Steady-State Phase, which provides data transmission using Time Division Multiple Access (TDMA). The election of cluster head node in LEACH has some deficiencies such as, some very big clusters and very small clusters may exist in the network at the same time, unreasonable cluster head selection while the nodes have different energy, cluster member nodes deplete energy after cluster head was dead. The algorithm does not take into account the location of nodes.

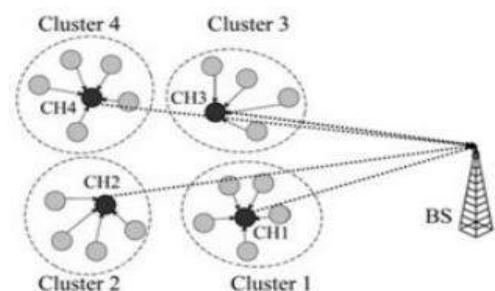


Fig 3: LEACH clustering communication hierarchy for WSNS

VI. CLUSTERING STRATEGIES

LEACH are low energy adaptive clustering hierarchy, while improving the limitations of LEACH, many clustering proposals for increasing network lifetime are reported suggesting different strategies of cluster head selection and its role rotation among the sensor nodes, using different parameters. Based on these parameters, these strategies of cluster head selection may broadly be categorized as deterministic, adaptive and combined metric (hybrid). In deterministic schemes special attributes of the sensor node such as their identification number (Node ID), number of neighbors they have (Node degree) and in adaptive schemes the resource information like remnant energy, energy dissipated during last round, initial energy of the nodes are used to decide their role during different data gathering rounds. Based on who initiates the cluster head selection, the adaptive schemes may be categorized as base station assisted or self organized (Probabilistic). Based on the parameters considered for deciding the role of a sensor node, the probabilistic schemes may further be classified as fixed parameter or resource adaptive.

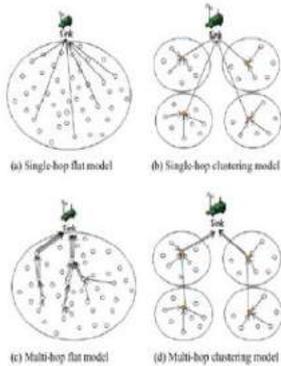


Fig 4: Classification of WSN topology

VII LEACH BASED CLUSTERING

An energy efficient routing protocol is a major concern in wireless sensor networks. In this paper we present energy efficient hierarchical routing protocols, developed from conventional LEACH routing protocol. main focus is how these extended protocols work in order to increase the lifetime and how quality routing protocol is improved for WSNs. LEACH assumes that each node has a radio powerful enough to directly reach the base station or the nearest cluster head, but that using this radio at full radio at full power all the time would waste energy. All nodes that are not cluster heads only communicate with cluster head in a TDMA fashion according to the schedule created by cluster head. They do so using the minimum energy needed to reach the cluster head and only need to keep their radios on during their time slots. LEACH protocol has a relatively good function in energy consumption through dynamic clustering, keeps the data transmission in cluster which reduces the energy consumption by communicating directly between nodes and the base station, but there are still a lot of inadequacies. The LEACH protocol

uses the mechanism of cluster-head rotation, elects cluster-head randomly, after several rounds of data transmission, the residual energy of the nodes will have a great difference, cluster-head or the nodes which are far from the base station will consume more energy in transmitting data of the same length relatively, if they are selected as cluster-heads after that, they will run out of energy and become invalid.

VII COMPARATIVE RESULTS

	DDCH	Energy efficient	Consumed energy
Network Life Time	50% more than LEACH	10% more than LEACH	47% - 57% than LEACH
Performance	Remains almost the same with any number of nodes	Increases when the initial energy is very large	Remains same with increase in number of nodes and distance between nodes and BS (to a limit).
Advantage	Suited for sensor system involving mobile nodes	Very practical and easy to implement	Even if the distance between base station and node is really high, it has no significant effect in network life. Network will never get stuck
Disadvantage	Node interaction result in energy loss	First two rounds similar to LEACH	Some nodes will be the cluster head for very long time and some may not get the chance to be the cluster head
Application (eg.)	Disaster recovery	Forest fire detection system	Military applications like intruder detection

Fig 5: comparative results with LEACH algorithm

VII CONCLUSION

Generally, clustering in WSNs has been of high interest. As it was pointed out, grouping nodes into clusters, thus leading to hierarchical routing and data gathering protocols, has been regarded as the most efficient approach to support scalability in WSNs. The hierarchical cluster structures facilitate the efficient data gathering and aggregation independent to the growth of the WSN, and generally reduce the total amount of communications as well as the energy spent. The main objective of most of the existing protocols lies on how to prolong the lifetime of the network and how to make a more efficient use of the critical resources. To maximize network lifetime in Wireless Sensor Networks (WSNs) the paths for data transfer are selected in such a way that the total energy consumed along the path is minimized. To support high scalability and better data aggregation, sensor nodes are often grouped into disjoint, non overlapping subsets called clusters. Clusters create hierarchical WSNs which incorporate efficient utilization of limited resources of sensor nodes and thus extends network lifetime. The objective of this paper is to present how the lifetime of WSNs are maximized by using cluster of cluster head based algorithm. Our paper presents a

taxonomy of energy efficient clustering algorithms in WSNs. And also present timeline and description of LEACH .

REFERENCES

- [1] M. I. Hossain , M. M. Rahman, and T. K. Godder., "Improving Energy Efficient Clustering Method for Wireless Sensor Network", International Journal of Information Technology and Computer Science, Vol. 5, No. 9, PP.73-79, 2013
- [2] M. O. Farooq, A. B. Dogar, and G. A. Shah, "MR-LEACH: Multi-hop Routing with Low Energy Adaptive Clustering Hierarchy", 2010 Fourth International Conference on Sensor Technologies and Applications, ©2010 IEEE.
- [3] M. Belkadi, R. Aoudjit, M. Daoui, and M. Lalam, "Energy-efficient Secure Directed Diffusion Protocol for Wireless Sensor Networks", International Journal of Information Technology and Computer Science, Vol. 6, No. 1, PP.50-56, 2014.
- [4] Z. Peng and X. Li, "The Improvement and Simulation of LEACH Protocol for WSNs", College of Information Engineering Capital Normal University Beijing China, ©2010 IEEE.
- [5] W. Xiaoping, L. Hong, L. Gang, "An Improved Routing Algorithm Based On LEACH Protocol", Journal: International Symposium on Distributed Computing and Applications to Business, Engineering and Science, © (2010) IEEE.
- [6] W. Jun and Z. Xin, "A Distance-based Clustering Routing Protocol in Wireless Sensor Networks", Journal: IEEE 12th International Conference on Communication Technology, (2010).
- [7] L.Q. GUO, Y. XIE, C. H. YANG, and Z. W. JING, "Improvement on LEACH by Combining Adaptive Cluster Head Election and Two-Hop Transmission", ©2010 IEEE.
- [8] V. Katiyar, N. Chand, G. C. Gautam, and A. Kumar, "Improvement in LEACH Protocol for Large-scale Wireless Sensor Networks ", ©2011 IEEE.
- [9] Laiali Almazaydeh, Eman Abdelfattah, Manal Al-Bzoor, and Amer Al-Rahayfeh, Performance Evaluation of Routing Protocols In Wireless Sensor Networks, International Journal of Computer Science & Information Technology, vol.2, no.2, pp. 64-73, 2010.
- [10] Wernhuar Tarng, Kuo-Liang Ou, Kun-Jie Huang, Li-Zhong Deng, Hao-Wei Lin, Chang Wu Yu, Kuen-Rong Hsieh and Mingteh Chen, Applying Cluster Merging and Dynamic Routing Mechanisms to Extend the Lifetime of Wireless Sensor Networks, International Journal of Communication Networks and Information Security, vol. 3, no. 1, pp. 8-16, 2011
- [11]Wernhuar Tarng, Kuo-Liang Ou, Kun-Jie Huang, Li-Zhong , Hao-Wei Lin, Chang Wu Yu, Kuen-Rong Hsieh and Mingteh Chen, Applying Cluster Merging and Dynamic Routing Mechanisms to Extend the Lifetime of Wireless Sensor Networks,International Journal of Communication Networks and InformationSecurity, vol. 3, no. 1, pp. 8-16, 2011.
- [12] X. Tang and J. Xu, Extending network lifetime for precision constrained data aggregation in wireless sensor networks, Proceedings of IEEE INFOCOM, Apr. 2006.
- [13] I. Akyildiz and W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks", IEEE Commun. Mag., vol. 8, (2002), pp. 102.
- [14] Laiali Almazaydeh, Eman Abdelfattah, Manal Al-Bzoor, and Amer Al-Rahayfeh, Performance Evaluation of Routing Protocols in Wireless Sensor Networks, International Journal of Computer Science & Information Technology, vol.2, no.2, pp. 64-73, 2011. H. R. Karkvandi, E. Pecht, and O. Yadid, "Effective lifetime-aware routing in wireless sensor networks," IEEE Sensors J., vol. 11, no. 12, pp. 3359–3367, Dec. 2011.
- [15] F. Ren, J. Zhang, T. He, C. Lin, and S. K. Das, "EBRP: Energy-balanced routing protocol for data gathering in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 12, pp. 2108–2125, Dec. 2011.
- [16] C. Wu, R. Yuan, and H. Zhou," A novel load balanced and lifetime maximization routing protocol in wireless sensor networks," in Proc. IEEE Vehicular Technol. Conf. VTC Spring, May 2008, pp. 113–117.
- [17] C. C. Hung, K. C. J. Lin, C.-C. Hsu ,C.-F. Cho u, and C.-J. Tu,"On enhancing network-lifetime using opportunistic routing in wireless sensor networks," in Proc. 19th Int. Conf. Compute. Commun. Netw. Aug. 2010, pp. 1–6.



Improving Face Annotation Using Bag of Features with Classification

Bushra Firdous

Dept. of electronic and communication engg
Anjuman college of engineering and technology
Nagpur, India
bushrafirdous93@gmail.com

Prof.S.M. Ali

Dept. of electronic and communication engg
Anjuman college of engineering and technology
Nagpur, India
ali_acet2003@yahoo.co.in

Abstract— This method can be observe as a type of multi-class image classification with a very huge no. of classes - as large as the vocabulary amount. generally, image inquiry in the form of extracted feature vectors and the coaching annotation words are used by machine learning approach to attempt to automatically handle annotations to newly added images. The first methods learned the interaction between image features and training annotations, then techniques were developed using machine adaptation to try to translate the textual vocabulary with the 'visual vocabulary', or clustered regions known as *blobs*. Work following these efforts have included classification approaches, relevance models and so on.

The advantages of automatic image annotation versus content-based image retrieval (CBIR) are that queries can be more naturally specified by the user. CBIR generally (at present) requires users to search by image concepts such as color and texture, or finding example queries. Certain image features in example images may override the concept that the user is really focusing on. The traditional methods of image retrieval such as those used by libraries have relied on manually annotated images, which is expensive and time-consuming, especially given the large and constantly growing image databases in existence.

I. INTRODUCTION

Due to the idolization of diverse digital cameras and the increasing growth of social media tools for internet-based photographs sharing[2], recent years have witnessed an explosion of the number of digital photos clicked and saved by consumers. A large portion of photographs shared by users on the Internet are human facial images. Some of these facial images are tagged with names, but many of them do not tagged properly.

This has inspired the inspection of auto face annotation, an important approach that intent to annotate facial images automatically. For example, with auto face annotation techniques, online photograph-sharing sites (e.g., Face book) can automatically annotate user's uploaded photographs to expedite online photograph search and management. Besides, face annotation can also be adapted in news video territory to

catch important persons appeared in the videos to expedite news video retrieval and summarization tasks [3],[4].

Classical face annotation approaches are often conducted as an lengthy face recognition problem, where various classification models are trained from a collection of bag of features of facial images by employing the supervised or semi-supervised machine learning techniques [3],[4],[5],[6],[7]. However, the "model-based face annotation" techniques are limited in several aspects.

First, it is usually time-consuming and costly to collect a large amount of human-labeled training facial photographs. Second, it is usually hard to generalize the models when new data or new persons are added, in which an intensive retraining process is usually compulsory. Last but not least, the annotation performance often scales poorly when the number of persons is very large.

Recently, some rising studies have attempted to analyze a promising search-based annotation paradigm for facial image annotation by scooping the World Wide Web (WWW), where an enormous number of bag of features of facial images are freely available. Instead of training explicit classification models by the regular model-based face annotation approaches, the search-based face annotation (SBFA) paradigm aims to tackle the automated face annotation task by exploiting content-based image retrieval (CBIR) techniques in scooping enormous bag of features of facial images on the web. The SBFA framework is data-driven and model-free, which to some extent is inspired by the search-based image annotation techniques [8],[9] for generic image annotations.

The main objective of SBFA is to assign correct name labels to a given query facial image. In particular, given a novel facial photo for annotation, we first retrieve a short list of top K-most similar facial images from a bag of features of facial image database, and then annotate the facial image by performing voting on the labels associated with the top K similar facial images.

In particular, we propose a novel unsupervised label refinement (URL) scheme by exploring machine learning techniques to enhance the labels purely from the weakly labeled data without human manual efforts. We also propose a clustering-based approximation (CBA) algorithm to improve the efficiency and scalability. As a summary, the main contributions of this paper include the following:

- We investigate and implement a promising search based face annotation scheme by mining large amount of weakly labeled facial images freely available on the WWW.
- We propose a novel ULR scheme for enhancing label quality via a graph-based and low-rank learning approach.
- We propose an efficient clustering-based approximation algorithm for large-scale label refinement problem.
- We conducted an extensive set of experiments, in which encouraging results were obtained.

We note that a short version of this work had appeared in SIGIR2011. This journal article has been significantly extended by including a substantial amount of new content. The remainder of this paper is organized as follows: Section 2 reviews the related work. Section 3 gives an overview of the proposed search-based face annotation framework. Section 4 presents the proposed unsupervised label refinement scheme.

II. RELATED WORK

Our work is related to various groups of research work.

The first group of related work is on the topics of face recognition and authentication, which are classic analysis complication in computer eyesight and pattern recognition and have been extensively studied for many years. Recent years have observed some emerging criterion studies of unconstrained face detection and verification techniques on facial photographs that are merge from the web, such as the LFW criterion studies. Some recent study had also attempted to increase classic face recognition techniques for face annotation tasks[8]. Complete reviews on face recognition and authentication topics can be found in some survey papers and books.

The second group is about the studies of generic image annotation. The classic image annotation approaches usually apply some existing object recognition techniques to train allocation models from human-features training images or attempt to assume the correlation/probabilities between images and annotated keywords. Given finite training data, semi-supervised learning methods have also been used for image annotation. For example, Wang et al. proposed to refine the model-based annotation results with a label similarity graph by following random walk principle. Similarly, Pham et al. proposed to annotate unlabeled facial images in video frames with an iterative label propagation scheme. Although semi-supervised learning approaches could leverage both labeled and unlabeled data, it remains fairly time-consuming and expensive to collect enough well-labeled training data to

achieve good performance in large-scale scenarios. Recently, the search-based image annotation paradigm has attracted more and more attention. For example, Russell et alia. Built a huge assemblage of web images with ground truth features to expedite object acceptance research. However, most of these works were concentrating on the ratio, search, and bag of feature techniques. dissimilar these existing works, we propose a unsupervised features clarification scheme that is concentrate on optimizing the features quality of facial images towards the content-based face annotation task.

The third group is about face annotation on personal/family/social photos. Several studies have mainly focused on the annotation task on personal photos, which often contain rich contextual clues, such as personal/family names, social context, geotags, time stamps and so on. The number of persons/classes is usually quite small, making such annotation tasks less challenging. These techniques usually achieve fairly accurate annotation results, in which some techniques have been successfully deployed in commercial applications, for example, Apple photos, Google Picasa, Microsoft easy Album, and Facebook face auto tagging solution.

The fourth group is about the studies of face annotation in mining weakly labeled facial images on the web. Some studies consider a human name as the input query, and mainly aim to refine the text-based search results by exploiting visual consistency of facial images. For example, Oscan and Duygul proposed a graph-based model for finding the densest sub-graph as the most related result. Following the graph-based approach, Le and Satoh proposed a new local density score to represent the importance of each returned images, and Guillemain et al. introduced a modification to incorporate the constraint that a face is only depicted once in an image. On the other hand, the generative approach like the Gaussian mixture model was also been adopted to the name-based search scheme [6] and achieved comparable results. Recently, a discriminate approach was proposed in to improve over the generative approach and avoid the explicit computation in graph-based

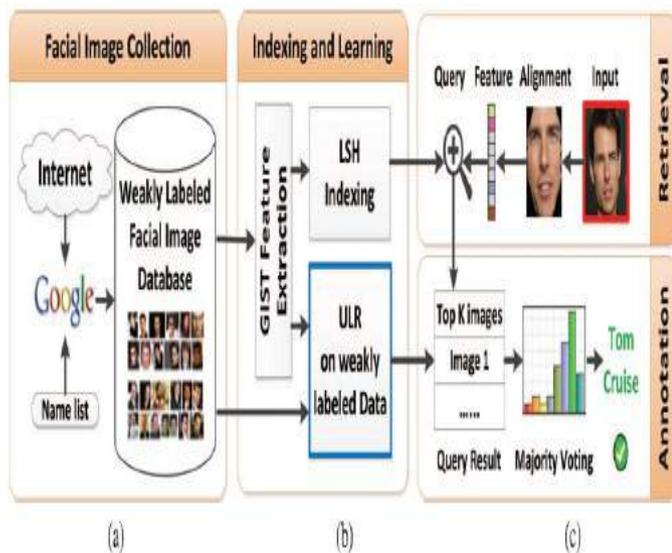


Fig. 1. The system flow of the proposed search-based face annotation scheme.

(a) We collect weakly labeled facial images from WWW using web search engines. (b) We preprocess the crawled web facial images, including face detection, face alignment, and feature extraction for the detected faces; after that, we apply LSH to index the extracted high-dimensional facial features. We apply the proposed ULR method to refine the raw weak labels together with the proposed clustering-based approximation algorithms for improving the scalability. (c) We search for the query facial image to retrieve the top K similar images and use their associated names for voting toward auto annotation.

By using ideas from query expansion, the performance of name-based scheme can be further improved with introducing the images of the “friends” of the query name. Unlike these studies of filtering the text-based retrieval results, some studies have attempted to directly annotate each facial image with the names extracted from its caption information. For example, Berg et al. proposed a possibility model combined with a clustering algorithm to estimate the relationship between the facial images and the names in their captions [5]. For the facial images and the detected names in the same document (a web image and its corresponding caption), Guillemin et al. proposed to iteratively update the assignment based on a minimum cost matching algorithm. In their follow-up work, they further improve the annotation performance by using distance metric learning techniques [5] to achieve more discriminative feature in low-dimension space. Our work is different from the above previous works in two main aspects. First of all, our work aims to solve the general content-based face annotation problem using the search-based paradigm, where facial images are directly used as query images and the task is to return the corresponding names of the query images. Very limited research progress has been reported on this topic. Some recent work mainly addressed the face retrieval problem, in which an effective image representation has been proposed using both local and global features. Second, based on initial weak labels, the proposed unsupervised label refinement algorithm learns an enhanced new label matrix for

all the facial images in the whole name space; however, the caption-based annotation scheme only considers the assignment between the facial images and the names appeared in their corresponding surrounding-text. As a result, the caption-based annotation scheme is only applicable to the scenario where both images and their captions are available, and cannot be applied to our SBFA framework due to the lack of complete caption information. The fifth group is about the studies of purifying web facial images, which aims to leverage noisy web facial images for face recognition applications. Usually these works are proposed as a simple preprocessing step in the whole system without adopting sophisticated techniques. For example, the work in applied a modified means clustering approach for cleaning up the noisy web facial images. Zhao et al. proposed a consistency learning method to train face models for the celebrity by mining the text-image co occurrence on the web as a weak signal [11] of relevance toward supervised face learning task from a large and noisy training set. Unlike the above existing works, we employ the unsupervised machine learning techniques and propose a graph-based label refinement algorithm to optimize the label quality over the whole retrieval database in the SBFA task. Finally, we note that our work is also related to our recent work of the WRLCC method in and our latest work on the unified learning scheme in.1 Instead of enhancing the label matrix over the entire facial image database, the WRLCC algorithm is focused on learning more discriminative features for the top retrieved facial images for each individual query, which thus is very different from the ULR task in this paper. Last but not least, we note that the learning methodology for solving the unsupervised label refinement task are partially inspired by some existing studies in machine learning, including graphbased semi supervised learning and multilabel learning techniques.

III. content-based image retrieval

Content-based image retrieval (CBIR), also known as query by image content (QBIC) and content-based visual information retrieval (CBVIR) is the application of computer vision techniques to the image retrieval problem, that is, the problem of searching for digital images in large databases (see this survey for a recent scientific overview of the CBIR field). Content-based image retrieval is opposed to traditional concept-based approaches [7],[3],[5].

“Content-based” means that the search analyzes the contents of the image rather than the metadata such as keywords, tags, or descriptions associated with the image. The term “content” in this context might refer to colors, shapes, textures, or any other information that can be derived from the image itself. CBIR is desirable because searches that rely purely on metadata are dependent on annotation quality and completeness. Having humans manually annotate images by entering keywords or metadata in a large database can be time consuming and may not capture the keywords desired to describe the image. The evaluation of the effectiveness of keyword image search is subjective and has not been well-

defined. In the same regard, CBIR systems have similar challenges in defining success.

The interest in CBIR has grown because of the limitations inherent in metadata-based systems, as well as the large range of possible uses for efficient image retrieval. Textual information about images can be easily searched using existing technology, but this requires humans to manually describe each image in the database [4]. This can be impractical for very large databases or for images that are generated automatically, e.g. those from surveillance cameras. It is also possible to miss images that use different synonyms in their descriptions. Systems based on categorizing images in semantic classes like "cat" as a subclass of "animal" can avoid the miscategorization problem, but will require more effort by a user to find images that might be "cats", but are only classified as an "animal". Many standards have been developed to categorize images, but all still face scaling and miscategorization issues.

Initial CBIR systems were developed to search databases based on image color, texture, and shape properties [6]. After these systems were developed, the need for user-friendly interfaces became apparent. Therefore, efforts in the CBIR field started to include human-centered design that tried to meet the needs of the user performing the search. This typically means inclusion of: query methods that may allow descriptive semantics, queries that may involve user feedback, systems that may include machine learning, and systems that may understand user satisfaction levels.

The most common method for comparing two images in content-based image retrieval (typically an example image and an image from the database) is using an image distance measure. An image distance measure compares the similarity of two images in various dimensions such as color, texture, shape, and others[6]. For example a distance of 0 signifies an exact match with the query, with respect to the dimensions that were considered. As one may intuitively gather, a value greater than 0 indicates various degrees of similarities between the images. Search results then can be sorted based on their distance to the queried image. Many measures of image distance (Similarity Models) have been developed.

a) Color

Computing distance measures based on color similarity is achieved by computing a color histogram for each image that identifies the proportion of pixels within an image holding specific values. Examining images based on the colors they contain is one of the most widely used techniques because it can be completed without regard to image size or orientation. However, research has also attempted to segment color proportion[9] by region and by spatial relationship among several color regions.

b) Texture

Texture measures look for visual patterns in images and how they are spatially defined[10]. Textures are represented by texels which are then placed into a number of sets, depending on how many textures are detected in the image. These sets not only define the texture, but also where in the image the texture is located.

Texture is a difficult concept to represent. The identification of specific textures in an image is achieved primarily by modeling texture as a two-dimensional gray level variation. The relative brightness of pairs of pixels is computed such that degree of contrast, regularity, coarseness and directionality may be estimated.

IV. Viola-Jones Algorithm With Cascade Object Detection

The Viola-Jones object detection groundwork is the first object detection groundwork to provide competing object detection rates in real-time, it was inspired primarily by the complication of face detection. The problem to be solved is detection of faces in an image. A human can do this easily, but a computer needs precise instructions and constraints. To make the task more manageable, Viola-Jones requires full view frontal upright faces. Thus in order to be detected, the entire face must point towards the camera and should not be tilted to either side. While it seems these constraints could diminish the algorithm's utility somewhat, because the detection step is most often followed by a recognition step, in practice these limits on pose are quite acceptable. The characteristics of Viola-Jones algorithm which make it a good detection algorithm are:

- Robust – very high detection rate (true-positive rate) & very low false-positive rate always.
- Real time – For practical applications at least 2 frames per second must be processed.
- Face detection only (not recognition) - The goal is to distinguish faces from non-faces (detection is the first step in the recognition process).
-

The algorithm has four stages:

1. Haar Feature Selection
2. Creating an Integral Image
3. Adaboost Training
4. Cascading Classifiers

Haar Features – All human faces share some similar properties. These regularities may be matched using Haar Features.

A few properties common to human faces:

- The eye region is darker than the upper-cheeks.
- The nose bridge region is brighter than the eyes.

Composition of properties forming matchable facial features:

- Location and size: eyes, mouth, bridge of nose
- Value: oriented gradients of pixel intensities

The four features matched by this algorithm are then sought in the image of a face (shown at left).

Rectangle features:

- Value = Σ (pixels in black area) - Σ (pixels in white area)
- Three types: two-, three-, four-rectangles, Viola & Jones used two-rectangle features
- For example: the difference in brightness between the white & black rectangles over a specific area
- Each feature is related to a special location in the sub-window

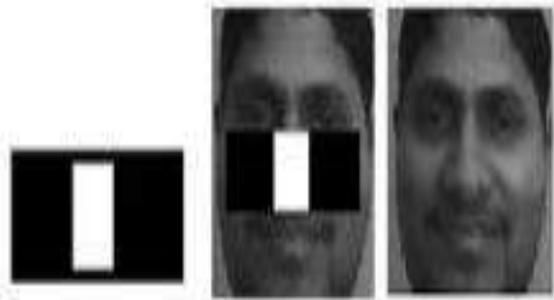


Fig 1: Haar Feature that looks similar to the bridge of the nose is applied onto the face

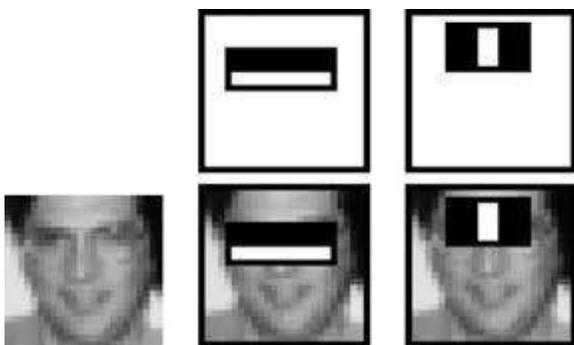


Fig 2: 3rd and 4th kind of Haar Feature

1. An image representation called the integral image evaluates rectangular features in *constant* time, which gives them a considerable speed advantage over more sophisticated alternative features. Because each feature's rectangular area is always adjacent to at least one other rectangle, it follows that any two-rectangle feature can be computed in six array references, any three-rectangle feature in eight, and any four-rectangle feature in nine[1][2].

2. The speed with which features may be evaluated does not adequately compensate for their number, however. For example, in a standard 24x24 pixel sub-window, there are a total of $M = 162, 336^{[4]}$ possible features, and it would be prohibitively expensive to evaluate them all when testing an image. Thus, the object detection framework employs a variant of the learning algorithm AdaBoost to both select the best features and to train classifiers that use them. This algorithm constructs a "strong" classifier as a linear combination of weighted simple "weak" classifiers.

$$h(\mathbf{x}) = \text{sign} \left(\sum_{j=1}^M \alpha_j h_j(\mathbf{x}) \right)$$

Each weak classifier is a threshold function based on the feature f_j .

$$h_j(\mathbf{x}) = \begin{cases} -s_j & \text{if } f_j < \theta_j \\ s_j & \text{otherwise} \end{cases}$$

The threshold value θ_j and the polarity $s_j \in \pm 1$ are determined in the training, as well as the coefficients α_j .

3. In cascading, each stage consists of a strong classifier. So all the features are grouped into several stages where each stage has certain number of features.

The job of each stage is to determine whether a given sub-window is definitely not a face or may be a face. A given sub-window is immediately discarded as not a face if it fails in any of the stages.

A simple framework for cascade training is given below:

- User selects values for f , the maximum acceptable false positive rate per layer and d , the minimum acceptable detection rate per layer.
- User selects target overall false positive rate F_{target} .
- P = set of positive examples
- N = set of negative examples

V. Comparison Schemes and Setup

In our analysis, we implemented all the algorithms described previously for solving the proposed task. We finally accept the soft-regularization formulation of the proposed ULR technique in our appraisal since it is analytically quick than the convex-constraint formulation conferring to our implementations. To better audit the adequacy of our technique, we also implemented some baseline annotation method and existing algorithms for comparisons. Specifically, the compared methods in our experiments include the following[1]:

- "ORI": a baseline design that easily accept the original features information for the search-based annotation scheme, denoted as "ORI" for short.
- "CL": a flexibility learning algorithm proposed to boost the weakly labeled facial photograph database, denoted as "CL" in short[1].
- "MKM": a altered K-means bundle algorithm proposed to bundle web facial photograph correlate with the extracted names from the neighboring captions, stand as "MKM" in short. We note that the original MKM algorithm was proposed to address a similar erroneous label improvement complication, but lightly contrasting from our setting in that the no. of raw erroneous labels of each facial photograph in their complication setting can be more than 1, which is, however, equal to 1 in our problem setting.
- "LPSN": a label multiplication through scant neighborhood algorithm proposed to propagate label

information amid the neighborhoods achieved by scant coding, denoted as “LPSN” in short.

- “ULR $_{\beta=0}$ ”: the proposed ULR algorithm formulation in without the absence regularizer $E_e(F)$.
- “ULR”: the proposed individually label clarification approach, stand as “ULR” in short.

To evaluate their annotation performances, we adopted the hit rate at top t annotated results as the performance metric, which measures the likelihood of having the true label among the top t annotated names. For each query facial image, we retrieved a set of top K similar facial images from the database set, and return a set of top T names for annotation by performing a majority voting on the labels associated with the set of top K images [1].

Further, we discuss parameter settings. For the ULR implementation, we constructed the sparse graph W by setting the number of nearest neighbors to 5 for all cases. In addition, for the two key regularization parameters and in the proposed ULR algorithm, we set their values via cross validation. In particular, we randomly divided the test data set into two equally-sized parts, in which one part was used as validation to find the optimal parameters by grid search, and the other part was used for testing the performance. This procedure was repeated 10 times, and their average performances were reported in our experiments [1].

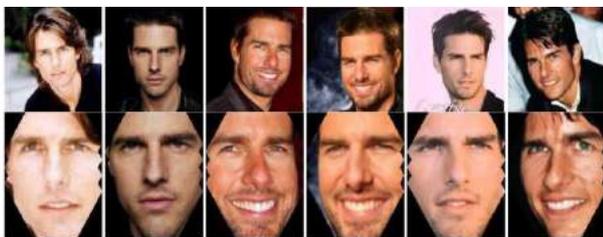


Fig.1. The examples of web facial images and the corresponding alignment results with the DLK algorithm.

The subscript for the permeability of empyiness μ_0 , and other common scientific constants, is zero with subscript formatting, not a small letter “o.”

In American English, commas, semi-colons, periods, question and exclamation marks are situated within quote marks only when a complete thought or name is cited, such as a title or full quote. When quote marks are used, rather of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quote marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis.

- A graph within a graph is an “inset,” not an “insert.” The word willingly is favored to the word “rather”.
- Do not use the word “essentially” to mean “relatively” or “effectively.”
- Be aware of the different meanings of the homograph “affect” and “effect,” “complement” and “compliment,” “discreet” and “discrete,” “principal” and “principle.”

- Do not confuse “imply” and “infer.”
- The noisy signal is passed through filters like, preprocessing filter[11]
- The affix “non” is not a word; it should be joined to the word it modifies, usually without a elbow.
- There is no time-period after the “et” in the classic abbreviation “et al.”
- The abstraction “i.e.” means “that is,” and the abstraction.
-

VI. CONCLUSIONS

This paper investigated a promising content-based face annotation groundwork, in which we attract on tackling the critical complication of boost the feature quality and proposed a violajones algorithm. To further increase the scalability, we also proposed a bundle-based approximation solution, which strongly increased the optimization assignment without introducing much performance degeneration. From an comprehensive set of experiments, we found that the proposed approach accomplish promising conclusion under a array of settings. Our experimental conclusion also determines that the proposed ULR approach significantly exceed the other regular approaches in article. Future work will address the problem of duplicate human names and analyze supervised/semi-supervised learning approach to further boost the features quality with economical human manual clarification exercise.

REFERENCES

- [1] Mining Weakly Labeled Web Facial Images for Search-Based Face Annotation Dayong Wang, Steven C.H. Hoi, Member, IEEE, Ying He, and Jianke Zhu, January 2014.
- [2] Social Media Modeling and Computing, S.C.H. Hoi, J. Luo, S. Boll, D. Xu, and R. Jin, eds. Springer, 2011.
- [3] S. Satoh, Y. Nakamura, and T. Kanade, “Name-It: Naming and Detecting Faces in News Videos,” IEEE MultiMedia, vol. 6, no. 1, pp. 22-35, Jan.-Mar. 1999.
- [4] P.T. Pham, T. Tuytelaars, and M.-F. Moens, “Naming People in News Videos with Label Propagation,” IEEE Multimedia, vol. 18, no. 3, pp. 44-55, Mar. 2011.
- [5] L. Zhang, L. Chen, M. Li, and H. Zhang, “Automated Annotation of Human Faces in Family Albums,” Proc. 11th ACM Int’l Conf. Multimedia (Multimedia), 2003.
- [6] T.L. Berg, A.C. Berg, J. Edwards, M. Maire, R. White, Y.W. Teh, E.G. Learned-Miller, and D.A. Forsyth, “Names and Faces in the News,” Proc. IEEE CS Conf. Computer Vision and Pattern Recognition (CVPR), pp. 848-854, 2004.
- [7] J. Yang and A.G. Hauptmann, “Naming Every Individual in News Video Monologues,” Proc. 12th Ann. ACM Int’l Conf. Multimedia (Multimedia), pp. 580-587. 2004.
- [8] J. Zhu, S.C.H. Hoi, and M.R. Lyu, “Face Annotation Using Transductive Kernel Fisher Discriminant,” IEEE Trans. Multimedia, vol. 10, no. 1, pp. 86-96, Jan. 2008.

[9] A.W.M. Smeulders, M. Worring, S. Santini, A. Gupta, and R. Jain, "Content-Based Image Retrieval at the End of the Early Years," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 22, no. 12, pp. 1349-1380, Dec. 2000.

[10] S.C.H. Hoi, R. Jin, J. Zhu, and M.R. Lyu, "Semi-Supervised SVM Batch Mode Active Learning with Applications to Image Retrieval," ACM Trans. Information Systems, vol. 27, pp. 1-29, 2009.

[11] S.M.Ali, Dr. P.t. karule Noise Removal From Pathological Speech Signal, Its Framing And Windowing , Proc. of the Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering,seek digital library ,2012,pp 118-121.



Energy Efficient Coverage and Connectivity In Wireless Sensor Network

ZEENAT FARZANA

*Dept. Of Electronic & telecommunication Engg.
Anjuman College of Engineering & Tech,
Sadar, Nagpur, India
zeenatrahman59@yahoo.com*

Prof. S. R. GANAR

*Dept .Of Electronic & telecommunication Engg.
Anjuman College of Engineering & Tech,
Sadar, Nagpur, India
Sanjay_r_ganar@yahoo.com*

Abstract— system has been developed for improving the coverage via energy efficient techniques. But these techniques do not take into consideration the movement of the node required for energy efficient coverage improvement. Thus the major energy of the node is spent on moving from location to location for coverage improvement. So each node had the responsibility to contribute for coverage efficiency of the entire network, which made the node to move from network to network in the entire area for coverage improvement which causes a huge energy consumption. Thereby reducing the overall energy of the network.

To overcome this problem we will use the concept of Voronoi diagrams to divide the entire network into regions of varying nodes. So a node will only have the responsibility to improve the coverage of the area in which Voronoi diagram has placed it. Thus the node movement is restricted. So the energy needed for movement will be reduced and the coverage area will be improved. This will allow the network to retain energy for a longer time duration.

Keywords—*Wireless Sensor Network; Coverage; Conectivity; Coverage Control; Sensorig Range;*

I. Introduction

Wireless sensor network is a comprehensive area of research in the field of wireless communication. A WSN involves of a number of electronic devices, mentioned to as a node that communicates through wireless transmission. Each node is prepared with a sensor to collect data from the environment.

Wireless sensor networks have involved tremendous research attention because of its number of applications like security surveillance, environmental monitoring, etc. All applications required a reliable detection, which can only be accomplished if there is no coverage holes in the target field which is monitored by the WSN. For instance a sensor network can be deployed in a remote island for monitoring wildlife habitat or near the crater of volcano to measure the temperature and pressure, in such cases the environmental conditions is not suitable for human intervention. Thus the sensor nodes will be arranged randomly or sprinkled from air and will remain

unattended for a extended time without any battery replacement. So energy consumption is also of a great importance here .So it is necessary to sense the coverage holes and to recover the coverage area and connectivity of wireless sensor networks to safeguard the full operability of the WSN.

Each sensor node is facilitated with the multiple power levels to transmit the data in the wireless channel. Each sensor node innings by the battery power and has sensing capability so it can sense the data within the restricted area called sensing radius .Coverage is usually interpreted as how well the nodes in the wireless sensor network monitor the specified environment. Along with the coverage, connectivity is likewise important in wireless sensor networks.

Connectivity is defined as the ability of any sensor node to conduct the collected information to the sink. If no route is available for the sensor node to send the data to the sink then there will be no connectivity and hence the collected data is unserviceable. Communication range of the node is defined as the area in which another node can be traced in order to receive the data. The sensing range is not the same which is defined as the area where a node can perceive an event.

Obstacles and environmental elements affect the network coverage and may consequence hole in the sensing area. Efficient sensor deployment strategies are established to increase the coverage in wireless sensor networks. The sensors invention coverage holes within their Voronoi polygon and then move in an appropriate direction to minimize them. The movement strategies are based on the expanses of each sensor and the points exclusive its Voronoi polygon from the edges and vertices of the polygon. The distances of each sensor from the vertices of its Voronoi polygon are obtained and the preferred location for the sensor is measured. Some approaches use Voronoi diagram and Delaunay triangulation to detect sensing holes in the network and create an optimal arrangement of the sensors to eliminate the holes. In order to achieve both coverage and connectivity in WSN, sensor

deployment also plays an key role .Sensor deployment is of two types i.e. dense deployment and sparse deployment. Dense deployment is usually helpful in situations where every event needs to be discovered or multiple sensors need to cover a desired area. Sparse deployment basically helps in accomplishing maximum coverage using minimum number of sensor nodes.

II. Related Work

In the previous work, system has been developed for improving the coverage via energy efficient techniques. But these techniques do not take into consideration the movement of the node required for energy efficient coverage improvement each node had the responsibility to contribute for coverage efficiency of the entire network, which made the node to move from network to network in the entire area for coverage improvement which causes huge energy consumption. Tian et al. [10] planned a coverage algorithm In this ,he proposed that complete coverage area Using the sponsored area technique.when a node receive the packet from active neighboring nodes then the nodes decides whether it will be considered as a redundant node or not on the sponsored area. The sponsored area is defined as maximal sector covered by the neighbor. if the sensing area of the nodes enclose by the active nodes of the neighbor then the nodes itself decided as redundant and gets deactivated. and all the nodes which are not redundant remain active. So in this paper author focus only the coverage, without considering connectivity.

In this, nodes will be presented in 3 states; That's are sleeping, probing and working. At the stating position each nodes are in sleeping state.after definite period of time each nodes wakeup and goes into the probing states'in this stage a node send to probe messege to find out whether any working nodes are there in its probing range or not.if no replay comes from the neighbors as working nodes then the present node change its own state to working state.otherwise its goes back to sleeping mode.The protocol is very simple and it gives provision to changing the probe range.so no of working nodes can be increase or decreased in order to satisfied to complete the coverage .

Gupta et al proposed a centralized as well as distributed algorithm for coverage .This protocol also .satisfied the connectivity in between the active nodes. The centralized algorithm constructs an optimal connected cover within O factor of the optimal size n is the no. of nodes.where as the distributed algorithm does not satisfy the same $O(\log n)$ Factor. Considering the fact that sensor nodes are consumed the energy.in this paper author is also purposed the weighted Version of the same protocol, Where each node is assigned with some weight. The protocol selected subset of nodes with minimum total weight. In order to to encompass the network life time, the node which have a less remaining energy can be assign with higher weight ,so that the selection of connect subset ,the node which have a higher remaining energy will get selected.

Zhang and Hou measured the coverage along with connectivity problem and proposed a theorem, in this if the communication radius of the node is at least twice of the sensing radius then the whole coverage of the curving area involves connectivity amid the set of active nodes. Authors have also designed a circulated geometry density control algorithm named OGDC which is only appropriate in the situation that the communication radius of the node is greater then or equal to 2 times of the sensing radius .there for we use this algorithm to active the sensor nodes at the starting stage of our suggested algorithm.

After analyzing the related work mentioned above,it is found that for maintaining connectivity between the active nodes, they trust upon the critical condition mentioned by Zhang et al. therefore in this paper we will use the concept the Voronoi diagram to divided the entire network into the region of the varying nodes .So a node will only have the responsibility to improve the coverage of the area in which Voronoi diagram has placed it. Thus the node movement is restricted. So the energy needed for movement will be reduced and the coverage area will be improved. This will allow the network to retain energy for a longer time duration.

III. Our Approach

In the previous work, system has been developed for improving the coverage via energy efficient techniques. But these techniques do not take into consideration the movement of the node required for energy efficient coverage improvement. Thus the major energy of the node is spending on moving from location to location for coverage improvement. So each node had the responsibility to contribute for coverage efficiency of the entire network, which made the node to move from network to network in the entire area for coverage improvement which causes a huge energy consumption. Thereby reducing the overall energy of the network.

To overcome this problem we will use the concept of Voronoi diagrams to divide the entire network into regions of varying nodes. So a node will only have the responsibility to improve the coverage of the area in which Voronoi diagram has placed it. Thus the node movement is restricted. So the energy needed for movement will be reduced and the coverage area will be improved. This will allow the network to retain energy for a longer time duration.

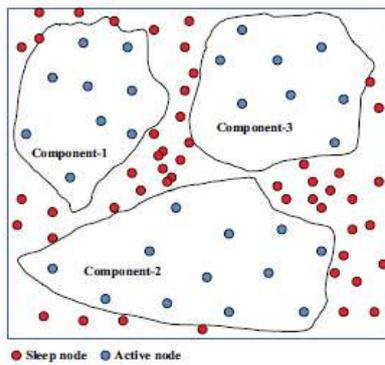


Figure 1. Complete coverage with multiple components in WSN

Frist we develop the Wireless sensor Network for improve Coverage due to this improving coverage and connectivity in between nodes .after that we find out the coverage based and random development .then we apply coverage improvement without Voronoi .then We will use the simulation tool i.e NS2 to implement the voronoi diagram and Delaunary triangle.From this concept we improve the coverage and consumed the energy

V. Conclusions

This review paper is concentrated to improve coverage and connectivity .we purposed the concept of voronoi diagram .The Voronoi diagrams to divide the entire network into regions of varying nodes. So a node will only have the responsibility to improve the coverage of the area in which Voronoi diagram has placed it. Thus the node movement is restricted. So the energy needed for movement will be reduced and the coverage area will be improved. This will allow the network to retain energy for a longer time duration.

VI. References

- [1]N. Ahmed, S. S. Kanhere, and S. Jha, "The holes problem in wireless sensor networks: A survey," SIGMOBILE Mob. Comput. Commun. Rev., vol. 9, no. 2, pp. 4–18, Apr. 2005. [Online]. Available: <http://doi.acm.org/10.1145/1072989.1072992>
- [2] P. A. Arora, "A line in the sand:a wireless sensor network for target detection ,classification, and tracking," in Computer Networks: The International Journal of Computer and Telecommunications Networking, December 2004, p. Volume 46 Issue 5.
- [3] S. B. K. Kar, "Node placement for connected coverage in sensor networks," in Proceedings of the Workshop on Modeling and Optimization in Mobile , Ad-Hoc and Wireless Networks (WiOpt'03). France: Sophia Antipolis, 2003.
- [4] Q. Zhao and M. Gurusamy, "Lifetime maximization for connected target coverage in wireless sensor networks," IEEE/ACM Trans. Netw., vol. 16, no. 6, pp. 1378–1391, Dec. 2008. [Online]. Available: <http://dx.doi.org/10.1109/TNET.2007.911432>
- [5] M. P. S. Megerian, F. Koushanfar and M. Srivastava, "Worst and best-case coverage in sensor networks," in IEEE Trans. Mobile Computing, vol. 4, no. 1., Jan-Feb 2005, pp. 84–92.
- [6] A. Saipulla, J.-H. Cui, X. Fu, B. Liu, and J. Wang, "Barrier coverage: Foundations and design," in The Art of Wireless Sensor Networks, ser.

Signals and Communication Technology. Springer Berlin Heidelberg, 2014, pp. 59–115.

[7] C. Zhu, C. Zheng, L. Shu, and G. Han, "A survey on coverage and connectivity issues in wireless sensor networks," Journal of Network and Computer Applications, vol. 35, no. 2, pp. 619 – 632, 2012, simulation and Testbeds.

[8] I. Dietrich and F. Dressler, "On the lifetime of wireless sensor networks," ACM Trans. Sen. Netw., vol. 5, no. 1, pp. 5:1–5:39, Feb. 2009.

[9] H. Zhang and J. C. Hou, "Maintaining sensing coverage and connectivity in large sensor networks," Ad Hoc & Sensor Wireless Networks, pp. 89–124, 2005.

[10] D. Tian and N. D. Georganas, "A coverage-preserving node scheduling scheme for large wireless sensor networks," in Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, ser. WSN '02. New York, NY, USA: ACM, 2002, pp. 32–41. [Online].



Image Enhancement with Super Resolution Using Sparse Priors

REHAN. A. KHAN

M.TECH student

Department of Electronics & Communication

Anjuman College of Engineering & Technology, Nagpur

e-mail: krehan797@gmail.com

PROF. TIRUPATI GOSKULA

Professor

Department of Electronics & Communication

Anjuman College of Engineering & Technology, Nagpur

e-mail: thiru_aar@rediffmail.com

Abstract – This is a new approach towards image enhancement by increasing the resolution of image with the help of sparse priors. High resolution of videos and images are being required for processing and analysis. In this paper, we tend to gift a unique software-based image enhancement technique that may be utilized in improvement in the quality of image which may get distorted due to motion blur and camera misfocus. There are different approaches for Super Resolution image reconstruction, but sparse representation enhances the image more efficiently. We take a sparse representation for each patch of the low-resolution input, and then use the coefficients of this representation to generate the high-resolution output. In this paper main aim of this technique is to improve the visual quality and consistency of available Low Resolution images.

Keywords: Super Resolution, Patches, sparse coding, image reconstruction.

I. INTRODUCTION

IN RECENT years, there has been increase in the demand of high quality of images and videos. Due to certain circumstances such as atmospheric and environmental effects & passage of time Image gets distorted. Degradation comes in many forms such as Motion Blur, Noise and Camera Misfocus. There is an inherent resolution limitation of low-cost imaging sensors (e.g., cell phone or surveillance cameras) allowing better utilization of the growing capability of high resolution displays (e.g. high definition LCDs). Such resolution enhancing technologies is proved to be very essential for the applications in medical imaging and satellite imaging where diagnosis or analysis from low-quality images can be extremely difficult.

The Super Resolution Image Reconstruction technique produces High Resolution Image from sequence of Low Resolution Images by taking more samples of the same scene and merges the samples to get High Resolution Image. Image enhancement is a method which eradicates the disadvantage or drawback of low Resolution Image by improving the quality of image by estimating amount of noise and blur involved in image thereby increasing the high frequency components and removing the degradations caused by the imaging process of the low resolution camera.

Conventional approaches to generating a SR image normally require as input multiple low-resolution images of the same scene which are aligned with sub pixel accuracy. The basic idea behind SR is to combine the non-redundant information contained in multiple low-resolution frames to generate a high-resolution image. Sparse representation has been successfully applied to many other related inverse problems in image processing, such as denoising and restoration. Sparse representation is one of the methods of super resolution increasing technique which give high resolution image and is proved to be essential in comparison with other techniques.

Researchers have specially made their attention towards developing good resolution of images which distinguishes between Low and High Resolution using different properties along with challenges. Similar to the aforementioned learning-based methods, we will rely on patches from the input image and according to these patches we will try to develop high quality of image. However, instead of working directly with the image patch pairs sampled from high- and low-resolution images. We learn a compact representation for these patch pairs to capture the co-occurrence prior by improving the speed of the algorithm.

II LITERATURE SURVEY

In this section we review various studies and development carried out by many researchers. We will also see various detection techniques.

[1] J. Yang, J. Wright, T. Huang, and Y. Ma has proposed a work on Super Resolution of image and discuss a novel approach in terms of coupled dictionaries jointly trained from high- and low-resolution image patch pairs with the help of sparse coding. To meet the requirements they have developed different algorithms to counter the low resolution images using sparse technique.

They have presented various schemes for dictionary training discussing their advantages and limitations based on parameters such as optimal size of dictionary, range and accuracy. By Providing good resolution and acceptable recognition performance. They worked on the SR problem by using patches i.e. each pair of high and low-resolution image patches have the same sparse representations with respect to the two dictionaries D_h and D_l . A straightforward way to obtain two such dictionaries is to sample image patch pairs directly.

Developing such scheme is very crucial as resolution of the image has increased to great extent.

[2] R. C. Hardie, K. J. Barnard, and E. A. Armstrong proposed work in estimating a high-resolution image, with reduced aliasing, from a sequence of under sampled frames. Many works in SR reconstruction have followed the Maximum a Posteriori (MAP) approach where the techniques vary in the observation model assumptions for the desired solution. There are different approaches applied to overcome the problem of aliased image.

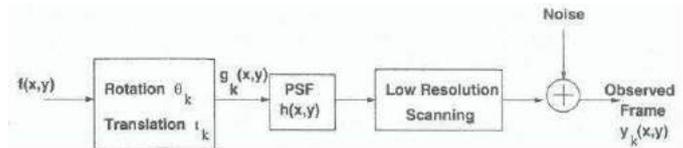
In the proposed method, the registration parameters are iteratively updated along with the high-resolution image. Quantitative error analysis is provided and several images are shown for subjective evaluation

[3] S. Farsiu, M. D. Robinson, has worked on a method to develop the Multi-frame Super Resolution. There have been several techniques developed in the field of Super Resolution. But this method is usually very sensitive to their assumed model of data and noise.

They have designed a robust super-resolution method to enhance the quality of a set of noisy blurred images and produce a HR image with less noise and blur effects. It also removes outliers efficiently resulting in images with sharp edges. For the development robust Multi-frame method they have proposed a frequency domain approach, which is simple and computationally cheap, they are extremely sensitive to model errors. Algorithm for a fast and robust super-resolution is developed for the regularization and the data fusion terms.

[4] M. E. Tipping and C. M. Bishop has proposed an image super resolution system that computes a high resolution image of a target from multiple low resolution images of the same target. Bishop proposed a Bayesian approach for SR where the unknown high-resolution image is integrated out and the marginal is used to estimate the point spread function (PSF) and motion parameters.

By using Bayesian analysis registration parameters and an acuity parameter are improved. In this method each low resolution image differs slightly in perspective from each of the other low resolution images. A low resolution image is optimized to determine the improved estimates of the registration parameters and the acuity parameter, which are used to solve for the high resolution image.



[5] S. Baker and T. Kanade has worked on all super-resolution algorithms are based on the fundamental constraints to generate high Resolution Image. They have used various kinds of schemes for low-resolution input images when appropriately warped and down-sampled to model the image formation process.

They propose a super-resolution algorithm that uses a different kind of constraint in addition to the reconstruction constraints. The algorithm attempts to recognize local features in the low-resolution images and then enhances their resolution in an appropriate manner. They called super-resolution algorithm a hallucination or reconstruction algorithm and then limits on super-resolution.

III CONCLUSION

This paper describes method of reconstructing High Resolution image from low-resolution image. It is observed that among various methods for SR reconstruction, sparse representation with learning dictionary is best suited and it is extensively used. It is concluded that after enhancing the low-resolution image is reconstructed and consistency is maintained with respect to original image.

IV REFERENCE:

[1] J. Yang, J. Wright, T. Huang, and Y. Ma, "Image super resolution as sparse representation of raw image patches," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2008, pp. 1-8.

[2] R. C. Hardie, K. J. Barnard, and E. A. Armstrong, "Joint map registration and high-resolution image estimation using a sequence of undersampled images," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1621-1633, Dec. 1997.

[3] S. Farsiu, M. D. Robinson, M. Elad, and P. Milanfar, "Fast and robust multiframe super-resolution," IEEE Trans. Image Process., vol. 13, no. 10, pp. 1327-1344, Oct. 2004.

[4] M. E. Tipping and C. M. Bishop, "Bayesian image super-resolution," in Proc. Adv. Neural Inf. Process. Syst. 16, 2003, pp. 1303-1310.

[5] S. Baker and T. Kanade, "Limits on super-resolution and how to break them," IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, no. 9, pp. 1167-1183, Sep. 2002.

[6] H. S. Hou and H. C. Andrews, "Cubic spline for image interpolation and digital filtering," IEEE Trans. Signal Process., vol. 26, no. 6, pp. 508-517, Dec. 1978.

[7] S. Dai, M. Han, W. Xu, Y. Wu, and Y. Gong, "Soft edge smoothness prior for alpha channel super resolution," in Proc. IEEE Conf. Comput. Vis. Pattern Class., 2007, pp. 1-8.

[8] J. Sun, Z. Xu, and H. Shum, "Image super-resolution using gradient profile prior," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2008, pp. 1-8.

[9] W. T. Freeman, E. C. Pasztor, and O. T. Carmichael, "Learning lowlevel vision," Int. J. Comput. Vis., vol. 40, no. 1, pp. 25-47, 2000.

- [10] J. Sun, N. N. Zheng, H. Tao, and H. Shum, "Image hallucination with primal sketch priors," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2003, vol. 2, pp. 729–736.
- [11] H. Chang, D.-Y. Yeung, and Y. Xiong, "Super-resolution through neighbor embedding," in Proc. IEEE Conf. Comput. Vis. Pattern Class., 2004, vol. 1, pp. 275–282.
- [12] S. T. Roweis and L. K. Saul, "Nonlinear dimensionality reduction by locally linear embedding," *Science*, vol. 290, no. 5500, pp. 2323–2326, 2000.
- [13] S. Baker and T. Kanade, "Hallucinating faces," in Proc. IEEE Int. Conf. Autom. Face Gesture Recognit., 2000, pp. 83–88.
- [14] C. Liu, H. Y. Shum, and W. T. Freeman, "Face hallucination: Theory and practice," *Int. J. Comput. Vis.*, vol. 75, no. 1, pp. 115–134, 2007.
- [15] W. Liu, D. Lin, and X. Tang, "Hallucinating faces: Tensorpatch superresolution and coupled residue compensation," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2006, vol. 2, pp. 478–484.
- [16] E. J. Candes, "Compressive Sampling," in Proc. Int. Congr. Mathematicians, 2006, vol. 3, pp. 1433–1452.
- [17] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
- [18] H. Rauhut, K. Schnass, and P. Vandergheynst, "Compressed sensing and redundant dictionaries," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, May 2008.
- [19] M. Elad and M. Aharon, "Image denoising via sparse and redundant representations over learned dictionaries," *IEEE Trans. Image Process.*, vol. 15, no. 12, pp. 3736–3745, Dec. 2006.
- [20] J. Mairal, G. Sapiro, and M. Elad, "Learning multiscale sparse representations for image and video restoration," *Multiscale Model. Sim.*, vol. 7, pp. 214–241, 2008.
- [21] M. Aharon, M. Elad, and A. Bruckstein, "K-svd: An algorithm for designing overcomplete dictionaries for sparse representation," *IEEE Trans. Signal Process.*, vol. 54, no. 11, pp. 4311–4322, Nov. 2006.

A Scalable and Modular Architecture for High Performance Packet Classification

Farha Sabir

Department of Electronics and Telecommunication
Nuva college of Engineering and Technology
Nagpur, India
farhasabir@rediffmail.com

Pooja Thakre

Department of Electronics and Telecommunication
Nuva college of Engineering and Technology
Nagpur, India

Abstract— Packet Classification is a crucial function used in an internet router, firewall, network security and quality of services. Packet classification technique is very crucial since various unauthorized and malicious networks are being exposed to. For secure networking and avoiding unauthorized access, incoming packets flow based on predefined rules available in a classifier. Available software solution's performance is not efficient for wire speed processing in high speed networks. To meet the line-card requirement and wire speed processing hardware solution is more efficient and secure than software solution. For implementing hardware architecture for wire speed processing different algorithms have been proposed. This paper presents review on different algorithm and technique used to implement packet classification architecture. High performance packet classification architecture can be implemented using Field programmable gate array (FPGA) and large number of rules can be stored using on-chip memory resource of FPGA

Keywords— Packet classification, 5-tuple, Quality of services, latency, throughput

I. INTRODUCTION

Modern packet processing system uses technique known as packet classification in place of de-multiplexing due to various advantages like high speed and ability to cross multiple layers. Various services like firewalls, Virtual Private Network (VPN), network security, policy-based-routing, traffic shaping and Quality of Services (QoS) require packet classification. This makes packet classification an integrated part of network intrusion detection system (NIDS). To access various services, it is required to figure out which rule matches with incoming packet and depending on it necessary action is taken. In other words, flows are decided by rules applied to incoming packets and each rule in a rule-set specifies a flow to which a packet may belong based on values in header fields.

Packet classification process involves inspection of multiple fields against a rule-set may be containing thousands of rules. This is one of the challenge and difficulty in the process of classification. Each rule in a classifier has a priority and action is taken according to their priority. Basic 5-tuple are present in the standard packets header which include destination and source IP address field, destination and source port number

field and the protocol type field as depicted in figure.1. For different combination of values of the fields require different matches like prefix match for destination and source IP address field, range match for destination and source port field and exact match for protocol field. For better performance, packet classification system must support all the type of match.

Source IP address 32-bit	Destination IP address 32-bit	Source port number 16-bit	Destination Port number 16-bit	Protocol Type 8-bit
--------------------------------	-------------------------------------	---------------------------------	--------------------------------------	---------------------------

Fig.1 Standard 5-tuple packet header fields

Considering the fact that packet classification system is the central part of firewalls, internet routers and various intrusion detection systems. Various packet classification algorithms have been proposed to perform packet classification; just because of special computational method most of the existing algorithms may not be suitable for hardware implementation. The main performance metrics that should be taken into an account while designing algorithms for implementing hardware packet classification system are as follow:

- **Memory requirement:** memory requirement for storing number of rules is limited in hardware solution. The on-chip SRAM of FPGAs can be used to store large number of rules.
- **Multi match classification:** packet classification algorithm should support exact match, prefix match and range match. It should also avoid the use of prefix to range match conversion which is memory inefficient.
- **High speed:** algorithm must meet the in-line requirement of 100/200/400 Gbps while supporting large number of rules.
- **Update, modify and delete rules:** Dynamic modification, updating and removing of out-dates rules is required for supporting various new applications.
- **Latency:** low latency application requires parallel orientation in cost of memory while in some application

series orientation is feasible. It is important that algorithm should be flexible in orientation for supporting all types of application.

Above performance matrices are very crucial while designing hardware packet classification architecture to avoid degradation of performance of the architecture. However, performance of architecture depends on an algorithm used for designing it.

II. DETAIL STUDY ON PACKET CLASSIFICATION TECHNIQUE

From literature survey and review of related work, it is observed that researchers have designed the packet classification architecture using algorithms based on these four methods: exhaustive search, decision tree based, tuple search and decomposition based method. Decision tree based approach and decomposition based approach are desirable for hardware implementation of packet classification system. Efforts have been undertaken by researchers for designing of multi-match packet classification architecture for firewalls and all type of intrusion detection systems. Researchers put their best to implement hardware solution for packet classification.

For one-dimensional packet classification, Ternary Content Addressable Memory (TCAM) is the desirable hardware solution because of its simple management and speed. To check all fields at a time and at high speed, TCAM based search engine is used. For multi-dimensional packet classification using TCAM, Yeim-Kuan Chang and Cheng-Chien Su have proposed an efficient range-encoding Scheme for Packet Classification using Gray code [3]. Experimental result's shows the proposed binary reflected gray code-based (BRGC) encoding scheme requires less TCAM storage than parallel packet classification encoding (PPCE) scheme. The BRGC based encoding scheme is proposed for range values of source and destination port number but it is also used for source and destination address field of packets having prefix addresses. Problems like limited scalability and the range to prefix blowout for large number of rule-set have solved using BRGC based encoding scheme.

Lu Sun, Hoang Le, Viktor K. Prasanna have proposed optimizing decomposition-based packet classification on FPGA [4]. Decomposition-based IP classification algorithms consist of two phase: in first phase, independent searches are performed on each field of packets, while in second phase: results from the first phase are combined. Due to limited resources and limited on-chip memory on FPGAs, the second phase of the decomposition based algorithms become challenging. To solve this problem, they have proposed a systolic-array-based architecture which efficiently combines the results of the first phase in the second phase. The proposed architecture on set intersection and compact representation of matching rules yields better performance in second phase of the algorithm. The design is more efficient, feasible and attractive in logic resources, in handling large rulesets and in area than any other decomposition based algorithm. The proposed architecture has implemented on Xilinx Virtex-6 XC6VLX760 with -2 speed grade as a target in Verilog using Xilinx ISE 12.4 tool. The implemented design achieves high throughput of 107 Gbps while supporting rules upto 64K of minimum packet size of 80 bytes.

Weirong Jiang and Victor K. Prasanna have introduced Field-Split Parallel Bit Vector (FSBV) based architecture [2]. The FSBV architecture is suitable for Snort rule and it is a novel SRAM-based architecture which exploited the use of BlockRAMs of current FPGA. It supports multi match packet classification and also handles the negation and value list problem. The architecture is memory efficient because range to prefix conversion is not used for range values. Proposed architecture used TCAM algorithm for source and destination address fields, CAM algorithm for protocol field and Bit Vector (BV) algorithm for source and destination port fields. The FSBV architecture achieved clock frequency of 167 MHz and processed two packets every clock cycle with the use of dual-port RAMs on a Xilinx Virtex-5 XCVFX200T device. Using SRAM-based architecture and low memory requirement, one fourth power reduction can be achieved over BV-TCAM.

Researchers have developed various software solutions for packet classification, but hardware solutions yield high performance and supports dynamic updates. Yun R Qu, Shijie Zhou, and Viktor K. Prasanna have proposed a high performance 2-dimensional pipelined architecture for packet classification on FPGA which supports dynamic updates of rules [6]. The proposed architecture consists of self-reconfigurable processing elements. A modular processing element (PE) can handle range match as well as prefix match and does not need range to prefix conversion. Multiple modular processing elements (PEs) are used in the architecture to construct a 2-dimensional architecture for handling large number of rules. Striding and clustering technique is used in the implemented architecture to vary size of sub-field and number of rules. The architecture can perform packet classification of s-bit subfield against a set of n rules using striding and clustering technique. A set of algorithm supports modification, deletion and insertion operations on the proposed architecture. Dynamic updatable of rules on hardware is possible without deteriorating the pipeline performance. The architecture is scalable with respect to large input length. The Proposed architecture maintains very high clock frequency of 324 MHz and can achieve throughput of 190 Gbps with 1K 15-tuple rule-set on Virtex-6 XC6VLX760 FFG1760-2 FPGA device.

A scalable and modular architecture for high performance packet classification have been proposed by Thilan Ganegedara, Weirong Jiang, and Viktor K. Prasanna [1]. They have proposed a novel modular Bit-Vector based architecture on field programmable logic array (FPGA) using StrideBV algorithm. Range integration search in the architecture avoids the use of range-to-prefix conversion and supports all type of match. The architecture is scalable on hardware and pipelined priority encoder is used for extracting highest priority match. Proposed serial and parallel versions of StrideBV based architecture are ruleset-feature independent solution. Their solution is flexible in orientation depending on an application and latency requirement. Proposed architecture is memory efficient, achieves 100+ Gbps throughput while supporting upto 28K rules using only on-chip resources on a state-of-the-art Xilinx Virtex-7 2000T FPGA device and evaluates the performance of both serial and parallel version of strideBV using post place-and-route results.

III. OUR PROPOSED WORK

StrideBV is the one of the efficient decomposition based packet classification technique which supports hardware implementation. StrideBV algorithm achieves low latency and sustains high throughput than any other existing technique. However, it is not memory efficient technique for large number of rules which is the major drawback of this technique. Because of all the above reasons, in this paper we presented our proposed method which classify a packets using XNOR gate. Our proposed method is memory efficient and can achieve low latency for same number of rules than StrideBV.

In our work we use 512 rules of ternary string format having values in '1', '0' and '-'. In strideBV, lookup table indicates status of rules. A look-up table is stored in a memory having depth (height) of 2^k and entry (width) in each row is equal to number of rules (N). An incoming stride extracts N-bit vector from the corresponding memory location. An N-bit vector from corresponding memory location contains matching result of rules with incoming stride. The memory required in this method is generally depends on number of rules and stride size. The priority encoder is used to select incoming stride for highest priority rule. The register transfer level view of priority encoder is depicted below in fig. 2.

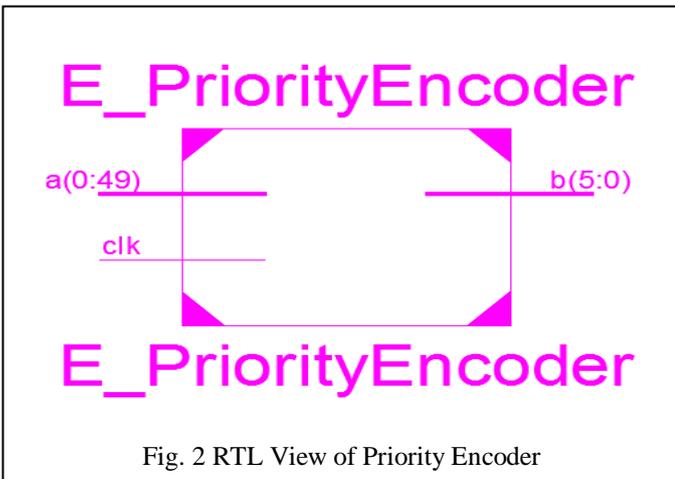


Fig. 2 RTL View of Priority Encoder

In proposed work, we use basic XNOR gate for matching incoming packets against a set of rule and produce bit vector of same size as that of rule and then ANDed all bits of match result and produce one bit for each rule. Each bit after ANDing operation gives status of incoming packet against each rule of the rule-set. For selecting highest priority rule from the rule-set, priority encoder is used. Technology schematic view of proposed work is shown in fig. 3. For same number of rules our proposed method of packet classification is memory efficient because each rule in our proposed work require only 32 bit whereas in strideBV each rule requires 2^{32} bit for lookup table.

We have designed and optimized the proposed method in VHDL using Xilinx ISE 13.1 tool. We select Spartan6 as a family and 6slx4tqg144-3 as target device for performing

synthesis and optimizing the design using Xilinx tool. Simulation results are shown in next section to check the functionality of designed module of packet classification.

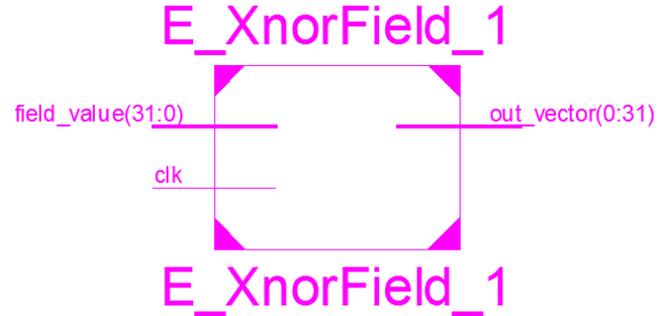


Fig. 3 RTL View of Xnor Based Packet Classification

IV. SIMULATION RESULT

Fig. 4 shows simulation result of priority encoder for input of 32-bit and output will be the highest match. Here, MSB has highest priority whereas LSB has lowest priority. It means rules should be arranged in descending order of their priority.

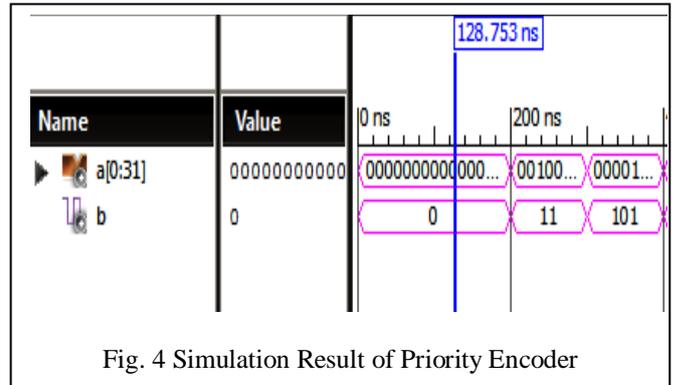


Fig. 4 Simulation Result of Priority Encoder

Fig. 5 shows simulation result of Xnor based packet classification where input packet is of 32-bit and output is a vector which indicates match and mismatch of rule against predefined ruleset. From simulation results it is cleared that we get output in one clock cycle. Pipelining stages are not used in this design to get less latency and also lookup table is not used to minimize the memory cost.

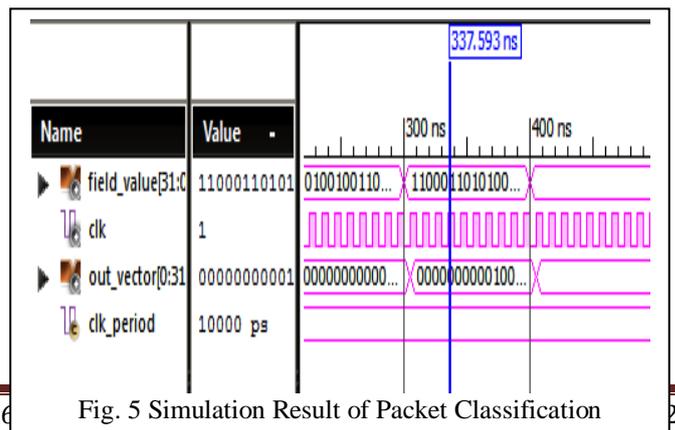


Fig. 5 Simulation Result of Packet Classification

V. CONCLUSION

Our proposed method of packet classification is latency and memory efficient as compared to strideBV algorithm. Latency achieved in proposed work is one clock cycle which is better as compared to strideBV for same rule-set. Memory required to represent one rule in the proposed work is less which has overcome the major bottleneck of hardware solution. In future we can implement the packet classification architecture for complete packet header field.

References

- [1] Thilan Ganegedara, Weirong Jiang, and Viktor K. Prasanna, Fellow, IEEE; "A Scalable and Modular Architecture for High-Performance Packet Classification"; IEEE Transactions on Parallel And Distributed Systems, Vol. 25, No. 5, May 2014; 1045-9219 _ 2013 IEEE, Pp.1135-1144)
- [2] J W. Jiang and V. K. Prasanna, "Field-split Parallel Architecture for High Performance Multi match Packet Classification using FPGAs," in Proc. of the 21st Annual Symp. on Parallelism in Algorithms and Arch. (SPAA), 2009, pp. 188–196.
- [3] Yeim-Kuan Chang and Cheng-Chien Su, "Efficient TCAN Encoding Scheme Packet Classification using Gray Code," in IEEE GLOBECOM 2007 proceedings @2007 IEEE.
- [4] Lu Sun, Hoang Le, Viktor K. Prasanna; "Optimizing Decomposition-based Packet Classification Implementation on FPGAs"; 2011 International Conference on Reconfigurable Computing and FPGAs; 978-0-7695-4551-6/11 \$26.00 © 2011 IEEE; pp. 170-175
- [5] Andrea Sanny, Thilan Ganegedara, Viktor K. Prasanna; "A Comparison of Ruleset Feature Independent Packet Classification Engines on FPGA; 2013 IEEE 27th International Symposium on Parallel & Distributed Processing Workshops and PhD Forum", 978-0-7695-4979-8/13 \$26.00 © 2013 IEEE
- [6] Yun R. Qu, Shijie Zhou, and Viktor K. Prasanna; "High- performance architecture for dynamically updatable packet classification on FPGA," Architecture for Networking and communication systems (ANCS), 2013 ACM/IEEE Symposium on @ 2013 IEEE, pp. 125-136
- [7] Pankaj Gupta and Nick Mckneown; "Algorithms for packet classification" in IEEE magazine, March/April 2001 pp. 24-32
- [8] Hung-Yi Chang, Chia-Tai Chan, Pi-Chung Wang, Chun-Liang Lee; "A Scalable Hardware Solution for Packet Classification," in ICCS @2004 IEEE.
- [9] Mahmood Ahmadi, S. Arash Ostadzadeh, and Stephan Wong; "An Analysis of Rule-Set Databases in Packet Classification,"
- [10] Nekoo Rafiei Karkvandi, Hassan Asgharian, Amir Kusedghi, Ahmad Akbari, "Hardware Network packet Classifier for High Speed Intrusion Systems" ;International Journal of Engineering and Technology; Volume 4 No.3, March, 2014.
- [11] Safaa O.AI-Mamory and Wesam S.Bhaya; "Taxonomy of Packet Classification algorithms", Journal of Babylon University/Pure and Applied Science/No.(7)/Vol.(21):201.



A Review of Improving Channel Selection in Cognitive Radio for Routing Protocols

Fiza Firdaus

Deptt. of Electronics & Comm. Engg.

G.H.R.A.E.T.

Nagpur, India.

Email: fiza.firdous8@gmail.com

Dr.Pankaj Agrawal

Deptt. of Electronics & Comm. Engg.

G.H.R.A.E.T.

Nagpur, India.

Email: pankaj.agrawal@raisoni.net

Abstract— The radio spectrum is one of the profoundly used and valuable natural resources in wireless communication. Cognitive radio is an rising technology to deal with the problem of radio spectrum scarcity and spectrum underutilization. In Cognitive radio, channel selection is the method by which one can choose a desired channel and it is one of the essential issues to be taken into account. In this project, improvement of channel selection will be done for routing protocol such as AODV (Ad-hoc On Demand Distance Vector) and DSR (Distance Source Routing) using the technique which is based on no. of packets and based on access time by the primary user. The evaluation of the performance of these routing protocols will be done using simulations in NS-2.

Keywords— *Cognitive radio, AODV (Ad-hoc on demand distance vector), DSR (Distance source routing), Channel Selection.*

I. INTRODUCTION

Cognitive Radio is a new method of implement radio communications which allows for further proficient use of the frequency spectrum. This is essential since currently there is a large part of the spectrum which is underutilize. The overall purpose of opportunistic spectrum access (OSA) is provide spectral access to secondary users without disturbing the consistency or performance of the primary users service. Cognitive networks (CN) are wireless networks which consist of two types of users primary and secondary (or cognitive) users.

- Primary users: These wireless users are the primary license-holders of the spectrum band of interest. In general, they have priority access to the licensed spectrum, as well as matter to certain Quality of Service (QoS) constraints which should be guaranteed.

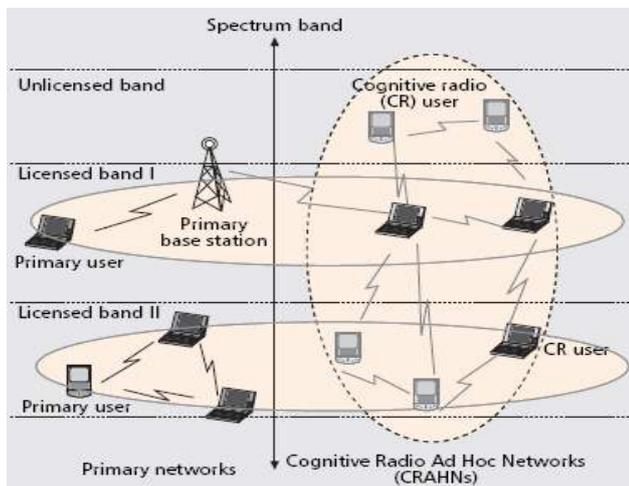
- Secondary users: These users could access the spectrum which is licensed toward the primary users and can opportunistically communicate in licensed spectrum by varying their communication parameters in an adaptive approach when spectrum holes are available.

There are various standard unlicensed bands. Some of the types of unlicensed radio bands are as and other devices that operate in the 900 MHz, 2.5 GHz, and 5.9 GHz bands. Unlicensed National Information Infrastructure (U-NII): This type defines the terms for the use of wireless devices such as WLAN access points and routers in the 4 GHz band. Unlicensed Personal Communications Services (UPCS): This kind defines the terms for devices operating in the 1.8 GHz band, wherever DECT6 cordless phones operate. Unlicensed National Information Infrastructure (U-NII): This type defines the terms for the use of wireless devices such as WLAN access points and routers in the 5 GHz band. Unlicensed Personal Communications Services (UPCS): This type defines the terms for devices operating in the 1.8 GHz band, wherever DECT6 cordless phones work.

II. RELATED WORK

A. Performance assessment of AODV-based and DSR-based Multi-radio Routing Protocols in Cognitive Radio Ad Hoc Network

We reviewed the attempt towards a comprehensive performance evaluation of AODV-based and DSR-based multi-radio routing protocols in CR. In this study, we reviewed about protocol performance of the AODV-MR, the extended DSR and the MR-LQSR in CRAHN was evaluated under CBR traffic with varying simulation period, using NS-2 simulator. Performance metrics considered are average throughput, average end-to-end delay and average jitter.[6]



B. Cognitive Radio Technology: System Evolution

We reviewed numerous techniques presented for detecting while the spectrum is within use, accessing the spectrum while not in use, selecting the mainly capable channel for use by the secondary user, and transmitting over channels by high interference. In every category, an optimal technique was planned. Upcoming work in cognitive radio might lead to the finding of how these techniques interrelate by each other to conclude if they are able to form an effective system as a whole.[1]

C. Performance Evaluation of AODV and DYMO Routing Protocols in MANET

We reviewed this paper in brief described the key features of the AODV and DYMO routing protocols and evaluated them based on packet-level simulations using an ns-2 simulator. The simulation results showed that while the path accumulation of DYMO less the routing overhead, the size of the routing packet was increased. Plus, at moving speeds between 1m/s and 9m/s, the total throughput of DYMO could outperform that of AODV. Though, at moving speeds among 11m/s and 15m/s, AODV might achieve a high throughput than DYMO.[3]

D. Our spectrum sharing between energy Harvesting Cognitive radio users & primary users

We reviewed in this the investigation of the maximum achievable throughput for an SU sharing the spectrum among a PU. The SU has a fixed capacity battery and is equipped with energy harvesting capability. We assume that the SU harvests energy from primary RF transmissions as well as natural resources .The obtained results reveal the promises of employing RF energy harvesting. They have showed that the SU throughput can be improved as the arrival rate to the primary queue increase. This is attributed to the raise in the total of energy that the SU harvests from primary RF transmissions. [2]

III. OUR APPROACH

We are improving channel selection for routing protocols on the basis of channel selection technique.

A. Based on no. of packets :

In this approach, selection of a threshold of packets sent by the primary user, if the no. of packets go beyond the particular threshold then one secondary user packet will be sent on the channel. This will make sure that the secondary user does not starve of communication & the packet flow is continuous without disturbing the primary user.

B. Based on Access time by the primary user:

In this case, first scanning of channel will be done. If the primary user is not accessing the channel for some amount of time then that channel will be allocated to the secondary user thereby optimizing the utilization of channel for both the user.

IV. COMPARISON

Algorithm	Comments
Myopic	Require awareness of channel statistics.
	Simple, yet not consistently accurate.
	Unable to track channel evolution.
Online Learning	Require no prior knowledge of the channel.
	Used with Thompson Sampling to find the greatest channel for unlicensed users.
	Used to predict whether switching channels or remaining on the same channel is optimal.
Based on no. of packets	Selection of threshold.
Based on access time by primary user	Scanning of channel is done.

V.CONCLUSION

In the previous system, channel selection was limited to only some selected routing protocols. This made application of cognitive radio restricting to only selected routing protocols. In this project, the concept of channel selection can be extending between primary user and secondary user in a flexible manner.

REFERENCES

- [1] Joanna Wallace, Kyle Richardson, Bob Gill, Stephen Makonin School of Energy, "Cognitive Radio Technology: System Evolution" International Conference on Wireless Networks and Embedded System IEEE 2015.
- [2] Ahmed EL shafie , Mahmaudn Ashour, Tamer Khattab Amr Mohamed,"On spectrum sharing between energy Harvesting Cognitive radio users & primary users" International Conference on Computing(ICNC), 978-1-4799-6959-3/15/ ,pp.214-220,IEEE 2015.
- [3] Dong-Won Kum, Jin-Su Park, You-Ze Cho, and Byoung-Yoon Cheon "Performance Evaluation of AODV and DYMO Routing Protocols in MANET " IEEE Comm. Society , 978-1-4244-5176-0/10,IEEE 2010.
- [4] Amir-Hamed Mohsenian-Rad, "Distributed Channel Selection and Randomized Interrogation Algorithms for Large-Scale and Dense RFID

- Systems"IEEE TRANSACTIONS ON WIRELESS COMMUNICATION, VOL. 9, NO. 4, pp.1402-1413 APRIL 2010.
- [5] Juan Liu, Zhigang Cao, Ying Jun Zhang, "Delay optimal scheduling for cognitive radios with Cooperative Beamforming: A structured Matrix-Geometric Method" IEEE TRANSACTION ON MOBILE COMPUTING, VOL.11, NO.8, pp.1412-1423, AUG. 2012.
- [6] Zamree Che-aron, Aisha Hassan Abdalla and Khaizuran Abdullah " The Performance Evaluation of AODV-based and DSR-based Multi-radio Routing Protocols in Cognitive Radio Ad Hoc Network".Research Journal of Applied Sciences Engineering & Technology, July 2013.
- [7] Matthew Sherman, Apurva N. Mody, Ralph Martinez, and Christian Rodriguez "IEEE Standards Supporting Cognitive Radio and Networks, Dynamic Spectrum Access, and Coexistence" IEEE Communications Magazine, pp.72-79, July 2008.
- [8] Yang Liu, Zhangdui Zhong, Gongpu Wang, and Dan Hu." Cyclostationary Detection Based Spectrum Sensing for Cognitive Radio Networks" Journal of Communications Vol. 10, No. 1, pp.74-79, January 2015.
- [9] Manveen Singh Chadha, Rambir Joon, Sandeep " Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, pp.375-381, July 2012.



Review of High Speed, Low Power Viterbi Decoder for Wireless Communication

Dipti J. Umalkar

M-Tech (ECE) Third Sem,
Abha Gaikwad College of Engineering
Nagpur, India
dipti.j.umalkar@gmail.com

Rahul Godghate

Ass. Professor Department of ECE
Abha Gaikwad-Patil College of Engineering
Nagpur, India
rahul.godghate@gmail.com

Abstract:

In wireless communication applications, low power encoders and Decoders are highly beneficial. This work presents Hybrid method Viterbi decoder which has less delay in data transmission compared to trace back type and register exchange type. Also it needs very less power and area. The Viterbi algorithm is a widely used algorithm for decoding of convolution codes. The algorithm helps to find a path of the trellis diagram, in which the sequence of output symbols is nearly equal to the received sequence.

To accomplish this task, it calculates for each path the path metric, which measures the distance to the received symbols sequence. The metric distance between the received noisy symbol and the output symbol of the state transition is calculated by branch metric unit. ACSU computes the accumulated metric associated with the sequence of transitions (path) to reach a state. When more than one path arrives to a state, ACSU selects the path with the lowest metric value, which is the survivor path. SMU (survivor memory unit) stores the information that permits to trace back from a state to the previous one. Hybrid unit is incorporated between ACS unit and SMU.

In Hybrid method number of memory blocks are reduced. This in turn reduces the area requirement. The two clock cycle is used, in which one is for trace back the information and another for storing the information in register block. This leads to a major gain in speed of data correction along with low power. The overall System will be designed using HDL language and simulation.

Keywords— Branch Metric Unit (BMU), Add Compare and Select Unit (ACSU), Survivor Memory Unit (SMU), Hardware description Language (HDL)

I. INTRODUCTION

Convolution codes, which allow for efficient hard-decision. It has been widely deployed in many wireless communication systems to improve the limited capacity of the communication channels. The Viterbi algorithm is the most extensively employed decoding algorithm for Convolutional codes. The availability of wireless technology has revolutionized the way communication is done in our world today. With this increased availability comes increased dependence on the underlying systems to transmit information

both quickly and accurately. Because the communication channels in wireless systems can be much more hostile than in “wired” systems, voice and data must use forward error correction coding to reduce the probability of channel effects corrupting the information being transmitted. Wi-Fi is a popular technology that allows an electronic device to exchange data wirelessly from transmitter to receiver. A new type of coding, called Viterbi coding, can achieve a level of performance that comes closer to theoretical bounds than more conventional coding systems.

The Viterbi Algorithm, an application of dynamic programming, is widely used for estimation and detection problem in digital communications and signal processing. It is used to detect signals in communication channels with memory, and to decode sequential error control codes that are used to enhance the performance of digital communication systems. Convolutional codes are frequently used to correct errors in noisy channels. They have rather good correcting capability and perform well even on very bad channels. Convolutional codes are extensively used in satellite communications. Although Convolutional encoding is a simple procedure, decoding of a Convolutional code is much more complex task. Several classes of algorithms exist for this purpose.

The Viterbi decoding algorithm, proposed in 1967 by Viterbi, is a decoding process for Convolutional codes in memory-less noise. The algorithm can be applied to a host of problems encountered in the design of communication systems. The Viterbi decoding algorithm provides both a maximum-likelihood and a maximum a posteriori algorithm. A maximum a posteriori algorithm identifies a code word that maximizes the conditional probability of the decoded code word against the received code word, in contrast a maximum likelihood algorithm identifies a code word that maximizes the conditional probability of the received code word against the decoded code word. The two algorithms give the same results when the source information has a uniform distribution.

II. PRELIMINARY RESEARCH

In the preliminary research it has been found that the constraint length associated with the input bits are large,

hence it needs to implement the larger constraint length with lesser hardware and lesser computations to decode the original data. So the proposed method uses Hybrid method of Viterbi decoder which will lower down the power consumption and increase the speed of operation.

III. LITURATURE SURVEY

Song Li and Qing-Ming Yi (2006) proposed a scheme based on Verilog language for the implementation of high-speed and low power consumption bi-directional viterbi decoder . The decoding was done in both positive and negative direction and the delay was half of that of the unilateralism decoder and the decoding speed was greatly improved.

Yun-Nan Chang and Yu-Chung Ding (2006) presented a low power design for viterbi decoder based on a novel survivor path trace mechanism. By incorporating the dynamic multiple path convergence scheme, the survivor path can be determined at earlier stage such that the overall survivor memory access can be reduced.

The experimental results show that the average memory reference can be reduced up to more than 30% for digital video broadcasting (DVB) application at high signal-to-noise ratio. The bit-error-rate (BER) performance of the proposed approach can be even better in some cases. This approach can lead to the reduction of power since memory operation is considered as the major power consumption of the entire decoders.

Lupin Chen et al (2007) presented a low-power trace-back (TB) scheme for high constraint length Viterbi decoder. This paper presents a new low-power memory-efficient trace-back (TB) scheme for high constraint length Viterbi decoder (VD). With the trace-back modifications and path merging techniques, up to 50% memory read operations in the survivor memory unit (SMU) can be reduced. The memory size of SMU can be reduced by 33% and the decoding latency can be reduced by 14%. The simulation results show that compared to the conventional TB scheme, the performance loss of this scheme is negligible.

Xuan-zhong Li et al (2008) discussed a high speed viterbi decoder which was based on parallel radix-4 architecture and bit level carry-save algorithm. Seongjoo Lee (2009) presented an efficient implementation method for parallel processing viterbi decoders in UWB systems.

From the literature survey, viterbi decoder is mainly used in all communication techniques. Logic styles like CMOS, Pseudo NMOS and Dynamic logic design of circuits at ACS level are done but the switching activity in these logic styles are high and hence lead to high power dissipation. From the literature survey we found that Viterbi decoder is designed by using Register Exchange method or Trace Back method.

1. Trace back method has very high delay. Suitable for larger constraint length of data.

2. Register Exchange method requires large area. suitable for shorter constraint length of data.

So that in proposed method we will try to combine both the methods so we will get the advantages of both the methods. By using Hybrid method Delay is reduced and area required is less as compare to register exchange method,

because in Hybrid method it will store alternative memory locations.

IV. PRESENT SYSTEM IN USE

Present system uses two basic ways to keep track of the best path to get to each state. These are the register-exchange, and the trace back method. The register exchange is very easy to

understand, and works well for small constraint lengths. The trace back method is a bit more difficult, but works well for longer constraint length codes.

V. FUTURE OBJECTIVE

The present system is complicated to use and has some limitations.

- Trace back method requires several reads to trace backwards to find exact path. This operation needs extra read ports. The address (word and bit) of the second step back is based on the value of the first step back. This means possibly doubling the clock to out of the RAM, or using a large MUX after the second read.
- Register exchange method results in complex hardware and high switching activity due to the need to copy the content of all the registers from state to state. It is time consuming process.
- So, by considering above limitations our future objective will be to implement Viterbi decoder using Hybrid method which will combine the processes and advantages of register exchange method and trace back method.
- Implement an efficient design of viterbi decoder.
- Reduce the power consumption without degrading the decoding speed.
- Reduce the Area and Delay.
- Design of area optimize synchronous pipelined architecture for high throughput core.
- Maximum operating frequency greater than 200Mhz for high speed application.

VI REFERENCES

- [1] Mahender Veshala, 2Tualsagari Padmaja and 3Karthik Ghanta, "FPGA Based Design and Implementation of Modified Viterbi Decoder for a Wi-Fi Receiver" Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013).

- [2] Susmitha.A ,Mahesh shetkar “Design and Efficient Implementation of Modified Viterbi Decoder for Communication Systems” International Journal of Advances in Electrical and Electronics Engineering ISSN: 2319-1112 Volume 3, No.2
- [3] Sharada Suresh Dambal & Dr.Bharathi S. H. “Design and Simulation of Hybrid Modified Viterbi Decoder for Fast Communication” International Journal of Innovations in Engineering and Technology ISSN: 2319 – 1058
- [4] D. Chakraborty¹, P. Raha², A. Bhattacharya³ , R. Dutta⁴ ,“Speed optimization of a FPGA based modified Viterbi Decoder”¹ , International Conference on Computer Communication and Informatics (ICCCI -2013), 2013 IEEE
- [5] Bhowal, “Transformation of ACS Module to CSA Module of Low-power Viterbi Decoder for Digital Wireless Communication Applications” , 2013 IEEE
- [6] Atish A. Peshattiwar, Shashant Jaykar, Tejaswini G. Panse,”ACSU Architecture with High Clock Speed for Viterbi Decoder Using T-Algorithm” , International Conference on Communication Systems and Network Technologies , 2012 IEEE

Implementation of Greenhouse Controller using ARM processor

Mr. Amit Bhattacharya, Prof. Nilesh A. Mohota²

¹PG Student, PG Department of Electronics Engineering,

J D College of Engineering and Management, Nagpur, India. Email: bshants@gmail.com

² Asst. Prof., Department of Electronics & Telecommunication Engineering,

J D College of Engineering and Management, Nagpur, India. Email: nileshmohota@gmail.com

Abstract- Agriculture is the backbone of India's economic activity and our experience during last 50 years has demonstrated the strong correlation between agricultural growth and economic prosperity. If India has to emerge as an economic power in the world then our agricultural productivity should equal to those countries, which are currently rated as economic power of the world.

About, 95% of plants (either food crops or cash crops) are grown in open field. But in some of the temperate regions where the climatic conditions are extremely adverse and no crops can be grown, man has developed methods of growing some high value crops using controlled environment, which is called as Greenhouse Technology. So, Greenhouse technology is a technique of providing favorable environment condition to the plants irrespective of the weather changes.

This paper gives design of prototype model of the hardware and firmware of the system. In this project we would be making a system which will be sued for proving favorable environment conditions to plants by monitoring parameters such as temperature, light intensity, humidity, moisture etc. using microcontroller.

Further this is a sponsored project by Sri Sai Fibers, Hyderabad.

I. INTRODUCTION

Presently the market of Greenhouse technology is growing a lot in India. Companies like ABB, Dupoint etc. are investing in this field as it has tremendous scope of development in India.

As we all know that the climate in India is becoming unfavorable fro plants day by day. Due to which farmers are incurring huge loss and due to this suicide of farmers is becoming common in India.

To overcome this problem the only feasible solution is to use Greenhouse technology i.e. growing plants in controlled environment irrespective of the exterior climatic changes. Greenhouse controllers are a small unit which is used for controlling the parameters such as Temperature, Humidity, Soil moisture, Controlling Light intensity etc. The main advantage of using Greenhouse Controller is that one can grow any plant in any place at any time by providing suitable environmental conditions with minimum labour. The Government of India is also taking initiative by giving subsidy and easy loan facility to farmers for installing Greenhouse technology.

Greenhouses are framed or inflated structures covered with transparent or translucent material large enough to grow crops under partial or fully controlled environmental conditions to get optimum growth and productivity. Currently PLC's are used for controlling the parameters. But in our project we will be replacing these PLC's by microcontroller. The prime intention of doing this is to reduce cost but provide the same facility so

that this technology can be used in a very high scale.

Some of the advantages of using Greenhouse controller are as follows:

1. The yield may be 10-12 times higher than that of outdoor cultivation depending upon the type of greenhouse, type of crop, environmental control facilities.
2. Reliability of crop increases under greenhouse cultivation.
3. Ideally suited for vegetables and flower crops.
4. Year round production of floricultural crops.
5. Off-season production of vegetable and fruit crops.
6. Disease-free and genetically superior transplants can be produced continuously.
7. Efficient utilization of chemicals, pesticides to control pest and diseases.
8. Water requirement of crops very limited and easy to control.

II. DESIGN AND ARCHITECTURE

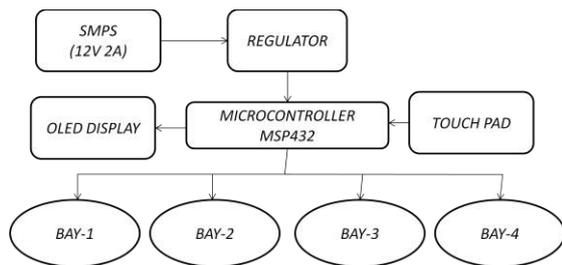


Figure 1 shows the Basic block diagram of the whole system.

The above block diagram explains the basic working of the project. As we can see that the MSP432 processor is the heart of the whole system.

As we can see in the above block diagram, basically we are controlling 4 bays using a single microcontroller which is not possible in the current PLC based system.

A 12V SMPS is used for giving the basic power to the whole circuit. But the voltage is regulated using a simple passive regulator. The output of the regulator is of 5V DC which is given

as an input to the MSP432 microcontroller the OLED display, the touchpad.

Next different bays are connected to the single microcontroller i.e. the MSP432 microcontroller. Each bay has its own set of sensors and the user can set different values for different bays according to the requirements.

For setting all the parameters a resistive touchpad with a graphic LCD will be used. All the current measurement parameters of all the bays will be displayed on the screen simultaneously. The main reason for using resistive type of touch screen is that it is more immune to electromagnetic interference from the environment.

Once the values are entered by the user and the user decides the mode of the system in which it will work i.e. Auto mode or Manual mode. The functioning of the unit will start accordingly.

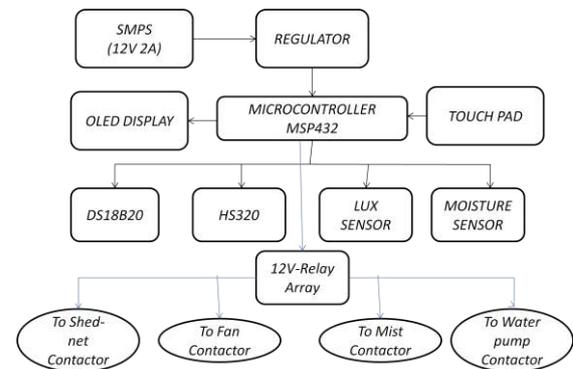


Figure 2 shows the Basic block diagram of each Bay.

As we can see in fig.2 each bay consists of four sensors for reading the physical parameters. The parameters that we are measuring are Temperature, Humidity, Light intensity, Moisture of the soil.

For measuring the temperature we are using a digital sensor DS18B20 which has a resolution of measuring the temperature of up to 0.1°C. The main reason behind using a digital sensor is that they are more immune to noise. As the Bay's

would be away from the main controller, noise gets into the wire and the impedance of the wire also plays a big role in analog sensors. But this is not the case with the digital sensors. Digital sensors can be used up to 100 feet's with a small pull-up resistance. This range can be increased by simply increasing the pull-up resistance values.

Next for measuring the humidity we would be using the analog sensor HS320. To reduce the cost of the system and make the system cheaper so that it can be sold in market like India where the farmers are very poor and can't afford costly greenhouse controlling system, we have used analog sensor. A good analog humidity sensor is approximately 5 times cheaper than a good digital humidity sensor, and due to this the cost of the system decreases drastically.

Both the Lux and Moisture sensors are analog sensors and would be used with the analog pin of the controller. Again the main reason of using analog sensor is to reduce the cost of the system.

Relays are being used to drive the 3-phase contactors which are controlling the 3-phase motors and fans.

The USB flash drive is used for storing the real time data for future references. This system can further be synchronized with network so that remote access to the system is possible.

This system would be having a manual button so that if the system gets failed then also the user can manually access the relays.

III. MSP432

MSP432 is a ARM 32-Bit Cortex-M4F CPU and can operate at frequency up to 48MHz. It has a 256KB of flash main memory which supports simultaneous read and execute during program or erase. This means that there will be no need to turn off the system when OTA (over the air) up gradation of the firmware is done.

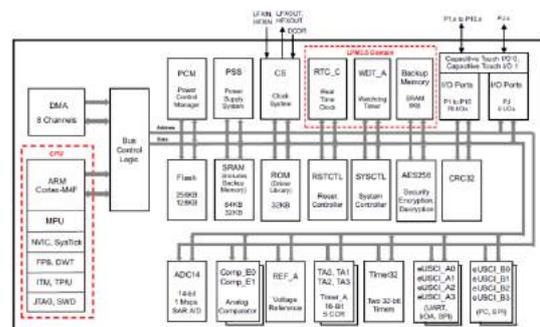
It has a 16KB of Flash information memory. It also has 64KB of SRAM and 32KB of ROM with Driver libraries.

It can work on a wide supply voltage range of 1.62V to 3.7V. The active power consumption is very low i.e. 90µA/MHz.

The stand-by power consumption is only 430nA. This makes it highly suitable for battery operated systems and in the systems which are at remote location and frequent power cuts happens.

Has a UART with automatic Baud-Rate detection. This makes it suitable for the systems in which many sensors are used and also the system in which master slave communication will take place.

It also has a 14-bit ADC which make is suitable for handling ultra high precision analog sensors. It also supports port mapping feature due to which one can reduce the PCB size and indirectly the cost of the system.



- [2] Sushama Arjun Kolhe, S. A. Annadate “Implementation of Green House Automation using ARM7 Controller” in IJCA 2012
- [3] Y.R.Dhumal, J.S.Chitode “Green House Automation using Zigbee and Smart Phone” in IJARCSSE 2013.
- [4] Datasheet of MSP432, LPC2418, DS18B20, HS220.
- [5] Yang Jiaqiang*, Jin Yulong, Gao Jian “An Intelligent Greenhouse Control System” in TELKOMNIKA 2013.



Design of Mobile ad-hoc network for different Mobilities

Akshay P. Kirmirwar
Student
Electronics & Commu.
Engineering,
Abha patil-Gaikwad college of
Engineering and Technology
Wardha road Nagpur, India
apkirmirwar@gmail.com

Sagar Ghormade
Guide; Assistant Professor
Electronics and Communication
Engineering
Abha Gaikwad Patil College of
Engineering, Nagpur, India
hod.ece@agpce.com

Sagar Pradhan
M.Tech Coordinator
Electronics and Communication
Engineering
Abha Gaikwad Patil College of
Engineering, Nagpur, India
sp.ece@agpce.com

Abstract- This paper presents mobile ad-hoc networks (MANETs) which are based on a fundamental aspect, which is the collaborative parameter. This parameter may compromise the networks. In MANET based on SISO (Single-Input Single-Output) technology, the interferences at the monitor no deco promise the observation and the accuracy of the cooperation report. That is why, we concentrates on the MIMO (Multi-Input and Multi-Output) technology to overcome these drawbacks and to significantly improve the monitoring process. Adopting Multiple Input-Multiple-Output (MIMO) technology, we devise two many-to-one cooperative plans under converge-cast for both static and mobile ad hoc networks (MANETs), respectively. We call them Convergimo Schemes. In fixed networks, our Convergimo scheme highly utilizes hierarchical cooperation MIMO transmission.

Keywords:- MANET, Throughput, Delay, MIMO, Packet Size, AODV, NS2(Network Simulator), TCL.

I. INTRODUCTION

As we know that significant progress has been made in securing MANETs via the development of secure routing protocols. The network topology in an ad hoc network is highly dynamic due to the movement of the nodes, hence mobility is a major limitations in designing routing protocols for them. Apart from mobility, the other major restriction s are bandwidth and resource availability. Basically Mobile Ad-hoc network (MANET) is a collection of independent mobile nodes that can liaise with each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others require the aid of intermediate

nodes to route their packets in multi-hop fashion. MANETs are used in tragedy recovery, rescue operations, military communication and many other applications. In multi-hop wireless ad hoc networks, designing energy logical routing protocols [1] is critical since nodes have very limited energy, computing power and communication abilities. Routing is an important aspect in mobile ad hoc Network. Routing protocol determines the path to be followed by data packets from a source node to a destination node. Mobile ad-hoc networks are wireless networks that offers multi- hop connectivity between self configuring & self organizing mobile hosts. Nodes are serves as routers &may arbitrarily. Self-configuring network of mobile routers (and related hosts) connected by wireless links. While MANETs are self contained, they can also be trussed to an IP-based global or local network – Hybrid MANETs. A set of nodes can be easily compromised such that detecting the malicious behavior is tedious.

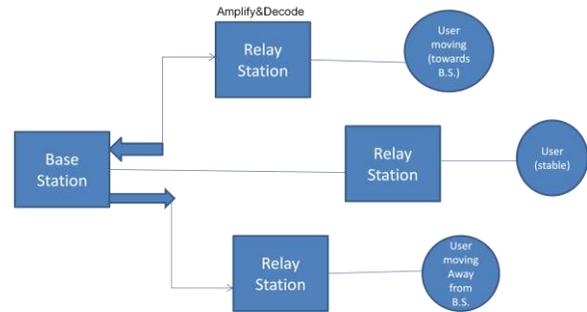
Such nodes inundation other nodes with routing traffic; advertise non –existent links, drop packets, changes the contents of packets and thus inflicting failure in network. One of the most well liked routing protocol, Ad-hoc on demand distance vector (AODV) is used in MANET. It is a source aligned routing protocol where routes are uncovered only on demand. However, AODV is unsafe to packet dropping attack. A malicious node stealthily drops some or all data packets or control packets without forwarding them to destination. A group of nodes can drop packets in collaboration in network at such a rate that message communication in network may get degraded or even disrupted. Due to lack of physical protection and

reliable mechanisms, packet dropping attack posts a serious threat to routing in MANETs.

MANETs are used in disaster recovery, rescue operations, military transmission and many other applications. In multi-hop wireless ad hoc networks, designing energy-efficient routing protocols [1] is critical since nodes have very limited energy, computing power and communication capabilities. Routing is an important aspect in mobile ad hoc Network. Routing protocol determines the path to be followed by information packets from a source node to a destination node. Concentrating on throughput and delay performance in this paper, we present a new type of many-to-one cooperative schemes with MIMO in both static and mobile networks, from the view of converge-cast. We call them Convergimo schemes. For Convergimo scheme in a static network, the whole network is split into clusters with equal number of nodes in each of them. Communications between clusters are coordinated through distributed MIMO transmissions amalgamate with multihop strategy while within a cluster, it is operated through joint dispatch of multiple nodes to others. Under mobile ad hoc networks (MANETs) where hierarchical cooperation cannot be accepted due to the mobility of nodes, we devise another Convergimo scheme where the network is still split into equal cells. In each time aperture, multiple nodes that possess information for the same destination are allowed for joint dispatch to other nodes within the cell. Other nodes will receive a combination of the information from these transmitters due to the outcome of MIMO through fading channels. This procedure continues, with the number of nodes that hold such mixed data increases, until all the destinations receive sufficient mixed information that can be decipher with high probability. Our main benefactions can be summarized

For our Convergimo scheme under MANETs, with optimal network division, the per-node throughput is \uparrow with the corresponding delay reduced to \downarrow . Our results well combine, and generalize some previous works since all of them can be easily implemented to other traffic modes. Especially, our plan in MANETs breaks the vacancy of such MIMO plan design remaining in mobile networks before.

II DESIGN AND IMPLEMENTATION



Comparing three scenarios:-

- User moving towards base station.
- user is stable.
- user moving away from base station.

Parameters of comparison:-

- Throughput.
- Packet delivery.
- Packet loss.
- Maximum delay

III. MOTIVATION

As we know that ,Wi-Fi and Wi-Max are both wireless technologies but Wi-Fi can only be operated in short ranges (max 250m) and Wi-Max could be operated in long ranges (around 30 kilo meters). Wi-Max has fixed and mobile version which could be used with higher bandwidth (around 40 mbps). And it uses connection oriented MAC protocol. Radio spectrum will be used 10 to 66 GHz for line of sight (LOS) and 2 to 11GHz for non line of sight (Non LOS). Adaptive modulation and coding that will be used. Thus in this project we are using Wi-Max instead of Wi-Fi to achive following parameter requirements:-

- Increased Packet delivery.
- Increased Throughput.
- Decreased Packet loss.
- Decreased Delay.

and also to increase network efficiency.

IV. PROBLEMS

First of all, the resources in MANETs are limited in terms of energy, bandwidth, etc. Then, the nodes try to increase their lifespan duration by reducing their energy consumption and the cost of the transmission operation is important in expressions of energy.

Secondly, when the nodes route and forward the packets of other nodes, this increases the delay of their own carton transmission and reduces their own average throughput. Thus, this operation may be recognized by nodes as punishment and not as global network interest. In order to deal with this problem, many researchers focus on the observeing mechanisms in order to detect the selfish nodes and to punish them.

However, all the proposed mechanisms are established on the classical SISO (Single-Input Single-Output) technology to monitor the communication channel and to diagnose the non forwarding nodes (selfish behavior). The most cited mechanism is Watchdog. Many proposed solutions are based on it, but it bears from the high false alarm rate [1]. The main problem of these mechanisms is related to the intervention at the monitor node which makes the results of its observations wrong. That is why we propose a new MAC agreement called MIMODog-SPACE-MAC based on MIMO (Multi-Input Multi-Output) technology, particularly a SPACE-MAC protocol to significantly cancel the potential interferences at the monitor nodes and to enhance the accuracy of the monitoring results. Our benefactions are summarized as follows:-

- The monitoring problem persists in MANETs, even when we employ MIMO technology,
- A new MIMO MAC protocol is proposed to cancel the interferences at the monitor nodes without influencing the total network ability.
- A different impact on the monitoring process with: DCF MAC, SPACE-MAC and MIMODog-SPACE-MAC is dispensed and discussed. MIMODog-SPACE-MAC significantly enhances the monitoring process without affecting the network ability.
- MIMODog network modelling is done and lower and upper bounds of the number of monitor nodes are investigated.

V. PROPOSED WORK

Mobile next generation wireless targeted as the demand emerging application. The key strategies will be used for data rate improvement that are MIMO and Adaptive modulation & coding. Mobile communication Simulation we will do. Coverage range will be up to 10 kilo-meter. WiMax – Large coverage area, high speed, low cost per bit, high mobility. Routing protocols-AODV. Use of MIMO in MANET. Implementing network for different mobility patterns for mobile user. Tool-Ns2.31 with wimax module. To improve the QoS -Throughput, Delay, Packet delivery ratio, Packet loss ratio & to

design MANET with Wi-Max. To design MIMO technique for sending and receiving data by using multiple channel. To AWK file of Throughput, Packet delivery, Packet loss. Also to compare different scenarios and to improve quality of service network. execution of MIMO (multiple input multiple output) for increasing network efficiency. Comparing all three scenario separately and calculate results based on various parameters.

VI. CONCLUSION

After complication of my project I will conclude that, this project having good 1. Throughput, 2. High packet delivery rate, 3. Low power loss.

VII. REFERENCES

- [1] S.Mangai & A.Tamilarasi#2Proceedings of the International Conference on Communication and Computational Intelligence – 2010, Kongu Engineering College, Perundurai, Erode, T.N.,India.27 – 29 December,2010.pp.404-409.
- [2] S. Mittal, P. Kaur, Performance Comparison of AODV,DSR and ZRP Routing Protocols in MANET's, 2009 International Conference on Advances in Computing, Control and Telecommunication Technologies (act 2009), 28-29 December 2009, Trivandrum, Kerala,India, pp. 165-168.
- [3] E. M. Royer, C. E. Perkins, An Implementation Study of AODV Routing Protocol, IEEE Wireless Communications and Networking Conference, 23-28 September 2000, Chicago, pp. 1003-1008. Protocols for Ad Hoc Networks, IEEE Personal Communications Magazine Special Issue on Ad hoc Networking, February 2001, pp: 16-28.
- [4] Weihong Hu, Homayoun Yousefi'zadeh, *Senior Member, IEEE*, and Xiaolong Li, *Member, IEEE* IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 10, NO. 11, NOVEMBER 2011.
- [5] Hamid R. Sadjadpour Depart. of Electrical Engineering Univ. of California (UCSC) Santa Cruz, CA 95064, USA "On the Link Ergodic Capacity of MIMO MANETs using Cooperation" 1424407850/06/\$20.00.
- [6] Luoyi Fu, Student Member, IEEE, Yi Qin, Student Member, IEEE, Xinbing Wang, Member, IEEE, and Xue Liu, Member, IEEE "Throughput and Delay Analysis for Convergecast with MIMO in

Wireless Networks” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 4, APRIL 2012.

[7] Abderrezak Rachedi and Hakim Badis Université Paris-Est Marne-la-Vallée (UPEMLV) Gaspard Monge Computer Science Laboratory (UMR 8049 LIGM) Champs sur Marne, France “MIMODog: How to solve the problem of Selfish Misbehavior Detection Mechanism in MANETs Using MIMO Technology” 978-1-4577-1379-8/12/\$26.00 ©2012 IEEE.

[8] Vladanka Acimovic-Raspopovic¹, Mirjana Stojanovic², Jelena Teodorovic³ University of Belgrade^(1,2), Institute for Educational Research (3) “The Undergraduate Training on Simulating IP Networks Using Network Simulator NS2, ISTET’09.

[9] Zahian Ismail Kuliyyah of Information Science and Technology Kolej Universiti Insaniah Alor Setar, Malaysia, Rosilah Hassan School of Information Science and Technology Universiti Kebangsaan Malaysia 43600 UKM Bangi, Selangor, Malaysia “Effects of Packet Size on AODV Routing Protocol Implementation in Homogeneous and Heterogeneous MANET” 2011 Third International Conference on Computational Intelligence, Modelling & Simulation.



Efficient Edge detection of Shadow Using Intrinsic Images

Sarita Chouhan

*ME Scholar, Department of Electronics &
Telecommunication Engineering,
Chhatrapati Shivaji Institute of Technology Durg, India.
Email: saritachouhan29@gmail.com*

Abhishek Misal

*Sr. Assistant Professor in Department of Electronics &
Telecommunication Engineering,
Chhatrapati Shivaji Institute of Technology Durg, India.
Email: abhishekmisal@csitdurg*

Abstract— Removal of shadow from any of the single image is a very difficult task. To produce a high quality of shadow free image which is indistinguishable from a true shadow free scene is even more difficult. Shadow in any image are affected by many things like lighting conditions, unwanted behavior of any shadowed surfaces and occluding object etc. Shadows regions may also in a post acquisition in image processing, transforming, e.g. contrast enhancement. An intrinsic image is the same purpose to be removing the shadow through edge detection method. In this proposed work intrinsic image is used for edge detection of image. For shadow detection and removal edge is very important. It differentiates the shadow affected area and other portion of image. We first derive a 2-D intrinsic image from a single RGB camera image based solely on colors, particularly chromaticity. We next present a method to recover a 3-D intrinsic image based on bilateral filtering and the 2-D intrinsic image. The luminance contrasting regions with similar surface reflectance due to geometry and illumination variances is effectively reduced in the derived 3-D intrinsic image, while the contrast in regions with different surface reflectance is preserved.

Keywords— *chromaticity, intrinsic image.*

I. INTRODUCTION

Shadows are created wherever an object obscures the light source. A shadow caused by the interaction of light with object claims a fraction of the image surface. Deriving intrinsic images from image sequences is based on image sequences. Hamiltonian path based shadow removal are used to find shadow edges of invariant and non-invariant images. Shadow detection and reconstruction in High-Resolution Satellite Images via morphological Filtering based on bimodal histogram used to determine shadow and non-shadow pixels. An approach to detect and remove shadows from a single still image is implemented till now. Shadow detection and removal using various methods has been used but are implemented only for single shadow removal. Shadow detection and removal using various methods has been used but a Derivation of 2-D

intrinsic image from a single RGB camera image based solely on colors, particularly chromaticity is used.

The texture of the surface that was under the shadow is preserved to a good extent and no harsh transition between the shadowed parts and non-shadowed parts. In digital photography, shadows are typically considered as artifacts in the image that need to be removed, whether for enhancing certain parts of the image or simply for esthetic reasons. The problem of generating an intrinsic image that is invariant to illuminations is very important but challenging. The problem of generating an intrinsic image that is invariant to illuminations is very important but challenging, and the recent methods can be divided into the following three categories.

1) Methods that use multiple images. Weiss [1] derived an intrinsic reflectance image of a scene given a sequence of images of the scene under a range of illumination conditions. Weiss's method implicitly assumes that the scene is composed of Lambertian surfaces. If a surface exhibits Lambertian reflectance, light falling on it is scattered such that the apparent brightness of the surface to an observer is the same regardless of the observer's angle of view. These methods produce successful results. However, multiple images acquired under the required conditions are not always available in practice, e.g., for dynamic scenes and moving cameras.

2) Methods that use a single image but require human interaction. Levin and Weiss [4] proposed a user-assisted method to perform reflection separation and one of its applications is shadow removal. Shadow formation problem as one of energy minimization guided by user-supplied hints in the form of a quad-map which can be specified easily by the user. These methods produce good results with careful user-assistance, but are not fully automatic.

3) Methods that use a single image without human interaction. Learning-based approach to separate reflectance edges and illumination edges in a derivative image. Although this

method successfully separates reflectance and shading for a given illumination direction used for training, it is not designed for arbitrary lighting directions. The transformation of RGB representation to a 1-D grayscale representation reduced the discrimination between every two surfaces in the image. Finlayson and Drew [10] extended this method to derive a 2-D intrinsic image using a four band camera, and theoretically proved that 3-D invariant images can be recovered with six-band cameras. in the image. Finlayson and Drew [10] extended this method to derive a 2-D intrinsic image using a four band camera, and theoretically proved that 3-D invariant images can be recovered with six-band cameras. The problem with this approach is that four-band and six band cameras are rarely used. The image can be then decomposed into two components using this correlation, and one of them is illuminant-invariant. The shadow removal problem is then equal to removing the other component which is related to the illumination temperature.

II. REMOVING ILLUMINANT DEPENDENCES

In this section, we give a detailed description of the derived 2-D and 3-D intrinsic images in which the illuminant dependences are removed. We start with a brief review of the adopted illumination and reflection model, then present the method for deriving the 2-D and 3-D intrinsic images, and finally consider the issue of camera calibration.

III. RESTORING LUMINANCE

The luminance contrast in regions with similar surface reflectance due to geometry and illumination variances is effectively reduced in the derived 3-D intrinsic image while the contrast in regions with different surface reflectance is preserved. However, the estimated 3-D intrinsic image may contain incorrect luminance values. In this section, we present a method which abstracts the luminance of the original image and transfers it to the intrinsic image such that a shadow-free image with correct luminance can be obtained.

IV. RELATED WORK

The template is this given project required the data at the base is of the multiple shadows from various website, real world images and the floured light images. Shadow removal is typically the part of which performed in two stages: (1) it is the detection stage in which through the shadows regions are detected and, mainly determining the shadows boundaries, and (2) it is the reconstruction stage in which the shadows is sufficiently removed and a shadow-free images is reproduced. (Eli Arbel and Hagit Hel-Or, 2011) In this section, we suggests a novel reconstruction stage for the shadow removal, i.e., removing the shadows to the image once they have been detected and. Any shadows detection algorithm will be used, but since our method is not in confined to images with the certain stage the part illumination conditions such as the outdoor scene images, one should use a shadow detection algorithm that should be the best method suits the illuminating conditions in a given images.

V. REMOVING SHADOW FROM INTRINSIC IMAGE USING EDGE DETECTION

This method works on only for a single image, in which invariant to the images are obtaining by finding an image that should be orthogonal and the direction of intensity and also the color change. Shadow detection using color and edge information classify a texture based approach for shadow detection. Deriving intrinsic images from images sequences is based on image sequences. Hamiltonian path based shadow removal are used to find shadow edges of invariant and non-invariant images Shadow detection and removal and further reconstruction in high resolution Satellite Images via morphological Filtering based on bi modal histogram used to determine shadow and non-shadow pixels (Huifang Li, 2014).This section shadow are detected through their edges and using that particular edges shadow free.

VI. INVARIANT IMAGES

This is showing that any original images which is captured through the camera this our original image and after the shadows detected the original images are rotated from the different different angle like 45,60,etc. But in this work all images are rotated into the 45degree of an angle and converted them to the invariant images and after this all the work both two images original and as well as invariant images must be cross correlation using them.

VII. MOTIVATION

Since the last decade, the study of image plays a very important role in security and sports event. We can see great progresses both in theory and in practice. However, the research interest in this field is still growing. The main motivations of this survey. With these goals in mind, we achieved the following research results: A study of the multiple shadow removal method. The image enhancement problem can also be addressed in the FHDl by utilizing the inter-scale dependencies of Histogram. By adapting to different edge shapes, we successfully estimate the high contrast images. Shadow detection and removal methods have been studied extensively in the literature. However, the method is basically correlations between the shadow effected area and the other background images.

VII. PROBLEM IDENTIFICATION

A. Multiple shadow color images

The aim of image is often to improve the visual quality, typically for the human observer and this report some concepts from this field will arise time and time again and we need to familiarize ourselves with them.

A.1 Basics of Digital Images

In this report we have the basic form of: digital image I (sometimes denoted J) is a two dimensional matrix of pixels, with some height n and some width m . We also adopt the standard way of thinking of I as a function M

→ V, with $M = \{(i,j):i \leq m, j \leq n\}$ and V being a set of pixel values, which means that by $I(i, j)$. We will denote the value of the pixel in row i and column j of image I. Throughout this report we will only deal with grey scale images which means that all pixels have a single (but variable) value: the pixel's intensity or grey level. The pixels can take on intensity values within some preened range V, e.g. $V = [0,255]$ in an 8-bit representation, where the smallest value in the range corresponds to black and the largest to white. Extending this notion to images, we consider a image $I = \{J_t\}$ to be a collection of images,. Correspondingly we let $I(i, j; t)$ point to the pixel in row i and column j.

A.2 Shadow in Images

Use the shadows are occurs when an object are partially or totally occludes direct light from a source is illumination. In general, shadows must be divided into two major classes: self shadows and cast shadows, a self shadow occurs in the portion of an object which is must not illuminated by direct light. A cast shadows are the area projected by the object in the direction of directed to the light. Figure 1 shows some examples of different kinds of shadows to an image. Figure.1 (a) (James J. Simpson and James R. Stitt, 1998) shows scene image with both cast and self shadows; Figure.1 (b) gives an example of cast shadow of two photographers on a grass field; (Yang Wang, 2009) Figure.1 (c) shows an example of self shadow. Cast shadows can be further classified into umbra and penumbra region, which is a result of multi-lighting and self shadows also have many Sub-regions such as shading and inter relation. Usually, the self shadows are vague shadows and do not have clear boundaries (James J. Simpson and James R. Stitt, 1998). On the other hand, cast shadows are hard shadows and always have a violent contrast to background. Because of these different properties, algorithms to handle these two kinds of shadows are different. For instance, algorithms to tack le shadows cast by buildings and vehicles in traffic systems could not deal with the attached shadows on a human face. Accordingly, this survey attempts to classify various shadow removal algorithms by the different kind of shadows they focus on and in fact, by the different assumptions they made to the shadows

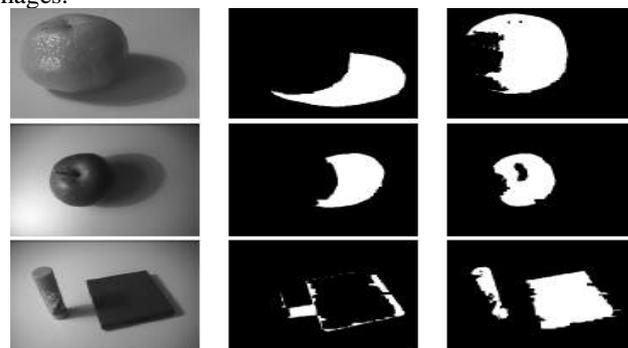


Figure A.1 Different Kinds of Shadows In Image: (A) An Overview of Different Kinds of Shadows In One Image, (B)

Cast Shadow In A Natural Scene Image,(C) An Example of Attached Shadow

A.3 Shadow Detection

In some applications, especially traffic analysis and surveillance system (YingLi Tian, 2011), the existence of shadows may cause serious problems while segmenting and tracking objects: shadows can cause object merging. For this reason, shadow detection is applied to locate the shadow regions and distinguish shadows from foreground objects. In some cases, shadow detection is also exploited to infer geometric properties of the objects causing the shadow (“shape from shadow” approaches). In spite of the different purposes, invariably the algorithms are the same and can extend to any of these applications. A. Prati et al (Hongya Zhang, 2014) conducted a survey on detecting moving shadows; algorithms dealing with shadows are classified in a two-layer taxonomy by the authors and four representative algorithms are described in detail. The first layer classification considers whether the decision process introduces and exploits uncertainty. Deterministic approaches use an on/off decision process, whereas statistical approaches use probabilistic functions to describe the class membership. As the parameter selection is a crucial problem for statistical methods, the authors further divided statistical methods into parametric and nonparametric method .For deterministic approaches, algorithms are classified by whether or not the decision can be supported by model-based knowledge. The authors reviewed four representative methods for their categories of his taxonomy and argued that Deterministic Model-based methods (Qingxiong Yang, 2012) rely so much on models of the scene that they inevitably become too complex and time-consuming T. Horprasert et all’s method (F. P. S. Luus, 2013) is an example of the statistical nonparametric approach and the authors denote it with symbol SNP. This approach exploits color information and uses a trained classify to distinguish between object and shadows. I. Mikic et al (Huifang Li, 2014) proposed a statistical parametric approach (SP) and utilized both spatial and local features, which improved the detection performance by imposing spatial constraints’. Salvador et al proposed an approach to detect and classify shadows for still images.



FigureA.2. Shadow detection and classification results of E. Salvador et al.(courtesy (Eli Arbel and Hagit Hel-Or, 2011))

(a) original image, (b) cast shadow map, (c) self shadow map.

IX. METHODOLOGY

According to literature serve as we find out the scope for the proposed work and as we set goal and mentioned in problem identification chapter so further we proceed forward to achieve that goal and taking Force Histogram Decomposition and Pair Region which is used for Shadow removal and find the best output which gives minimum difference, maximum mean and standard deviation

B. Shadow Detection

the process of the shadow detection could be a primary step for compensation of the shadows are followed by an eventual step of the image analysis task, such as object are recognition or it should be a fundamental steps where the detection results are directly using by 3D shape estimation and there similar tasks. In any cases, shadows detection is the initial process for the final image analysis task. Hence, the performance of the final task is a highly dependent on the shadow detection performance

B.1 Shadow Features

In this section, shadow features are analyzed. Changes in shadow are analyzed on image samples, which are colored as Yellow, Black, Blue, Green, Red and White. The sample images are given in figure 8. An example setup of these sample pictures is given in figure 9. In these setups a uniform colored paper is laid on the surface, an obstructing object is set beside to the side of the sun light and a shadowed part is obtained. Then by using a photo editor program the sample images are cropped. No further image processing or filtering is applied to preserve original color on the sample image. The shadows appear in areas where the light from a source does not reach directly. An object can also cast a shadow on itself. The Force Histogram Decomposition (FHDI) decomposes the image along its intensity level-sets into N layers encodes two types of information First-order: shape contour information. (F. P. S. Luus, 2013) Second-order: relative spatial relations, histogram of forces between two different layers. Histograms of forces computed with 180 directions. Constant force for shape information. Gravitational force for spatial organization.



Figure B.1– Sample images that are used for shadow feature analyses

B.2 Overview of Shadow Detection Methods

Shadow detection methods are to be classified according to the input data of the given image. The work in the literature survey should be divided into mainly two classes; one class is deals with moving shadow detection and the other class deals with static formation of the images shadow detection

B.3 Moving Shadow Detection

Shadow detection in dynamic scenes are referred to moving shadow detection (Yang Wang, 2009) and usually their detection method approach and their steps are different from non-dynamic scenes (still images). Also the purpose of the shadow detection is in dynamic scenes should be change detection method, scene matching and surveillance so that it is different them and also the purpose for shadow detection is in dynamic scenes could be change. Scene matching or surveillance that it is different them and There are several studies on moving shadow detection.

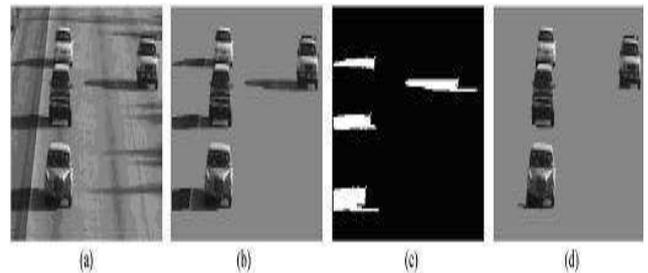


Figure B.2 –Moving shadow detection and foreground detection result in

XI. CONCLUSION

We have introduced an automatic shadow removal method in this paper. Two illuminant-invariant image representations were first derived in this paper: 2-D intrinsic image computed based solely on colors, and 3-D intrinsic image estimated based on the 2-D intrinsic image and joint bilateral filtering. The details of the 3-D intrinsic image were then transferred to the original image to reduce the luminance contrast in regions with similar surface reflectance due to geometry and illumination variances. Unlike most previous methods, the presented technique does not require shadow detection.

XII. REFERENCES

- [1] James J. Simpson and James R. Stitt, , A Procedure for the Detection and Removal of Cloud Shadow from AVHRR Data over Land IEEE transactions on geoscience and remote sensing, vol. 36, no. 3, may 1998.
- [2] James J. Simpson, Zhonghai Jin, and James R. Stitt ,Cloud Shadow Detection Under Arbitrary Viewing and Illumination Conditions IEEE transactions on geoscience and remote sensing, vol. 38, no. 2, march 2000.
- [3] Christopher Jaynes, Member, Stephen Webb, and R. Matt Steele Camera-Based Detection and Removal of Shadows from Interactive

- Multiprojector Displays IEEE transactions on visualization and computer graphics, vol. 10, no. 3, may/june 2004.
- [4] Xiaodong Gu, Daoheng Yu, *Senior* and Liming Zhang, Image Shadow Removal Using Pulse Coupled Neural Network IEEE transactions on neural networks, vol. 16, no. 3, may 2005.
- [5] Yang Wang, Real-Time Moving Vehicle Detection With Cast Shadow Removal in Video Based on Conditional Random Field IEEE transactions on circuits and systems for video technology vol. 19, no. 3, march 2009.
- [6] Eli Arbel and Hagit Hel-Or, Shadow Removal Using Intensity Surfaces and Texture Anchor Points IEEE transactions on pattern analysis and machine intelligence, vol. 33, no. 6, June 2011.
- [7] YingLi Tian, Rogerio Schmidt Feris, Haowei Liu, Arun Hampapur, and Ming-Ting Sun, Robust Detection of Abandoned and Removed Objects in Complex Surveillance Videos IEEE transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 41, no. 5, september 2011.
- [8] Sang Jae Nam, and Nasser Kehtarnavaz, Flash Shadow Detection and Removal in Stereo Photography S. J. Nam, and N. Kehtarnavaz:
- [9] Qingxiong Yang, Kar-Han Tan, Narendra Ahuja., Shadow Detection and Removal in Stereo Photography. Shadow Removal Using Bilateral Filtering IEEE transactions on image processing, vol. 21, no. 10, october 2012.
- [10] F. P. S. Luus, F. van den Bergh, and B. T. J. Maharaj The Effects of Segmentation-Based Shadow Removal on Across-Date Settlement Type Classification of Panchromatic QuickBird Images IEEE journal of selected topics in applied earth observations and remote sensing, vol. 6, no. 3, june 2013.
- [11] Huifang Li, Liangpei Zhang and Huanfeng Shen, An Adaptive Nonlocal Regularized Shadow Removal Method for Aerial Remote Sensing Images IEEE transactions on geoscience and remote sensing, vol. 52, no. 1, january 2014.
- [12] Hongya Zhang, Kaimin Sun, and Wenzhuo Li Object-Oriented Shadow Detection and Removal From Urban High-Resolution Remote Sensing Images IEEE transactions on geoscience and remote sensing, vol. 52, no. 11, november 2014

*Stress Level Detector Using Microcontroller**

Amruta Pathe.
Department of VLSI
Jhulelal Institute Of Technology,
Nagpur, India.
amruta.pathey@gmail.com and Contact No-.9561156133.

2nd Affiliation (Author)
line 1 (of Affiliation): dept. name of organization
line

Abstract—Now-a-days, Stress is one of the major problems. There is hardly a week passes without hearing and reading about stress and its hazardous effects on body or health we can say. In general, overall response of the body to any demand is called Stress. In this work, we present a solution for the stress experience of people, by considering skin temperature of person and its heart rate also. Main motto to alert people suffering from stress just by sensing our body or skin temperature. This will probably helps person to live healthy life, one should keep himself away from the hazardous mental and physical diseases.

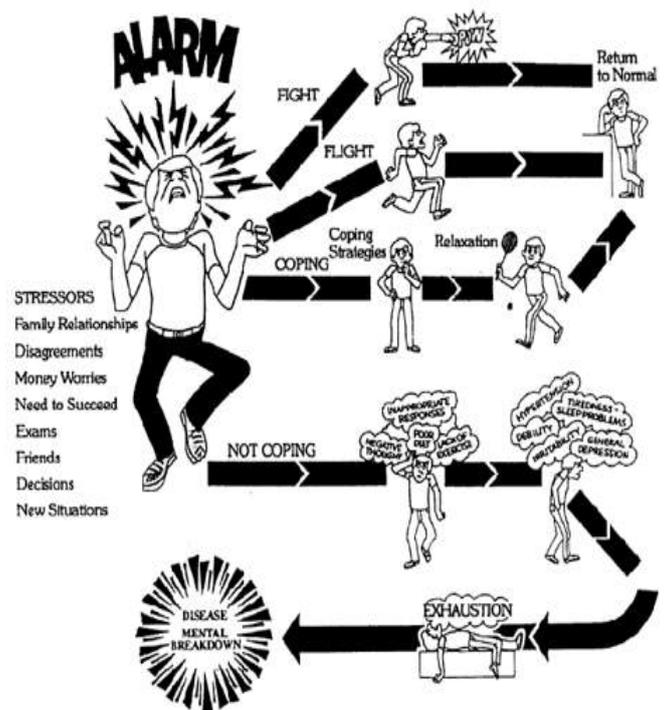
Keywords—stress, heart rate, skin temperature, stress detection.

I. INTRODUCTION (Heading 1)

Work is such a state of life through which everyone should get happiness pride and health. But because of increasing development in every field competition increases rapidly. Every person is running behind the name, fame and money; so interest related to work is no more. Work is now equal to the mass production. Therefore, Stress is directly proportional to work of any kind. It can be industrial, official, or can be domestic workload. Work at offices, that too at corporate offices affects people of different professions, age. This is all because the globalization in economy, new information and communication, increasing mental workload.

Sometimes stress is caused by the heavy workload and mental fatigue and sometimes it is caused if very uncertain situation happens with us or in front of us. If someone gave us a task of which we have a phobia then it also leads to stress. i.e. person may suffer from stress. If a particular person is always dominated by the others or if a person posses negative thoughts throughout their mind then it leads to increase mental stress of that particular person.

Lets have a diagrammatic view of a person if he fails to handle or manage stress.



Quick view of a stressor

A. Causes of stress

This stress results in increased heart rate, respiratory rate, sweating, muscle tightening, skin diseases. All the above changes are easily dignosable. i.e. one can easily recognise these changes just by observing the stressor. But some changes are tere which are not easily dignosable. For eg- increased blood pressure, diabetes, metabolism, circulation fats, hormonal imabalance etc.

B. Measurement of stress

Here are some quick ways to measure stress-

To check muscle tension:-

Usually when person is under stress tightening of muscles takes place. Tightening of muscles of jaws, forehead is very usual and observable when person is under stress.

To check the body temperature:-

Put your hands on the side of the neck and if your hand temperature is noticeably cooler than neck then particular person is under stress.

To check sweating:-

When person is under stress; person sweats a lot. This is because of secretion of stress hormones. Sweating is one of the simple indicator to identify stressor.

To check pulse rate:-

Pulse rate usually increases and if it is greater than 75 bpm i.e. 75 beats per minute then that particular person is a stressor one.

One of the simple identifications we are considering in this project is-

Without taking any help of external equipment just by sensing our skin temperature.

If skin is cooler (wet) – under stress

If skin is warmer (dry) – no stress

C. Reason behind the cooling of hand temperature-

When person is under stress then body functioning is somewhat gets disturbed. Tightening of muscles takes place. And generally temperature of hands and feet gets cooler.

This is because the muscles at the top of the fingers of hands and feet gets contract and therefore it obstructs the blood supply to flow to that parts of the body. (specially hands and feet). Since there is very fewer amount of blood supply over those parts so temperature undoubtedly becomes cooler and cooler. This is the main reason behind the cooling of body temperature.

II. SOURCES OF STRESS

There are three categories of Stress-

1. Situational Stress
2. Body Stress
3. Mind Stress

Situational Stress-

The stress which is entirely depend upon the situations in our day to day life is called the situational stress. Situational stress is nothing but your environment where you lives, works etc.

If environment at a workplace is quiet unhealthy, busy then one must have to run back and forth, deal with the people of different professions of different age groups at different situations, handle their work according to their availability then one must experience a high level of situational stress.

Body Stress-

The stress which is caused by abuse and neglectance is a body stress. Body stress is a physical stress.

Abuse generally includes consuming too much drugs, alcohol, too much exercise.

Neglectance generally includes the ignorance to body requirement with respect to proper sleep, nutrition etc.

All these leads to increase the body stress.

Mind Stress-

The stress which is generally caused by negatively perceiving life events are called mind stress. In this case, person usually think in a negative direction i.e. he always conclude the negative side of the situation and reacts accordingly. A person, under bad conditions, holds himself responsible for the cause. So such type of behavior often found under this source.

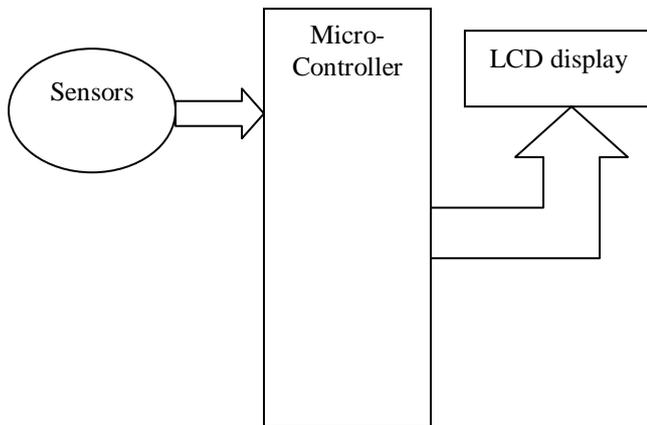
III. METHODOLOGY

By considering the hazardous effects of stress; one should not reach to the critical condition. So to avoid stress this project will make people aware of their state of mind just by sensing skin temperature. Person will get his stress level in terms of figure. So he could take the preventive action from becoming a stressor.

So the basic methodology behind this is given below-

It basically contains three main blocks-

- 1 Sensor
- 2 Micro-controller
- 3 LCD display



So simple methodology behind this is-

Sensor will sense the skin temperature through the fingers of hands and then its output is sent to the microcontroller. Microcontroller then send the signal to A/D converter and finally we get the output on LCD display in figures.

This is how person can measure his stress level. Using this device we can very well tell the person's stress level depending upon the body or skin temperature.

Standard and general format to identify stress condition according to the Dr.s is given below-

Below 26 degree celcius => Highly tense

Between 26-29 degree celcius => Slightly tense

Between 29-32 degree celcius => Mildly calm

Between 32-35 degree celcius => Quietly calm

Above 35 degree celcius => Deeply relaxed

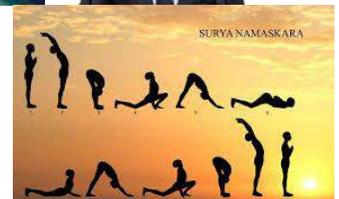
So by considering these level we can tell the person's stress level at any instant and can take action to control stress.

IV. DEALING STRESS

There are certain ways through which person can reduce our stress and maintain a good mental condition and can leave a better life.

- ⇒ Daily exercise and yoga- Exercise like walking, jogging that too in the early morning and yoga (suryanamaskar & various asnas) keeps you fresh throughout a day. It also gives you energy to do lots of activities.
- ⇒ Meditation- Meditation keeps your mind stable and calm. It also gives positivity which keeps you away from mind stress.

- ⇒ Sharing your feelings- This is one of the best methods to keep ourselves away from being a stressor. Because sharing your problems as well as joys with your friends, family members, or with loved one gives a solution on your problems. So we can able to face the critical conditions. It is said that 70% of stress gets reduced just by sharing your problems or feelings with friends and etc.
- ⇒ Listening to songs- Listening to light music or your favorite songs also reduces your stress and makes you fresh.
- ⇒ "Say no" depending on the conditions- If a particular person has lots off workload, responsibilities which are somewhat difficult to handle for himself and during that condition someone is asking to do their work then just say no. If that person fail to say no to the other person then it is very difficult to handle or fulfill both the responsibilities at a time. And finally it results in a poor performance followed by stress.



- ⇒ Avoid alcohol, smoking, drugs etc- Consumption of alcohol, smoking, drugs increases stress to large extent. It also increases fatigue, drowsiness, irritability. It also leads to vitamin deficiency, kidney problems, heart problems, cancer. It also affects lungs.
- ⇒ Avoid much consumption of sugar, salt- Much consumption of sugar leads to dizziness, hunger, headaches, irritability, diabetes. All these directly or indirectly depend to increase stress level
- ⇒ Much consumption of salt also leads to high blood pressure, abnormal mental activities through which stress can be increased rapidly.

So all these ways are useful to balance or maintain your stress level. We can also say that all these are the remedies to control the stress or come out from the stress.

V. ADVANTAGES OF THE DEVICE

Main objective of the project is to make a stress level detector which gives digital output using microcontroller.

To make people aware of their state of mind and the conscious of how they feel.

- It's a Biomedical device.
- It is a non invasive device.
- It is an economical device
- Device can be easy in handling.
- One can measure at any instant of time.

REFERENCES

- [1] "Microcontoller based fault detector"; technical research paper published in International Journal of Advancement in Research & Technology Volume 1, Issue5, Oct 2012 ISSN 2278-7763.
- [2] Mohnesh Singh, Neelam rup Prakas, "Miniaturisation of wearable sensor for stress monitoring"; International Journal of Innovative in Science Engineering & Technology; Volume4, Issue5, May 2015.
- [3] Jorn Bakker, Mykola Pechenizkiy "Detection of stress pattern using GSR sensors";2011 11th IEEE International conference.
- [4] Lekha G, Mehala Devi, Mohana Ragavi R, Parimala J, Chella ganesha valli S, "Detection of stress and reduction of two wheelers speed using microcontroller"; International Journal of Innovative in Science Engineering & Technology; Volume 13, Issue 38, aug-sept 2014.
- [5] Akane sano, Rosalind W Picard; "Stress recognition using wearable sensors and mobile phones"; 2013 Humaine Association Conference on Affective Computing and Intelligent Interaction.
- [6] Sano, Akane, and Rosalind W. Picard. "Understanding Ambulatory and Wearable Data for Health and Wellness." Proceedings of the 2014 AAAI Spring Symposium Series (March 2014).
- [7] J. Hernandez; R. R. Morris; R. W. Picard, "Call center stress recognition Interaction, vol. 6974, pp. 125–134, 2011.
- [8] C. Setz, B. Arnrich, J. Schumm, R. La Marca, G. Tröster, and U. Ehlert, "Discriminating stress from cognitive load using a wearable EDA device.," IEEE transactions on information technology in biomedicine : a publication of the IEEE Engineering in Medicine and Biology Society, vol. 14, no. 2, pp. 410–7, Mar. 2010.
- [9] F. Mokhayeri, M.-R. Akbarzadeh-T, and S. Toosizadeh, "Mental stress detection using physiological signals based on soft computing techniques," in 2011 18th Iranian Conference of Biomedical Engineering (ICBME), pp. 232–237, 2011.
- [10] B. Arnrich, C. Setz, R. La Marca, G. Tröster, and U. Ehlert, "What does your chair know about your stress level?," IEEE transactions on information technology in biomedicine : a publication of the IEEE Engineering in Medicine and Biology Society, vol. 14, no. 2, pp. 207 14, Mar. 2010.
- [11] S. Butt and J. G. Phillips, "Personality and self reported mobile phone use," Computers in Human Behavior, vol. 24, no. 2, pp. 346–360, Mar.2008.
- [12] S. Thomée, A. Härenstam, and M. Hagberg, "Mobile phone use and stress, sleep disturbances, and symptoms of depression among young adults--a prospective cohort study.," BMC public health, vol. 11, p. 66, Jan. 2011.
- [13] Y. Ma, B. Xu, Y. Bai, G. Sun, and R. Zhu, "Daily Mood Assessment Based on Mobile Phone Sensing," in 2012 Ninth International Conference on Wearable and Implantable Body Sensor Networks, pp.142–147, 2012.
- [14] S. T. Moturu, I. Khayal, N. Aharony, W. Pan, and A. S. Pentland, "Sleep, mood and sociability in a healthy population.," Conference proceedings : Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Conference, vol. 2011, pp. 5267–70, Jan. 2011.
- [15] G. Chittaranjan, J. Blom, and D. Gatica-Perez, "Who's Who with Big-Five: Analyzing and Classifying Personality Traits with Smartphones," in 2011 15th Annual International Symposium on Wearable Computers, pp. 29–36, 2011.
- [16] A. Muaremi, B. Arnrich, and G. Tröster, "Towards Measuring Stress with Smartphones and Wearable Devices During Workday and Sleep," BioNanoScience, vol. 3, no. 2, pp. 172–183, May 2013.

Comparative Enhancement in Security Level of Modified RSA using Four Prime Numbers

Madhurima Dubey

*M.E. Scholar, Electronics and Telecommunication
Chhatrapati Shivaji Institute of Technology
Durg, (C.G.)
dubeymadhurima@gmail.com*

Mrs.Yojana Yadav

*Associate Professor, Electronics and Telecommunication
Chhatrapati Shivaji Institute of Technology
Durg, (C.G.)
yojanayadav@csitdurg.in*

Abstract— Now a day’s, Secure Communication is an important part of any type of internet applications. With the fast growth in the field of information technology, it also needs the basic requirement like better security, authentication, and integrity over the environment. Basically Cryptography is based on the complex calculation for determining the private and public key. This paper aims to increase the security of traditional RSA algorithm by calculating the keys using four prime numbers. As the security depends on the public component ‘N’, here N is calculated by using 4 prime numbers and also both the keys are dependent on it. This proposed method is not being easily breakable. Comparison of traditional RSA and proposed technique, in terms of time, traditional RSA is fast but in terms of security, proposed technique is stronger than traditional RSA.

Keywords—Cryptography, RSA.

I. INTRODUCTION

Cryptography is divided into two parts crypto and graphy, Greek word crypto means “hidden, secret” and graphy means “writing”. A technique in which secret messages are transferred from one person to another over the communication Channel, the process is called Cryptography. Earlier, the cryptography is used by the kings of the states that were simply writing a secret message into the code words that most of the person could not be able to recognise it. Initially only the symmetric key cryptography is invented, later on with the need of security increases then asymmetric key cryptography is being introduced.

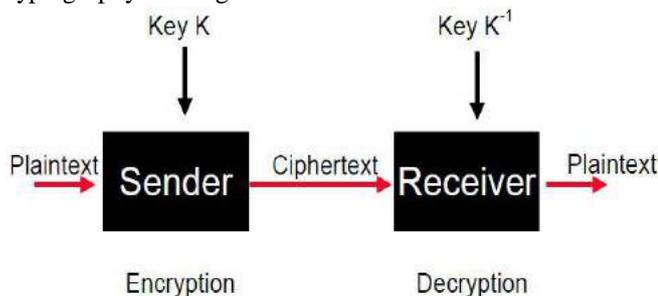


Fig 1: Basic Diagram for Cryptography

RSA is a asymmetric key cryptography technique which uses both the private key and public key. RSA is the short form of Rivest Shamir Adleman. It was develop by Rivest, Adi Shamir and Leonard Adleman of MIT in 1997.

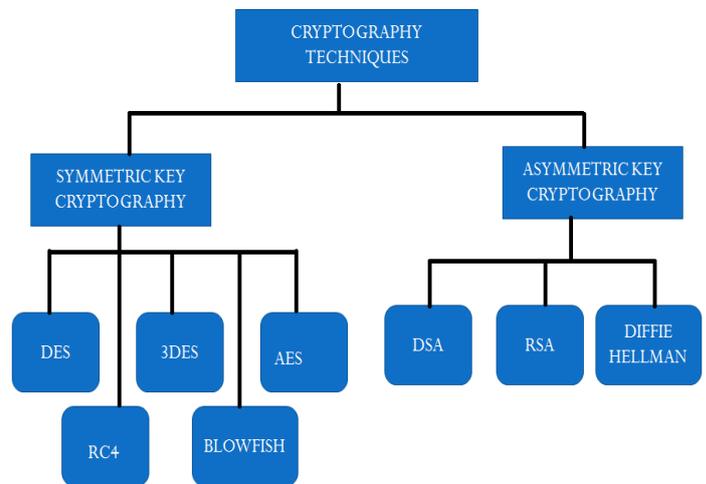


Fig 2: Classification of Cryptography.

Similarly the other cryptography technique RSA also works with three steps - Key generation, Encryption and Decryption. RSA algorithm security basically depends on the product of prime number i.e. modulus ‘N’. Only two prime numbers are used in the traditional algorithm, having a probability that it can be cracked by the attacker if the modulus is small. For security purpose no. of prime used and the modulus ‘N’ is large is necessary. In this paper, proposed algorithm use four prime numbers and modified the calculation part of modulus ‘N’. Hence calculation is complex and takes little more time than traditional algorithms but it couldn’t be breakable easily. Encryption and Decryption techniques are remained same only the key generation process is modified for security purpose.

II. LITERATURE SURVEY

B.Persis Urban Ivy, Purshotam Mandiwa and Mukesh Kumar proposed modified RSA cryptosystem to use 'n' prime numbers and provide maximum security. In this implemented method 'n' prime numbers are used which are not easily breakable and decompose. But this work only depends on the no. of prime number used not on the process of calculation of modulus "N" [11]. Hybrid RSA and Diffie Hellman encryption algorithm is also proposed by Shilpi Gupta and Jaya Sharma in order to achieve higher security. Thus it gives the better efficiency in terms of complexity of time. A limitation of this paper is that size of algorithm is large [16]. Modified RSA based algorithm is described by Ritu Patidar and Rupali Bhartiya, keys are stored offline before process start so that speed of execution get increased. Here only three prime numbers are used. If small prime number can be used than 'N' could be decomposed by the attacker [5, 10]. Sami A Nagar and Saad Alshamma works on high speed implementation with modified key exchange. This works focus on the key exchange through offline storage real values of N, e and d in the SQL database and exchange through gateway. But this method only provides the speed but not the security to the original RSA algorithm [15]. For data communication, comparative analysis of encryption algorithms is done by Shashi Mehtrota and Seth Rajan Mishra. The result of the survey is that DES gives better result than RSA. It has suggested the several improvements in RSA or RSA should hybrid with other cryptography technique [22]. An Enhanced and Secured RSA Key Generation Scheme is introduced and implemented by M.Thangavel, P. Varalakshmi, Mukund Murrari and K. Nithya uses the four prime numbers for the enhancement of key generation. Thus the system is highly secure and not easily breakable, but the time consumption by this proposed method is large as compare with RSA algorithm[6].

III. PROPOSED METHODOLOGY

In proposed method, key generation involves the usage of four prime numbers. The value of E, D depends on the value of N, which is the product of 4 prime numbers. Most RSA systems are easily breakable because the computation of keys is based on n. This n can be easily found by factoring methods because it is only a product of 2 primes. If this n is obtained, the hacker can easily find the keys and thus break the system. Only the value of n is kept as public and private component. Thus the attacker with the knowledge of n cannot determine all the primes which are the basis for finding the value of N and subsequently D. The encryption and decryption are based on n but the computation of keys is not based on n but on N. This makes the system secure and not easily breakable. The proposed algorithm is described below-

Key Generation

1. Enter the four prime numbers p, q, r and s.
2. Calculate modulus N
 $N = n * m$
 Where $n = p * q$ and $m = r * s$

3. Calculate Euler $\phi(N)$
 $\phi(N) = \phi(n) * \phi(m)$
 Where, $\phi(n) = (p-1) * (q-1)$
 and $\phi(m) = (r-1) * (s-1)$
4. Find a random number e, such that $1 < e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$.
5. Compute a random number d, such that $1 < d < \phi(N)$ and $e * d \bmod \phi(N) = 1$.

Encryption

Cipher text (C) = $M^e \bmod N$
 Where M is the plain text or input message.
 e is the public key component.

Decryption

Plain text (M) = $C^d \bmod N$
 Where d is the private key component.

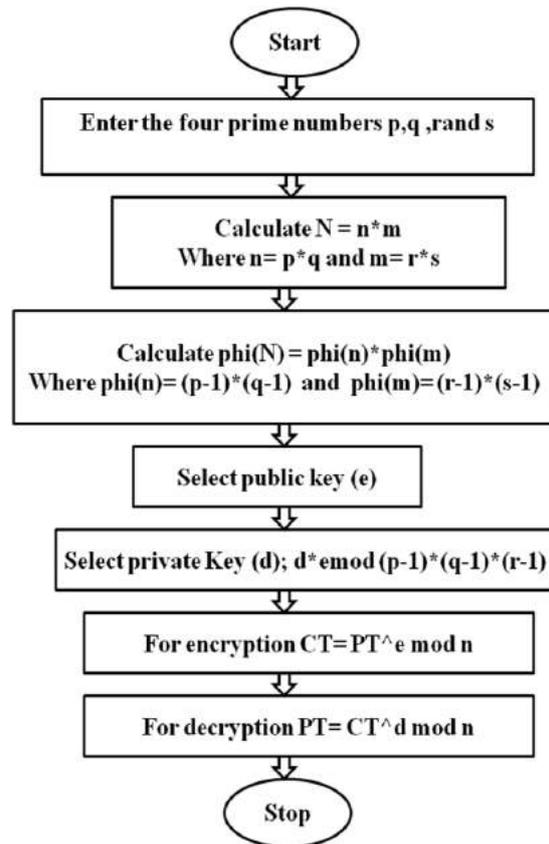


Fig 3: Flowchart of Proposed Algorithm

IV. RESULT AND DISCUSSION

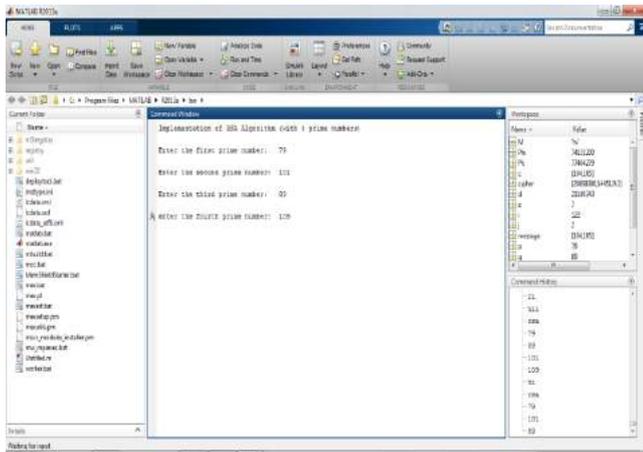


Fig 4: Input of the proposed algorithm

Inputs of the proposed algorithm for key generation are four large prime numbers. Calculation of keys i.e. both public and private key takes more time than original RSA algorithm but proposed algorithm provide the stronger key than original RSA algorithm.

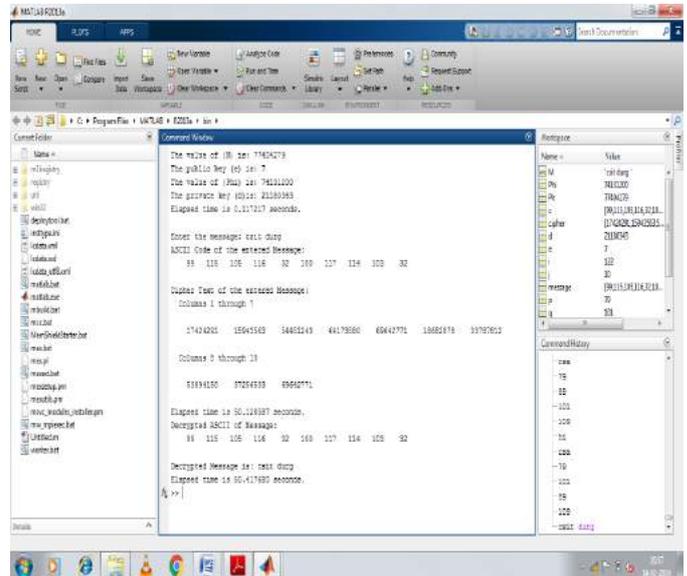


Fig 6: Output of Encryption and Decryption

The comparison table is prepared in terms of prime number used, execution time and security which show the highly secured algorithm is proposed algorithm but its process is time consuming.

Table1: Comparison of Different RSA based Algorithms.

ALGORITHM	NO. OF PRIME NUMBERS USED	EXECUTION TIME (in seconds)	SECURITY
RSA	2	0.33345	Low
Modified RSA	3	0.33291	Medium
Proposed Algorithm	4	2.5725	High

V. CONCLUSION

In this paper, proposed algorithm is implemented in MATLAB R2013a, the various modifications on RSA algorithm are based on its security. In this proposed method only few concepts are modify, further RSA can be modified with many logical changes in mathematical calculation and also it can be merging with Digital signature and also it can be further implemented in image, video, etc.

VI. REFERENCES

- [1] Srinivasan Nagaraj, Dr.G.S.V.P.Raju and V.Srinadth, "Data Encryption and Authentication using Public Key Approach ", Elsevier International conference on Intelligence Computing, Communicationa and Convergence , pp. 126-132, 2015.
- [2] Sarika Khatarkar and Rachana Kamble, "A Survey and Performance Analysis of Various RSA based Encryption Techniques", International Journal of Computer Applications, vol.114, issue-7, pp. 30-33,2015.
- [3] Joshi Maitri and Fenil Khatiwala, " Survey of Different Modified RSA Techniques and Analysis", International Journal of Engineering

- Technology, Management and Applied Sciences, vol.3, issue- 2, pp. 126-132,2015.
- [4] Shyam Deshmukh and Prof. Rahul Patil, "Hybrid Cryptography Technique using Modified Diffie-Hellman and RSA", International Journal of Computer Science and Information Technologies ,vol.5 (6) , pp.7302-7304, 2014.
- [5] Ms.Ritu Patidar and Mrs. Rupali Bhartiya, "Implementation of Modified RSA Cryptosystem Based on Online Storage and Prime Number", International Journal of Computing and Technology,vol.1,issue-5, pp.205-209, 2014.
- [6] M. Thangavel, P. Varalakshmi, Mukund Murralli and K. Nithya, "An Enhanced and Secured RSA Key Generation Scheme (ESRKGGS) ", Elsevier, pp. 1-8, 2014.
- [7] Ali E.Taki El_Deen,El-Sayed A.El-Badawy and Sameh N.Gobarn, "Digital Image Encryption Based on RSA Algorithm", International Journal of Electronics and Communication Engineering, vol.9, issue-1, pp. 69-73, 2014.
- [8] Amar Odeh, Khaled Elleithy, Munner Alshowkan and Eman Abdelfattah,"Quantum Key Distribution by using Public Key Algorithm (RSA)",IEEE 3rd International Conference on Innovative Computing Technology, pp.83-86, 2013.
- [9] Norhidayah Muhammad, Jasni Mohamad Zain and Md Yazid Mohd Saman," Loop Based RSA Key Generation Algorithm using String Identify", 13th International Conference on Control, Automation and System, pp.255-258, 2013.
- [10] Ms. Ritu Patidar and Mrs. Rupali Bhartiya ,"Modified RSA Cryptography Based on Offline Storage and Prime Numbers", IEEE International Conference on Computational Intelligent and Computing Research, pp. 1-6, 2013.
- [11] B.Persis Urbana Ivy, Purshotam Mandiwa and Mukesh Kumar," A Modified RSA Cryptosystem Based on 'n' Prime Numbers ", International Journal of Research in Science and Engineering, vol.1, issue-8, pp.63-66, 2013.
- [12] S.H.Mortazavi and P.S.Avadhani, " RSA Cryptography Algorithm : An Impressive Tool in Decreasasing Intrusion Detection System (IDS) Vulnerabilities in Network Security ",International Journal of Innovative Technology and Exploring Engineering, vol.2, issue-4, pp. 306-310, 2013.
- [13] Faraz Fatemi Moghaddam and Iman Ghavam, " A Client Based User Authentication encryption Algorithm for Secure Accessing to Cloud Server", IEEE Student Conference on Research and Development, pp.175-180 , 2013.
- [14] Prof.Dr.Alaa Hussein Al-Hamami and Ibrahim Abdallah Aldariseh," Enhanced Method for RSA Cryptosystem Algorithm", IEEE International Conference on Advanced Computer Science Applicationa and Technologies, pp.402-408, 2012.
- [15] Sami A.Nagar and Saad Alshamma, "High Speed Implementation of RSA Algorithm with Modified Keys Exchange",IEEE 6th International Conference on Science of Electronics , Technologies of Information and Telcommunication, pp. 639-642, 2012.
- [16] Shilpi Gupta and Jaya Sharma," A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman", IEEE International Conference on Computational Intelligent and Computing Research, pp. 1-4, 2012.
- [17] Ravi Shankar Dhakar and Amit Kumar Gupta, "Modified RSA Encryption algorithm (MERA)", IEEE 2nd International Conference on Advanced Computing and Commnication Technologies, pp. 426-429, 2012.
- [18] Vishal Grag and Rishu, "Improved Diffie-Hellman Algorithm for Network Security Enhancement ",International Journal of Computer Technology and Applications ,vol.3 issue-4,2012.
- [19] P. Saveetha and S.Arumugam, " Study of Improvement in RSA Algorithm and its Implementation", International Journal of Computer and Communication Technology, vol.3, issue-6,2012.
- [20] Xin Zhou and Xiaofei Tang,"Research and Implementation of RSA Algorithm for Encryption and Decryption", IEEE The 6th International Forum on Strategic Technology, pp. 1118 - 1121, 2011.
- [21] Liang Wang and Yonggui Zhang, "A New Personal Information Protection Approach Based on RSA Cryptography ", IEEE International Symposium on IT in Medicine and Education , pp.591-593, 2011.
- [22] Shashi Mehrotra Seth and Rajan Mishra, " Comparitive Analysis of Encryption Algorithms For Data Communication", International Journal of Computer Science and Technology, vol.2, issue-2, pp. 292-294, 2011.
- [23] Wenxue Tan , Xiping Wang , Xiaoping Lou and Meisen Pan, "Analysis of RSA based on Quantitating Key Security Strength",Elsevier Advanced in Control Engineering and Information Science , pp. 1340-1344, 2011.
- [24] Sonal Sharma, Prashant Sharma and Ravi Shankar Dhakar, "RSA Algorithm Using Modified Subset Sum Cryptosystem", IEEE International Conference on Computer & Communication Technology, pp.457-461, 2011.
- [25] Yunfei Li,Qing Liu and Tong Li," Design and Implementation of an Improved RSA Algorithm", IEEE International Conference on E-Health Networking,Digital Ecosystems and Technologies, pp.390-393,2010.
- [26] Allam Mousa ,"Sensitivity of Changing the RSA Parameter on the Complexity and Performance of the Algorithm", Journal of Applied Science, vol.5, issue-1, pp.60-63, 2005.
- [27] Aloka Sinha and Kehar Singh, "A Technique for Image Encryption using Digital Signature", Elsevier Optics Communications, pp.239-234, 2003.
- [28] Subbarao V. Wunnava and Ernest Rassi , "Data Encryption Performance and Evaluation Schemes", IEEE Proceedings IEEE Southeastcon, pp.234-238, 2002
- [29] David A.Carts ,"A Review of the Diffie-Hellman Algorithm and its Use in Secure Internet Protocol", SANS Institute, pp.1-7, 2001.
- [30] Rajorshi Biswas and Shibdas Bandyopadhyay," A Fast Implementation of the RSA Algorithm Using the GNU Implementation ", pp. II-30.1-II-30.15.
- [31] Atul Kahate, Cryptography and Network Security,Fourth Edition, Tata McGraw-Hill.
- [32] William Stallings, Cryptography and Network Security – Principles and Practice, Fifth Edition, Pearson Publication.
- [33] R.L.Rivest,A.Shamir and L.Adleman ,"A Method for Obtaning Digital Signatures and Public Key Cryptosystem ", Communication of ACM, vol.21,pp.120-126, 1978.

Removing Interference using Adaptive Filter with LMS Algorithm

Shivangi Namdeo

*Dept. of Electronics & Telecommunication Engineering
Chhatrapati Shivaji Institute of Technology
Durg(C.G.)
shivanginamdeo6@gmail.com (9893390017)*

Mrs. Ashalata sharma

*Dept. of Electronics & Telecommunication Engineering
Chhatrapati Shivaji Institute of Technology, Durg
Durg(C.G.)
ashameenu1411@gmail.com(8871727789)*

Abstract— Adaptive filter are primary method to remove power line interferences from biomedical signal like ECG signal. There are Digital filter i.e. FIR filter based on various window and IIR filter that are very efficient to remove or minimize of such a low frequency signal. Adaptive filter with LMS algorithm are more sufficient method to remove noises from ECG signal due to its simplicity and robustness properties which have made to uses in many applications and this Application includes adaptive channel equalization, adaptive predictive speech coding, Noise Suppression and system identification. These algorithm are used for faster convergence rate and better result of tracking properties than earlier techniques could offer. The LMS algorithm is currently the most popular method for adapting a filter, because of its simplicity and robustness properties. When the signal and noises are passed through the LMS filter there are sign, sign-sign and sign regression are represent.

Keywords— ECG, Adaptive Filter, LMS algorithm, Noises.

I. Introduction

ECG (electrocardiography) signal is most important for **diagnosis** and many other cardiac problem but when ECG signals are recorded it may be corrupted by noises like as power line interferences, base line wandering, electrode contact noise, motion artifacts, muscle contraction etc. Adaptive filters are computational device and it is self designing system and Adaptive filter with LMS algorithm shows good performance for analyzing of ECG signal so there are algorithm is used due to its simplicity [1]. LMS algorithm is most important for cancel the noise from ECG signal due to its simplicity and robustness properties. LMS algorithm have a weight update equation given as-

$$W(n+1) = W(n) + \mu e(n) X^*(n) \quad \dots(1)$$

Where, $x(n)$ = input vector, $W(n+1)$ = value of the new weight at time $(n+1)$, $W(n)$ = value of the weight at time n and μ = step size.

$$e(n) = d(n) - y(n) \quad \dots(2)$$

$$y(n) = \sum W_n(k) X^*(n - k) \quad \dots(3)$$

There are LMS algorithm is used when the cost is major criteria. In LMS algorithm, the update function is obtained by the multiplication of the step size with the current value of the error signal and input signal and does not depend other previous value [3].

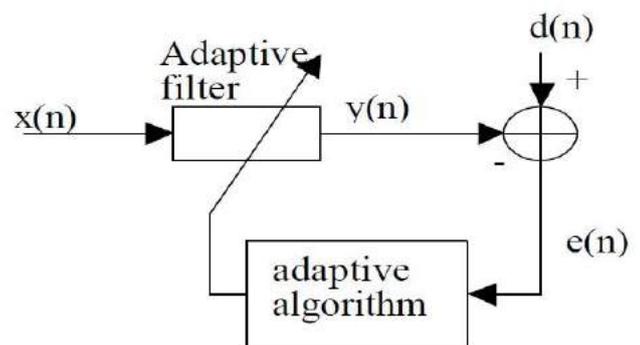


Fig - adaptive filter

II. LITERATURE REVIEW

Uzzal biswas and Md. Maniruzzaman has used two Adaptive filter, such as normalized least mean square (NLMS) adaptive filter and recursive(RLS) adaptive filter and compare with notch filter both in time and frequency domain to remove power line interference from ECG signal. The affected segment create problem during the diagnosis of arrhythmia. So to obtain a reliable ECG signal for the diagnosis of arrhythmia it has become very crucial to remove the 50 Hz of power line interference from the recorded ECG signal. A comparison of the performance of FIR notch filter, wiener filter and adaptive filter in reducing power line interference in ECG[1]. M. Sushmitha and T. Balaji has be introduced Kalman based least mean square filter. The Kalman base, least mean square filter are essentially to remove or minimize the mean square error and 50 Hz power line interference and uses different Adaptive filter algorithm such as BLMS, DLMS filtered XLMS and Kalman based LMS algorithm [2]. Akash Singh Bhoi, Karma Sonam Shepra, Devakishore Phurailatpam, jitendra singh Tmang introduced noise cancellation of ECG

signal. It seems that ECG signal are most important for heart related diagnosis and many other cardiac problem, and there are ECG signal is very low frequency about (0.5-100Hz) . ECG signal i.e. recorded during ambulatory process that signal is corrupted by noise, hence in signal processing noise removal is important so there are five type of filter median, Low Pass Butter worth, FIR, Weighted Moving Average and Stationary Wavelet Transform (SWT) with their filtering effect on noisy ECG are presented remove noises. After study the paper there are morphological changes in ECG waveforms are shown in the filtering results of median and FIR filters where as there is no significant change in the noisy and filtered signal in case of LP Butterworth filter [4].

III. Methodology

The least mean square algorithm adjust the filter coefficient to minimize the cost functions. When ECG signal is passed through the LMS filter than there are ECG signal and type of noises like as power noise , color noise and Gaussian noise can corrupted signal. Adaptive filter are adapt the signal and there are Adaptive filter with LMS algorithm are shows better performance for processing and analyzing of infected ECG signal.

A. ECG Signal

ECG signal is electrocardiography Today diagnosis problems are increasing day by day and the ECG signal play important role in biomedical. Electrocardiography (ECG) is a diagnosis tool which is used for recording the electrical activity of heart with the help of electrodes that attached from skin.

B. Type of Noise in ECG signal

There are different types of noises that can change the characteristics of ECG signal: power line interference, base line wandering, muscle contraction , electrode contact noise ect.

C. Adaptive Filter

Adaptive filter is a computational device Adaptive Filter is a computational device that are attempted to model give the relationship between two signal in real time in iterative manner. An Adaptive filter may be called as a self modifying digital filter. These filters are adjusts its coefficient in order to minimizing an error function. The result of the filter parameters a moment ago, automatically adjust the filter Parameters of the present moment, to adapting to the unknown Signal [2] Types of Adaptive filter: LMS , RLS ,NLMS, kernel , Kalman , weiner Adaptive Filter.

Following the flow chart that demonstrate the algorithm that are used:

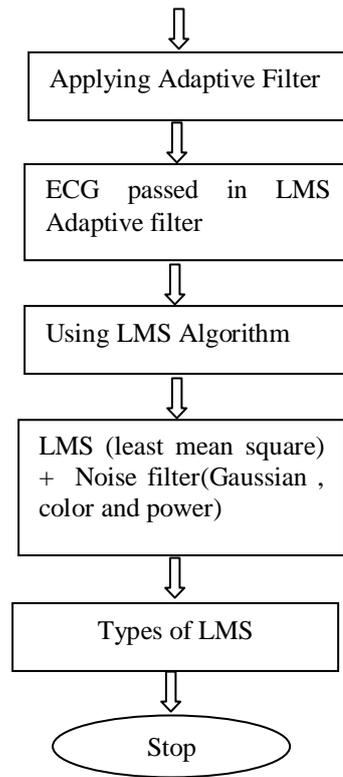
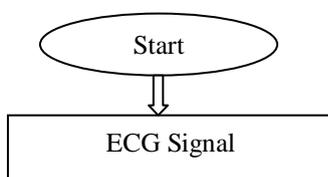


Fig: Flow Chart

D. LMS Adaptive Filter

The least mean square adaptive filter adapts the signal then it compute filter output error and weight using LMS adaptive filtering. The filtered LMS algorithm is currently the most popular method for adapting a filters, due to its simplicity and robustness properties, which have made it widely adopted in many applications and this Applications are includes adaptive channel equalization, adaptive predictive speech coding, Noise Suppression and on-line system identification.

E. LMS Algorithm

Introducing LMS adaptive algorithm, a number of new adaptive filter algorithms have been briefly explained and applied to use for faster convergence rate and better result of tracking properties than earlier techniques could offer. The Filtered LMS algorithm is currently the most popular method for adapting a filter, because of its simplicity and robustness properties, which have made it to use to adopted in many other applications. Those Applications are adding adaptive channel equalization, adaptive predictive speech coding, Noise Suppression and on-line system identification [3].

There are types of ECG signal and Noises:

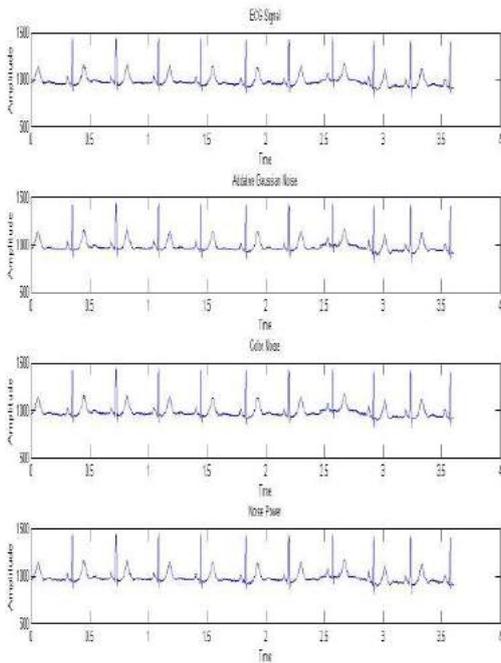


Fig - ECG Signal and Noises

IV. result

There are result obtained after simulation of various filters in MATLAB and result got after filtration. The result of the noise cancellation with LMS as well as the proposed technique are presented. The generated sequence was considered as the input. The noise in the signal from channel was almost removed. Following figure shows the output of the signal where the ECG signal is passed through LMS filter algorithm. In the figure results are indicate signal value and coefficient value, where blue line show desired signal, green line shows output and red line is error signal.

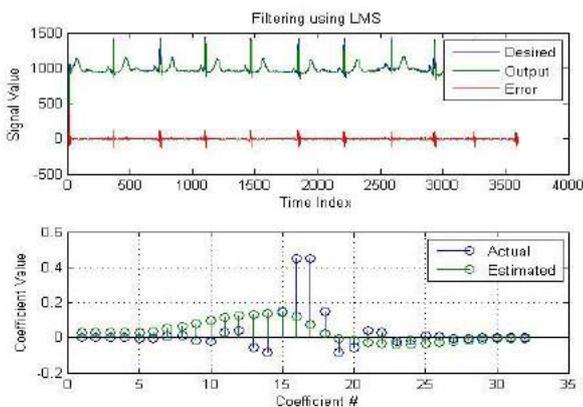


Fig. ECG signal passed to the LMS adaptive filter

There are when the ECG signal passed to the LMS filter then there are types of LMS (least mean square) are included.

- Sign LMS
- Sign- Sign LMS
- Sign regression LMS

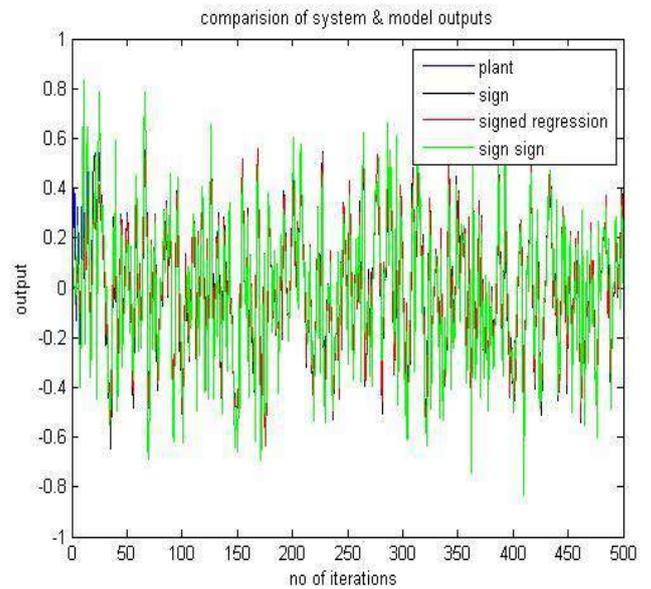
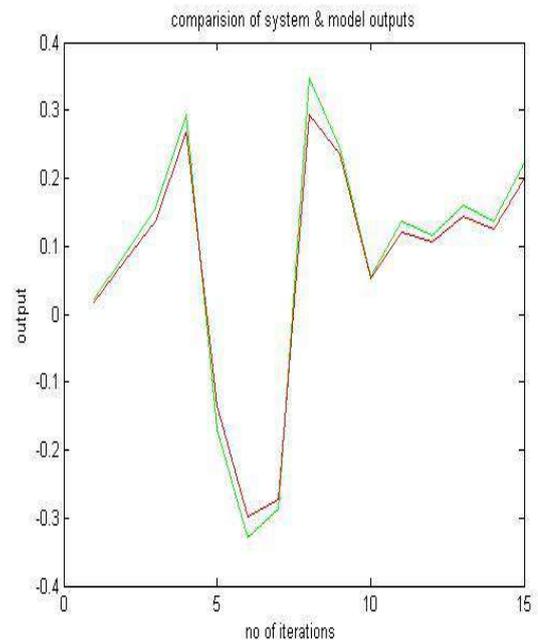


Fig- sign LMS



.Fig- Sign -Sign LMS

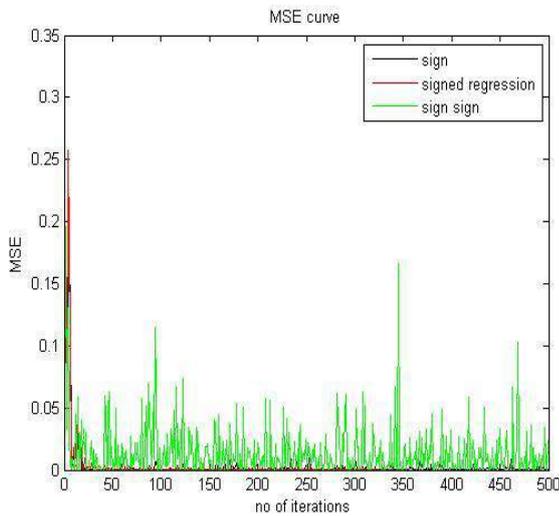


Fig - Sign Regression LMS

V. CONCLUSION

In these algorithm discussed the LMS adaptive algorithm used in adaptive filters, because it give good performance for analysis and processing of biomedical (ECG) signal. LMS algorithm is used when cost is about major criteria. There are Adaptive filter with LMS algorithm is better because its simplicity and robustness.

- [1] Uzzal Biswas and Md. Maniruzzaman ,“Removing Power Line Interference From ECG Signal Using Adaptive Filter,” IEEE Conference on electrical engineering and Information & Communication Technology (ICEEICT),2014.
- [2] M. Sushmitha and T. Balaji“Removing Power Line Interference From ECG Signal Using Adaptive Filter ,” IJCSNS, International Journal of Computer Science and Network Security,vol.14 ,No.11 November 2014.
- [3] S. Radhika Sivabalan Arumugem, “A Survey on Different Adaptive Algorithm used in Adaptive Filter ,”. International Journal of Engineering Research & Technology(IJERT) vol.1 issue 9 NOV. 2012.
- [4] Akash Kumar Bhoi, Karma Sonam Shepra, Devakishore Phurailatpam, Jitendra Singh Tamng “Multidimensional Approach for Noise Cancellation of ECG Signal .” international conference on communication and signal processing, india 2015.
- [5] C. Mohan Rao ,Dr. B. Stephen Charles, Dr. M N Giri Prasad “A Variation of LMS Algorithm for Noise Cancellation .” International Journal OF Advanced Research in Computer and Communication engg , vol2 issue 7, july 2013.
- [6] Bhumika Chandrakar, O.P. Yadaw, V.K.Chandra “A Survey on Noise Removal Technique for ECG Signal .” international journal on Advanced Research vol 2 March 2013.
- [7] Hyeong Geon Lee, Jae- Young Park , Suk Lee “Performance Analysis of Adaptive LMS Filter through Regression Analysis using System C .” international journal of computer, energetic electronics and communication engg vol 7 no 2, 2013.
- [8] Zhang Jingjing ,“Variable Step Size LMS Algorithm,” International Journal of Future Computer and Communication,vol.1,No.4,December 2012.



PERFORMANCE ANALYSIS OF PARALLEL SELF TIMED ADDER

Shafaque Farheen Khan
M.tech VLSI Design, Department of ECE
J.D. College of Engg.
Nagpur.

shafaquefarheenkhan@gmail.com, 8856052085

Abstract: A Parallel self timed adder is been discussed in brief with a recursive approach. A multibit binary addition can be easily performed by the discussed design. It gives good performance without any special speed up circuitry It consists of simple circuitry along with a special completion detection unit. The use of recursive method decreases the power consumption.

KEYWORDS: CMOS DESIGNS, ASYNCHRONOUS CIRCUIT, RECURSIVE APPROACH

I. INTRODUCTION

The most basic operation that a processor performs is binary addition. Developing clockless circuit is of high interest nowadays. Synchronous circuits involve many problems which can be easily eliminated by the use of clockless circuits as these circuits do not involve any quantization of time. The logic flow in asynchronous circuit is controlled by a request and acknowledge signal. These are called handshaking signals.

Here we are discussing Parallel Asynchronous Self Timed Adder. The design consists of half adders, multiplexers and a completion detection unit. Using explicit blocks for handshaking signals in small elements like adders becomes very expensive. Therefore dual rail carry propagation is used. Asynchronous adders are either based on full dual rail encoding of all signals or pipelined operation using single-rail data encoding and dual-rail carry representation for acknowledgments. The design is efficient for proper VLSI implementation. For independent carry chain blocks, the design works in parallel manner. The feedback consists of XOR gate which constitute a single rail cyclic asynchronous sequential adder. Cyclic circuits are more efficient than their acyclic counterparts. The discussed circuit takes care of inertial and propagation delay involved in the circuit path. By doing so it manages the automatic single rail pipelining of the carry inputs.

BACKGROUND

Binary adders have many designs but here we will discuss asynchronous adders. The logical circuits that assume time for correct operation are referred to as self timed circuit.

The self timed adders are capable to run faster as compared to clocked circuits. The early completion sensing in self timed circuit can avoid the bundled delay mechanism which is a problem related to synchronous circuit. Self timed circuits can be classified as follows:

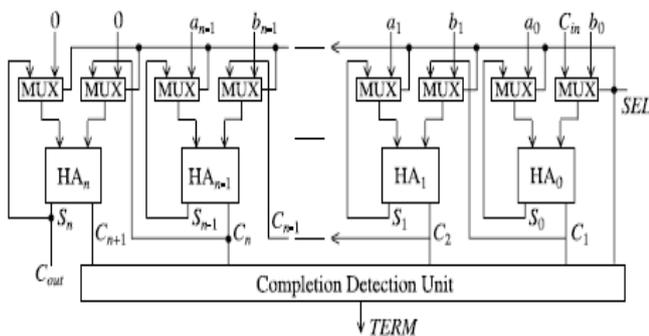
1. PIPELINED ADDER USING SINGLE RAIL DATA ENCODING: To enable the adder block as well as to establish the flow of carry signals asynchronous handshaking signals are used. For internal bitwise flow of carry output, a dual rail carry convention is used. It provides more than two logic values and thus provides bit level acknowledgement when a bit operation is completed. When all bit acknowledgement signal are received, the final completion is sensed. An example of pipelined adder is carry completion sensing adder. It uses full adders and functional blocks.

2. DELAY INSENSITIVE ADDER USING DUAL RAIL ENCODING: Bundling constraints or delay insensitive operations are asserted by delay insensitive adder. These adders are asynchronous in nature. Hence in presence of unknown gate and wire delays they can operate correctly. There are various types of DI adders, such as DI carry look ahead adder (DICLA) and DI ripple carry adder (DIRCA). Dual rail encoding is used by DI adders and it increases the complexity. The wire complexity gets doubled in dual rail encoding but capable to produce efficient circuits such as single rail variants. The DICLA defines carry propagate, generate and kill equations in terms of dual rail encoding just like. The carry signals are organized in hierarchical tree rather than connecting them in a chain. So, it can perform operation much faster where there a long carry chain exists. By setting either 0 or 1 path dual rail encoding logic can get benefited. In dual rail logic there is no need to wait for the evaluation of both paths. The speed of carry look ahead adder circuitry can be increased. This increased speed can be used to send carry generate/carry kills signal to any level in the tree.

DESIGN OF PASTA

Architecture and PASTA theory is presented in this section. On each bit half addition is performed by the adder when it accepts two input operand. Earlier generated carry is used for subsequent iteration. Half additions are performed till all the carry bits become zero.

A.PASTA Architecture: The architecture of PASTA is shown in fig 1. Here the select line of a two input multiplexer corresponds to the request hand shaking signal. This signal is a single 0 to 1 transition..When the SEL is 0 it will select the actual input operand .When SEL is 1 then the feedback/carry path for the iteration process will get selected. The multiple iterations will be continued by feedback paths in half adders till all carry signals will become zero.



B.STATE DIAGRAMS:

In the proposed architecture there are two phases namely the initial phase and the iterative phase .State diagram of both these phases have been shown in fig 2. (C_{i+1}, S_i) pair is present in in each state. C_{i+1}, S_i stand for carry out and sum values from the i th bit adder block respectively. The circuit in its initial phase works only as a combinational half adder during the initial phase. State (11) cannot appear due to the presence of half adders instead of full adders..The feedback path through the multiplexers are activated when the SEL is 1.During this the circuit is in iterative phase.To complete the recursion, the carry transitions (C_i) are allowed as many times as its needed .As the inputs and outputs have to go through several transitions before a final output is produced, this design cannot be said as fundamental mode circuit .State diagram in fig 2 shows the many transition involved in the circuit. It is similar to cyclic sequential circuits because it separate individual state

by using gate delays.

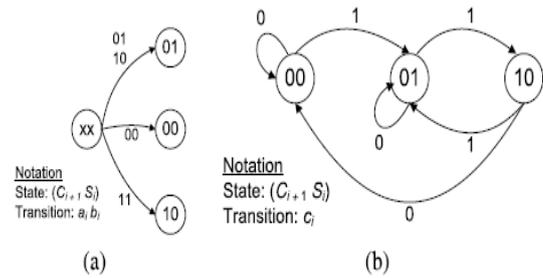


Fig. 2. State diagrams for PASTA. (a) Initial phase. (b) Iterative phase.

RECURSIVE APPROACH USED IN DESIGN:

S_{ij}, C_{j+1} represent the sum and carry, respectively, for i th bit at the j th iteration. For the initial condition when $j=0$,the formulae for addition are as follows:

$$S_i^0 = a_i \oplus b_i$$

$$C_{i+1}^0 = a_i b_i.$$

For the j th iteration the recursive addition formulae are given as:

$$S_i^j = S_i^{j-1} \oplus C_i^{j-1}, \quad 0 \leq i < n$$

$$C_{i+1}^j = S_i^{j-1} C_i^{j-1}, \quad 0 \leq i \leq n.$$

When the following condition is met at k th iteration , the recursion is terminated:

$$C_n^k + C_{n-1}^k + \dots + C_1^k = 0, \quad 0 \leq k \leq n.$$

The recursive formula's correctness is checked by the following theorem:

Theorem 1: The formula for recursion gives the correct sum result irrespective of the number of bits and within finite time it will get terminated.

CMOS IMPLEMENTATION OF PASTA

Fig 3 shows CMOS implementation of recursive circuit. Implementation of transmission gate XOR is used in multiplexers to match the delay with AND gate. To obtain an active high completion signal, the completion detection unit is negated. A large fan in n input NOR gate is required for above purpose..The high fan in problem in completion detection unit can be avoided by using pseudo N-MOS design .Since it has all connections in parallel. .To ensure that completion detection unit do not gets turned ON accidentally during the initial phase ,the negative of SEL signal is also included along with Cis in TERM signal.

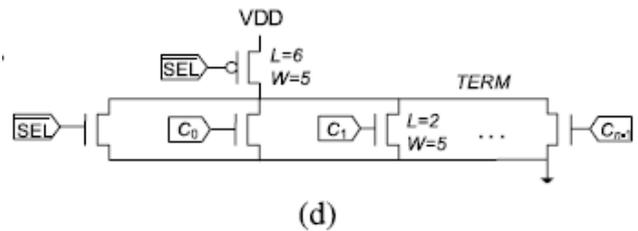
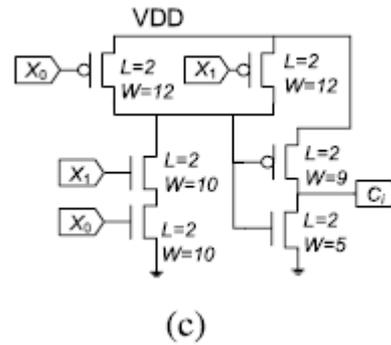
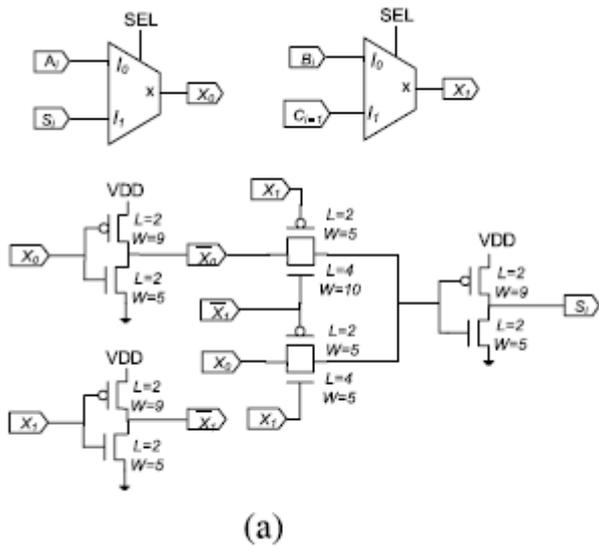
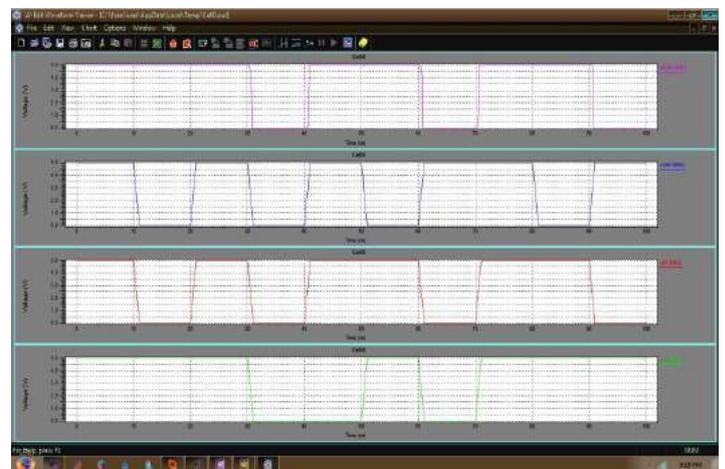


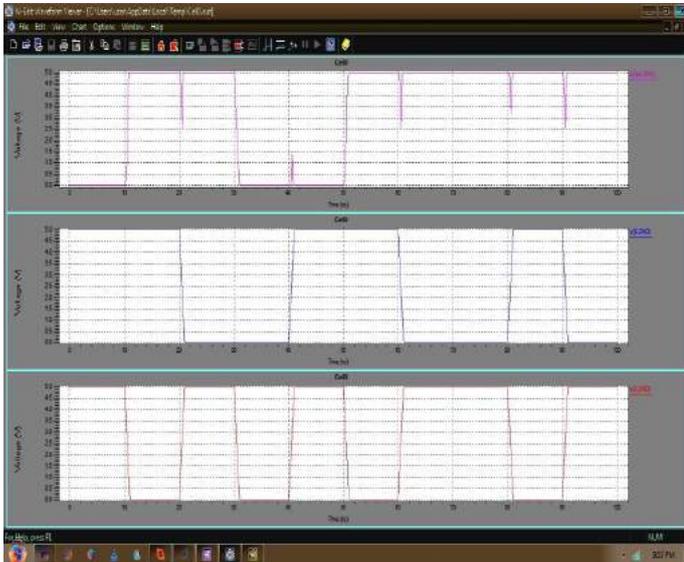
Fig.3. CMOS implementation of PASTA. (a) Sum module for single bit (b) 2:1 mux for single bit adder. (c) Module for single bit carry (d)Completion detection unit.

SIMULATION RESULTS

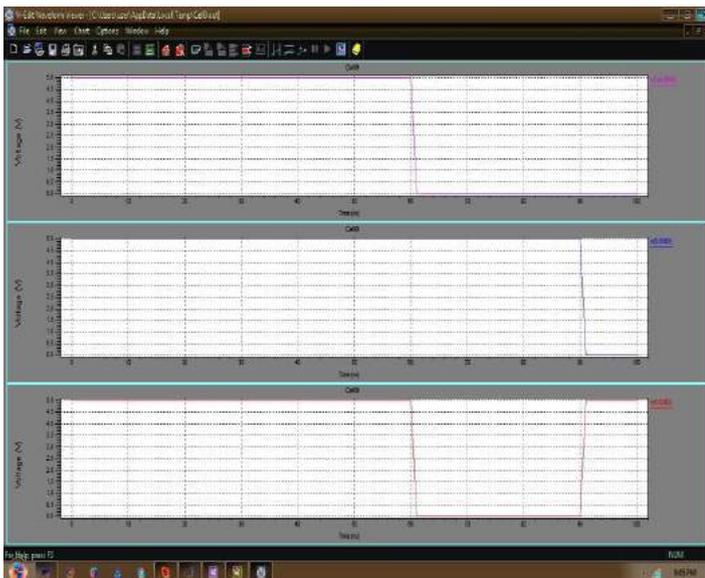
Mux simulation:



SUM SIMULATION



CARRY SIMULATION:



Above results are the simulation results for MUX,SUM and CARRY respectively.The simulations are performed in microwind tool.Among self timed adders PASTA performs best. PASTA completes the first iteration of the recursive formulation when “SEL = 0.”

Therefore, the best case delay represents the delay required to generate the TERM signal only and of the order of picoseconds.

CONCLUSION

This brief presents Performance Analysis Of Parallel Self Timed Adder.CMOS implementation and architectural designs are presented.A very simple n bit adder using a recursive approach is used.For independent carry chain the circuit works in parallel manner. As in today’s case there is a need of highly compact chips size so here we will try to make the circuit more area efficient.

Power is a very important criteria and here we will also try to reduce the power requirement of the circuit.

REFERENCES

- Mohammed Ziaur Rahman, Lindsay Kleeman, and Mohammad Ashfaq Habib” Recursive Approach to the Design of a Parallel Self-Timed Adder”2014
- M. Z. Rahman and L. Kleeman, “A delay matched approach for the design of asynchronous sequential circuits,” Dept. Comput. Syst.Technol., Univ. Malaya, Kuala Lumpur, Malaysia, Tech. Rep. 05042013.
- R. F. Tinder, *Asynchronous Sequential Machine Design and Analysis: A Comprehensive Development of the Design and Analysis of Clock-Independent State Machines and Systems*. San Mateo, CA, USA: Morgan, 2009.
- F.-C. Cheng, S. H. Unger, and M. Theobald, “Self-timed carry-look ahead Adders,” *IEEE Trans. Comput.* vol. 49, no. 7, pp. 659–672, Jul. 2000.
- R. F. Tinder, *Asynchronous Sequential Machine Design and Analysis: A Comprehensive Development of the Design and Analysis of Clock-Independent State Machines and Systems*. San Mateo, CA, USA: Morgan, 2009



EFFICIENT DESIGN OF DOUBLE TAIL COMPARATOR

Tanveer khan

M.tech VLSI Design, Department of ECE

J.D. College of Engg.

Nagpur.

khantanveer02@gmail.com, 7385541569

Abstract—Comparator is an important device in many high speed applications. For these high speed devices, a major emphasis is given towards low power methodologies. Also comparators are the basic building blocks for designing various analog and mixed signal systems. Low power high speed comparators with low chip area are required by many high speed analog to digital converters. In this paper an efficient design of double comparator is proposed which operates at a high speed and consumes less power.

Keywords—double tail comparator, positive feedback, switching transistor, cross coupled transistors.

I. INTRODUCTION

The most widely used component in many applications is a comparator. It is used in applications like analog to digital converters, phase locked loops, high speed ADCs. The operation of a comparator is just like an operational amplifier in which it has two inputs (inverting and non-inverting) and an output. The function of CMOS comparator is to compare two voltages or currents and produces a binary output based on the comparison. Comparators are also known as 1 bit analog to digital converters and thus are widely used in Analog to digital converters. In analog to digital conversion first the input signal is sampled, this sampled signal is then applied to a combination of comparators to determine the digital equivalent of the analog signal. The speed of the comparator depends on decision making time of comparator. The performance of comparator plays a crucial role in the overall performance and cost of the high speed application.

When supply voltage is smaller it becomes more difficult to design high speed comparators. Thus, in order to achieve high speed large size transistors are required so as to compensate for the reduced supply voltage and to achieve high speed. But large size transistors means more die area and power is required. Also low voltage operation limits the

common mode input range. This common mode input range is important in many high speed architectures

The two most important features of the comparator are fast speed and low power consumption which are essential for the overall performance of high speed ADCs. In this paper the design of conventional dynamic comparator and double tail comparator are shown which will be compared with the modified design of double tail comparator. This paper is organized as follows. Section II, describes the working of conventional dynamic comparator, its advantages and disadvantages. Section III describes conventional double tail dynamic comparator, its working, advantages and disadvantages. Section IV describes the proposed double tail comparator. Section V describes simulation result for conventional dynamic comparator and conventional double tail comparator. Section VI draws the conclusion of the work done.

II. CONVENTIONAL DYNAMIC COMPARATOR

Conventional dynamic comparators are mostly used in analog to digital converters. The advantages of this comparator are high input impedance, rail to rail output swing and zero static power consumption. The diagram of the conventional dynamic comparator is shown in fig 1.

The operation of the comparator is as follows. During reset phase when $CLK=0$ M_{tail} is off. Thus a start condition is established as the reset transistors M_7 and M_8 pull both the output nodes Out_n , Out_p to V_{DD} . Hence a logical level is obtained in the reset phase.

During comparison phase, when $CLK = V_{DD}$, transistor M_{tail} is on and transistors M_7 and M_8 are off. Depending on corresponding input voltages (V_{INP} , V_{INN}), output nodes (Out_p , Out_n) which are previously charged to V_{DD} , start to discharge at different rates. When $V_{INP} > V_{INN}$, the output node Out_p discharges faster as compared to output node Out_n , hence with Out_p (discharged by transistor M_2 drain current), falling

down to $V_{DD}-|V_{thp}|$ before $Outn$ (discharged by transistor M_1 drain current), the corresponding PMOS transistor (M_5) will turn on to initiate the latch regeneration caused by back-to-back inverters (M_3 - M_5 and M_4 - M_6). Thus, the output node $Outn$ pulls to V_{DD} and $Outp$ discharges to ground. If the input voltage V_{INP} is less than V_{INN} , the circuit works vice versa.

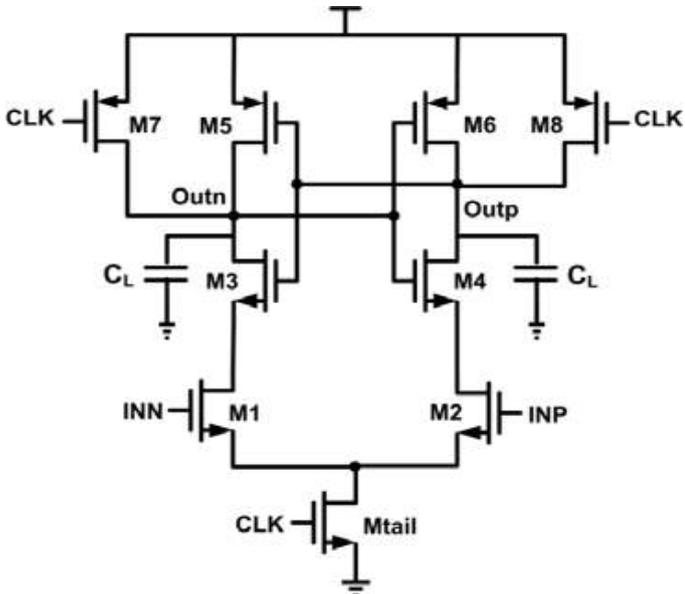


fig1. Conventional Dynamic Comparator

Though the comparator has number of advantages, it has also got a disadvantage. As the design have several stacked transistors, it needs a high supply voltage for its operation. Thus this comparator cannot be used in applications where the supply voltage is small.

III. CONVENTIONAL DOUBLE TAIL COMPRATOR

The schematic diagram of conventional double tail comparator is shown in the fig 2. The design shown has less stacking and therefore can operate at lower supply voltages. Thus this structure is efficient than the conventional dynamic comparator.

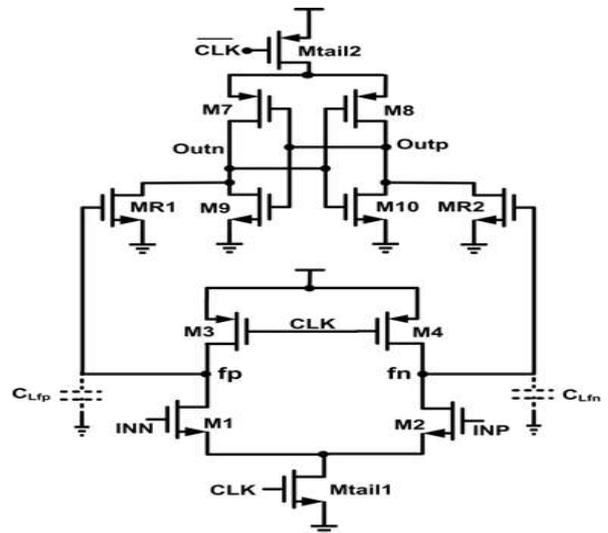


Fig.2 Conventional Double Tail Comparator

The double tail comparator has a wider M_{tail2} which enables a large current in the latching stage. Thus fast latching takes place which is independent of the input common mode voltage (V_{cm}). Because of smaller M_{tail1} , small current flows in the input stage, which is required for low offset.

The operation of the conventional double tail comparator is described below.

During reset phase, when $CLK=0$, transistors M_{tail1} and M_{tail2} are off, the transistors M_3 and M_4 precharge the nodes fn and fp to V_{DD} . This makes transistors M_1 and MR_2 to discharge output nodes $Outn$ and $Outp$ to ground.

During comparison phase when $CLK = V_{DD}$, transistors M_{tail1} and M_{tail2} get switched ON. The transistors M_3, M_4 turn off and thus the voltages at nodes fn , fp start to drop with the rate defined by $I_{M_{tail1}}/C_{fn(p)}$ and an input-dependent differential voltage $\Delta V_{fn(p)}$ builds up. the transistors MR_1 and MR_2 forms the intermediate stage that passes $\Delta V_{fn(p)}$. Thus providing a good shielding between input and output so as to get a reduced value of kickback noise.

Various advantages of this structure are, it does not require boosted voltage or stacking of too many transistors, Separate designing of input and cross coupled stage results in faster operation that results in power savings.

During reset phase, nodes fn and fp have to be charged from ground to V_{dd} which means more power consumption, which is undesirable.

IV. PROPOSED DOUBLE TAIL COMPARATOR

The schematic diagram of the proposed double tail comparator is shown in fig.3. The proposed double tail comparator is designed by modifying the existing double tail comparator as it performs well when the supply voltage is small.

V. SIMULATION RESULTS

The various comparator architecture are simulated using microwind simulation tool

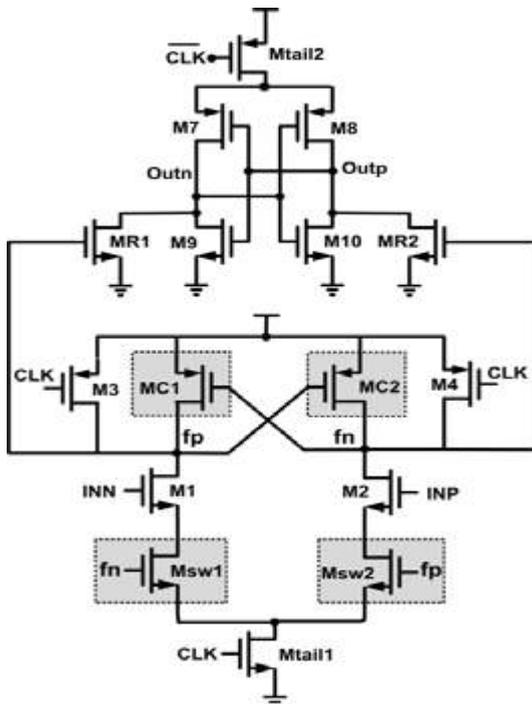


Fig.3. Proposed Double Tail Comparator

The total power consumption in the circuit is greatly reduced in this circuit. For this, two switching transistors M_{n1} and M_{n2} are added to the second stage in series with M_1 and M_2 transistors.

The operation of the proposed double tail comparator is as follows. During the reset phase $CLK = 0$ transistors M_{tail1} and M_{tail2} are off, thus avoiding static power. Transistors M_3 and M_4 pull nodes f_n and f_p to V_{DD} . MR_1 and MR_2 are the intermediate transistors that reset both output latches to ground.

During comparison phase when $CLK = V_{DD}$, transistors M_{tail1} and M_{tail2} are switched ON and transistors M_3 and M_4 are turned OFF, since f_n and f_p are precharged to V_{DD} . According to the input voltages the output nodes f_n and f_p start to drop with different rates. Assume that $V_{INP} > V_{INN}$ then f_n drops faster than f_p , as transistor M_2 provides more current than transistor M_1 . As f_n continues to fall, the corresponding PMOS transistor M_3 starts to turn on, thereby pulling f_p node back to the V_{DD} , thus another transistor M_4 remains off. This allows f_n to get completely discharged. Thus in the proposed double tail comparator as soon as the comparator detects that for example node f_n discharges faster, the PMOS transistor M_3 gets ON, thereby pulling other node f_p back to V_{DD} . This is very unlikely to the conventional double tail comparator, in which $\Delta V_{fn/fp}$ is a function of input voltage difference and input transistor transconductance. Thus with the passage of time, the difference between f_n and f_p ($\Delta V_{fn/fp}$) increases exponentially and hence reducing the latch regeneration time.

Thus in the proposed structure, the average power consumption of the circuit is reduced when compared to the existing double tail comparator.

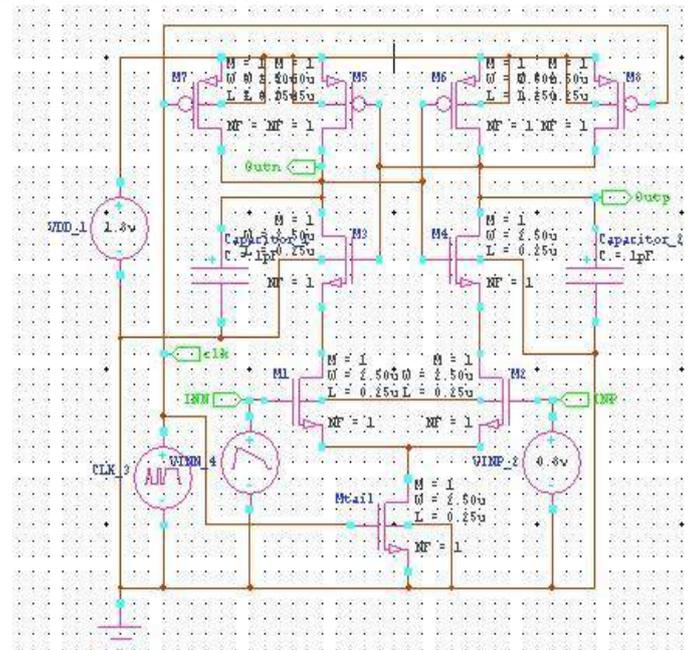


Fig.4 Design Of Conventional Comparator

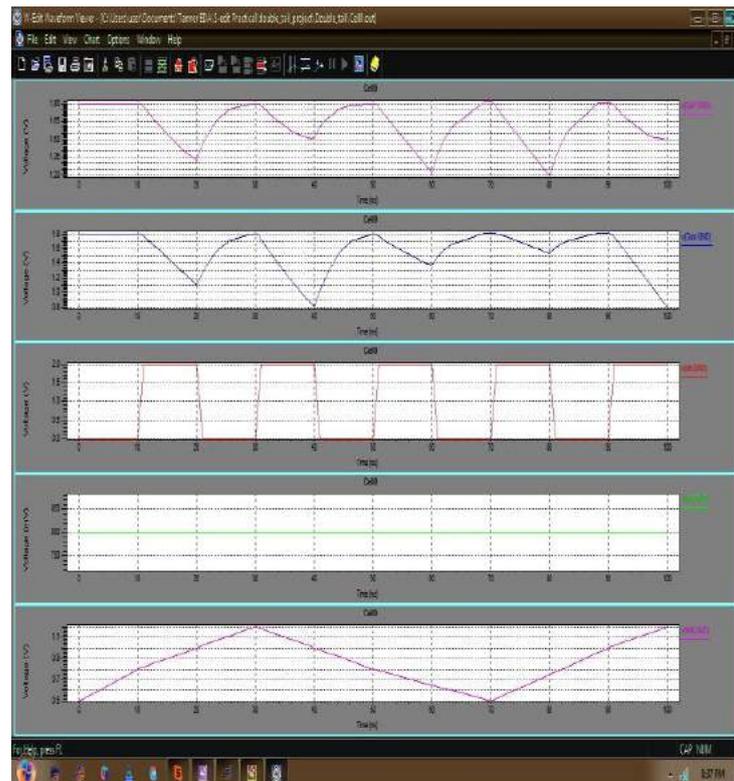


Fig.5 Simulation results for conventional comparator

VI. CONCLUSION

In this paper, an efficient design of double tail comparator is proposed. From the simulated results it is found that the delay is lesser in conventional double tail comparator as compared to the conventional dynamic comparator. Also from the study of the proposed design it is observed that it will consume less power than the existing comparators. Hence the proposed double-tail comparator can be used for the design of high speed applications that require low power.

REFERENCES

- 1] S. Babayan-Mashhadi and R. Lotfi, "Analysis and design of low voltage low power double tail comparator," *IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS*, VOL.22, No.2, FEBRUARY 2014.
- 2] B. Goll and H. Zimmermann, "A comparator with reduced delay time in 65-nm CMOS for supply voltages down to 0.65," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 56, no. 11, pp. 810–814, Nov. 2009.
- 3] S. U. Ay, "A sub-1 volt 10-bit supply boosted SAR ADC design in standard CMOS," *Int. J. Analog Integr. Circuits Signal Process.*, vol. 66, no. 2, pp. 213–221, Feb. 2011
- 4] D. Shinkel, E. Mensink, E. Klumperink, E. van Tuijl, and B. Nauta, "A double-tail latch-type voltage sense amplifier with 18ps Setup+Hold time," in *Proc. IEEE Int. Solid-State Circuits Conf., Dig. Tech. Papers*, Feb. 2007, pp. 314–315
- 5] Masaya Miyahara, Akira Matsuzava, "A Low-Offset Latched Comparator Using Zero-Static Power Dynamic Offset Cancellation Technique," *IEEE A Solid-state Circuits*, Vol. 56, no. 5, pp. 911-919, May 2009.
- 6] B. Goll and H. Zimmermann, "Low-power 600MHz comparator for 0.5 V supply voltage in 0.12 μm CMOS," *IEEE Electron. Lett.*, vol. 43, no. 7, pp. 388–390, Mar. 2007

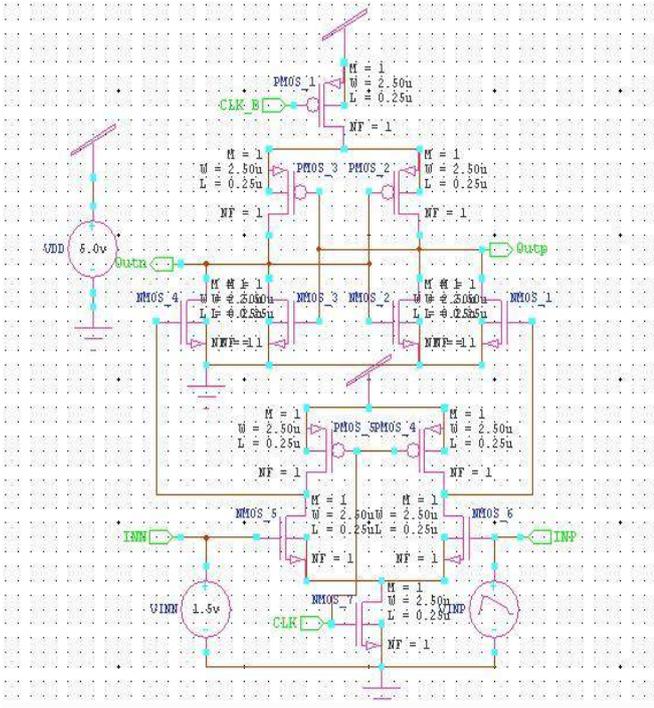


Fig.6 Design Of Conventional Double Tail Comparator

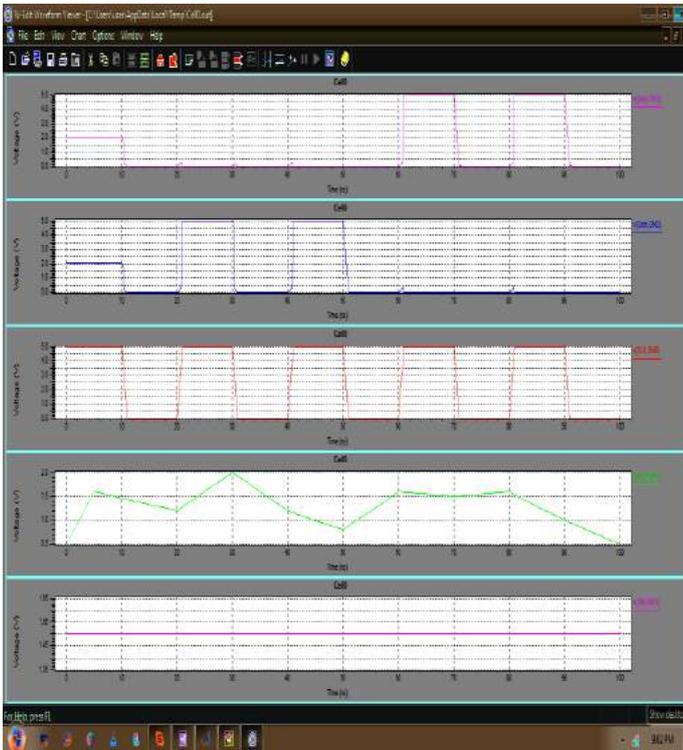


Fig.7 Simulation Results of Conventional Double Tail Comparator



Implementation of Rijndael Algorithm Using VHDL

¹Manisha Mankar, ²Dr. R. V. Kshirsagar, ³M. V. Vyawahare
¹Student of M.Tech, Electronics Department, ²Principal, ³Professor
^{1,3}Priyadarshini college of Engineering, ²P.I.G.C.O.E.T, Hingna, Nagpur, India.
¹manshree379@gmail.com, ²ravi_kshirsagar@yahoo.in, ³mvvyawahare@yahoo.in

Abstract— For the secured transmission of data, many cryptographic algorithms are in use. It enables us to transmit the sensitive information across insecure networks so that unauthorized persons cannot access it. Rijndael represents an algorithm for advanced encryption standard consists of different operations required in the steps of encryption and decryption. The design uses lookup table implementation of S-box with block size of 128 bits and key size of 192 bits. This gives low complexity architecture and easily achieves low latency as well as high throughput. Simulation results are generated and compared with previous reported designs. Quartus II Modelsim Project Navigator is used for synthesis and simulation of this proposed architecture purpose. Implementation of Encryption and Decryption, also known as Rijndael Algorithm which has been selected a new algorithm by the National Institute of Standards and Technology (NIST) as US FIPS 197 in November 2001 after a 5-year standardization process.

Keywords—Rijndael; cryptography; key; encryption; decryption; VHDL.

I. INTRODUCTION

Rijndael algorithm is an efficient cryptographic technique consists of different operations in iterative looping approach in order to minimize hardware consideration, with block size of 128 bit, lookup table implementation of S-box. It includes generation of ciphers for encryption and inverse ciphers for decryption by performing four rounds of transformations by 192 bit key size cipher

On October, 2, 2000, The National Institute of Standards and Technology (NIST) announced Rijndael as the new Encryption Standard. The Predecessor to the encryption standard was Data Encryption Standard (DES) which was considered to be insecure because of its vulnerability to brute force attacks. DES was a standard from 1977 and stayed until the mid 1990's. However, by the mid 1990s, it was clear that the DES's 56-bit key was no longer big enough to prevent attacks mounted on contemporary computers, which were thousands of times more powerful than those available when the DES was standardized. The Rijndael is a 128 bit Symmetric block Cipher.

This paper includes the complete step by step implementation Rijndael Technique, i.e. encrypting and decrypting 128 bit data using the Rijndael algorithm and its modification for enhanced reliability and security. The encryption process

consists of the combination of various classical techniques such as substitution, rearrangement and transformation encoding techniques. The encryption and decryption modules include the Key Expansion module which generates Key for all iterations. The modifications include the addition of an arithmetic operation and a route transposition cipher in the attacks iterative rounds. The Key expansion module is extended to double the number of iterative processing rounds in order to increase its immunity against unauthorized attacks.

II. RIJNDAEL ALGORITHM

Rijndael algorithm is the winner of the contest, held in 1997 by the US Government, after the Data Encryption Standard was found too weak because of its small key size & the technological advancements in processor power. Fifteen candidates were accepted in 1998 and based on public comments the pool was reduced to five finalists in 1999. In October 2000, one of these five algorithms was selected as the forthcoming standard: a slightly modified version of the Rijndael.

The Rijndael, whose name is based on the names of its two Belgian inventors, Joan Daemen and Vincent Rijmen, is a Block cipher, which means that it works on fixed-length group of bits, which are called blocks. It takes an input block of a certain size, usually 128, and produces a corresponding output block of the same size. The transformation requires a second input, which is the secret key.

It is important to know that the secret key can be of any size (depending on the cipher used) and that encryption standard uses three different key sizes: 128, 192 and 256 bits. While Encryption standard supports only block sizes of 128 bits and key sizes of 128, 192 and 256 bits, the original Rijndael supports key and block sizes in any multiple of 32, with a minimum of 128 and a maximum of 256 bits.

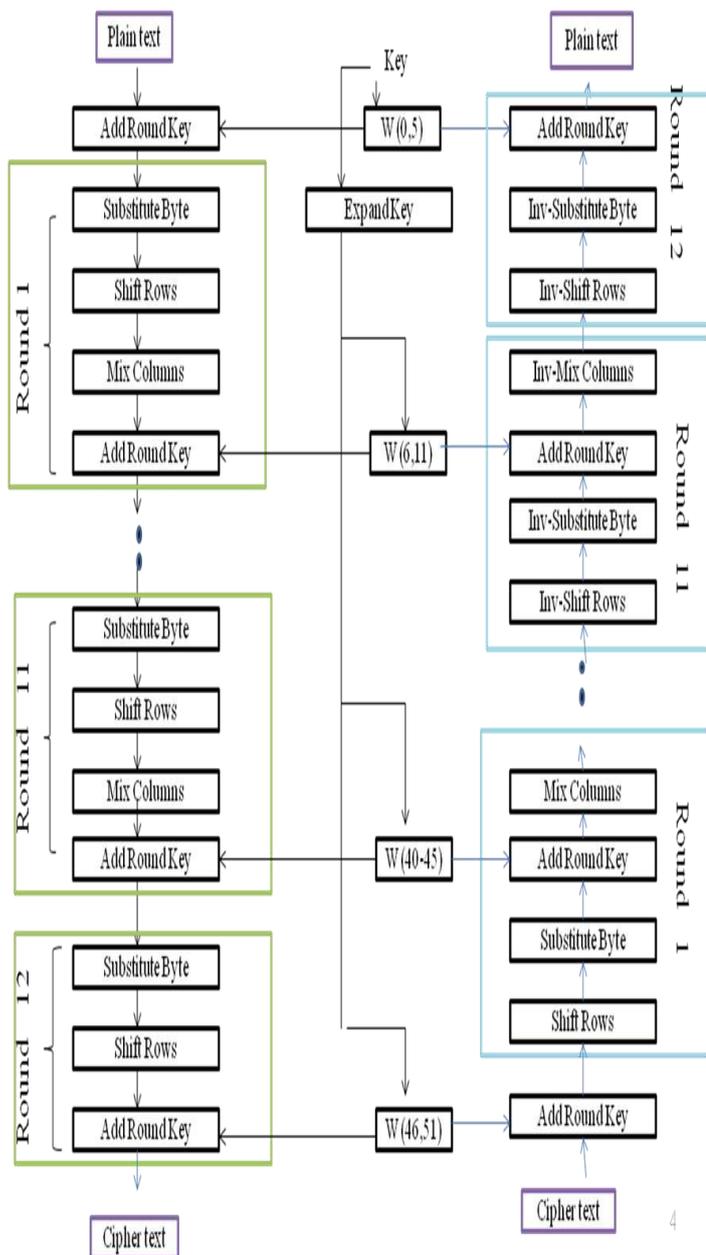


Fig1: Complete Rijndael Encryption and Decryption process

A. Algorithm Specification

Rijndael is an iterated block cipher with a fixed block size of 128 and a variable key length. The different transformations operate on the intermediate results, called state. The state is a rectangular array of bytes and since the block size is 128 bits, which is 16 bytes, the rectangular array is of dimensions 4x4. (In the Rijndael version with variable block size, the row size is fixed to four and the number of columns varies. The number of columns is the block size divided by 32 and denoted Nb). The cipher key is similarly pictured as a rectangular array with four rows. The number of columns of the cipher key, denoted Nk, is equal to the key length divided by 32.

It is very important to know that the cipher input bytes are mapped onto the state bytes in the order $S_{0,0}, S_{1,0}, S_{2,0}, S_{3,0}$,

$S_{0,1}, S_{1,1}, S_{2,1}, S_{3,1} \dots$ and the bytes of the cipher key are mapped onto the array in the order $k_{0,0}, k_{1,0}, k_{2,0}, k_{3,0}, k_{0,1}, k_{1,1}, k_{2,1}, k_{3,1} \dots$. At the end of the cipher operation, the cipher output is extracted from the state by taking the state bytes in the same order. Rijndael uses a variable number of rounds, which are fixed: A key of size 128 has 10 rounds. A key of size 192 has 12 rounds. A key of size 256 has 14 rounds.

Table 1: Key/Block/Round Size

Type	Key length (Nk words)	Block Size (Nb Words)	Number of Rounds (Nr words)
Rijndael-128	4	4	10
Rijndael-192	6	4	12
Rijndael-256	8	4	14

The complete assembly of Rijndael can be grasped through fig: 1. The input is just a single data of 128 bit for the purpose of decryption & encryption and is recognized as the in dimension plain text is of as a 128 bit and key is of 192 bit square dimension of bytes. This key is later expanded into a dimension of key schedule words (32 bits) (the w matrix). It need to be noted that the during of bytes within the in matrix is by column. The same is applicable to the w dimension. During each round.

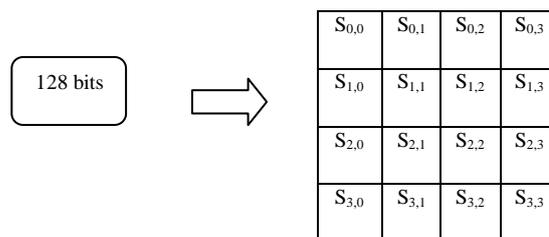


Fig 2 (a) Conversion of 128 bits data to state array

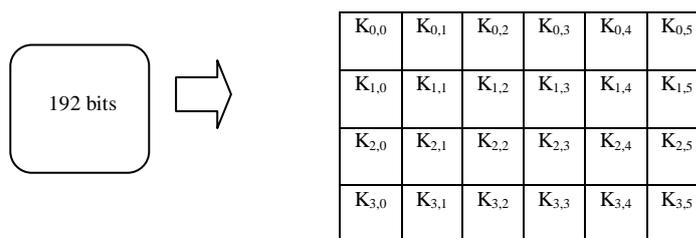


Fig 2(b) Conversion of 192 bits data of key in matrix

The four bytes in each column of the state array form 32 bit words, where the row number r provides an index for the four bytes within each word. For ex. state can be considered as an array of four words ($W_0 - W_3$) and key length of four as-

$$W_0 = S_{0,0}, S_{1,0}, S_{2,0}, S_{3,0} \quad W_2 = S_{0,2}, S_{1,2}, S_{2,2}, S_{3,2}$$

$$W_1 = S_{0,1}, S_{1,1}, S_{2,1}, S_{3,1} \quad W_3 = S_{0,3}, S_{1,3}, S_{2,3}, S_{3,3}$$

For 192 bit key, state considered as an array of six words ($W_0 - W_5$) so that's why the key length is represented by $Nk = 6$ by

$$W_0 = K_{0,0}, K_{1,0}, K_{2,0}, K_{3,0} \quad W_2 = K_{0,2}, K_{1,2}, K_{2,2}, K_{3,2}$$

$$W_1 = K_{0,1}, K_{1,1}, K_{2,1}, K_{3,1} \quad W_3 = K_{0,3}, K_{1,3}, K_{2,3}, K_{3,3}$$

$$W_4 = K_{0,4}, K_{1,4}, K_{2,4}, K_{3,4} \quad W_5 = K_{0,5}, K_{1,5}, K_{2,5}, K_{3,5}$$

After an initial round key addition, the state array is transformed by implementing a round function depending on the key length ,with the final round differing slightly from the first $Nr-1$ rounds. The final state is copied to the output .The round function is parameterized using a key schedule that consists of a one-dimensional array of four – byte words derived using the key expansion routine.

B. Rijndael Encryption Process

The algorithm initiates from Add round key process followed by total of 11 iterations of four transformations and the 12th iteration of 3 transformations. This is applicable for both encryption and decryption . Four transformations used are as given below :

1. Add Round Key
2. Shift rows
- 3 Subbyte
4. Mix column

The 12th iteration just doesn't use the Mix Columns transformation. Different key for each round and derived from the Rijndael key schedule Salient Features:

- The cipher key is expanded into a larger key, which is later used for the actual operations
- The round Key is added to the state before starting the with loop
- The Final Round () is the same as Round (), apart from missing the Mix Columns () operation.
- During each round, another part of the Expanded Key is used for the operations
- The Expanded Key shall always be derived from the Cipher Key & never be specified directly.

Rijndael Operations

1. The AddRoundKey operation:

In this operation, a Round Key is applied to the state by a simple bitwise XOR. The Round Key is derived from the Cipher Key by the means of the key schedule.The Round Key length is equal to the block key length (=24bytes).A 16 byte state matrix and 24 byte key matrix results 16 byte cipher matrix representation is shown as follows:Input state matrix XOR with key size matrix ,result is new state matrix.Each round key consist of Nb wordsfrom round key. Nb words are added to the column of the state we get

$$[S'_{0,0} \ S'_{1,0} \ S'_{2,0} \ S'_{3,0}] = [S_{0,0} \ S_{1,0} \ S_{2,0} \ S_{3,0}] \text{ xor } [W_{\text{round} * Nb + c}]$$

for $0 < c < Nb$

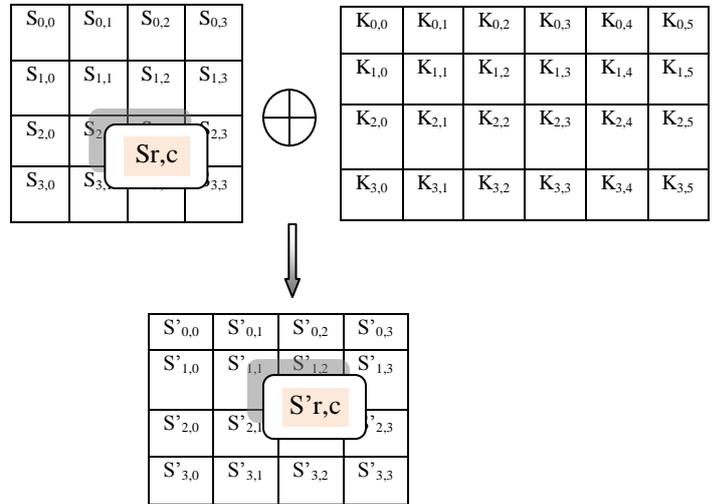


Fig.3: Add Round Key Operation

2. The ShiftRow operation:

In this operation, each row of the state is cyclically shifted to the left, depending on the row index.

- The 1st row is shifted 0 positions to the left.
- The 2nd row is shifted 1 position to the left.
- The 3rd row is shifted 2 positions to the left.
- The 4th row is shifted 3 positions to the left.

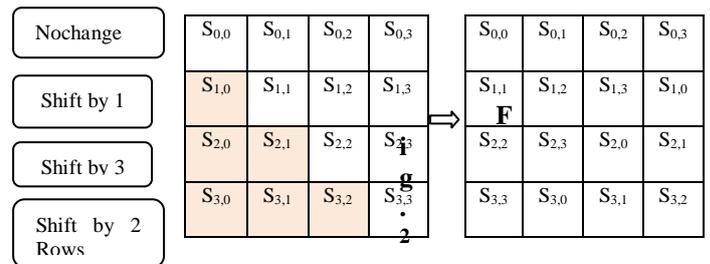


Fig.4: Shift-Operation

3. SubBytes operation:

The SubBytes operation is a non-linear byte substitution, operating on each byte of the state independently. The substitution table (S-Box) is invertible and is constructed by the composition of two transformations:

1. Take the multiplicative inverse in Rijndael's finite field
2. Apply an affine transformation which is documented in the Rijndael documentation.

Since the S-Box is independent of any input, pre-calculated forms are used. Each byte of the state is then substituted by the value in the S-Box whose index corresponds to the value in the state:

$$a(i,j) = SBox[a(i,j)]$$

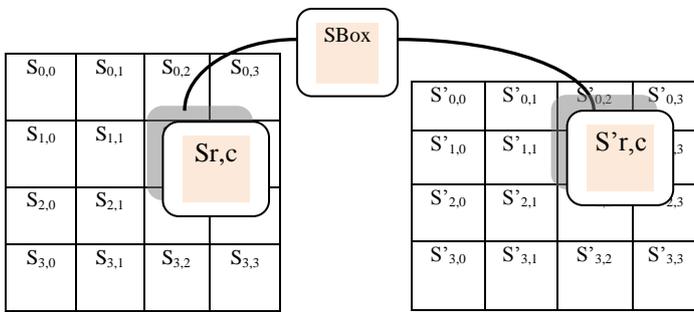


Fig 5 : SubBytes () applies SBox to each byte of the State

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Fig 7: Mixcolumn () operates on state column-by-column

SBox used in SubByte() transformation in hexadecimal form

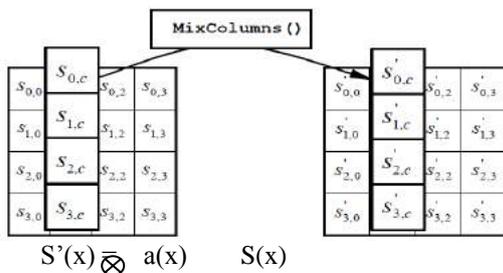
		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig 6 SBox: Substitution values for byte xy (in hexadecimal format)

For Example: If $S_{1,2} = \{89\}$ then substitution value is determined by intersection of row with index '8' and column with index '9', the result in $S'_{1,2}$ is $\{a7\}$.

4. The MixColumn Operation:

Mixcolumn operates on the state column by column, treating each column as four term polynomial. The columns are considered as polynomials over $GF(2^8)$ and multiplied modulo $x^4 + 1$ with fixed polynomial $a(x)$ as $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + 01$



For Example:

lets take the first column of a matrix to be $s_{0,0} = \{87\}$, $s_{1,0} = \{6E\}$, $s_{2,0} = \{46\}$, $s_{3,0} = \{A6\}$.

$$(02 \cdot 87) (03 \cdot 6E) 46 A6 = 47$$

Inversr MixColumn() is inverse of MixColumn () transformation.

$$S'(x) = \text{inv } a(x) \otimes S(x)$$

C. Rijndael Decryption Process

For decryption the same process occurs simply in reverse order taking the 128-bit block cipher text and converting back into plaintext by application of inverse of four operation. Addround key is same for both encryption and decryption this process in the inverse of encryption process. The last round values of both data and key are the first round inputs for the decryption process and follows in decreasing order.

III. The Rijndael Key Schedule

- The Key Schedule is responsible for expanding a short key into a larger key, whose parts are used during the different iterations. Each key size is expanded to a different size:
 - 128 bit key is expanded to an 176 byte key.
 - An 192 bit key is expanded to an 208 byte key.
 - An 256 bit key is expanded to an 240 byte key.
- There is a relation between the cipher key size, the number of rounds and the Expanded Key size. For an 128-bit key, there is one initial AddRoundKey operation plus there are 10 rounds and each round needs a new 16 byte key, therefore we require 10+1 Round Keys of 16 byte, which equals 176 byte. The same logic can be applied to the two other Cipher key sizes. The general formula is that:

$$\text{Expanded Key Size} = (\text{nbrRounds} + 1) * \text{Block Size}$$

Table 2: Expanded Key Size in Bytes

Key Size (Bytes)	Block Size (Bytes)	Expansion Algorithm Rounds	Rounds Key Expansion	Expanded Key(Bytes)
16	16	44	40	176
24	16	52	46	208
32	16	60	52	240

The Rijndael key extension calculation takes input as a 6-word key and crops a direct cluster of 52 words (32 bits). Every one round uses 4 of these words. Each one expression holds 32 bytes which implies each one sub key is 192 bits in length. The key is duplicated into the initial four expressions of the stretched key. The rest of the stretched key is packed in 4 words at once. Each one included word $w[i]$ hinge on the promptly going before word, $w[i - 1]$, and the expression 4 places back $w[i - 4]$. In 3 out of 4 cases, upfront XOR is utilized. For a statement whose location in the w exhibit is a numerous of four, a more random capacity is utilized.

- RotWord just rotates the word data by a one-byte round left movement. This implies that a data word $[a_0, a_1, a_2, a_3]$ is changed into $[a_1, a_2, a_3, a_0]$.
- SubWord substitutes every bytes of the word using byte substitution method, utilizing the S-box portrayed prior.
- The consequence of above processes is bitwise XORed with round constant, known as $Rcon[j]$. The round constant (RCON) is a word (32 bit) which has the 3 right hand-side bytes are zero every time. Therefore, the result of an XOR of the word with Rcon is just only to achieve an XOR on the left hand-side byte of word. The round constant is dissimilar for each iteration and is well-defined as $Rcon[j] = (Rc[j] / 000)$ with $Rc[1]=1$, $Rc[j] = 2 * Rc[j-1]$ and multiplication is done over the GF (2^8).
- The key expansion remained intended to be impervious to recognized cryptanalytic assaults. The consideration of a round-needy round steady dispenses with the symmetry, or comparability, between the courses in which adjust keys are produced in diverse iterations. Schedule uses the same S-Box substitution as the main algorithm body.

IV. RESULTS

FPGA was designed as shown for the purpose of encryption and decryption using Rijndael algorithm. Here we have provided plain text of unknown length. We can clearly see the cipher text in fig. 8 and the decipher text in fig.11 as generated.

- **Encryption Result**

Input Plaintext – 0101 0010
 Key – 0110 1000
 Output CipherText – 0011 1010

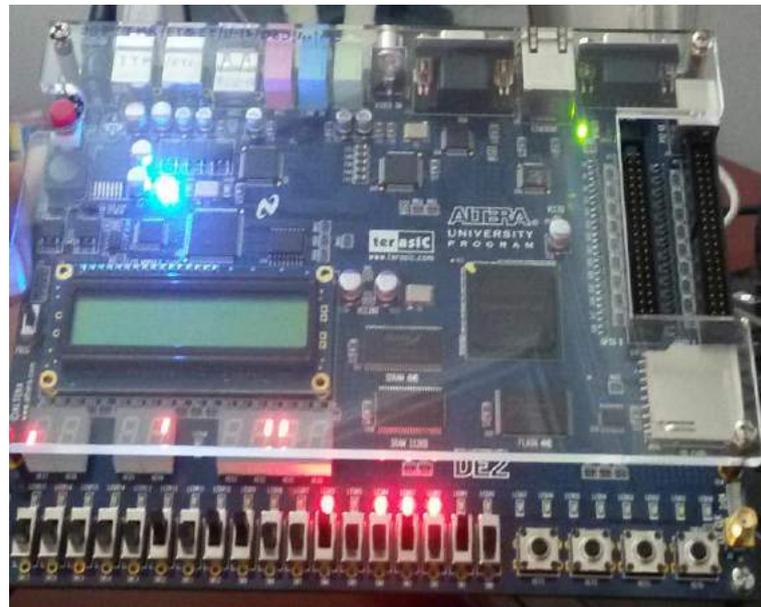


Fig 8: Implementation of Encryption Result on FPGA

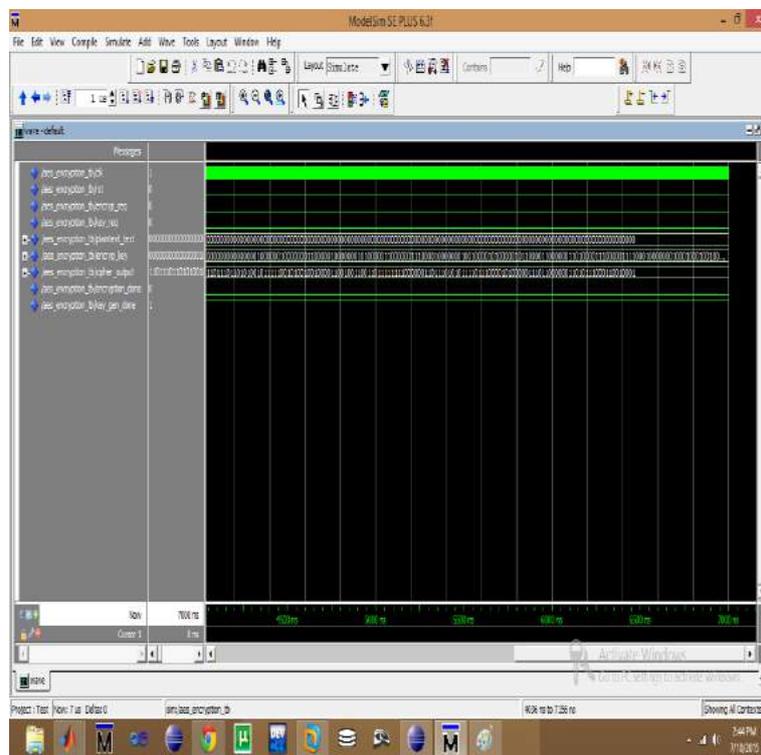


Fig 9: Waveforms of Encryption Process

The above figure 9 signifies the waveforms produced by encryption process. plaintext 128-bits state input and 192 bit key is used whose outcome is encrypted as described in Rijndael algorithm. We get Ciphertext output by encryption process.

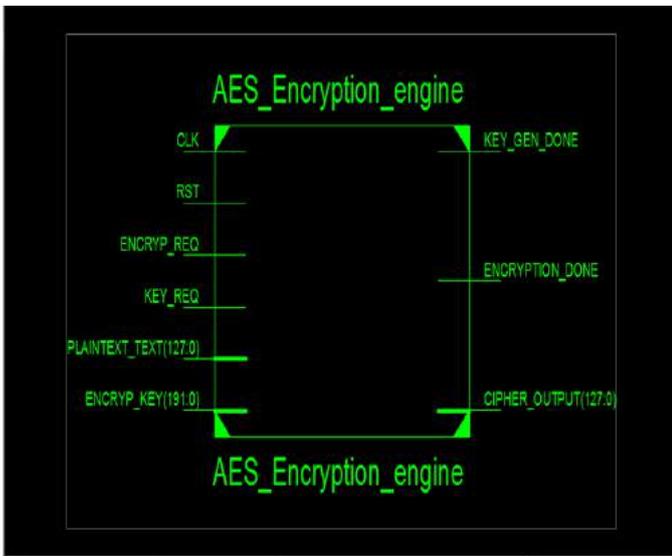


Fig 10: RTL Schematic of Encryption process

Rijndael Encryption architecture takes 128 bits of data as input along with the 192 bits of key along with control signal clk, reset signal each of single bit. The block diagram of the Rijndael Encryption block is provided above in fig.10, gives the 128 bit Cipher output when Encryption Done = 1.

- **Decryption Result**

Input Cipher Text – 0011 1010

Key – 0110 1000

Output Plaintext – 0101 001

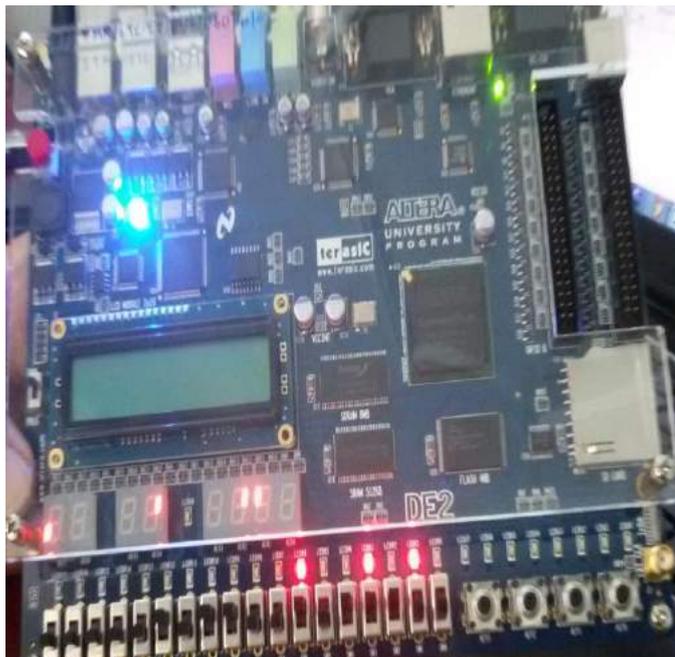


Fig 11: Implementation of Decryption Result on FPGA

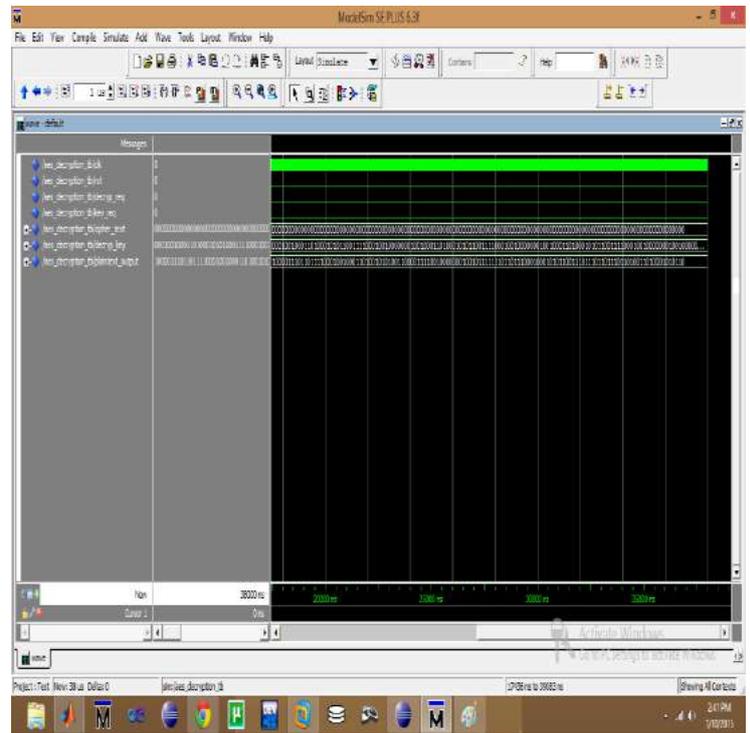


Fig 12: Waveforms of Decryption Process

The above figure 12 signifies the waveforms produced by the 128-bit Decipher and its block architecture. 128-bit state as a std_logic_vector whose outcome is decrypted as described in Rijndael algorithm.

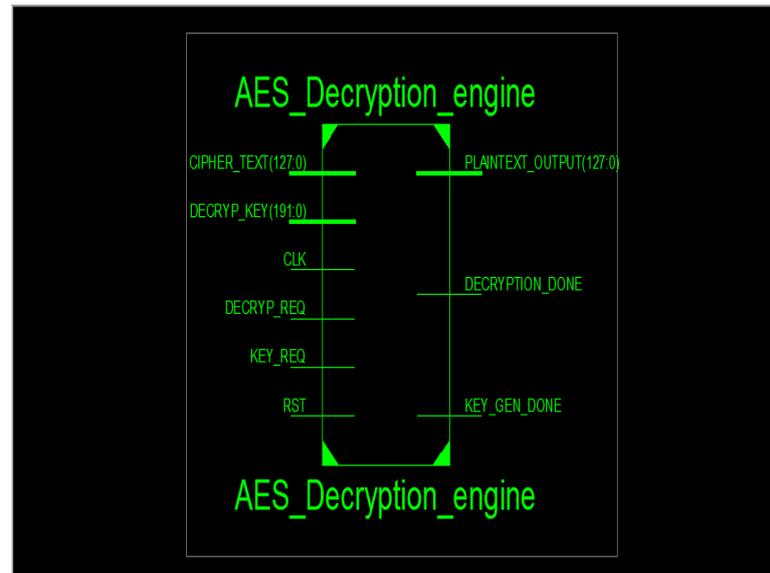


Fig 13: RTL Schematic of Decryption process

Inside of Rijndael comprises of Cipher block and a Decipher block. Cipher block is connected to decipher block Cipher block takes all the input provided to Rijndael block and give us a Cipher Text of 128 bits as output. Cipher block controls the processing of decipher block, it keeps the decipher block in wait state unless it is ready with the cipher text., Decipher block takes the cipher text as input 128 bit and provide us the

decipher text 128 bit which would be exactly similar to the input data with 192 bit decryption key and control signals clk and reset.

V. CONCLUSION

Rijndael Algorithm is an iterative symmetric block cipher that can process data blocks of 128 bits through the use of cipher keys with lengths of 128, 192 and 256 bits.

An FPGA implementation of 128 bit using block and 192 bit key Rijndael Algorithm design is implemented on Altera Quartus II ,Optimized and Synthesizable VHDL code is developed for the implementation of both 128 bit data encryption and decryption process & description is verified using modelsim functional simulator from Altera Quartus II. All the transformations of algorithm are simulated using an iterative design approach in order to minimize the hardware consumption. Each program is tested with some of the sample vectors provided by NIST. The throughput reaches the value of 2Gbps and frequency 580.948MHz for both encryption and decryption process with device cyclone II EP2C35F672C6 of Altera Quartus II.

REFERENCES

- [1] Mazen El Maraghy,SalmavHesham &Mohamed A.El Ghany"Real – Time FPGA Implementation of AES Algorithm"978-1-4799-1166-0/13,2013,IEEE
- [2] Bin Liu, Student Member, IEEE, and Bevan M. Baas, Senior Member, IEEE; "Parallel AES Encryption Engines for Many-Core Processor Arrays", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 3, MARCH 2013
- [3] Kamalika Datta ,Vishal Shrivastav ,Indranil Sengupta, Hafizur Rahaman "Reversible Logic Implementation of AES Algorithm"8th international conference on design & technology Integrated systems in nanoscale era,978-1-4673-6040-1/13/\$31.00,2013 IEEE.
- [4] N.Anitha Christy and P.Karthigaikumar "FPGA implementation of AES algorithm using Composite Field Arithmetic "International conference on devices circuits and systems,978-1-4577-1546-4/12/\$26.00,2012 IEEE
- [5] Hong Trang;Nguyen Van Loi;"An efficient FPGA implementation of the advanced Encryption Standard algorithm"978-1-4673-0309-5/12,2012,IEEE..
- [6] Nabihah Ahmad, N.; Hasan, R.; Jubadi, W.M; "Design of AES S-Box using combinational logic optimization", IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699, 31.00,2010 IEEE.
- [7] Alex panato Marcelo Barcelos,Ricardo Reis "An IP of an Advanced Encryption Standard For Altera Devices", IEEE Symposium on Integrated circuits and systems Design (SBCCI'02)0-7695-1807-9/02,2002, IEEE.
- [8] Borkar"FPGA Implementation of AES Algorithm"978-1-4244-8679-3/11,2011,IEEE
- [9] Hrushikesh S.Deshpand, Kailash J.Karande, Altaaf O.Mulani "Efficient Implementation Of AES Algorithm on FPGA" International Conference on Communication and Signal Processing, April 3_5,2014,IEEE.
- [10] Girish Kumar P, Mahesh Kumar "Implementation of AES algorithm using verilog" International Journal of VLSI and Embedded Systems,vol-4,Article 05090;june 2013
- [11] Hrushikesh S.Deshpand, Kailash J.Karande, Altaaf O.Mulani "Efficient Implementation Of AES Algorithm on FPGA" Progress In Science in Engineering Research Journal ,PISER 11,vol.02,ISSN 2347-6680 (E),2014.
- [12] Vijaya Kumar.B, T.Thammi Reddy "Fpga Implementation of High speed AES Algorithm For Improving The System Computing speed" International Journal of Computer trends and Technology(IJCTT)-VOLUME 4 Issue 9-Sep 2013.
- [13] J. Nechvatal , Report on the development of Advanced Encryption Standard, NIST Publication, Oct,2000.
- [14] J. Daemen and V Rijmen, "AES Proposal: Rijndael", AES Algorithm Submission, September 3, 1999.
- [15] National Institute of Standards and Technology (NIST), Data Encryption Standard (DES), National Technical Information Service, Spring field, VA 22161, Oct. 1999.
- [16] N Radhika, Obili Ramesh, Priyadarshini, "Design and Verification of Area-Optimized AES Based on FPGA using verilog HDL"International Journal of Engineering Trends and Technology-volume 4 Issue9-Sep 2013
- [17] Manoj.B,Manjula N Harihar"Image Encryption & Decryption using AES"International Journal of Engineering & Advanced Technology,ISSN:2249-8958,Volume-Issue-5,June 2012
- [18] Reshma Nadaf,Veena Desai"Hardware Implementation of Modified AES with Key Dependent Dynamic S-Box



S-Box Implementation of AES-192

Priti Mankar

*Student of M.E Electronics Department
PIIT New Panvel
Navi Mumbai, India
pmankar@mes.ac.in*

Prof.R.H.Khade

*Electronics Department
PIIT New Panvel
Navi Mumbai, India
rhhade@mes.ac.in*

Abstract— Now a day, secure transmission of data is the biggest challenge in communication. AES is a cryptographic algorithm enables us to transmit the sensitive information across insecure networks so that unauthorized persons cannot access it. It consists of different operations in iterative looping approach in order to minimize hardware consideration. The design uses lookup table implementation of S-box with block size of 128 bits and key size of 192 bits. This gives low complexity architecture and easily achieves low latency as well as high throughput. Simulation results are generated and compared with previous reported designs. Xilinx ISE 14.2 Project Navigator is used for synthesis and simulation of this proposed architecture purpose.

Keywords—AES; decipher; key expansion; cipher; VHDL; FPGA.

I. INTRODUCTION

For a long time, the Data Encryption Standard (DES) was considered as a standard for the symmetric key encryption. DES has a key length of 56 bits. However, this key length is currently considered small and can easily be broken. In October 2000, the Rijndael algorithm was approved by the National Institute of Standards and Technology (NIST) as the Advanced Encryption Algorithm (AES) providing strong security and high flexibility.

AES can be specified with key and block sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits. Therefore, the problem of breaking the key becomes more difficult [1]. In cryptography, the AES is also known as Rijndael [2]. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits. The proposed implementation supports the AES-192 Encryption and Decryption.

This paper is organized as follows. Section II is a brief description of the AES cryptographic algorithm. In section III AES algorithm process is described. Then section IV presents simulation results and section V, VI describes conclusion and future scope.

II. AES ALGORITHM

The AES algorithm, developed by Joan Daemen and Vincent Rijmen was selected as the winner of the AES development process in October 2000. The advanced Encryption Standard (AES) algorithm is a symmetric block cipher that processes data blocks of 128 bits using three different cipher key lengths 128, 192 or 256 bits. Based on the key length used, the number of execution rounds of the algorithm is 10, 12 or 14 respectively. The proposed implementation supports the AES-192 encryption.

The algorithm is composed of three main parts: Cipher, Inverse Cipher and Key Expansion. Cipher converts data to an unintelligible form called cipher text or encrypted data while Inverse Cipher converts data back into its original form called plaintext or decrypted data. Key expansion generates a Key Schedule that is used in Cipher and Inverse Cipher procedure.

The 128 data bit as well as 192 bit cipher key are formulated into a 4×4 state matrix and 4×6 key matrix respectively. At the start of the algorithm, the state matrix is initialized with the original plaintext while the key matrix is initialized with the input master key. The basic unit of AES algorithm process is a byte.

Table 1: Key/Block/Round Size

AES Types	Block Size Nb words	Key Length Nk words	Number of Rounds Nr
AES 128-bits key	4	4	10
AES 192-bits key	4	6	12
AES 256-bits key	4	8	14

AES can be implemented in many languages i.e. Matlab, C, Java and VHDL. The AES algorithm is basically used in ATM machines for security of transactions and Windows Vista fault analysis program software to provide configuration file

security. It is used in broad applications including smart cards and cellular phones, WWW servers and automated teller machines, and digital video recorders.

III. AES PROCESS

The AES block structure is as shown in following figure

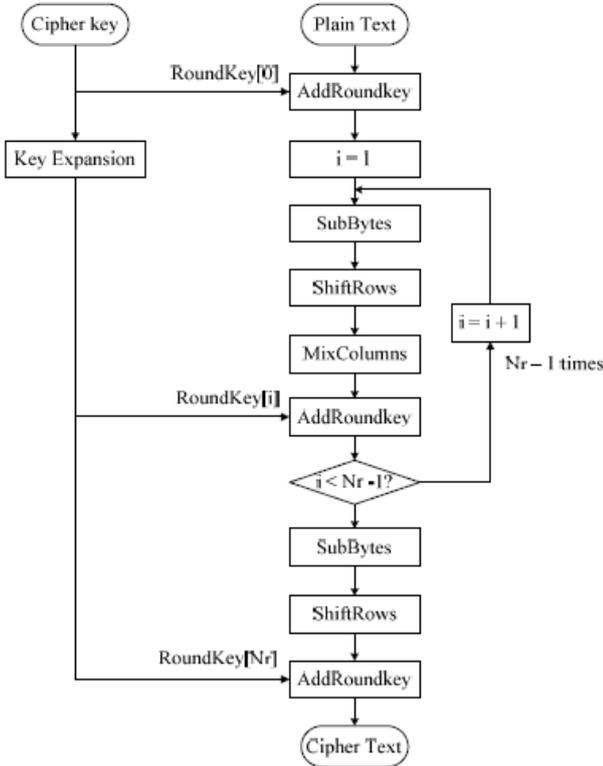


Fig1: AES Encryption and Decryption process

Each round consists of mainly four transformations: for Encryption they are SubByte, ShiftRow, MixColumn and Addroundkey, similarly for Decryption they are InvSubByte, InvShiftRow InvMixColumn and Addroundkey.

A. SubByte transformation :

The SubBytes transformation is a non-linear byte substitution, operating on each of the state bytes independently. The SubBytes transformation is done using a once-precalculated substitution table called S-box. That S-box table contains 256 numbers (from 0 to 255) . In this design, we use a look-up table as shown in Table I. This is a more efficient method than directly implementing the multiplicative inverse operation followed by affine transformation.

Encryption S-Box:

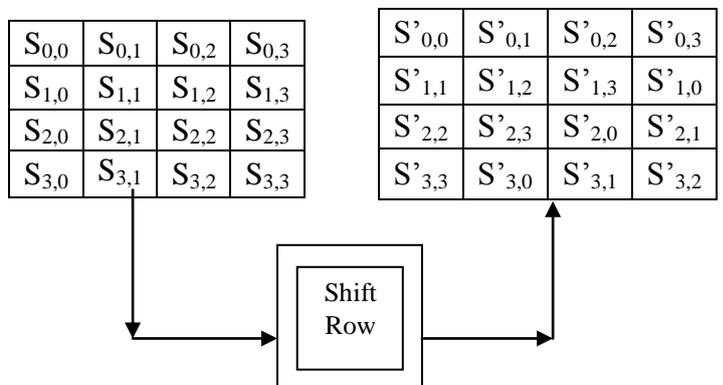
		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76	
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0	
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15	
3	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75	
4	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84	
5	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf	
6	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8	
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2	
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73	
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db	
a	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79	
b	e7	c9	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8	
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a	
d	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e	
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df	
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16	

Decryption S-Box:

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	9	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb	
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb	
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e	
3	8	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25	
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92	
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84	
6	90	d8	ab	0	8c	bc	d3	0a	f7	e4	58	5	b8	b3	45	6	
7	d0	2c	1e	8f	ca	3f	0f	2	c1	af	bd	3	1	13	8a	6b	
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73	
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e	
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1a	
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4	
c	1f	dd	a8	33	88	7	c7	31	b1	12	10	59	27	80	ec	5f	
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef	
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61	
f	17	2b	4	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d	

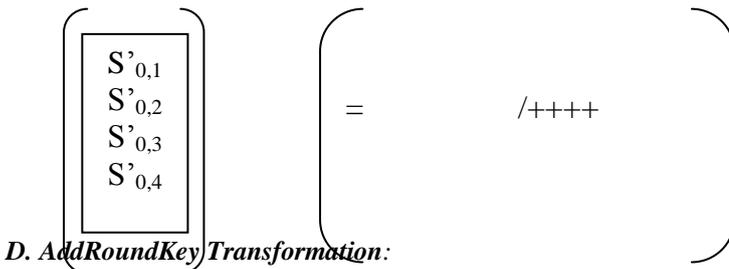
B. ShiftRow Transformation:

In ShiftRows transformation, the rows of the state are cyclically left shifted over different offsets. Row 0 is not shifted; row 1 is shifted one byte to the left; row 2 is shifted two bytes to the left and row 3 is shifted three bytes to the left.



C. MixColumn Transformation:

In MixColumns transformation, the columns of the state are considered as polynomials over GF (28) and multiplied by modulo $x^4 + 1$ with a fixed polynomial $c(x)$, given by: $c(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$.



D. AddRoundKey Transformation:

In the AddRoundKey transformation, a Round Key is added to the State - resulted from the operation of the MixColumns transformation - by a simple bitwise XOR operation. The RoundKey of each round is derived from the main key using the KeyExpansion algorithm. The encryption/decryption algorithm needs eleven 128-bit RoundKey, which are denoted RoundKey[0] RoundKey[12] (the first RoundKey [0] is the main key).

E. Key Expansion:

This phase works on the original 192bit cipher key generating 12 different expanded keys to be used respectively in each round of the AES algorithm. Each new key value is generated column by column from its preceding expanded round key value as described by

$$W_{r,i} = W_{r-1,i} \text{ XOR } W_{r,i-1}, \quad 0 < i \leq 3,$$

$$W_{r,0} = \text{SubWord}(\text{RotWord}(w_{r-1,3})) \text{ XOR } \text{Rcon}[r] \text{ XOR } W_{r,0}$$

The function SubWord() applies the SubByte transformation on each of the 32-bit word. the function RotWord() performs a left cyclic shift on the bytes of the given word. the Rcon[r] is the 32bit word given by $\{x^{-1}, \{00\}, \{00\}, \{00\}\}$.

III. VHDL IMPLEMENTATION

For the software implementation VHDL language is used in order to design the hardware elements, which will be run time reconfigured. Some important features of VHDL are: it is one of the most used HDL, it has a large and flexible syntax which allows describing a circuit by using different abstraction levels, it is possible to indicate low-level constraints etc. The synthesis of VHDL components is done by means of XST tool Xilinx ISE Project Navigator 14.2. the parallelism of code is done for calculating total cipher text or original plain text.

All the transformation of both Encryption and Decryption are simulated using iterative design approach in order to minimize the hardware consumption with less number of slices.

IV. SIMULATION RESULT

The simulation outputs is as follows by using Xilinx14.2 ISE software

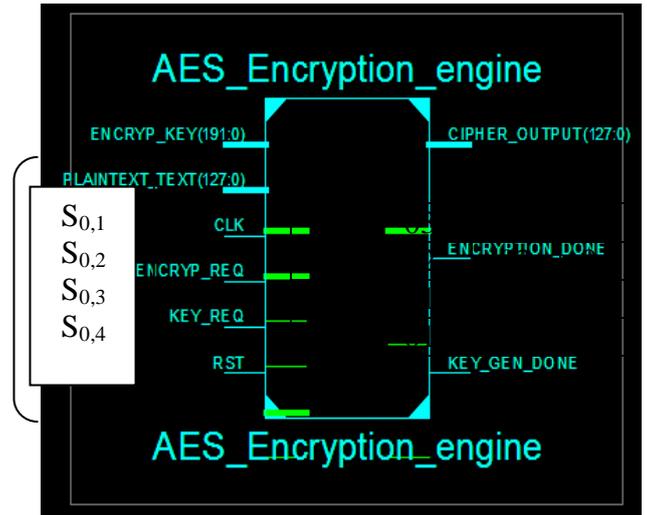


Fig. 2: Encryption RTL structure

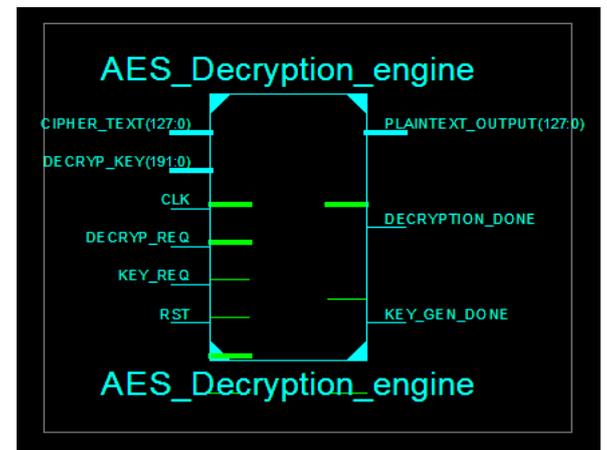


Fig. 3: Decryption RTL structure

AES encryption simulation:

Plaintext Input:
E9E93E1C603334C2ED2833F5E20A8A40

Key:
123456789012345678901234567890120123456789123456

Cipher text Output:
00001111222233334444555566667777

V. CONCLUSION

An AES implementation with 128 bit plaintext and 192 bit key using VHDL code is developed and results are verified using Xilinx ISE 14.2 both for encryption and decryption.

REFERENCES

- [1] Kamalika Datta ,Vishal Shrivastav ,Indranil Sengupta, Hafizur Rahaman “Reversible Logic Implementation of AES Algorithm”8th international conference on design & technology Integrated systems in nanoscale era,978-1-4673-6040-1/13/\$31.00,2013 IEEE
- [2] Hrushikesh S.Deshpand, Kailash J.Karande, Altaaf O.Mulani “Efficient Implementation Of AES Algorithm on FPGA” International Conference on Communication and Signal Processing, April 3_5,2014,IEEE.
- [3] Bin Liu, Student Member, IEEE, and Bevan M. Baas, Senior Member, IEEE; “Parallel AES Encryption Engines for Many-Core Processor Arrays”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 3, MARCH 2013
- [4] Mazen El Maraghy,SalmavHesham &Mohamed A.El Ghany”Real – Time FPGA Implementation of AES Algorithm”978-1-4799-1166-0/13,2013,IEEE
- [5] N.Anitha Christy and P.Karthigaikumar “FPGA implementation of AES algorithm using Composite Field Arithmetic ”International conference on devices circuits and systems,978-1-4577-1546-4/12/\$26.00,2012 IEEE
- [6] Hong Trang,Nguyen Van Loi, ”An efficient FPGA implementation of the advanced Encryption Standard algorithm”978-1-4673-0309-5/12,2012,IEEE..
- [7] Nabihah Ahmad, N.; Hasan, R.; Jubadi, W.M; “Design of AES S-Box using combinational logic optimization”, IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699, 31.00,2010 IEEE.
- [8] Alex panato Marcelo Barcelos,Ricardo Reis “An IP of an Advanced Encryption Standard For Altera Devices”, IEEE Symposium on Integrated circuits and systems Design (SBCCI’02)0-7695-1807-9/02,2002, IEEE.
- [9] Borkar”FPGA Implementation of AES Algorithm”978-1-4244-8679-3/11,2011,IEEE
- [10] Girish Kumar P, Mahesh Kumar “Implementation of AES algorithm using verilog” International Journal of VLSI and Embedded Systems,vol-4,Article 05090:june 2013
- [11] Hrushikesh S.Deshpand, Kailash J.Karande, Altaaf O.Mulani “Efficient Implementation Of AES Algorithm on FPGA” Progress In Science in Engineering Research Journal ,PISER 11,vol.02,ISSN 2347-6680 (E),2014.
- [12] Vijaya Kumar.B, T.Thammi Reddy “Fpga Implementation of High speed AES Algorithm For Improving The System Computing speed” International Journal of Computer trends and Technology(IJCTT)-VOLUME 4 Issue 9-Sep 2013.
- [13] J. Nechvatal , Report on the development of Advanced Encryption Standard, NIST Publication, Oct,2000.
- [14] J. Daemen and V Rijmen, “AES Proposal: Rijndael”, AES Algorithm Submission, September 3, 1999.
- [15] National Institute of Standards and Technology (NIST), Data Encryption Standard (DES), National Technical Information Service, Spring field, VA 22161, Oct. 1999.

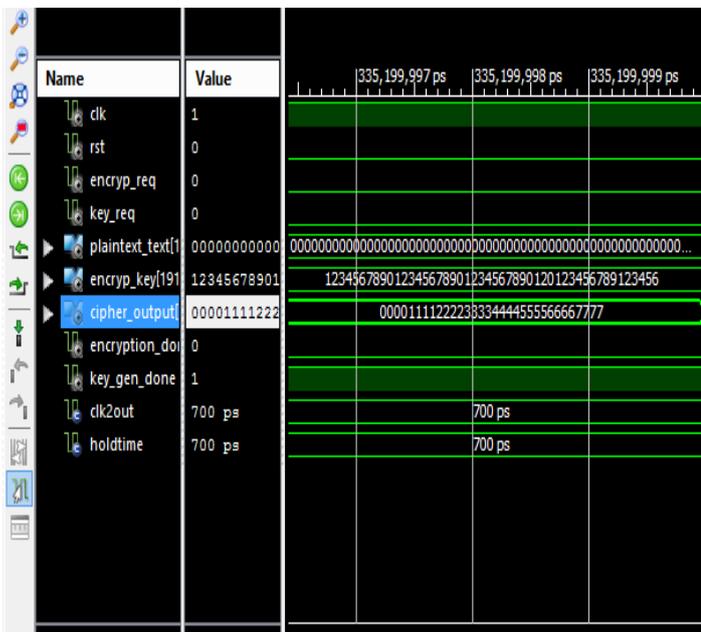


Fig. 4: Waveforms Generation by Encryption Process

AES decryption simulation:

Cipher text Input:

00001111222233334444555566667777

Key:

123456789012345678901234567890120123456789123456

Plaintext Output:

E9E93E1C603334C2ED2833F5E20A8A40

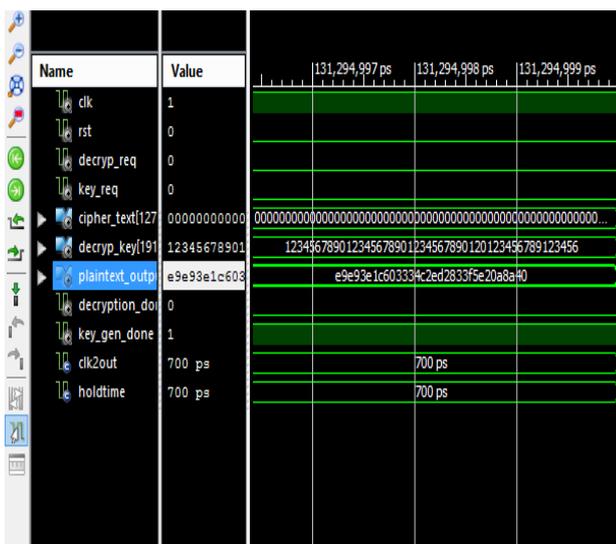


Fig. 5: Waveforms Generation by Decryption Process



DUST SPOT DETECTION AND MATCHING USING NORMALIZE CROSS CORRELATION FUNCTION BASED MULTIMEDIA FORENSIC FOR IMAGE SOURCE IDENTIFICATION

Mrs. Hemlata Meharkure
Assistant Professor, EED,
Kavikulguru Institute of Technology and Science,
Ramtek Nagpur, Maharashtra, India.
hemalanje@gmail.com, 9730018596

Abstract— Multimedia forensic for image source identification is based on digital single lens reflex (DSLR) camera. Digital single lens reflex (DSLR) camera has interchangeable lenses due to that whenever lenses attached or detached environmental dust attracted towards the imaging sensor and it creates a persistent pattern and that pattern act as a unique fingerprint for the source identification. Multimedia Forensics has become important in the last few years. There are two main interests, namely source identification and forgery detection. Source identification focuses on identifying the source digital devices (cameras, mobile phones, camcorders, etc) using the media produced by them, while forgery detection attempts to discover evidence of tampering by assessing the authenticity of the digital media (audio clips, video clips, images, etc). In this paper, uses a novel source DSLR camera identification method based on detection and matching of dust-spot characteristics that settle in front of the imaging sensor create a persistent pattern in all captured images of camera, mobile phones, camcorders, etc. To prevent false detections, lens parameter dependent characteristics of dust spots are also taken into consideration.

Keywords— *Multimedia Forensic, Digital Single*

Lens Reflex (DSLR), Sensor Dust, Normalized cross correlation

I. INTRODUCTION.

Multimedia Forensics has become important in the last few years. There are two main interests, namely source identification and forgery detection. Source identification focuses on identifying the source digital devices (cameras, mobile phones, camcorders, etc) using the media produced by them, while forgery detection attempts to discover evidence of

tampering by assessing the authenticity of the digital media (audio clips, video clips, images, etc). In the analog world, an image (specifically a photograph) has generally been accepted as a "proof of occurrence" of the event it depicts. In today's digital age, however, the creation and manipulation of digital images, audio and videos are made simple through digital processing tools that are easily and widely available. As a consequence, they can no longer take the authenticity of images and videos for granted, be they analog or digital. This is especially true when it comes to legal evidence. Image audio and video forensics, in this context, is concerned with uncovering some underlying fact about an image audio or video. In this paper, review several techniques in digital camera image forensics, i.e. in source camera identification and in forgery detection. Source camera identification methods explore different processing stages of the digital camera for unique characteristics and exploit the presence of 1) lens radial distortion 2) sensor imperfections, 3) color filter array (CFA) interpolation 4) inherent image features etc. Image forgery includes splicing of images to construct a new concocted image, applying region duplication/swapping to hide/relocate certain objects in the image and applying image editing to remove/add new objects from/into the image. For forgery detection, some of the methods inspect the image for inconsistencies in chromatic aberration, lighting, and camera response function (CRF) as signs of forgery. Others try to detect certain modes of manipulation using JPEG quantization tables, bicoheren and robust matching.

A. Digital single lens reflex (DSLR)

This paper uses a novel source camera identification method based on detection and matching of dust-spot characteristics that settle in front of the imaging sensor create a persistent

pattern in all captured images of Digital Single Lens Reflex (DSLR) camera. In this paper DSLR camera is used because it has unique features like sensor dust pattern than other cameras. It is used in high profile function, larger and higher quality sensors, low noise power, parallax-free optical viewfinder that allows error free viewing of the scenery, less shutter lag, interchangeable lenses, and better control over depth of field.

DSLR cameras showed a consistent growth with a total market and a 59% increase from the 2009 figure. Not surprisingly, DSLR cameras also take the top place in most popular camera lists of photo sharing websites like and social networking like Facebook. For instance, the top five cameras for November 2010 in Flickr (flickr.com) and Pbase (pbase.com) photo sharing websites are all DSLR cameras. Unlike the compact camera market which is cluttered with various brands like Sony Olympus, Canon, Nikon have over 95% market share in DSLR market in India of which Nikon claims to have 55% market share.

In Section II, we investigate the optical characteristics of sensor dust as a function of imaging parameters. In section III, a model-based dust spot detection method and its use in source camera identification. Section IV, V and VI are presented by conclusion, acknowledgment and references.

B. Related Work

Choi et al [2006] proposed the lens radial distortion as a fingerprint to identify source camera. Radial distortion causes straight lines to appear as curved lines on the output images and it occurs when the transverse magnification MT (ratio of the image distance to the object distance) is not a constant but a function of the off-axis image distance r . Although this method is not tested for two cameras of the same model, based on the authors' arguments on radial distortion differences, they can expect a low accuracy. Additionally, this method will fail to measure radial distortion if there is no straight line in the image since the distortion is measured using the straight line method.

Geradts et al [2001] examine the defects of CCD pixels and use them to match target images to source digital camera. Pixel defects include point defects, hot point defects, dead pixel, pixel traps, and cluster defects. To find the defect pixels, a couple of images with black background are taken by each of the 12 cameras tested and compared to count the common defect points that appear as white. The result shows that each camera has distinct pattern of defect pixels. Furthermore, for cameras with high-end CCD, the authors cannot find any visible defect pixel, which means that not all cameras necessarily have pixel defects. In addition, most cameras have built-in mechanisms to compensate for the defective pixels. Therefore, the method cannot be directly applied for all digital cameras.

Identifying source camera based on sensor pattern noise is proposed by Lukas et al [2006]. The pixel non-uniformity (PNU), where different pixels have different light sensitivities due to imperfections in sensor manufacturing processes, is a major source of pattern noise. This makes PNU a natural feature for uniquely identifying sensors. The study 9 camera

models where 2 of them have similar CCD and 2 are exactly the same model. The camera identification is 100% accurate even for cameras of the same model. The result is also good for identifying compressed images. One problem with the conducted experiments is that the authors use the same image set to calculate both the camera reference pattern and the correlations for the images. It runs several experiments with this model for cropped images. It turns out that the model fails to predict the source camera of cropped images.

Bayram et al [2005] explores the CFA interpolation process to determine the correlation structure present in each color band which can be used for image classification. The main assumption is that the interpolation algorithm and the design of the CFA filter pattern of each manufacturer (or even each camera model) are somewhat different from others, which will result in distinguishable correlation structures in the captured images. No experiment is run for cameras of the same model but we expect the method to fail because cameras of the same model normally share the same CFA filter pattern and interpolation algorithm. In addition, the authors have pointed out that this method does not work well for compressed images.

Kharrazi et al [2004] identify a set of image features that can be used to uniquely classify a camera model. The 34 proposed features are categorized into 3 groups: Color Features, Image Quality Metrics, and Wavelet Domain Statistics. Features are extracted from images of two cameras, which are then used to train and test the classifier. The result is as high as 98.73% for uncompressed images and 93.42% for JPEG images compressed with a quality factor of 75. The accuracy rate drops to 88% when five cameras are used. Hence, this method does not work well for cameras with similar CCD and is unsuitable for identifying source cameras of the same model. Furthermore, it requires all cameras to take images of the same content and resolution, which is not easy in practice.

II. DUST SPOT CHARACTERISTICS.

A. Intensity Degradation due to Dust Spot

Essentially, dust spots are the shadows of the dust particles in front of the imaging sensor. The shape and darkness of the dust spots are determined primarily by the following factors: distance between the dust particle and imaging sensor, camera focal length, and size of aperture. A general optical model showing the formation of dust spots is given in Fig. 1. When the focal plane is illuminated uniformly, all imaging sensors will yield the same intensity values. However, in the presence of sensor dust, light beams interact with the dust particles and some of the light energy is absorbed by the dust particles. The amount of the absorbed energy is directly related to the parameter f -number ($F/\#$) which is defined as the ratio between the focal length f and aperture A

$$f\text{-number} = \frac{f}{A}. \quad (1)$$

At small apertures and high f-numbers, the light source can be assumed to be a pinpoint source resulting in a relatively narrow light cone which can be blocked mostly with a tiny sensor dust. As a result, a strong dust shadow will appear on the image. This phenomenon is illustrated in Fig.1. On the other hand, for wide apertures or small f -numbers which cause wide light cones in the DSLR body, most light beams pass around the dust spots causing a blurry and soft blemish in the image. In Fig.2 the actual intensity degradations caused by dust spots are shown for different f-numbers. It can be seen from the figures that the change in f-number affects the intensity and radius of the dust spot wherein an increase in the f -number (smaller aperture) causes dust spots to appear darker and smaller.

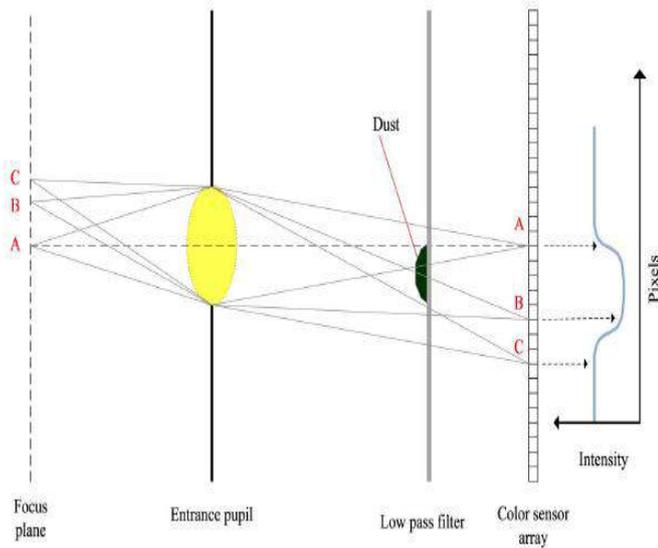


Fig1. Formation of Dust Spot under uniform illumination

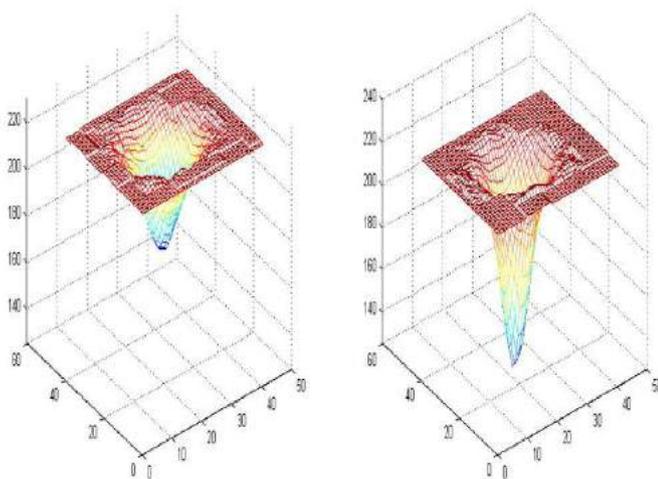


Fig.2 :Intensity Degradation due to the dust spot.

B. Dust-Spot Shape:

The dust particles in front of the imaging sensor mostly appear as round-shaped blemishes. However, dust spots with different shapes are also possible due to larger particles, such as lint or hair (Fig.3). Since these large spots, with unique shapes, are likely to cause very large intensity degradations, they are easily noticeable.

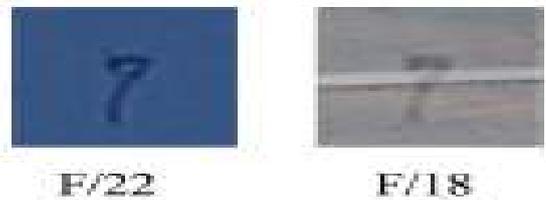


Fig.3: Spot of hair/lint for different f -numbers (Nikon D40).

Although this type of sensor dust is very suitable for camera identification, it is likely to attract the user’s attention due to their annoying appearance. As a result, they are more likely to be cleaned out. Therefore, in this paper, we will focus on dust spots due to much smaller particles that yield round-shaped dust spots that are less likely to be cleaned by many users and are, in fact, difficult to clean as discussed earlier.

C. Dust Spot Size

The formation of dust spots as a function of the camera parameters is analyzed.

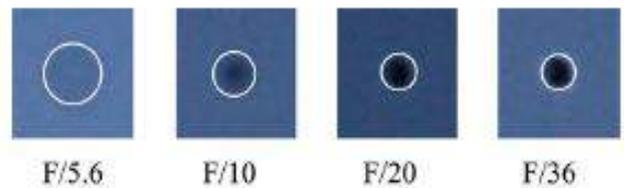


Fig. 4. Same dust spot for different f –numbers

Fig.4 shows the change in diameter of a dust spot for fixed focal length and different apertures. It can also be seen from the table 1 that the dust-spot size decreases with a decrease in aperture.

Table1. Dust-Spot properties for different –f-numbers (f = 55 mm)

F-number	5.6	10	20	36
Aperture	9.82	5.5	2.75	1.53
Max-intensity degradation	11	46	61	83
Dust-spot diameter[pixels]	20	14	11	10

III. FORENSIC USE OF SESOR DUST

In this section, we develop a technique for camera identification based on sensor dust detection. The use of dust spots for Source camera identification first requires determining the positions of dust spots in an image. Since dust particles do not tend to move easily, they appear in all images taken with high f-numbers, and their proper cleaning is not trivial, these dust-spot locations can be used as a unique fingerprint of a DSLR camera. This fingerprint can be represented by a camera dust template that includes information on all detectable dust spots. It must be noted that this template can be directly obtained from images taken by the camera at a high f-number setting or from a number of images when the camera is not available by collating dust spots detected from different images together. To decide whether an image is taken by a given DSLR, the dust spots detected in an image can be compared to those in the camera dust template and a decision is made depending on the match between detected dust spots and the template.

A. Dust Model

Our sensor dust model relies on the observation that sensor dust has two major characteristics: (a) causing an abrupt change on the intensity surface (e.g., intensity loss) depending on the aperture size; and (b) appearing most generally the form of rounded shapes, see figure 4. To model the intensity degradation due to sensor dust we utilize a 2D inverse gaussian function with a particular standard deviation and gain. It should be noted that as f-number increases the diameter of the dust spot in the image decreases and the intensity loss in the dust spot increases. Moreover, the shape of the intensity loss becomes more kurtotic. Since the dimensions of the dust is related with aperture, it is also essential to detect f-number to locate dust spot properly. (In our work we assume the EXIF data of the image is not available.) To locate the position of the dust speck, we apply fast normalize fast correlation with estimate dust model in eq.1

$$dustmodel(x, y) = -G \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2+y^2}{2\sigma^2}} \quad (1)$$

Where G– Gain factor, σ - Standard deviation

In the equation G refers to the intensity loss. The diameter of the dust speck is controlled by $\frac{3}{4}$. We estimate the diameter of dust speck based on cross-correlation results obtained under different $\frac{3}{4}$ values ranging from 1 to 3. The sigma value which produces the maximum cross-correlation is chosen as the dust model parameter, and the corresponding correlation output is used to detect dust specks. Once the correlation output is computed, the local maximums higher than a empirically determined threshold (such as 0.4) are labelled as dust

candidates. In order to eliminate false positives, dust candidates in highly detailed regions are ignored.

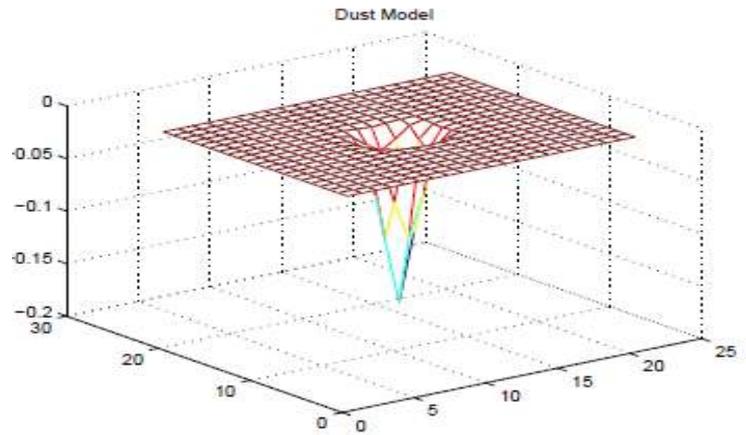


Fig.5: Dust model, G=1.0, $\sigma = 1:0$

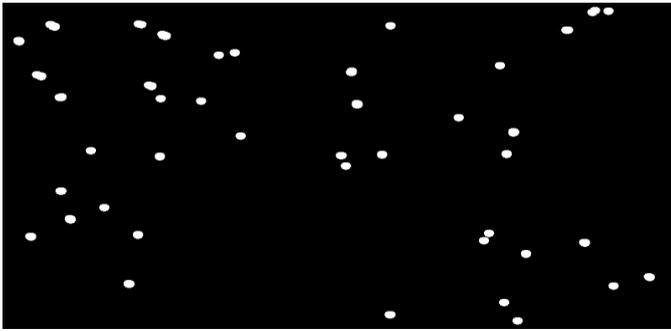
B. Camera Dust Pattern Generation

a. Digital Camera Available

In this case the dust pattern of an image can be generated by taking the picture of distant smoothly varying scenery by manually setting the focal length to high values (f/32 or f/36). Then proposed dust detection method is applied to create dust pattern of the camera.

b. DSLR Camera Unavailable.

When the camera is not available but rather a number of images taken by the camera is present, the dust points that are determined by correlation and through shape characteristics in each image is superimposed together to form the dust pattern/template of the camera. Once the template is created, a threshold is applied to the template to reduce the number of falsely labeled specks in the dust pattern. The underlying idea of applying a threshold to the template is that the actual dust speck should show up at least in two or more images. Since the probability of getting a false dust candidate at the same position in multiple images is very low, we expect that false positives due to image content will be eliminated after thresholding. The dust candidates which have higher confidence values than a fixed threshold are considered to represent the dust pattern of the camera



the camera dust template. The identification process is comprised of three steps:

- Step 1) dust-spot detection and matching;
- Step 2) computing a confidence value for each matching dust
- Step 3) decision making.

In the first step, dust spots are detected as explained in Section III. Once dust spots are located, each dust position is matched with the dust positions in the camera dust template. The comparison is realized by measuring Euclidian distances. If the distance is lower than a predetermined value, the corresponding dust position is added to the matching dust-spot list. In the second step, three metrics are computed for each of the matching dust spots as follows.

- 1) The dust occurrence metric m_1 is the number of coinciding dust for the corresponding dust spot in the dust template. Higher values of correspond to salient dust spots.
- 2) Smoothness metric m_2 presents the smoothness of the region in which a dust spot was detected. Measuring the amount of local intensity variations is essential in making decisions since dust spot detection in smooth regions is more reliable than in busy regions. This is computed via the intensity gradient around the dust spot as a binary value. For a smooth region, becomes one, and for a nonflat or nonsmooth region m_2 around the dust spot, it becomes zero.
- 3) Shift validity metric m_3 indicates the validity of a dust spot based on the shift it exhibits. To compute, we do the following
 - a) Each dust spot in the matched dust-spot list is tracked in all template images, used in template generation. (It should be noted a different subset of dust spots will be detected in each image.)
 - b) For each dust spot in the list, a set of the shift vectors (i.e., magnitude and angle) is computed by measuring the shifts between a dust spot and its matched counterparts in the template images).
 - c) Shift vectors associated with each of the template images are collected together.

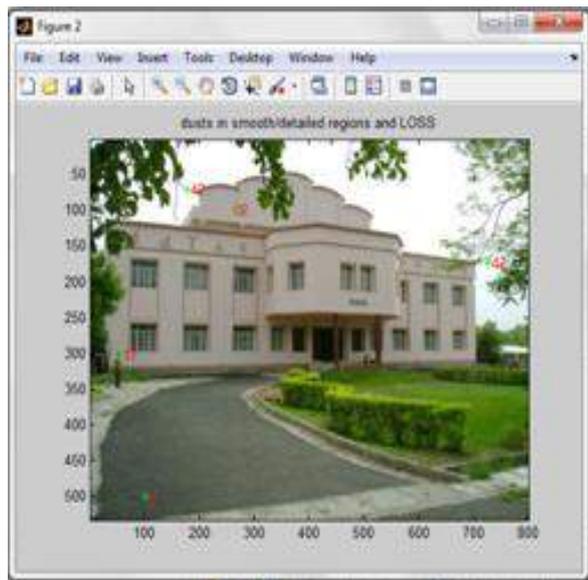
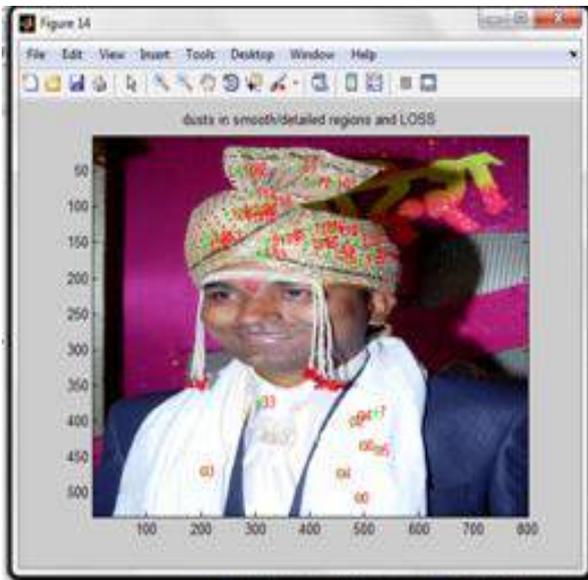


Fig.6 Dust template of camera 3 and the images used in template generation

A. Camera Identification:

The final step of DSLR camera identification is done by matching the dust spots detected in an image with dust spots in

VI. EXPERIMENTAL RESULTS

Our experiments are based on the assumption that the digital camera is not available and that the sensor dust pattern has to be obtained from a number of images taken by a DSLR camera where obtaining a precise dust template is not easy. To create an image set we have downloaded DSLR images from three different personal galleries at www.pbase.com. All images are taken with Sigma SD10. We also created an alternative image data set taken from compact consumer cameras. In order to reduce computation time of cross-correlation, all images are resized to 800×533 pixels. Since dust spots are almost invisible at large aperture rate.

Almost invisible at large aperture rates, images with low f numbers (below than 8) are not used at experiments. From each three gallery, we randomly select 10 images to create a dust template. As described in Section III, we computed the cross-correlation outputs for each image and then superimposed all the outputs to create a camera dust pattern. The contour analysis is then used to refine the final result.

After dust patterns of three cameras are computed, in the testing and verification step previously unseen images in each image gallery are analyzed to determine if they include any traces of dust patterns in the locations pointed in the dust template of the camera. In Figure 7 and 8, we provide results, when the dust template is generated only from 10 images, and tested on 20 images taken by the same and 60 random images taken by other cameras. Our matching results indicate that, we achieve a detection rate around 92% with 0% false positive rate by setting the confidence threshold 1.2. In the figures x-axes shows the image index and y-axis is the proposed metric indicating confidence in the match. Spot becomes a challenging task. Another important problem is the detection of dust spot in non-smooth, complex regions without yielding many false-positives. In the future work, we will address these

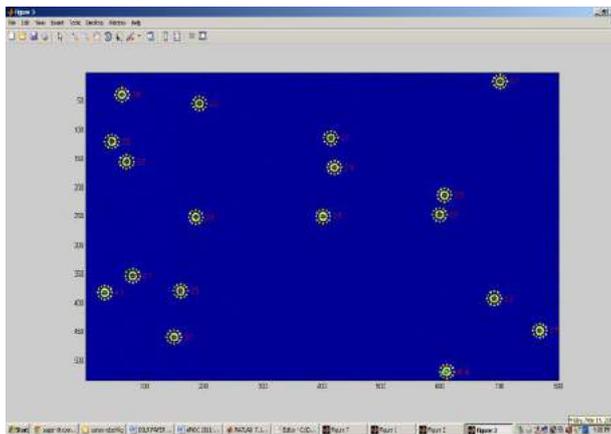


Fig.7 Num. of matches between the template of the camera 3 and dust candidates. (num. of dusts in the template : 18)

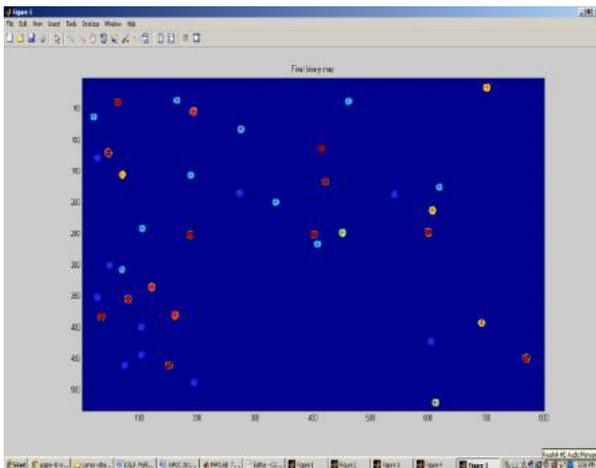


Fig.8. Num. of matches between the templates of the camera 2 and dust candidates. (num. of dusts in the template : 38)

V. CONCLUSION

In this paper, we have introduced a latest technique of multimedia forensic in that we have concentrate on source DSLR camera identification scheme based on sensor dust

traces. The location and shape of dust specks in front of the imaging sensor and their persistence make dust spots a useful fingerprint for DSLR cameras. Although many DSLR cameras come with built-in dust removal mechanisms, these hardware-based removal solutions are not as effective as they claim to be. Besides, since most dust spots are not visible or visibly irritating, most DSLR users ignore them completely. To the our best knowledge, this is the first work in the literature which uses sensor dust spots for individual camera identification. The efficacy of the proposed camera identification scheme is tested on higher than 1000 images from different cameras. Experimental results show that the proposed scheme provides high detection accuracy with very low false alarm rates. The biggest challenge in this research direction is the detection of dust spots in very complex regions and low f-numbers.

ACKNOWLEDGMENT

The author would like to thank HOD of Electronics department , KITS Ramtek, India for suggesting this line of research.

REFERENCES

1. Z. J. Geradts, J. Bijhold, M. Kieft, K. Kurosawa, K. Kuroki, and N. Saitoh, February 2001. Methods for Identification of Images Acquired with Digital Cameras, *Proc. of SPIE, Enabling Technologies for Law Enforcement and Security*, vol. 4232.
2. Chang-Tsun Li, 2010. Source Camera Identification Using Enhanced Sensor Pattern Noise, in: *IEEE Transactions on Information Forensics and Security*, 5:2(280-287).
3. M. Kharrazi, H. T. Sencar, and N. Memon, October 2004. Blind source camera identification, in *IEEE International Conference on Image Processing*, , vol. 1, pp. 709–712.
4. Y. Long and Y. Huang, Oct. 2006. Image based source camera identification using demosaicking, in *Proc. IEEE 8th Workshop Multimedia Signal Processing, Victoria, BC, Canada*, , pp. 4190–424.
5. Yanmei Fang, Ahmet Emir Dirik, Xiaoxi Sun and Nasir Memon, 2009. Source Class Identification for DSLR and Compact Cameras, in: *IEEE Workshop on Multimedia Signal Processing*.
6. A. E. Dirik, T. H. Sencar, and M. Nasir, Apr. 2007. Source camera identification based on sensor dust characteristics, in *Proc. IEEE Workshop Signal Processing Applications for Public Security and Forensics*, pp. 1–6
7. N. Khanna, A. K. Mikkilineni, G. T. C. Chiu, J. P. Allebach, and E. J. Delp, Feb. 2007. Scanner identification using sensor pattern noise, *Proc. SPIE Security, Steganography, Watermarking of Multimedia Contents IX*, vol. 6505, p. 65051.
8. S. Bayram, H. T. Sencar, N. Memon, and I. Avcibas, 2005. Source camera identification based on cfa Interpolation in *Proc. of IEEE ICIP*.
9. T. V. Lanh, K.-S. Chong, S. Emmanuel, and M. S. Kankanhalli, 2007. A survey on digital camera image forensic methods, in *Proc. IEEE Int. Conf. Multimedia Expo.*, pp. 16–19.
10. J. Luká's, J. Fridrich, and M. Goljan, , Jun. 2006. Digital camera identification from sensor noise, *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 205–214.
11. K. S. Choi, E. Y. Lam, and K. K. Y. Wong, 2006. Source camera identification using footprints from lens aberration, *Proceedings of the SPIE*.
12. J. Lewis, 1995. Fast normalized cross-correlation, *Proc. Vision Interface*, pp. 120–123,

13. T. V. Lanh, K.-S. Chong, S. Emmanuel, and M. S. Kankanhalli, 2007. A survey on digital camera image forensic methods, in *Proc. IEEE Int. Conf. Multimedia Expo*, pp. 16–19.
14. E. Steinberg, P. Bigioi, and A. Zamfir, May 2007. Detection and removal of blemishes in digital images utilizing original images of defocused scenes, pub. A1.
15. P. Blythe and J. Fridrich, Aug. 2004. Secure digital camera, in *Proc. Digital Forensic Research Workshop*, pp. 11–13.
16. M. Chen, J. Fridrich, and M. Goljan, Feb. 2007. Digital imaging sensor identification (further study), *Proc. SPIE Security, Steganography, Watermarking of Multimedia Contents IX*, vol. 6505, p. 65050.
17. A. Krainiok and R. T. Minner, May 2001. Method and system for detecting and tagging dust and scratches in a digital image, U.S. Patent 6 233 364 B1.
18. S. Bayram, I. Avciabas, B. Sankur, and N. Memon, October-December 2006. Image manipulation detection, *Journal of Electronic Imaging*, vol. 4.
19. A. Popescu and H. Farid, 2005. Exposing digital forgeries in color filter array interpolated images, *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3948–3959.
20. A. Popescu and H. Farid, 2004. Exposing digital forgeries by detecting traces of re sampling, *IEEE Transactions on Signal Processing*.
21. R. Willson, M. Maimone, A. Johnson, and L. Scherr, September 2005. An optical model for image artifacts produced by dust particles on lenses, in *8th International Symposium on Artificial Intelligence, Robotics and Automation in Space (i-SAIRAS)*.
22. A. Krainiok and R. T. Minner, May 2001. Method and system for detecting and tagging dust and scratches in a digital image, United States Patent, Patent number, 6,233,364 B1.
23. A.C. Popescu and H. Farid, 2004. Exposing digital forgeries by detecting duplicated image regions, Technical Report TR2004-515, Department of Computer Science, Dartmouth College.
24. Z. Lin, R. Wang, X. Tang, and H.-Y. Shum 2005. Detecting doctored images using camera response normality and consistency, in *CVPR*, pp. 1087–1092.
25. M.-J. Tsai and G.-H. Wu, 2006. USING Image Features to Identify Camera Sources, *ICASSP*.
26. A. Zamfir, A. Drimbarean, M. Zamfir, V. Buzuloiu, E. Steinberg, and D. Ursu, Feb. 2007. An optical model of the appearance of blemishes in digital photographs, *Proc. SPIE, Digital Photography III*, vol. 6502, pp. 011–0112.

Diagnosis of Neuromuscular Disorder using EMG Signal and Neural Network

Syed Irfan Ali

*Department of Electronics and Communication Engg.
PIET
Nagpur, India
irfan_extc@hotmail.com and 9860492850*

Sunita Parihar

*Department of Electronics and Communication Engg.
PIET
Nagpur, India
sunitaparihar1824@gmail.com and 9422506546*

Deepak Kapgate

*Department of Electronics and Communication Engg.
PIET
Nagpur, India
deepak.kapgate@rediffmail.com and 9049996103*

Syed Akbar Ali

*Department of Electronics and Telecomm. Engg.
ACET
Nagpur, India
akbar_acet@yahoo.com and 8855093867*

Abstract—EMG Signal classification has become the area of interest for the researchers since past years. Electromyography is a technique which plays an important role in diagnosing neuromuscular disorders in the field of biomedical engineering. Multiple methods have been proposed for the classification of EMG signals. But the scholars are focusing on neural network due to its classification accuracy and Motor Unit Action Potential (MUAP) as a feature of classification to the neural network.

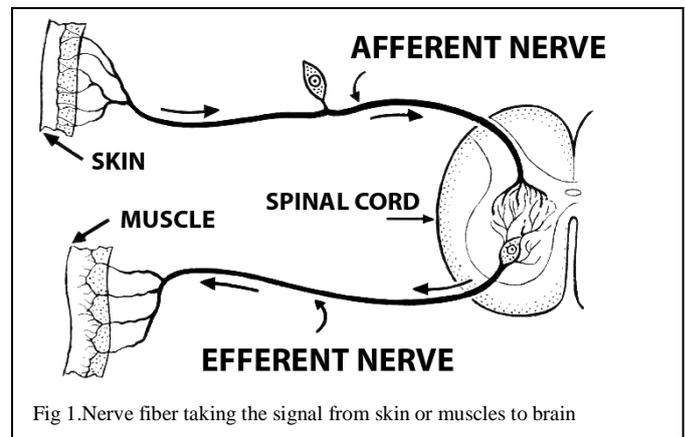
This paper explores an approach for processing the EMG signal and its classification based on Artificial Neural Network (ANN) whereas Discrete Wavelet Transform (DWT) as a tool for classification of neuromuscular disorder. In this work a multilayer feed forward neural network with back propagation algorithm is used to train the Neural Network. For achieving maximum efficiency Back Propagation Algorithm (BPA) with Discrete Wavelet Transform (DWT) is used to classify the Neurological and Neuromuscular Disorders. This work explores a comparison between k-Nearest Neighbours (kNN) classifier and Feed Forward Neural Network (fNN).

Keywords—*Electromyography (EMG); Artificial neural network (ANN); Motor unit Action Potential (MUAP); Amyotrophic Lateral Sclerosis (ALS); k-Nearest Neighbors (kNN); Discrete wavelet transform (DWT); feed forward neural network (fNN)*

I. INTRODUCTION

Human body generates a set of electrical signals as a function of time. Electromyography evaluates and records electrical variations of skeletal muscles with time. Our interest is to make a tool for diagnosing neuromuscular disorders. The neurons that connect muscles and brain surface i.e. grey matter generates electrical signals to and fro as shown in figure 1. These neuron fibers actually take the signal from brain to muscle or skin and from muscle to brain, thereby control the muscle movements.

Multiple types of electrodes are available for recording of EMG signal. Needle Electrode is used to read muscle EMG



signal and Surface Electrode is used to read skin EMG signal. For this research, a 25 mm Needle Type Electrode is suitable under hygienic clinical environment to read potential of motor nerve. This is called as Motor Unit Action Potential or MUAP. These signals are generated by muscles and goes to Central Nervous System CNS through motor nerve. This is shown in

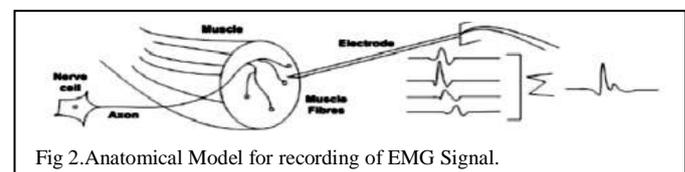


figure 2.

The Neurophysiologist usually decode the MUAPs information from graphical patterns using oscilloscope [1]. As a single needle electrode makes the contact with multiple nerves, therefore receives a composite signal of different shapes and sizes on graphical screen. To classify muscular disorders visually from the received composite signal is very difficult, thus various algorithms have been developed.

In this work, to classify between myopathy, ALS and healthy patient signals we have used wavelet based classification scheme. This has been accomplished through Feed Forward Neural Network using Back Propagation Neural Network.

Here, features are extracted using DWT (discrete wavelet transform). As we know that in practical case, EMG signal is a continuous composite signal varying with time, thus, decomposing it using wavelet transform is quite efficient. For decomposing a software known as EMG-LODEC is specially developed for recording multichannel long-term signals. The wavelet based algorithm distinguishes single MUAP by superposing the input signal [3].

II. METHODOLOGY

Classification of EMG signal needs following steps, which include (1) Reading EMG signal in wave format, (2) Feature extraction using wavelet, (3) Classification using NN. The block diagram of proposed work is shown in figure 3.

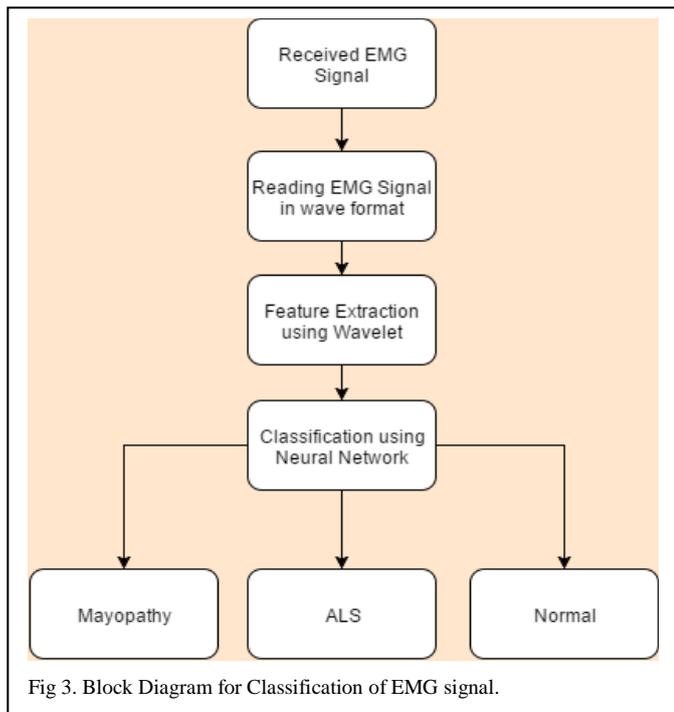


Fig 3. Block Diagram for Classification of EMG signal.

The EMG signal samples of a myopathy, ALS and a normal person were collected from [4]. Signals from arm biceps of different persons are taken. The recording is done at low level but just above the threshold of constant contraction. The HPF of EMG amplifier is set at 2 Hz while LPF is set at 10 kHz [5].

III. DWT FEATURE EXTRACTION

Any classification method can't be directly to the EMG samples, due to the large amount and the high dimension of the examples are necessary to describe such a big variety of clinical situations. A set of algorithms is usually adopted to perform a quantitative description of the signal and a parameter extraction from the signal conditioning to the measurements of average wave amplitudes, durations, and areas, [6].

Discrete wavelet transform (DWT) in comparison with discrete Fourier transform (DFT) is an efficient time-frequency approach which has been used for processing multiple biomedical engineering signals, viz. EMG. Thus, for EMG, DWT provides the time and frequency information simultaneously [7]. Equation (1) shows wavelet function.

$$X(a, b) = \frac{1}{\sqrt{b}} \int_{-\infty}^{\infty} x(t) \Psi\left(\frac{t-a}{b}\right) dt \quad (1)$$

Where 'a' and 'b' are the dilation and the translation parameters respectively. In this present work Db4 (Wavelet Daubechies-4) wavelet is used. For best result, the pre-processed EMG signal is decomposed by using the discrete wavelet transform up to the 10th level because only 262134 samples are available with this work. The feature set consists of levels 1 to 10 and coefficients cd1 to cd10 and ca10. The energy peak of the EMG signal lies between 0.5 Hz and 40 Hz. This energy of the wavelet coefficients is much intense in the lower sub-bands ca10, cd10, and cd9. The levels 1 to 8 and coefficients cd1 to cd8 are ignored as they lack information and intolerable noise is present in the frequency band of these levels. Coefficients cd9 and cd10 shows the highest frequency components and ca10 shows the lowest one. The obtained feature vectors from Db4 and wavelets decomposition is given as an input to the Neural Network classifier.

A. Discrete wavelet algorithm

The EMG Signal information is passed through two convolutions functions (filters), each of which gives an output stream which is half in length to that of original input. One half of the output is produced by the LPF given by equation (2).

$$y_1[k] = \sum_n x(n) h_0[2k - n] \quad (2)$$

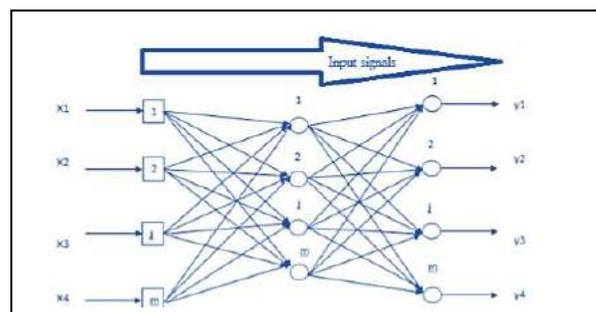
While another half of it is produced by the HPF given by equation (3).

$$y_2[k] = \sum_n x(n) h_1[2k - n] \quad (3)$$

Where y_1 and y_2 are the output of LPF & HPF respectively, which are known as an approximate and detail component. These outputs are down sampled by a factor of 2, which is known as 1-level decomposition. This process is repeated up to 10 levels of decomposition, which results in a reduction of samples from 262134 to 262. This is suitable for training of neural network.

IV. NEURAL NETWORK AS A CLASSIFIER

The neural network is one of the efficient and accurate classifier. It has dense parallel structure & it learns from previous experience. The accuracy of the classification is based on training of the neural network. Here, Multilayer Feed Forward Neural Network with Back Propagation Algorithm is used.



The information obtained from experience is stored in the form of connection weights. The weights update after training, which runs in multiple iterations to get the desired level of training. Since this algorithm is a supervised training algorithm, three issues need to be solved in designing an ANN for a specific application. In this work, total 14 hidden neurons are used, simplified network is shown in figure 4.

V. K-NEAREST NEIGHBOR TECHNIQUE

The k-Nearest Neighbor is denoted by k-NN. If the cost of error is same for each class, the estimated class of an unknown sample is chosen to be the class, which is normally represented in the collection of its K nearest neighbors. This technique does not consider a priori assumptions about the distributions wherefrom the training samples are taken. For classification of a new sample, the distance to the nearest training case is calculated then the sign (plus or minus) of this point classifies the sample. The k-NN classifier picks the k nearest points and allot the sign of the majority. Large value of k reduces the effects of noisy points within the training data set, and cross-validation is used to choose the value of k. This way, its Euclidean distance d is calculated. Equation (4) with all the training samples classifies to the class of the minimal distance.

$$q(x, y) = \sqrt{\sum_{j=1}^n (x_j - y_j)^2} \quad (4)$$

Each training example with a class label is a vector in a multidimensional feature space. The algorithm's training phase includes only storing of the feature vectors and class labels of the training samples. The algorithm's classification phase has 'k' as a user-defined constant, and the unlabeled vector is classified by assigning the label. Even if the Euclidean distance is only applicable to continuous variables, it is used as the distance metric.

VI. RESULT AND DISCUSSION

In this method, features are extracted using wavelet for neural network. Decomposition up to 10 levels for the samples from ALS, Myopathy and Healthy person is shown in figure 5. Decomposition to higher levels depends on the number of samples present in a given signal. To get clear information for a very large number of samples, it can be decomposed to a level higher than tenth level.

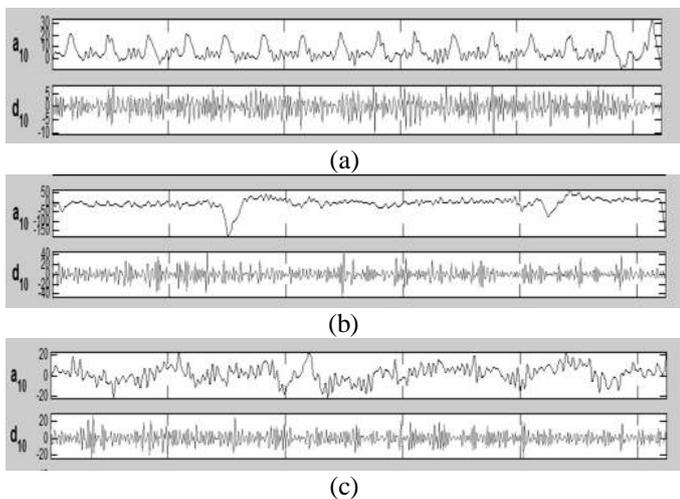


Fig 5. (a) Healthy (b) ALS (c) Myopathy

After tenth level of db4, the Histograms of samples shown in figure (6) distinguish the three classes, which are to be given to neural network.

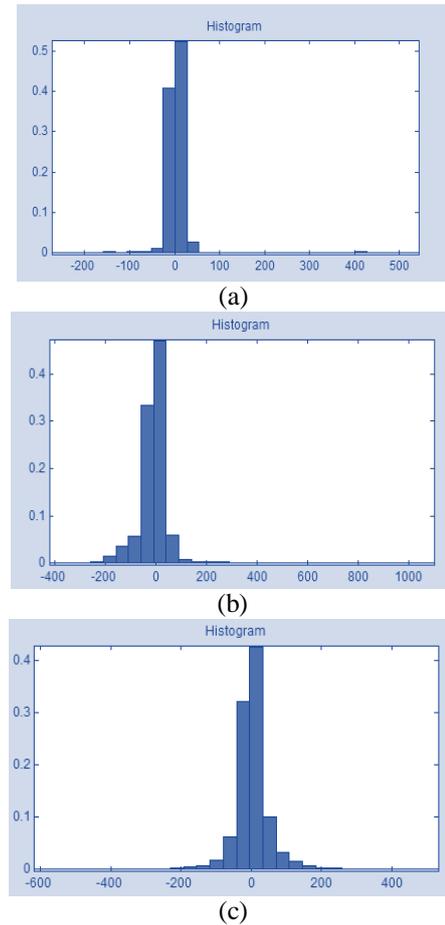


Fig 6. Histogram of (a) Healthy (b) ALS (c) Myopathy

VII. CONCLUSION

The results of Decomposition and Histogram is clearly showing the difference between Healthy, ALS & Myopathy. The kNN and fNN classifiers will be used to differentiate between Healthy, ALS and Myopathy. These classifiers are efficient to classify the data with a greater accuracy. This work will be an assistive contribution to doctors for a neuromuscular disorder.

REFERENCES

- [1] Samaneh Kouchaki, Reza Boostani, Soona shabani, "A new feature selection method for classification of EMG signals", The 16th CSI International Symposium on Artificial Intelligence and Signal Processing (AISP 2012).
- [2] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.
- [3] Daniel Zennaro, Peter Wellig, Volker M. Koch, George S. Moschytz, "A software package for the decomposition of long-term multichannel EMG signals using wavelet coefficients," IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING, VOL. 50, NO. 1, JANUARY 2003.

- [4] Nikolic M. Detailed Analysis of Clinical Electromyography Signals EMG Decomposition, Findings and Firing Pattern Analysis of Patients with Myopathy and Amyotrophic Lateral Sclerosis. PhD Thesis, Faculty of Health Science, University of Copenhagen, 2001.
- [5] M. Sc. MikiNikolic, "Detailed analysis of clinical electromyography signals," APh.D. dissertation submitted to the university of copenhagen the faculty of health science August, 2001.
- [6] Ali Hussein Ali Al-Timemy, Nebras Hussein Ghaeb, Taha Yassin Khalaf, "Wavelet neural network based Emg signal classifier," The 1st Regional Conference of Eng. Sci. NUCEJ Spatial ISSUE vol.11, No.1, 2008 pp 137-144
- [7] Akhila Devi B V, S.Suja Priyadharsini, "Diagnosis of neuromuscular disorders using softcomputing techniques," International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-5, November 2013.



“ Portable road side sensor base real time vehicular system”

Minal A. Kahurke

M.Tech(IV)

Electronics & Communication

Abha Gaikwad Patil College of Engg

Mohgaon, Nagpur(MS)

kahurkeminal@gmail.com

Cont no-7588242518

Shubhangi Dhengre

Professor(ECE)

Department of ECE

Abha Gaikwad Patil College of Engg

Mohgaon, Nagpur(MS)

Abstract— This paper focuses on the development of a portable roadside magnetic sensor system for vehicle counting, classification, and speed measurement. This paper describes a portable sensing system that can be placed adjacent to a road and can be used for vehicle counting, vehicle classification, and vehicle speed measurements. The proposed system can make these traffic measurements reliably for traffic in the lane adjacent to the sensors. The developed signal processing algorithms enable the sensor to be robust to the presence of traffic in other lanes of the road. Project proposed to add RFID device for vehicle classification

Keywords— *RFID Tagg; WSN; Vehicle Detection, Vehicle Speed Measurement. Portable Sensor platform; GPS; ARM7LPC2148 platform*

I. INTRODUCTION

The sensor system consists of wireless anisotropic magnetic devices that do not require to be embedded in the roadway—the devices are placed next to the roadway and measure traffic in the immediately adjacent lane. An algorithm based on a magnetic field model is proposed to make the system robust to the errors created by larger vehicles driving in the nonadjacent lane. These false calls cause an 8% error if uncorrected. The use of the proposed algorithm reduces this error to only 1%. Speed measurement is based on the calculation of the cross correlation between longitudinally spaced sensors. Fast computation of the cross correlation is enabled by using frequency-domain signal processing techniques. An algorithm for automatically correcting for any small misalignment of the sensors is utilized. A high-accuracy

differential Global Positioning System is used as a reference to measure vehicle speeds to evaluate the accuracy of the speed measurement from the new sensor system. The results show that the maximum error of the speed estimates is less than 2.5% over the entire range of 5–27 m/s (11–60 mi/h). Vehicle classification is done based on the magnetic length and an estimate of the average vertical magnetic height of the vehicle. Vehicle length is estimated from the product of occupancy and estimated speed. The average vertical magnetic height is estimated using two magnetic sensors that are vertically spaced by 0.25 m. Finally, it is shown that the sensor system can be used to reliably count the number of right turns at an intersection, with an accuracy of 95%. The developed sensor system is compact, portable, wireless, and inexpensive. Data are presented from a large number of vehicles on a regular busy urban road in the Twin Cities, MN, USA.

II. PROPOSED WORK

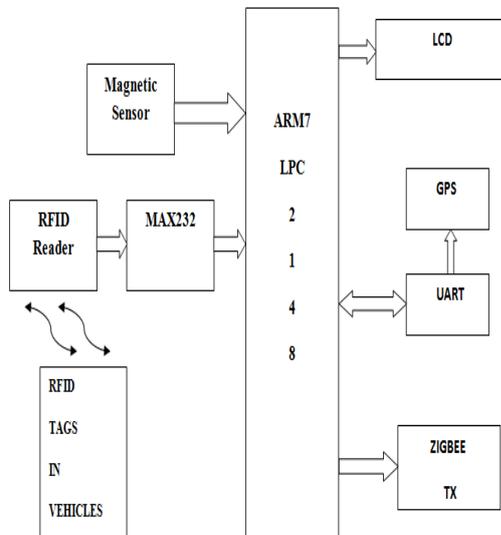
The use of the proposed algorithm reduces previous problems. Speed measurement is based on the calculation of the cross correlation between longitudinally spaced sensors. Fast computation of the cross correlation is enabled by using frequency-domain signal processing techniques. An algorithm for automatically correcting for any small misalignment of the sensors is utilized. A high-accuracy differential Global Positioning System is used as a reference to measure vehicle speeds to evaluate the accuracy of the speed measurement from the new sensor system.

The work in the project proposed to add RFID device to the WIM sensor. An RFID Tag responds

to the magnetic field of each vehicle (just like an inductive loop). RFID Tags are currently already being used as traffic sensors. RFID Tags cannot measure the number of axles or the weight of any axle. However, they can reliably count vehicles, differentiating one consecutive vehicle from another.

Herewith we develop the system with data identification system and data monitoring system. Data identification system with sensorized arrangement with magnetic sensor and RFID reader. It provides input to ARM7 according to application. ARM7LPC2148 get location form GPS with 2D position of system then information about every vehicle transfer to DATA monitoring unit. Maintaining the Integrity of the Specifications

DATA IDENTIFICATION SYSTEM:



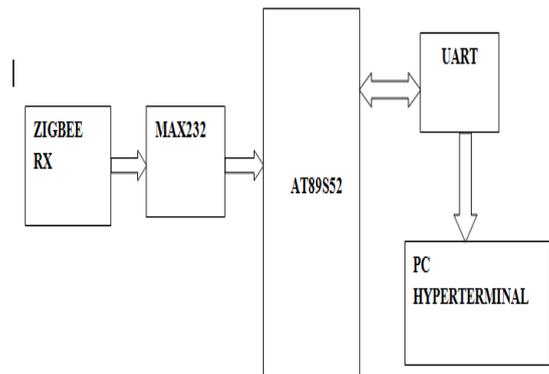
Problem Defination:

The sensor system consists of wireless anisotropic magnetic devices that do not require to be embedded in the roadway—the devices are placed next to the roadway and measure traffic in the immediately adjacent lane. An algorithm based on a magnetic field model is proposed to make the system robust to the errors created by larger vehicles driving in the nonadjacent lane. These false calls cause an 8% error if uncorrected.

Motivation:

This paper describes a portable sensing system that can be placed adjacent to a road and can be used for vehicle counting, vehicle classification, and vehicle speed measurements. This paper presents an improved algorithm based on Saber Taghvaeeyan and Rajesh Rajamani' Portable roadside sensors for Vehicle counting, Classification, and Speed Measurement'

DATA MONITORING SYSTEM:



The increasing traffic volume over the last decades poses high challenges on today's traffic research and planning. Detection, Counting and classification of vehicles in a video has become a potential area of research due to its numerous applications to video-based intelligent transportation systems. For most traffic surveillance systems, major stages are used to estimate desired traffic parameters, i.e., vehicle detection, Counting, tracking, and classification. Each year, motor vehicle crashes account for about thousands deaths, more than million injuries. Counting vehicles over a period of time on a busy intersection will help the concerned authority to efficiently control the duration of traffic signal on road thus reducing the level of traffic congestion during rush hours. It helps in minimizing the possibilities of fraudulent activities in toll collection. It is necessary to provide better traffic surveillance to reduce the accidents. So the main Goal of our paper is to provide better traffic surveillance.

The proposed method has several advantages.

1. To avoid the Traffic in Cities.
2. Stolen vehicle or theft vehicle detection With This system
3. Using Classification we can classify vehicle types.
4. Local network implementation.
5. Magnetic sensors have also been evaluated for vehicle classification
6. RFID have also been evaluated for vehicle

Future Scope:

Currently in our system we are just accessing the system from embedded based system. So in future we can implement a system with IOT using Wi-Fi. Then we manage complete network by web portal.

CONCLUSION

In the project, we have presented a computer vision system which uses a video to count and classify vehicles with the aim of replacing ILDs, particularly on highways. Additionally, this system distinguishes itself from other computer-vision-based approaches in the way in which it can handle the system without the need for any hardware other than cameras, such as GPS. This makes the system inexpensive to use. In this, we have presented two different parameters for the traffic surveillance system, one is counting the vehicles and other is classification of the vehicles. The processing is carried out on pre recorded video. Vehicle counting is done by finding the centroid and the distance between the marked border and the vehicle. Classification is done by finding the area and thresholding method. New traffic sensing devices based on wireless sensing technologies were designed and tested. Such devices encompass a cost-effective, battery-free, and energy self-sustained architecture for real-time traffic measurement over distributed points in a transportation system. This scalable technology can monitor traffic parameters such as flow, occupancy, point speed, and vehicle classification on road systems in real-time.

- [1] S. Jeng and S. Ritchie, "Real-time vehicle classification using inductive loop signature data," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2086, pp. 8–22, 2008. [Online]. Available: <http://dx.doi.org/10.3141/2086-02>.
- [2] S. Gupte, O. Masoud, R. F. K. Martin, and N. P. Papanikolopoulos, "Detection and classification of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 3, no. 1, pp. 37–47, Mar. 2002.
- [3] H. Cheng, H. Du, L. Hu, and C. Glazier, "Vehicle detection and classification using model-based and fuzzy logic approaches," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 1935, pp. 154–162, 2005. [Online]. Available: <http://dx.doi.org/10.3141/1935-18>.
- [4] J. Medina, M. Chitturi, and R. Benekohal, "Effects of fog, snow, and rain on video detection systems at intersections," *Transp. Lett., Int. J. Transp. Res.*, vol. 2, no. 1, pp. 1–12, Jan. 2010. [Online]. Available: <http://dx.doi.org/10.3328/TL.2010.02.01.1-12>.
- [5] M. J. Caruso and L. S. Withanawasam, "Vehicle detection and compass applications using AMR magnetic sensors," in *Sens. Expo Proc.*, 1999, pp. 477–489.
- [6] S. Cheung, S. Coleri, B. Dunder, S. Ganesh, C. Tan, and P. Varaiya, "Traffic measurement and vehicle classification with single magnetic sensor," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 1917, pp. 173–181, 2005. [Online]. Available: <http://dx.doi.org/10.3141/1917-19>.
- [7] S. Kaewkamnerd, J. Chinrungrueng, R. Pongthornseri, and S. Dumnin, "Vehicle classification based on magnetic sensor signal," in *Proc. IEEE ICIA*, 2010, pp. 935–939.
- [8] M. Bottero, B. Dalla Chiara, and F. P. Deflorio, "Wireless sensor networks for traffic monitoring in a logistic center," *Transp. Res.—Part C: Emerg. Technol.*, vol. 26, pp. 99–124, Jan. 2013.

- [1] S. Jeng and S. Ritchie, "Real-time vehicle classification using inductive loop **Page 1994** signature data," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2086, pp. 8–22, 2008. [Online]. Available: <http://dx.doi.org/10.3141/2086-02>.
- [2] S. Gupte, O. Masoud, R. F. K. Martin, and N. P. Papanikolopoulos, "Detection and classification of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 3, no. 1, pp. 37–47, Mar. 2002.
- [3] H. Cheng, H. Du, L. Hu, and C. Glazier, "Vehicle detection and classification using model-based and fuzzy logic approaches," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 1935, pp. 154–162, 2005. [Online]. Available: <http://dx.doi.org/10.3141/1935-18>.
- [4] J. Medina, M. Chitturi, and R. Benekohal, "Effects of fog, snow, and rain on video detection systems at intersections," *Transp. Lett., Int. J. Transp. Res.*, vol. 2, no. 1, pp. 1–12, Jan. 2010. [Online]. Available: <http://dx.doi.org/10.3328/TL.2010.02.01.1-12>.
- [5] M. J. Caruso and L. S. Withanawasam, "Vehicle detection and compass applications using AMR magnetic sensors," in *Sens. Expo Proc.*, 1999, pp. 477–489.
- [6] S. Cheung, S. Coleri, B. Dundar, S. Ganesh, C. Tan, and P. Varaiya, "Traffic measurement and vehicle classification with single magnetic sensor," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 1917, pp. 173–181, 2005. [Online]. Available: <http://dx.doi.org/10.3141/1917-19>.
- [7] S. Kaewkamnerd, J. Chinrungrueng, R. Pongthornseri, and S. Dumnin, "Vehicle classification based on magnetic sensor signal," in *Proc. IEEE ICIA*, 2010, pp. 935–939.
- [8] M. Bottero, B. Dalla Chiara, and F. P. Deflorio, "Wireless sensor networks for traffic monitoring in a logistic center," *Transp. Res.—Part C: Emerg. Technol.*, vol. 26, pp. 99–124, Jan. 2013.

- [1] S. Jeng and S. Ritchie, "Real-time vehicle classification using inductive loop **Page 1994** signature data," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2086, pp. 8–22, 2008. [Online]. Available: <http://dx.doi.org/10.3141/2086-02>.
- [2] S. Gupte, O. Masoud, R. F. K. Martin, and N. P. Papanikolopoulos, "Detection and classification of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 3, no. 1, pp. 37–47, Mar. 2002.
- [3] H. Cheng, H. Du, L. Hu, and C. Glazier, "Vehicle detection and classification using model-based and fuzzy logic approaches," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 1935, pp. 154–162, 2005. [Online]. Available: <http://dx.doi.org/10.3141/1935-18>.
- [4] J. Medina, M. Chitturi, and R. Benekohal, "Effects of fog, snow, and rain on video detection systems at intersections," *Transp. Lett., Int. J. Transp. Res.*, vol. 2, no. 1, pp. 1–12, Jan. 2010. [Online]. Available: <http://dx.doi.org/10.3328/TL.2010.02.01.1-12>.
- [5] M. J. Caruso and L. S. Withanawasam, "Vehicle detection and compass applications using AMR magnetic sensors," in *Sens. Expo Proc.*, 1999, pp. 477–489.
- [6] S. Cheung, S. Coleri, B. Dunder, S. Ganesh, C. Tan, and P. Varaiya, "Traffic measurement and vehicle classification with single magnetic sensor," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 1917, pp. 173–181, 2005. [Online]. Available: <http://dx.doi.org/10.3141/1917-19>.
- [7] S. Kaewkamnerd, J. Chinrungrueng, R. Pongthornseri, and S. Dumnin, "Vehicle classification based on magnetic sensor signal," in *Proc. IEEE ICIA*, 2010, pp. 935–939.
- [8] M. Bottero, B. Dalla Chiara, and F. P. Deflorio, "Wireless sensor networks for traffic monitoring in a logistic center," *Transp. Res.—Part C: Emerg. Technol.*, vol. 26, pp. 99–124, Jan. 2013.

Paper Setting:

Paper Title: Font: Times New Roman, Bold, Style: Italics, Font Size: 24

Author Name: Style: Italics, Font Size: 11

Affiliation: Style: Italics, Font Size: 10

Abstract: Font: Times New Roman, Bold, Font Size: 9

Keywords: Font: Times New Roman, Bold, Style: Italics, Font Size: 9

Introduction (All Headings): Font: Times New Roman, Bold, Font Size: 10

Subtitle: Style: Italics, Font Size: 10

Running Text: Font: Times New Roman, Font Size: 10

References: Heading (10), Text: Font: Times New Roman, Font size: 8

Spacing: 10 pt Single



Review On Design And Implementation of Innovative Steganographic 3 Bit Process

*Mr.Sanket Yeole¹;
AGPCE ,Nagpur
sanketyeole2011@rediffmail.com*

*Prof. Sagar Ghormade²
AGPCE ,Nagpur
sagarghormade@gmail.com*

Abstract

This paper brings the idea of novel approach to steganography where the data in one medium is hidden in an message in the last three LSB bits of the pixels of the carrier color image. This paper overcome the drawback on previous method where the bits of the secrete audio data are hidden in the only last two bits of the cover image thus offers more key based secure data transmission and reception with same cover medium. other medium in such way that no one except sender and receiver suspect the existence of the message. In this we are using Least Significant Bit method to hide the content of the encoded audio

Keywords: *steganography, RGB channels, LSB substitution, bit array conversion*

1. Introduction

Major requirement of today's computer communication is to prevent the data to be disclosed to the illegal user. Various technique of such data hiding are steganography, cryptography, watermarking etc. Apart from these three ,Steganography is the method of hiding confidential or sensitive informational data related to finance or anything within something that will not appears to any one . Both the techniques stignography and watermarking are use to protect important information. The difference between the two is that Steganography involves hiding information so it appears like no information is hidden at all. Steganography in the modern era sense of the world usually refers to information or a file that has been concealed inside a digital picture, video or audio file. What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside them, although there are programs available that can do what is called steganalysis process . An computer

algorithm can perform stignalysis process very easily and effectively. Data hiding, or steganalysis, is a challenging and interesting area for research which has attracted much attention of researchers for centuries. As an active area of research, new techniques are constantly emerging using 3 bit LSB algorithm. In contrast to the active research focusing on image or video schemes, there has been a little research on data hiding in audio formats. However, effective audio data hiding in an color image can create robust and imperceptible data thus allowing high protection or secret data exchange over communication channels.

2. RGB color channels and LSB substitution method

An image can be represented by a collection of color pixels arranged in systematic manner . These pixels are having various color intensities .The individual pixels are represented by their optical characteristics like "brightness", "intensity""contrast",etc. Each of these characteristics can be digitally expressed in terms of 1's and 0's. These images are a collection of different color pixels haviing different intensities. There are three color channels that present different forms for storing images. A color space method is a method by which it is possible to specifically, create and visualize color pixels. The most common color space among all is RGB (Red, Green, and Blue). The RGB color model is additive in the sense that the three light beams are added together, and their light spectra are added , to make the final color's spectrum. Each pixel in a 24-bit bitmap image in this space is described by 3 sets of 8 bits (3 bytes), that each set contains the intensity value of individual red, green and blue.

For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

```
(100110011 11001110 101110010)
( 011010011 11001010 101111010)
(11001000 00100111 111100100)
```

When the character B, which binary value equals 10000010, is inserted, the following grid results

```
(00100111 11101000 11001000)
(00010110 11001000 00001000)
(11001000 00100111 11101000)
```

3. Proposed methodology of LSB

The conventional method says, one LSB can be replaced with the data bit. Instead of hiding a single bit in each byte, two bits of data can be hidden in a single byte as it can cause no change in the image as per the human visual system. As there are 8 bits in a byte, first and the second and third bits can be hidden in Red values and next three bits in the green value and next three in the blue value byte. For example, consider the 24 bit pixel value-

11001000 00100111 101000100

Consider the data byte- 111 010 110

Data can be hidden in the following way-

00100111 010010101 1010110

The main advantage of this technique is the increase in the amount of space for hiding the data. Thus 1 byte of audio data can be hidden in the one pixel of the cover image.

4. Block Processing

Encoder block used for hiding the audio message in the image. This audio message is first sampled and then transformed into binary format and then encoded with color image using 3bit LSB substitution technique that is discussed above,

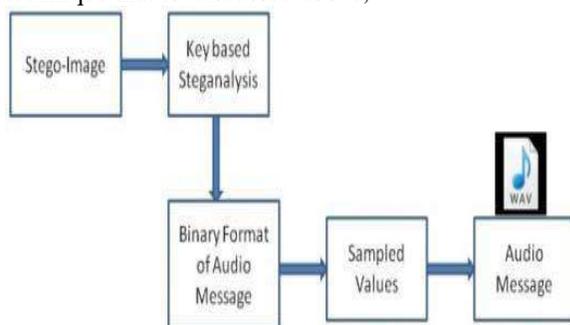


Figure 1. Hiding the audio message

The main advantage of this technique is the increase in the amount of space for hiding the data. Thus 1 byte of audio data can be hidden in the one pixel of the cover image.

5. Implementation and Proposed Output

Using image processing toolbox above proposed work has been implemented. We obtained the screenshot of the result which show the color image encoded into the binary format shown in fig 1. The changes that has been made in the cover image in which the audio is hidden are so small that cannot be observed by the human perception. Thus, steganographic image looks like the cover image and the recovered audio message will also appears identical to the original data that was sent.

6. Conclusion

This technique provide greater amount of flexibility to the user since it allow the hide the audio content in the last three bit of each byte. Therefore it avoids the major limitation of conventional method so more data can be hidden within same medium.

7. References

- [1] V. J. Rehna, Member, IACSIT and M. K. Jeya Kumar ,“A Strong Encryption Method of Sound Steganography by Encoding an Image to Audio”, *International Journal of Information and Electronics Engineering*, Vol. 2, No. 3, May 2012.
- [2] M.I.Khalil, “Image Steganography, Hiding short audio messages in digital images”, *JCS&T Vol 11 No.2*.
- [3]Jeremiah J. Harmsen,” *Capacity of Steganographic Channels” IEEE Transactions On Information Theory*, Vol. 55, No. 4, April 2009.
- [4]Nicholas Hopper, Luis von Ahn, and John Langford” *Provably Secure Steganography” IEEE Transactions On Computers*, Vol. 58, No. 5, May 2009.
- [5]Mauro Barni” *Watermark Embedding: Hiding a Signal within a Cover Image”, IEEE Communications Magazine* August 2001.

A Review paper on Heart Rate Measurement Using Sensor

Utkarsha Thatte
Electronics department
Priyadarshini College of engineering
Nagpur
E-mail: utkarshathatte@gmail.com,8983040168

Mrs.K.M.Bogawar
Electronics department
Priyadarshini College of engineering
Nagpur
E-mail.:karuved@rediff.com,8600437050

Abstract— Nowadays , the biomedical instrumentation holds a prominent position within medicine . Heart rate is the number of heartbeats per unit of time, typically expressed as beats per minute. Heart rate can vary as the body’s need to absorb oxygen and excrete carbon dioxide changes during exercise or sleep. The measurement of heart rate is used by professionals to assist in the diagnosis and tracking of medical conditions .These devices are mostly used in hospitals and clinics but are gradually finding their way into domestic use. This paper demonstrates on an approach to design a cheap, accurate and reliable device which can easily measure the heart rate of a human body.

Keywords – Finger tip sensor; Microcontroller ; Opamp, RF module, PCB.

I. INTRODUCTION

Heart rate is the number of heartbeats per unit of time, typically expressed as beats per minute (bpm). Heart rate is the speed of the heartbeat measured by the number of contractions of the heart per unit of time, typically beats per minute (bpm) . The heart rate can vary according to the body's physical needs, including the need to absorb oxygen and excrete carbon dioxide. It is usually equal or close to the pulse measured at any peripheral point. Activities that can provoke change include physical exercise, sleep, anxiety, stress, illness, ingesting, and drugs. The measurement of heart rate is used by medical professionals to assist in the diagnosis and tracking of medical conditions. Heart rate measurement is one of the very important parameters of the human cardiovascular system. Electro-cardiogram (ECG) is accurate method for measuring the heart rate.ECG is an expensive device and its use for the measurement of heart rate only is not economical. Wrist watches are also available for instantaneous measurement of heart rate but their cost is usually in excess of several hundred dollars, making them uneconomical.

This paper describes the design of a very low-cost device which measures the heart rate of subject by keeping the fingertip on fingertip sensor and then displaying the result on a

text based LCD. The device has the advantage that it is microcontroller based and thus can be programmed to display various quantities, such as the average, maximum and minimum rates over a period of time and so on. Another advantage of such a design is that it can be expanded and can easily be connected to a recording device or a PC to collect and analyses the data for over a period of time.

II. BLOCK DIAGRAM

Heart rate signal is found using a fingertip sensor. After getting the signal, it must be amplified, because the signal amplitude is very low. This is done using amplifier circuit. Then the amplified signal is counted using microcontroller. Finally, the signal is transmitted by the RF transmitter. Figure 1 shows the block diagram of proposed design.

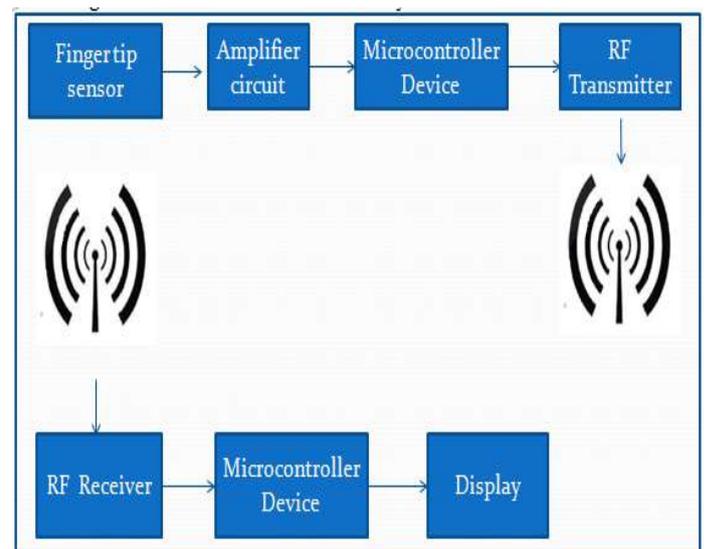


Figure 1: Block diagram of Heart rate measurement System

After transmitting the heart beat signal, it is received by the RF receiver. Then signal will be shown on 16*2 LCD display through another amplifier.

III. CIRCUIT DESIGN

There are two parts in the heart rate measurement circuit. One is transmitting circuit and another one is receiving circuit.

A. Transmitting Part

The transmitting circuit consists of Pulse Sensor, ATmega8, RF transmitter.

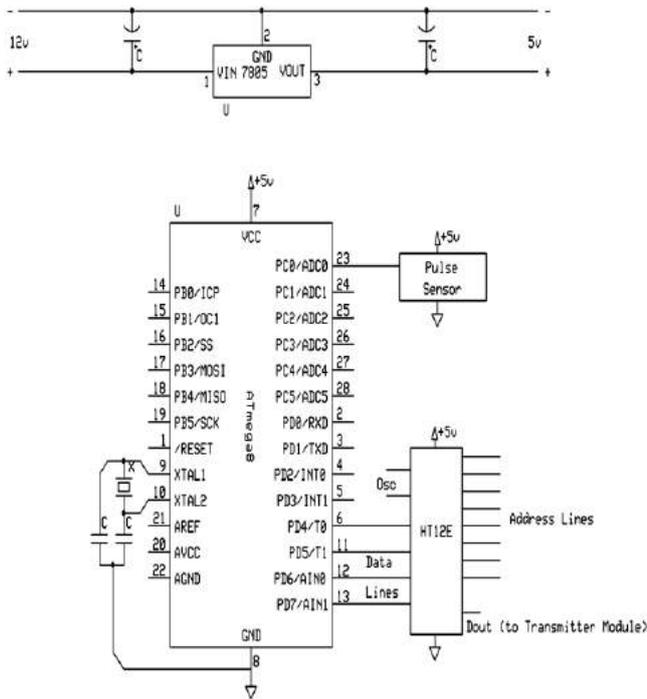


Figure 2: Schematic of heart rate measurement and transmitting circuit

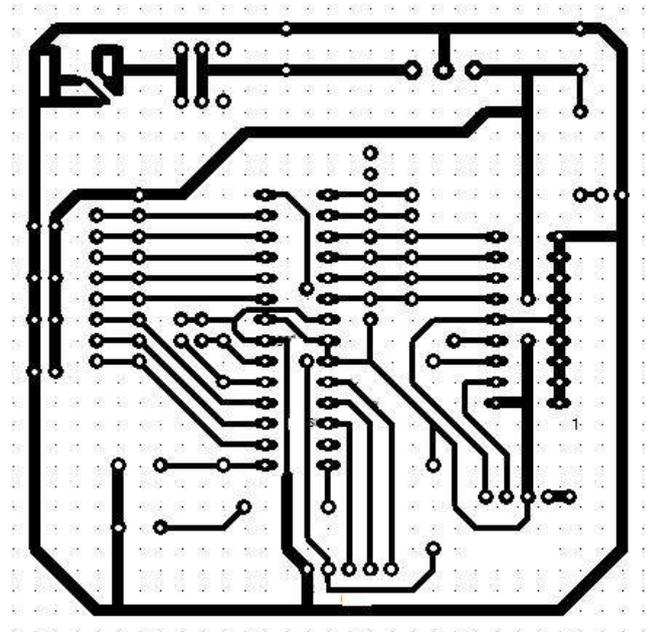


Figure 3: PCB layout (Transmitting Circuit)

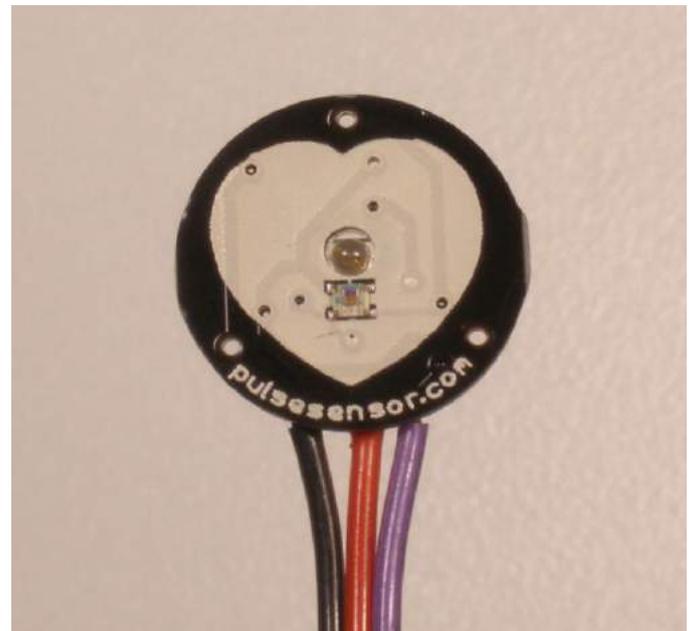


Figure 4: Pulse sensor

Consider figure 4, The front of the sensor is the pretty side with the Heart logo. This is the side that makes contact with the skin. On the front you see a small round hole, which is where the LED shines through from the back, and there is also a little square just under the LED. The square is an ambient light sensor, exactly like the one used in cell phones, tablets, and laptops, to adjust the screen brightness in different light conditions. The LED shines light into the fingertip or earlobe, or other capillary tissue, and sensor reads the light that bounces back. The back of the sensor is where the rest of the parts are mounted. We put them there so they would not get in the way of the of the sensor on the front. Even the LED we are using is a reverse mount LED.

The cable is a 24" flat color coded ribbon cable with 3 male header connectors.
 RED wire = +3V to +5V, BLACK wire = GND
 PURPLE wire = Signal.

B. Receiving Part

The receiving circuit consists of RF receiver, ATMEGA8 and a LCD display. Figure 5 shows the receiving circuit. The ATMEGA8 runs at 8.0 MHz using internal oscillator. Measurement is completed in 15 seconds and the result is transmitted to receiver circuit and it is displayed in 16*2 LCD Display.

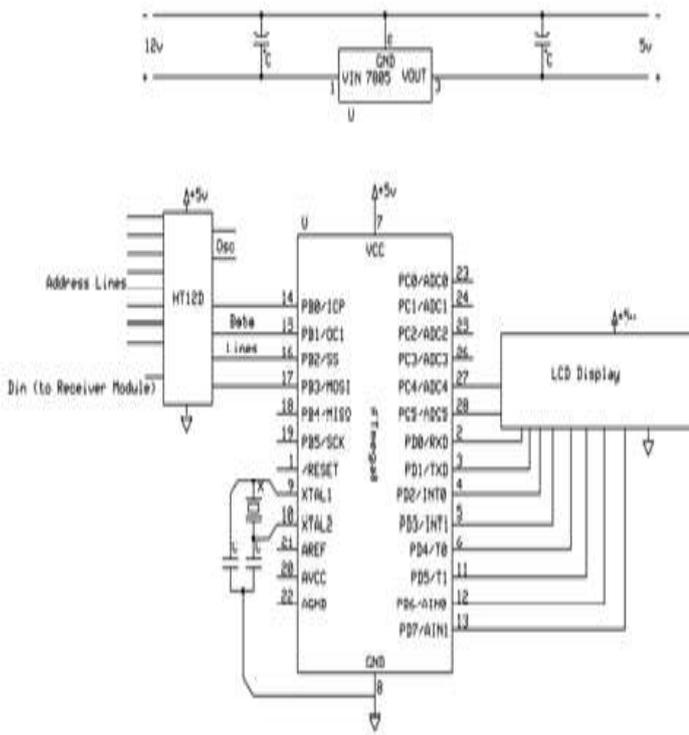


Figure 5: Schematic of the signal receiving circuit

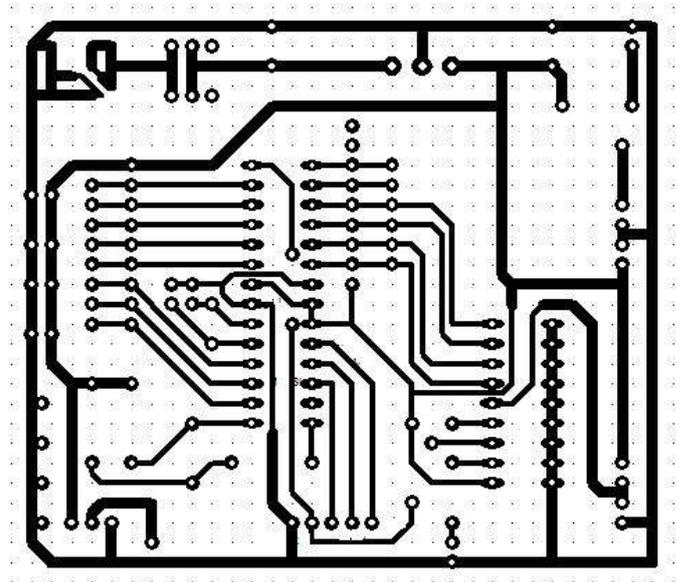


Figure 6: PCB layout (Receiving Circuit)

IV. HARDWARE IMPLEMENTATION OF HEART RATE MEASUREMENT SYSTEM

This microcontroller based wireless heart bit rate measurement device has been fabricated in Printed Circuit Board (PCB).

A. Hardware design of transmitting Part

Consider the figure 7; There is a on-off switch above the microcontroller which is used for getting power supply. There are two push to on switches for the users. On the left of the PCB there is black chip which is microcontroller we are using. In this PCB it is ATMEGA8. On the left side of PCB we have transmitter and antenna.



Figure 7: Hardware implementation of heart rate measurement device
(Transmitting part)

B. Hardware design of receiving Part

On the left side of PCB another ATMEGA8 microcontroller is used. In the below of the figure there is LCD where the output result will be shown.



Figure 8: Hardware implementation of heart rate measurement device
(Receiving part)

V. CONCLUSION

This microcontroller based heart beat monitoring system is portable device. This type of technology can be used by doctor from any remote place like villages. Any non professional educated person can also operate this type of device. So the heart rate device which is being designed is cheap in terms of cost also easier to understand.

REFERENCES

- [1] Md.Rifat Hazari, Effat Jahan, Md.Rashedul Amin,Md.Ashrafal Alam "Design and Implementation of Heart Rate Measurement Device using Wireless System",IEEE Conference on Informatics,Electronics & Vision (ICIEV),2014
- [2] How the Heart Works, December 26, 2011 Available:<http://www.webmd.com/heart.disease/guide/how-heartworks>.
- [3] Heart rate measurement from finger tip Available:<http://embedded-lab.com/blog/?p=1671>.
- [4] <https://pulse-sensor.googlecode.com/.../PulseSensorAmpedGettingStarted..>
- [5] John R. Hampton, "The ECG in Parctice".
- [6] M. Malik and A.J.Camm., "Heart Rate Variability".Futura Publishing Co.Inc.,sept.1995.
- [7] K.Ramesh,S.V.Aswin Kumer, "Efficient health monitoring system using sensor networks", International Journal of Scientific & Engineering Research Volume 3,Issue 6, June-2012.



An Efficient Approach for Driver Fatigue Detection

Priyanka Dangore
M.Tech Scholar, Electronics Engineering
J.D.College of Engineering & Management
Nagpur, India
dangorepriyanka@gmail.com
Contact No. 7387553055

Prof. Sunil Gupta
H.O.D of Electronics Engineering
J.D.College of Engineering
Nagpur, India
Sungt_in@yahoo.com
Contact No. 8007861972

Abstract—Fatigue is a dormant physical condition that can be witnessed right before one falls asleep. Fatigue affects one's reaction time, ability, concentration and general understanding particularly while driving on road adversely. This thing is primarily based on the movement of human eyelid which distinguished level of alertness. Various visual causes that generally characterize the level of alertness of a person are extracted systematically combined to check the fatigue level of the person. A probabilistic model is developed to model human fatigue and to predict fatigue based on the visual causes obtained. The simultaneous use of multiple visual causes and their systematic combination yields a much more robust and accurate fatigue characterization than using a single visual cause. The system uses a camera that points directly towards the person's face and monitors the person's eyes in formed to detect fatigue. In such a case when fatigue is detected, a warning signal is issued to alert the driver. This system describes how to detect the eyes, and also how to determine if the eyes are open or closed. The system deals with using information obtained for the binary version of the image to find the edges of the face, which narrows the area of where the eyes may exist. Once the face area is found, then eyes are found by computing the horizontal averages in the area. After finding the eyes to monitor the eye movement in the real time capturing the video in the camera is specific consecutive frame that gives 10 up to the 200 frames. The proposed system will be designed in MATLAB.

Keywords—MATLAB(Matrix Laboratory), Computer Vision System Toolbox

I. Introduction

Driver fatigue is a significant factor in a large number of vehicle accidents. The development of technologies for detecting or preventing drowsiness at the wheel is a major challenge in the field of accident avoidance systems. Because of the hazard that drowsiness presents on the road, methods need to be developed for counteracting its affects. The aim of this project is to develop a prototype drowsiness detection system. The focus will be placed on designing a system that will accurately monitor the open or closed state of the person's

eyes. By monitoring the eyes the symptoms of person fatigue can be predicted. Detection of fatigue involves a sequence of images of a face, and the observation of eye movements and blink patterns. The analysis of face images is a popular research area with applications such as face recognition, virtual tools, and human identification security systems. This project is focused on the localization of the eyes, which involves looking at the entire image of the face, and determining the position of the eyes, by a self-developed image-processing algorithm. Once the position of the eyes is located, the system is designed to determine whether the eyes are opened or closed, and detect fatigue. Skin color and textures are important physiological traits that people use consciously or unconsciously to infer variety of culture-related aspects about each other

II. Proposed Work

In this proposed work we detect closed eyes simultaneously to observed and alert the driver on fatigue detection. This is done with the help of mounting a camera in front of the driver and continuously captured its real time video using skin detection, eye detection and Hough Transform algorithm.

The conventional fatigue detectors are most efficient and successful only on frontal images of faces. The system can barely cope with 45° face rotation. The detection area is both around the vertical and horizontal axis. Another shortcoming with these processes was that they were perceptive to lighting conditions. For a few cases the designed system detected multiple recognition of the same face, due to overlapping sub-windows.

The system uses a camera that points directly towards the person's face and monitors the person's eyes in formed to detect fatigue. In such a case when fatigue is detected, a warning signal is issued to alert the driver. This system describes how to detect the eyes, and also how to determine if the eyes are open or closed. The system deals with using information obtained for the binary version of the image to find the edges of the face, which narrows the area of where the eyes may exist. Once the face area is found, then eyes are

found by computing the horizontal averages in the area. After finding the eyes to monitor the eye movement in the real time capturing the video in the camera is specific consecutive frame that gives 10 up to the 200 frames. If the eyes are open, it shows eyes in the normal condition mean Fatigue is not predicted. If the eyes are open and close in some consecutive way it shows the possible fatigue detection. If the eyes are continuously close for a while it predicted the fatigue is detected. It gives warning signal given by the system so it alerts to the user to avoid an accident.

In this proposed design take test cases up to 200 frames. This system describes a method to track the eyes and detect whether the eyes are closed or open. The next item to be considered in image acquisition is the video camera. To demonstrate the project we have used the simple Laptop camera. To create the video frames used **Computer Vision System Toolbox**.

The camera uses the function **vision.CascadeObjectDetector** creates a System object, detector that detects objects using the **Viola-Jones algorithm**. The Classification Model property controls the type of object to detect. By default, the detector is configured to detect faces. Computer Vision System Toolbox provides algorithms, functions, and apps for the design and simulation of computer vision and video processing systems. Using this tool box the system can perform object detection and tracking, feature detection and extraction, feature matching, stereo vision, camera calibration, and motion detection tasks. The system toolbox also provides tools for video processing, including video file I/O, video display, object annotation, drawing graphics, and compositing. Algorithms are available as MATLAB functions, System objects, and Simulink blocks.

III. SOFTWARE USED

MATLAB, which stands for Matrix Laboratory, is a state-of-the-art mathematical software package, which is used extensively in both academia and industry.

It is an interactive program for numerical computation and data visualization, which along with its programming capabilities provides a very useful tool for almost all areas of science and engineering.

Unlike other mathematical packages, such as MAPLE or MATHEMATICA, MATLAB cannot perform symbolic manipulations without the use of additional Toolboxes.

To create the video frames we have used “Computer Vision System Toolbox” of MATLAB.

The camera uses Viola-Jones algorithm for identifying the face of the driver. Our Mat lab Code creates a System object that detects objects using the Viola-Jones algorithm.

IV. METHODOLOGY

Step 1. It captures the video and opens a facial view where the user has to point his face properly in front of the camera.

Step2. The MATLAB script detects the face and displays the image and lets the user place a bounding box around the face.

Step 3.Afterwards one the eye, mouth portions of the frame are recognized, it rescales the eye, mouth portions to 24*24 pixels.

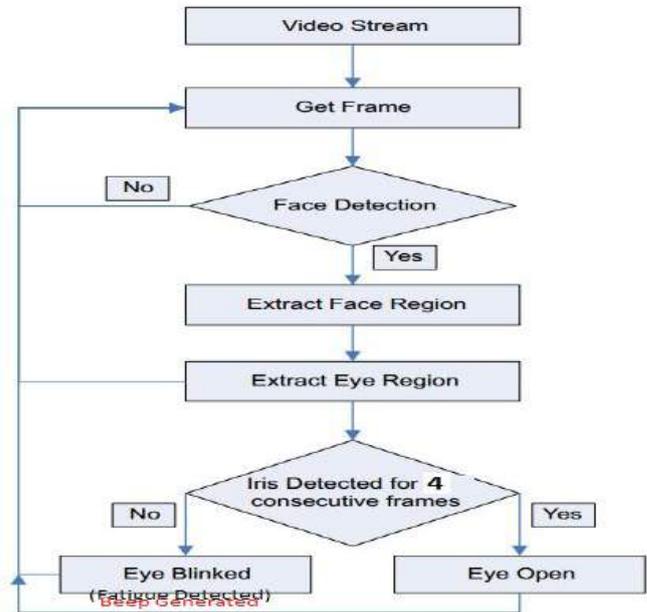


Figure 1: Proposed Work Flow Chart

The camera uses Viola-Jones algorithm to scan a sub-window capable of detecting faces across a given input frame. The standard image processing approach would be to rescale the input image to different sizes and then run the fixed size detector through these frames.

A. Image Acquisition

We will have to capture an image using camera. The user’s face is captured by camera with some frame intake and processed in MATLAB software.

B. Face Detection

The first step in MATLAB is to detect the face of the driver. We will use two algorithms that are Skin detection and Viola Jones. First step in extraction skin color pixels from the image is to convert the image to gray scale image and then subtract all non-skin color pixels from the original RGB image. We use pixels adjustment method to differentiate between skin color and non-skin color pixels. Pixels having value near to 0 (i.e. black) are

rounded to 0 and pixels having value near to 1 (i.e. white) are rounded to 1.

Once we detect face our next step is to detect eyes and mouth. In this paper, we have detected eyes from the face detection.

C. Eye Detection

After inputting a facial image, pre-processing is first performed by binarizing the image. The top and sides of the face are detected to narrow down the area of where the eyes exist. Using the sides of the face, the centre of the face is found, which will be used as a reference when comparing the left and right eyes. Moving down from the top of the face, horizontal averages of the face area are calculated. Large changes in the averages are used to define the eye area. The following explains the eye detection procedure in the order of the processing operations. All images were generating in MATLAB using the image processing toolbox.

The process of detecting Skin and Eye is shown in the below figure's by the Step by Step execution in the MATLAB.

- a) Take the input image from the web-cam.
- b) Apply the Skin detection algorithm to the input image.
- c) Label the face parameters.
- d) Apply Eye detection algorithm to the Image.
- e) Measure the distance between two eyes.



Figure 2

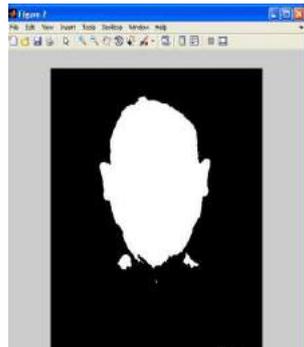


Figure 3

Figure2 above shows the input image from the web cam for Face Detection and Finding the Eye Distance.

Figure3 above shows the Skin Detection of the input image after applying skin detection algorithm

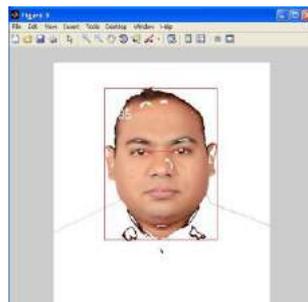
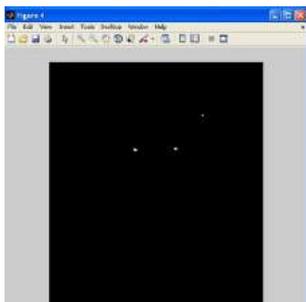


Figure 4

Figure 5

Figure4 shows the after applying eye detecting algorithm to find the circular point on the screen (that is circular region is in circular plot).

Figure5 shows the distance between two eyes after applying the eye detection algorithm.

V. FUTURE SCOPE

The proposed work in this paper is till eye detection, to detect fatigue detection of the driver we have to also detect mouth detection which signifies fatigue that is yawning. To detect fatigue of the driver the two most vital parameters will be eyes and mouth detection. In this paper, we have done three parts of the methodology that is image acquisition, face detection and eye detection. The future work will be mouth detection which will give the complete scenario of the fatigue detection.

VI. CONCLUSION

This paper describes fatigue detection system based on Viola Jones algorithm using MATLAB software. In this paper we have focused on the image acquisition by using laptop camera, the image captured in then processed into MATLAB for further processing of the image. After image acquisition we have detected the face by using Skin detection and Viola Jones algorithm. Hence ,a system that can be detect oncoming driver fatigue and issue timely warning could help in preventing many accidents .

VII. REFERENCES

- [1] Ijaz Khan, Hadi Abdullah, Mohd Shamian Zainal, Shipun Anuar,Hazwaj Mhd, Mohamad Md."Vision Based Composite Approach for Lethargy Detection". Md,2014 IEEE CSPA2014,7-9 Mac.2014 kuala Lumpur, Malaysia.
- [2] Amandeep Singh, Jaspreet Kaur, "Driver Fatigue Detection Using Machine Vision Approach", Robotics and Autonomous Systems, Kaur,978-1-4673-4529-3/12/\$31.00@2012 IEEE.
- [3] D.J.M.Bomriver,," Vision-based Real-time Driver Fatigue Detection System for Efficient Vehicle Control," nternational Journal of Engineering and Advance Technology(IJEAT)ISSN:2249-8958,Volume-2 Issue-1 Oct 2012 .
- [4] Narendra Kumar,Dr.N.C.Barwar "Analysis of Real Time Driver Fatigue Detection Based on Eye and Yawning", ,(IJCSIT)international Journal of Computer Science and Information Technologies Vol5(6),2014.78217826.
- [5] Narendra Kumar,Dr.N.C.Barwar, " Detecting of Eye Blinking an Yawning for Monitoring Drivers Drowsiness in Real Time" International journal of Application or Innovation in Engineering & Management(IJAIEM) Volume 3,Issue 11,November 2014
- [6] 021Mr. Swapnil V. Deshmukh #1, Ms.Dipeeka P. Radake*2, Mr. Kapil

N. Hande#3, "Driver fatigue Detection Using Sensor Network".
International Journal of Engineering Science and Technology (IJEST),
NCICT Special Issue Feb 2011.

Survey". IEEE Transaction on Pattern Analysis and Machine Intelligence,
Vol. 24, pp. 34-58 (2008).

[7] Yang M. H., Kriegman J. and Ahuja N, "Detecting Faces in Images: A



Review on Relative Analysis of Peak to Average Power Ratio(PAPR) Enhanced BER Performance For OFDM

Sneha Metkar¹

Department of Electronics and Communication Engineering
Abha Gaikwad-Patil College of Engineering
Nagpur, Maharashtra, India
e-mail:sneha.metkar7@gmail.com

Prof. Sagar Pradhan²

Department of Electronics and Communication Engineering
Abha Gaikwad-Patil College of Engineering
Nagpur, Maharashtra, India
e-mail: sp8728@outlook.com

Abstract— Orthogonal frequency division multiplexing (OFDM) is vastly used in wireless networks. Its superiority relies on the fact that information can be split in large amount of frequencies. Each frequency is called information subcarrier. OFDM exhibits excellent annotation in channel fades and interferers as only a few subcarriers can be affected and consequently a small part of the original data stream can be lost. Orthogonality between frequencies ensures better spectrum management and obviates the danger of intersymbol interference. However, an essential problem exists. OFDM systems have high peak to average power ratio. This implies large fluctuations in signal power, ending up in increasing complexity of ADCs and DACs. Also, power amplifiers must work in a larger linear dynamic region. In this review paper we present two new techniques for reducing Peak to Average Power Ratio (PAPR), that can be added in any OFDM system and we compare them with other existing schemes.

Keywords: *OFDM, Convolutional Encoding, QPSK, Zero padding, IFFT, Cyclic Prefix, ISI, PAPR, Soft Reduction, μ -Law Algorithm, Clipping Ratio (CR), Peak Ratio (PR), BER, CCDF, μ LSR, μ LaCP.*

I. INTRODUCTION

Orthogonal Frequency Division Multiplexing (OFDM) has been distinguished between other types of data transmission and reception schemes, for its excellent tolerance towards multipath fading and for supporting even higher data rates. OFDM has been a primary part of interest in many scientific researches and it has been included and implemented in various standards and application fields. Digital Audio Broadcasting (DAB), Terrestrial Digital Video Broadcasting (DVB-T), Wireless Local Area Network (WLAN – IEEE 802.11), High-Performance LAN type 2 (HIPERLAN/2), Broadband Wire- less Access (BWA – IEEE 802.16), Mobile Broadband Wireless Access (802.20), WiMAX, Broadcast Radio Access Network (BRAN), Digital Subscriber Lines (DSL) and Multimedia Mobile Access Communication (MMAC) have all adopted OFDM [1].

II. PROBLEM REVIEW

The key feature of splitting data in various orthogonal information carriers along with the fact of introducing a guard band called cyclic prefix for avoiding ISI, characterizes a strong candidate transceiver for all future wireless applications. The main drawback is Peak to Average Power Ratio. This essential problem of subcarriers power fluctuation imposes undesirable complexity in Digital to Analog converters as they must operate in a wider dynamic range. Also the power amplifier, located on the transmitter part, must operate in a very large linear region for preventing spectral growth and consequently out-of-band noise. All previous demands relevant to existence of high PAPR, increase the overall cost of an OFDM system.

III. PROBLEM DEFINATION

Many schemes for reducing PAPR have been proposed and are worth mentioning not only for their innovations but also due to hard work that appears to have been done by all authors. Clipping is very simple and has a quick

implementation [2]. Unfortunately it causes out- of-band radiation. Even if digital filtering is used for reducing radiation [3] which is very proper to do, BER deteriorates. Constellation shaping using SLM method in conjunction with Hadamard code [4] offers good results but complexity of this method is relatively high compared to others, like Low Complexity Technique which utilizes simple algorithm [5]. The latest still requires magnifier in receiver. Also in-depth BER performance is not mentioned. But, we must not omit the fact that its PAPR performance is fine. Another scheme is PAPR reduction with Huffman Coding [6] but it introduces the necessity of transmitting the encoding table to receiver. Even if bandwidth will not be affected, a serious drawback remains. System complexity is high. Another excellent idea is about recovering the clipped part of the OFDM signal [7], but it has restrictions, like trading-off between low CR and increasing the amount of the copied signal which in turn introduces redundancy in the transmitted data. Using a root commanding transform technique still requires expander in the receiver and exhibits good trade-off between PAPR and SER. SER Performance appears to be good but not innovative. Other technique using combined interleaving and commanding [6][7] exhibits good CCDF performance but introduces the necessity of k interleavers in transmitter's part. Also side information must be sent to receiver containing identities of corresponding interleavers. This deteriorates simplicity of system design.

IV. PROBLEM ANALYSIS

The review first part of our work involved with the study of selected companders and was focused especially in two already known schemes which are soft reduction and μ -algorithm. We selected these as they are simple techniques compared to others. We didn't use the expanded parts of these algorithms in the receiver in order to avoid overall complexity. Then we conducted various simulations ending up in finding two new

strong candidates for PAPR reduction without deteriorating BER system performance. In the third part of our study final simulations of an OFDM system (with IFFT subcarriers) were conducted. This system was consisted of a convolutional encoder [10] and a viterbi decoder along with other blocks.

V. OBJECTIVES

Our platform which is used as a basic simulation testbed, forms an OFDM system. All system delays were computed in order to apply a perfect synchronization between transmitter and receiver. Also, each time we added or removed blocks we calculated the power characteristics of the new generated OFDM signal, in order our simulations to produce the highest possible accurate results. Transmitter system under test was constituted of a random generator, a convolutional encoder, a QPSK modulator, a serial to parallel converter, an oversampling procedure using double zero padding, an IFFT block, a cyclic prefix generator and an unbuffering procedure. All inverse computations were implemented in receiver's part. Specifically for implementing convolutional encoder we used a design with one input, six shift registers and two adders complying with industry standard rate of 1/2 [1]. The review simulation system that we developed is proposed to produce to from 64 to 8192 subcarriers in IFFT output. Table characteristics of up to 4096 subcarriers system were used from our previous study on noise effects in large number of subcarriers [2][3]. Simulation testbed of 8192 subcarriers in IFFT output was conformed accordingly to table structure of previous paper. Our system design appears in **Figure 1**.

VI. DESIGN ANALYSIS

The proposed scheme μ -Law Soft Reduction – μ LSR introduces the attachment of a new compressor after Cyclic Prefix function[4][5]. Companded output can be represented by following equations without the need of expanding it in receiver's part:

$$\mu\text{LSR}_{\text{OUT}} = V_{\text{SR}} \log(1 + \mu |x_{\text{SR}}| / V_{\text{SR}}) / \log(1 + \mu) * \text{sgn}(x_{\text{SR}}) \text{-----}(1)\text{Equn.}$$

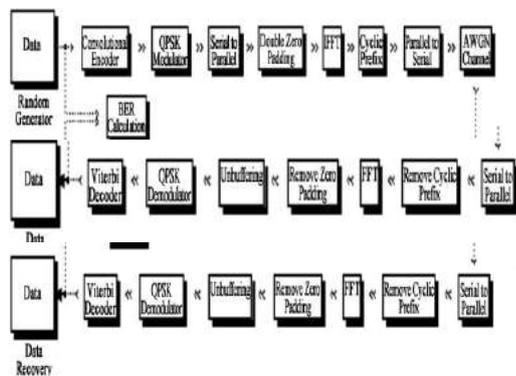


Figure 1. OFDM system overview

By using Soft Reduction (SR) in the output of Cyclic Prefix, signal peaks which exhibited larger values than others in relation to threshold, were attenuated in a greater

extend [6]. PAPR decreased along with the peak-to-peak amplitude of the CP. This led us to connecting this algorithm with μ -Law compression technique for PR = 2 [7]. Result was the amplification of the reduced signal x_{SRout} , while giving gain superiority to lower amplitudes and decreasing even more. Also, in **Figure 2**, BER performance of μ LSR is compared to SR, to μ -Law, and to OFDM system without convolutional encoder. There is clearly shown that BER performance of the proposed scheme is identical to that of SR and μ -Law compressor ($\mu = 3$, PR = 2) with the amplification in original power levels can be accomplished easily by using a gain block. In our simulations we didn't implement the previous block in order to keep low complexity in system design.

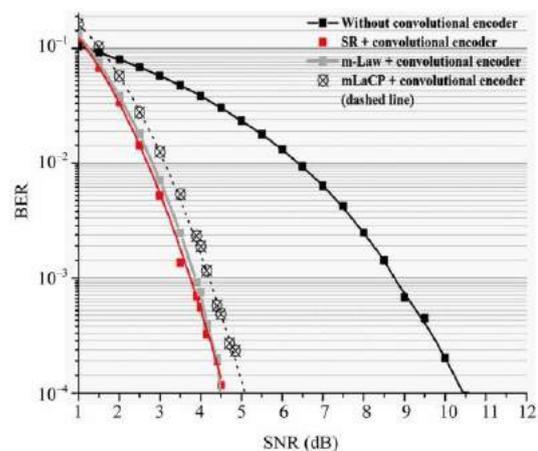


Figure 2. BER Performance of μ LaCP for 8192 subcarriers respectively (IFFT output).

VII. METHODOLOGY

As maximum PAPR rarely occurs additional simulations had to be conducted with higher amount of information data. This was done in order to verify the innovative performance of the proposed methods through the calculation and plotting for 64 and 128 OFDM carriers. Actually, **Figure 2** shows that μ LSR (for 64 carriers) with proposed Equation(1) has better performance compared to μ -Law and to OFDM system with convolutional encoder, by almost 1 dB and 2.5 dB PAPR respectively (for theoretical maximum PAPR). Also μ LSR (for 128 carriers) exhibits PAPR decrease by almost 0.5 dB and 2.5 dB compared to previously mentioned systems.

VIII. TOOLS USED

In terms of various simulations an integrated environment based with Tanner Tools is been used compatible with operating systems based on 32-bit Windows XP, Windows 7 with supported MATLAB environments.

IX. CONCLUSION AND FUTURE SCOPE

In this paper we are in review process of proposed two new techniques for decreasing Peak to Average Power Ratio. The primary concern was to accomplish this with no BER deterioration and hence to keep complexity of the system as low as possible. BER curves for μ LSR and μ LaCP which were derived from simulations (in the absence of ADC and DAC)

showed clearly not a severe deterioration. μ LSR had a slightly better performance (0.5 dB) compared to μ LaCP, but the last exhibited a superior PAPR performance in terms of probability and maximum PAPR. Also, μ LaCP is even simpler technique compared to μ LSR. Both techniques don't include an expander in receiver's part, for simplicity reasons. This is also a future goal of us, along with the design of a final OFDM system (vast number of subcarriers) introducing precise channel estimation. reduced, which could result in higher-speed with reference to dynamic scaled data transfer.

REFERENCES

- [1] B. Das , S. Tiwari, S. Das, "Performance Study of Discrete Wavelet Packet Based MB-OFDM System for Short Range Indoor Wireless Environment", International Journal of Devices and Communications (ICDecom) , Feb. 2011.
- [2] Le Chung Tran and Alfred Mertins, "Space-Time-Frequency Code Implementation in MB-OFDM UWB Communications: Design Criteria and Performance", International Journal of WIRELESS COMMUNICATIONS, Feb. 2009.
- [3] Tiejun (Ronald) Wang, John G. Proakis, James R. Zeidler, "Techniques for Suppression of Intercarrier Interference in OFDM Systems", International Journal of Wireless Communications and Networking, 2005.
- [4] Ahmad Gomaa, Naofal Al-Dhahir, "A Sparsity-Aware Approach for NBI Estimation in MIMO-OFDM", International Journal of WIRELESS COMMUNICATIONS, 2011.
- [5] Ming Jiang, Lajos Hanzo, "Multiuser MIMO-OFDM for Next-Generation Wireless Systems" , Proceedings of the IEEE , July 2007.
- [6] Raghuvver M. Rao, "Wavelet Transforms Introduction to Theory and Applications" , Pearson Fifth Impression , pp 135, 2011.
- [7] Theodore S. Rappaport, "Wireless Communications Principles and Practice" , Pearson Fourth Impression , pp 329, 2011.



Development of SIM 900 Systems to Control Wastage of Power

Yogesh kale

M.Tech.-Communication

Yeshwantrao Chavan College of Engineering

Nagpur, Maharashtra, India

ycceetyogesh@gmail.com, 9373611479

Parimal Joshi

B.E Electronics and telecommunication

Yeshwantrao Chavan College of Engineering

Nagpur, Maharashtra, India

parimal12050026@gmail.com, 7276168414

Eqbal Nasim

B.E Electronics & telecommunication

Yeshwantrao Chavan College of Engineering

Nagpur, Maharashtra, India

eqbalnasim28@gmail.com, 8087900861

Akshay Kumar Dhull

B.E Electronics & telecommunication

Yeshwantrao Chavan College of Engineering

Nagpur, Maharashtra, India

akshaykumardhull15@gmail.com, 8551920535

Abstract – Automation of the surrounding environment of a modern human being allows increasing his work efficiency and comfort. There has been a significant development in the area of an individual's routine tasks and those can be automated. In the present times, we can find most of the people clinging to their mobile phones and smart devices throughout the day. Hence with the help of his companion a mobile phone, some daily household tasks can be accomplished by personifying the use of the mobile phone. Analyzing the current smart phone market, novice mobile users are opting for phones. Home Automation System (HAS) has been designed for mobile phones in which GSM is interfaced with microcontroller which controls a number of home appliances like lights, fans, bulbs and many more using on/off relay. This paper presents the automated approach of controlling the devices in a household that could ease the tasks of using the traditional method of the switch. The most famous and efficient technology is GSM wireless communication system. The HAS system for users is a step towards the ease of the tasks by controlling different appliances in any home environment. Previous established automation systems

Keywords- *Home Automation System, GSM, Microcontroller, Mobile Phone, Appliance*

1. INTRODUCTION

GSM based Control System” implements the emerging applications of the GSM technology. Using GSM networks, a control system has been proposed that will act as an embedded system which can monitor and control appliances and other devices locally using built-in input and output peripherals. Remotely the system allows the user to effectively monitor and control the house appliances and equipments via the mobile phone by sending missed calls to the GSM kit and receiving the appliances status. The main concept behind the project is to provide miss call to the GSM kit and processing it further as required to perform several operations. The type of the

operation to be performed depends on the number of rings provided in miss calls. The principle in which the project is based is fairly simple. First, a miss call is provided to the GSM chip and polled from the receiver mobile station and then the required control signal is generated and sent to the

intermediate hardware. A microcontroller based system has been proposed for our project. There are several terminologies that are used extensively throughout this project. GSM (Global System for Mobile Communications): It is a cellular communication standard.

There are many definitions of home automation available in the literature. [1] describes home automation as the introduction of technology within the home to enhance the quality of life of its occupants, through the provision of different services such as multimedia entertainment and energy conservation. There has been significant research into the field of home automation. The X10 industry standard, developed in 1975 for communication between electronic devices, is the oldest standard identified from the author's review, providing limited control over household devices through the home's power lines. Recently, research into the field of home automation has continued to receive much attention in academia. [2] developed a Java based home automation system. An embedded board physically connected all the home automation devices and, through integration with a personal computer (PC) based web server, provided remote access to the system. The use of Java technology, which incorporates built-in network security features, produces a secure solution. However, the system requires an intrusive and expensive wired installation and the use of a high end PC. [3] introduced a Bluetooth based home automation system, consisting of a primary controller and a number of Bluetooth sub-controllers. Each home device is physically connected to a local Bluetooth sub-controller. The home devices communicate with their respective sub-controller using wired communications. From the sub-controller all communications are sent to the primary

controller using wireless communications. It is desirable for each home device to have a dedicated Bluetooth module.

However, due to the fiscal expense of Bluetooth technology, a single module is shared amongst several devices. This architecture reduces the amount of physical wiring required and hence the intrusiveness of the installation, through the use of wireless technology. However, the architecture does not completely alleviate the intrusiveness of the installation due to the incorporation of some wired communications.

Moreover the sharing of single Bluetooth module between numerous devices has the disadvantage of incurring an access delay. Introduced a phone based remote controller for home and office automation. The system differs in that all communications occur over a fixed telephone line and not over the Internet. The system can be accessed using any telephone that supports dual tone multiple frequency (DTMF). The disadvantages of this system are threefold: users are not provided with a graphical user interface, users have to remember an access code, and they have to remember which buttons to press for the control of connected devices. [5] proposed a novel control network, using hand gestures. The controller uses a glove to relay hand gestures to the system. The problem with the system lies in the inaccuracy of hand gestures, with the potential for normal arm movements being inaccurately interpreted as commands. Moreover, there is the risk of user fatigue if repetitive hand gestures are required. The introduction provides a short review of the existing academic research into home automation. The publically available research into home automation lies predominantly in the academic arena, with little industrial research being publically available. The adoption of home automation technologies into commercial systems has been limited, and where available consumer uptake has been slow. The aforementioned systems offer little in the way of interoperability. Attempts have been made to provide network. Interoperability and remote access to home automation systems through the development of home gateways. [6] Defined a home gateway as the point of ingress between a personal area network and a public access network. They developed a web server based home gateway to interconnect IEEE1394; with a power line based home automation system, and the Internet. To make the system more attractive to home owners, a real time AV transcoding capability was included. The system offers an insightful look into the development of a home gateway; however, the use of power lines as the communication medium limits the positioning of devices within the home to areas in close proximity to power sockets. [7] Proposed a home energy management focused home Gateway, which connects the home network with the Internet. The system was installed in twenty houses in the Tokyo area. [8] Proposed a home gateway based on the OSGI (Open Service Gateway Initiative), which allows service providers to access home automation systems for administration and maintenance services. The proposed system is divided into two subsystems. The first is the DSM (Digital Home Service Distribution and Management System), which provides a user interface for the control and monitoring of connected home automation devices. The second is the Home Gateway, which is responsible for managing the home automation system. This open architecture raises privacy problems which, for some users, may be much greater than the advantages offered by

granting third party access. [9] Implements a home gateway that accepts mobile phone signals and activates or deactivates

A. LED representing a home device.

These systems have made a significant contribution to the Development of a home gateway. However, the existing Network infrastructure within the home environment has not been taken into consideration when selecting the networks for integration with the respective home gateways. Moreover, the existing research has focused on the provision of remote connectivity and has largely neglected .

B. Analysis of the Existing Systems

The adoption of home automation technology by consumers has been limited. We propose that, from the home automation domain analysis, the problems limiting wide spread consumer adoption can be grouped into five general categories. Firstly, complex and expensive architecture: the existing systems architectures generally incorporate a personal computer for the purposes of network management and provision of remote access. This adds additional complexity to the system, hence increasing the overall fiscal expense. Secondly, intrusive installation: the majority of systems require varying levels of physical wiring in their architectures. This, in some cases, is due to the expense of the alternative wireless technologies. Hence, these systems require intrusive and expensive installations. Thirdly, lack of network interoperability: both home networks and the home automation systems which utilise them have been developed and adopted in an unplanned and ad-hoc manner. This has lead to a home environment consisting of a complex maze of heterogeneous networks. These networks and the systems that utilise them normally offer little interoperability; leading to three potential problems.

- Duplication of monitoring activities, due to lack of Interoperability;
- The possibility of interference, between co-existing Networks;
- The potential for two simultaneous, autonomous actions on co-existing networks, interacting and resulting in an undesirable outcome. Fourthly, interface inflexibility: the existing systems offer varying approaches for users to control and monitor the connected devices. However, this is normally limited to a single method of control, which offers users limited flexibility.

The systems which provide more than one interface ndevice normally provide different user interfaces and risk confusing users. Finally, security and safety: the existing approaches have not focused on security and safety problems that may arise from their implementation. Moreover, the systems that offer some degree of security have neglected the problems with sharing information between devices produced by multiple vendors for the purposes of establishing security.

C. Features of the proposed System

This paper presents a novel, stand alone, low-cost and flexible ZigBee based home automation system. The architecture is designed to reduce the system's complexity and lower fiscal costs. Hence, the system endeavours not to incorporate complex and expensive components, such as a high end personal computer, where possible. The system is flexible and

scalable, allowing additional home appliances designed by multiple vendors, to be securely and safely added to the home network with the minimum amount of effort. The system allows home owners to monitor and control connected devices in the home, through a variety of controls, including a ZigBee based remote control, and any Wi-Fi enabled device which supports Java. Additionally, users may remotely monitor and control their home devices using any Internet enabled device with Java support. A home gateway is implemented to facilitate interoperability between heterogeneous networks and provide a consistent interface, regardless of the accessing device. A virtual home pre-processes all communications before they are realised on the real home automation system. All communications are checked for security and safety before being allowed to continue to their respective destinations. This paper is organised as follows: Section 2 discusses the developed home automation architecture, including a review of the technology used. Section 3 describes the implementation of the proposed system. Section 4 provides a discussion of the system evaluation and Section 5 provides a conclusion .

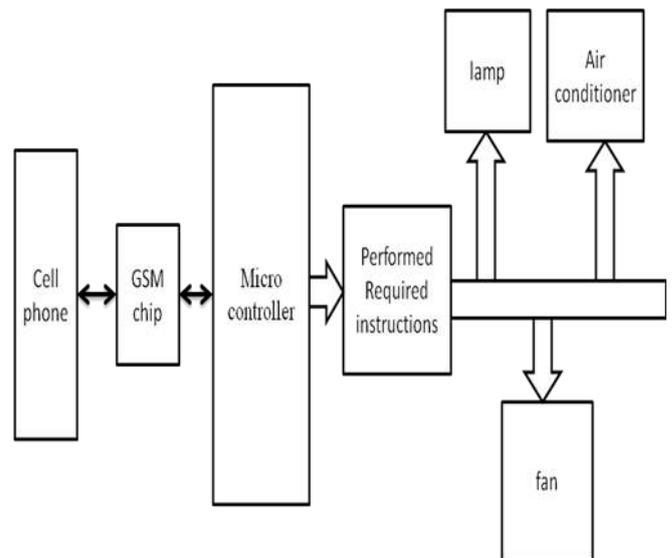


fig 2 Shows GSM Based Control System

Assuming that the control unit is powered and operating properly, the process of controlling a device connected to the interface will proceed through the following steps;

- The remote user provides miss call to the receiver.
- GSM receiver receives the rings of miss call sent from the user cell phone , GSM receiver sends the miss call as a signal to the microcontroller.
- Microcontroller issues commands to the appliances and the devices connected will switch ON/OFF.

SYSTEM ARCHITECTURE

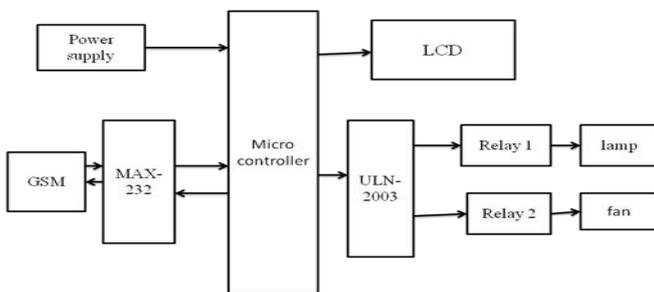


fig 1 shows system architecture

DESCRIPTION

The figure shown above is the simple block diagram of our project. It is a simple illustration of how we have implemented our project and the various parts involved in it. From the above representation, the first Mobile station is used as a transmitting section from which the user provides miss call to the GSM chip which is based on a specific area where our control system is located. The received miss call is given to the microcontroller and processed accordingly to carry out specific operations. The relay driver (BUFFER ULN2003) is used to drive the relay circuits which switches the different appliances connected to the interface. The operation performed by the microcontroller and also its inclusion makes the overall system user-friendly. The input from different sensors are feed to micro-controller and processed to operate respective task semi autonomously and autonomously.

Goals and Objectives

The project “GSM based Control System” at the title suggests is aimed to construct a control system that enables the complete control of the interface on which it is based. General objectives of the project are defined as;

- a. To co-ordinate appliances and other devices by providing miss call to the GSM chip.
- b. To effectively receive and transmit data via SMS
- c. To eliminate the need of being physically present in any location for tasks involving the operation of appliances within a household/office.
- d. Minimize power and time wastage

Intended Users and Uses

This system is aimed toward all the average users who wish to control their household/office appliances remotely from their cell phones provided that the appliances are electrically controllable. Example of feasible appliances and applications under consideration include; enable/disable security systems, fans, lights, kitchen appliances, and adjusting the temperatures settings of a heating/ventilation/air conditioning system.

Circuit Components

A. Micro-Controller

An embedded microcontroller is a chip, which has a computer processor with all its support function (clocking and reset), memory (both program storage and RAM), and I/O (including bus interfaces) built into the device. These built in function minimize the need for external circuits and devices to the designed in the final applications. The improvements in micro-controller technology has meant that it is often more cost-effective, faster and more efficient to develop an application using a micro-controller rather than discrete logic. Creating applications for micro-controllers is completely different than any other development job in computing and electronics. In most other applications, number of subsystems and interfaces are available but this is not the case for the micro-controller where the following responsibilities have to be taken.

- Power distribution
- System clocking
- Interface design and wiring
- System Programming
- Application programming
- Device programming

There are two types of micro-controller commonly in use. Embedded micro-controller is the micro-controller, which has the entire hardware requirement to run the application, provided on the chip. External memory micro-controller is the micro-controller that allows the connection of external memory when the program memory is insufficient for an application or during the work a separate ROM (or even RAM) will make the work easier.

B. ATMEL Micro-controller

The AT89C52 is a low-power; high performance CMOS 8-bit microcomputer with 8K bytes of Flash programmable and erasable read only memory (PEROM). The device is manufactured using Atmel's high-density non-volatile memory technology and is compatible with the industry-standard 80C51 and 80C52 instruction set and pin out. The On-chip Flash allows the program memory to be reprogrammed in-system or by a conventional non-volatile memory programmer. By combining a versatile 8-bit CPU with Flash on a monolithic chip, the Atmel AT89C52 is a powerful microcomputer which provides a highly-flexible and cost-effective solution to many embedded control applications.

The main features of this micro-controller are as follows;

- Compatible with MCS-51TM \Products
- 8K Bytes of In-system reprogrammable Flash Memory
- Endurance: 1,000 write/erase cycles
- Fully static operation: 0 Hz to 24 MHz
- Three-level Program Memory Lock
- 256 x 8-bit internal RAM
- 32 Programmable I/O lines
- Three 16-bit Timer/Counters
- Programmable Serial Channel
- Low-power Idle and Power-down Modes

C. Relay

NC: - Normally Connected

NO: - Normally Open

COM: - Common

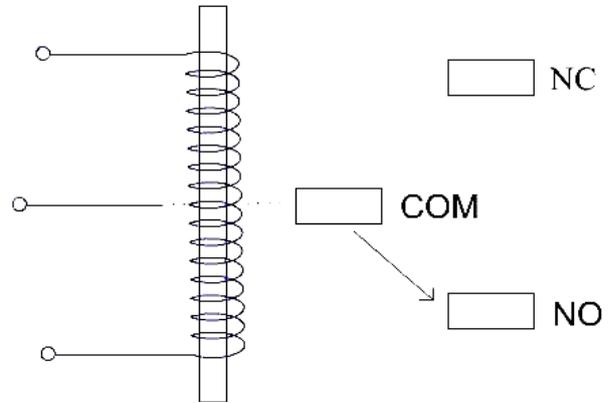


Fig 2: shows relay circuit

The relay driver is used to isolate both the controlling and the controlled device. The relay is an electromagnetic device, which consists of solenoid, moving contacts (switch) and restoring spring and consumes comparatively large amount of power. Hence it is possible for the interface IC to drive the relay satisfactorily. To enable this, a driver circuitry, which will act as a buffer circuit, is to be incorporated between them. The driver circuitry senses the presence of a "high" level at the input and drives the relay from another voltage source. Hence the relay is used to switch the electrical supply to the appliances. From the figure when we connect the rated voltage across the coil the back emf opposes the current flow but after the short time the supplied voltage will overcome the back emf and the current flow through the coil increase. When the current is equal to the activating current of relay the core is magnetized and it attracts the moving contacts. Now the moving contact leaves from its initial position denoted "(N/C)" normally closed terminal which is a fixed terminal. The common contact or moving contact establishes the connection with a new terminal which is indicated as a normally open terminal "(N/O)". Whenever, the supply coil is withdrawn the magnetizing force is vanished. Now, the spring pulls the moving contact back to initial position, where it makes a connection makes with N/C terminal. However, it is also to be noted that at this time also a back emf is produced. The withdrawal time may be in microsecond, the back emf may be in the range of few kilovolts and in opposite polarity with the supplied terminals the voltage is known as surge voltage. It must be neutralized or else it may damage the system.

D. ULN2003 IC

The ULN2003 is a monolithic high voltage and high current Darlington transistor arrays. It consists of seven NPN Darlington pairs that feature high-voltage outputs with common-cathode clamp diode for switching inductive loads. The collector-current rating of a single Darlington pairs 500mA. The Darlington pairs may be paralleled for higher current capability. Applications include relay drivers, hammer drivers, lamp drivers, display drivers (LED gas Discharge),

line drivers, and logic buffers. The ULN2003 has a 2.7kΩ series base resistor for each Darlington pair for operation directly with TTL or 5V CMOS devices.

Features:

- 500mA rated collector current (Single output)
- High-voltage outputs: 50V
- Inputs compatible with various types of logic.
- Relay driver application.

GSM Based Control System 22

Logical Diagram

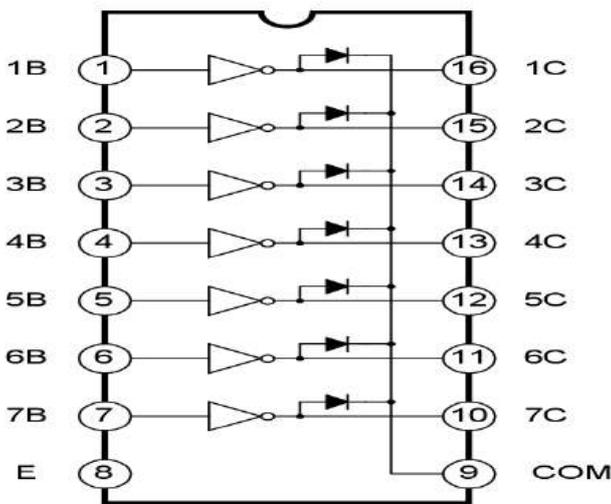


Fig 3: shows ULN 2003 IC

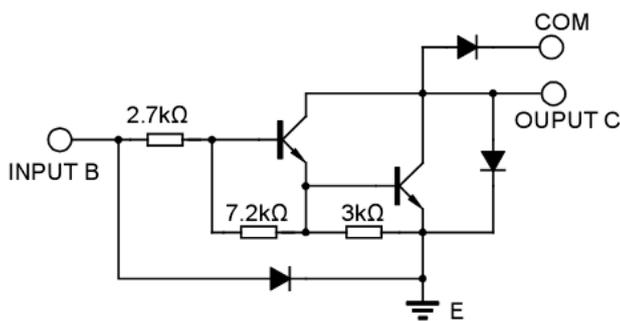


Fig 4: Shows Schematic Diagram (Each Darlington Pair)

GSM TECHNOLOGY

GSM is a global system for mobile communication GSM is an international digital cellular telecommunication. The GSM standard was released by ETSI (European Standard Telecommunication Standard) back in 1989. The first commercial services were launched in 1991 and after its early introduction in Europe; the standard went global in 1992. Since then, GSM has become the most widely adopted and fastest-growing digital cellular standard, and it is positioned to become the world's dominant cellular standard. Today's second-generation GSM networks deliver

high quality and secure mobile voice and data services (such as SMS/ Text Messaging) with full roaming capabilities across the world. GSM platform is a hugely successful technology and as unprecedented story of global achievement. In less than ten years since the first GSM network was commercially launched, it become, the world's leading and fastest growing mobile standard, spanning over 173 countries. Today, GSM technology is in use by more than one in ten of the world's population and growth continues to soar with the number of subscriber worldwide expected to surpass one billion by through end of 2003. Today's GSM platform is living, growing and evolving and already offers an expanded and feature-rich 'family' of voice and enabling services. The Global System for Mobile Communication (GSM) network is a cellular telecommunication network with a versatile architecture complying with the ETSI GSM 900/GSM 1800 standard. Siemen's implementation is the digital cellular mobile communication system D900/1800/1900 that uses the very latest technology to meet every requirement of the standard.

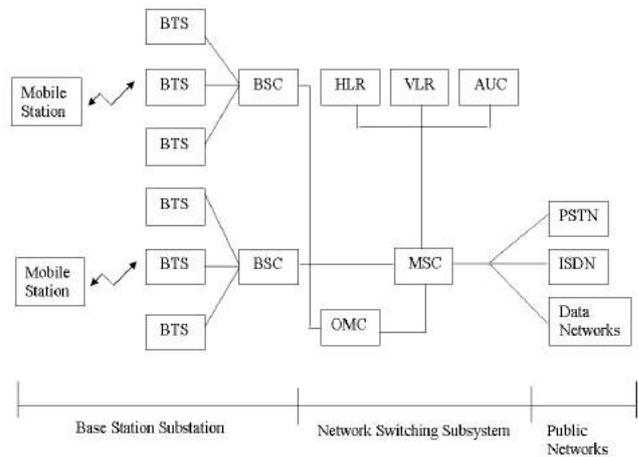


Fig 5: Shows GSM Architecture

Basic Specification in GSM

Parameter Specifications

- 1 Reverse Channel frequency 890-915MHz
- 2 Forward Channel frequency 935-960 MHz
- 3 Tx/Rx Frequency Spacing 45 MHz
- 4 Tx/Rx Time Slot Spacing 3 Time slots
- 5 Modulation Data Rate 270.833333kbps
- 6 Frame Period 4.615ms
- 7 Users per Frame 8
- 8 Time Slot Period 576.9microsec
- 9 Bit Period 3.692 microsecond
- 10 Modulation 0.3 GMSK
- 11 ARFCN Number 0 to 124 & 975 to 1023
- 12 ARFCN Channel Spacing 200 kHz
- 13 Interleaving 40 ms
- 14 Voice Coder Bit Rate 13.4kbps

Advantages

1. It Reduces wastage of power.
2. Helpful for handicapped Person.
3. Due to missed call approach no charges required.

Disadvantages

1. As, it depends on GSM network in absence of network call cannot be done.
2. More than 14 appliances cannot be connected.

Application

- Home Appliances
- Industries
- Institutions

Future Improvements

The future implications of the project are very great considering the amount of time and resources it saves. The project we have undertaken can be used as a reference or as a base for realizing a scheme to be implemented in other projects of greater level such as weather forecasting, temperature updates, device synchronization, etc. The project itself can be modified to achieve a complete Home Automation System which will then create a platform for the user to interface between himself and his household.

References

- [1] Mazidi, Muhammad ali, The 8051 Microcontroller and Embedded Systems, Second Edition, Prentice Hall, 2007
- [2] www.embedtronics.com, October 2008
- [3] ETSI TS 127 007 V5.3.0 (2003-03) Digital cellular telecomm. System, Universal Mobile Telecommunications System (UMTS); AT command s3G User Equipment (UE) (3GPP TS 27.007 version 5.3.0 Release 5, available online: <http://www.etsi.org>.
- [4] www.wikipedia.org



Frequency Synchronization in OFDM

Priyanka G. Kanaskar

Department of Electronics & Telecommunication
Anjuman College Of Engineering & Technology
Sadar, Nagpur, India
priyankakanaskar@yahoo.com

Prof. S. Ganar

Department of Electronics & Telecommunication
Anjuman College Of Engineering & technology
Sadar, Nagpur, India
sanjay_r_ganar@yahoo.com

Abstract— Orthogonal Frequency Division Multiplexing (OFDM) is one technique that has been proposed to offer substantially higher data rates than those currently available to the mobile user. As with any communications system effective, reliable and efficient techniques are required that will allow synchronization of remote terminal. Accurate frequency and timing synchronization of OFDM system is required in order to achieve good performance. The property that these systems rely on – orthogonality of the subcarriers will be lost if synchronization is inaccurate. In this paper we focus on the frequency synchronization. This paper presents a simple frequency synchronization technique that provide robust frequency offset over wide variety.

Keywords— OFDM, carrier frequency offset (CFO)

I. Introduction

Orthogonal frequency division multiplexing (OFDM) is a digital multi-carrier modulation technique that has been come increasingly popular scheme in modern digital communication. It is the attractive technique for high speed wireless communication. It is robust against frequency selective fading in multipath channel. Several wireless communication system adopt OFDM as a modulation technique such as wireless local area network (WLAN), wireless fidelity (Wi-Fi), 3rd generation partnership project long term evolution (3GPP LTE) & 4G LTE. It is also integrated in Digital Audio Broadcasting (DAB), Digital Video Broadcasting (DVB), DVB-T.

In OFDM, there are various domain of synchronizations such as timing synchronization, frequency synchronization and symbol synchronization. In this paper we examine the frequency synchronization. OFDM is very sensitive to carrier frequency offset (CFO) in the received signal due to Doppler shift or instability in local oscillator and results in a loss of subcarrier orthogonality. Hence it is required to reduce the frequency errors to small fraction of the subcarrier spacing. In this paper there are various techniques

have been proposed for the frequency synchronization in OFDM.

II. Ease of Use

- Dynamically allocates high speed serial bit streams to subscribers.
- Increases the spectral efficiency.
- Increases the channel capacity.
- To allow the flexible bandwidth allocation.
- In OFDM, the sub-carrier frequencies are chosen so that the sub-carriers are orthogonal to each other, meaning that cross-talk between the sub-channels is eliminated and inter-carrier guard bands are not required.

III. literature review

Moose [1] derived the maximum likelihood estimation (MLE) for carrier frequency offset (CFO) in frequency domain. The limit of acquisition for the CFO is $\pm 1/2$ of subscriber spacing. Schmidl and Cox [2] proposed frequency and timing synchronization algorithm by using repeated data symbol. Wei Zhong [3] proposed a novel integral frequency offset estimation which examined the phase changes of synchronization signals in frequency domain this method provides very low computational complexity. C. Geetha priya and A.M. Vasumathi [4] proposed accurate frequency synchronization method using Zadoff-chu sequence. Eric Bjornemo [5] proposed a Bayesian analysis in this way enables using fast frequency acquisition without pilots at low SNR. Ching-Liang Wang [6] proposed method of to make a modulatable orthogonal sequence partially geometric for Large CFO estimation. E.C. Kim [7] proposed enhanced the performance of frequency offset compensation by adding the ternary sequence to OFDM signals. Haling Minn [8] proposed frequency offset estimation approach using a maximum

likelihood principle with sliding observation vector. Adegbenga B. Awoseyila [9] proposed a novel technique for 3GPP LTE specifications using one training with simple structure of two identical parts to achieve robust and full range time-frequency synchronization in OFDM system.

IV. proposed synchronization solution

This paper proposed a new technique for frequency synchronization using a multidimensional filter banks. In OFDM, receiver carrier and transmitter carrier are generated from local oscillator. These local oscillator are not phase synchronous hence it creating the arbitrary phase error. Therefore deviations from local oscillators values will create carrier frequency offset (CFO).

$$\Delta f = f(tc) - f(rc)$$

The frequency error estimation should be performed after the receiver filter bank. If frequency error estimation is done then at the same time frequency error correction should be performed in front of filter bank. Since, the carrier frequency is the derivative of carrier phase with respect to time. The OFDM system with frequency estimation after filter bank will produce error estimates at maximum rate of $1/T$. In this frequency estimation, their having one filter-bank which carries filtered signal. And other is filtering feedback delay circuit which provides error frequency signal and this feedback frequency error signal is applied to frequency error correction through the feedback. If error will arises then it will correcting through feedback loop by using a filter bank.

V. CONCLUSION

We conclude that this filter bank approach is very efficient and time consuming having a very simple

circuit. With this type filter bank approach we will conclude frequency offset. Similarly we will conclude phase offset by adding phase error correction block.

VI. References

- [1] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Commun.*, vol. 45, pp. 1613–1621, Dec. 1997.
- [2] G. L. Ren, Y. L. Chang, H. Zhang and H. N. Zhang, "A Novel Burst Synchronization Method for OFDM Based WLAN Systems," *IEEE Trans. Consumer Electron.*, Vol. 50, 2004, pp. 829-834. doi:10.1109/TCE.2004.1341687
- [3] A. B. Awoseyila, C. Kasparis and B. G. Evans, "Robust Time-domain Timing and Frequency Synchronization for OFDM Systems," *IEEE Transactions on Consumer Elec-tronics*, Vol. 55, 2009, pp. 391-399.
- [4] Frequency Synchronization in OFDM System C. Geetha Priya1, A. M. Vasumathi2 *Journal of Signal and Information Processing*, 2013, 4, 138-143 doi:10.4236/jsip.2013.43B024 Published Online August 2013 (<http://www.scirp.org/journal/jsip>)
- [5] J. J. van de Beek, M. Sandell, and P. O. Borjesson, "ML Estimation of Time and Frequency Offset in OFDM Systems," *IEEE Trans. on Sig. Proc.*, vol. 45, no. 7, July 1997
- [6] Erik Bjornemo "Frequency Synchronization in OFDM," *IEEE Trans. On signal*., vol.0-7803-8887-9, 2005
- [7] B. Chen and H. Wang, "Blind Estimation of OFDM Carrier Frequency Offset via Oversampling," *IEEE Trans. Signal Processing*, vol.52, pp. 2047-2057, July 2004.
- [8] W. Zhong, "A Simple and Robust Estimation of Integral Frequency Offset for OFDM Systems," *IEEE Transac-tions on Consumer Electronics* Vol. 54, 2008, pp.41413. doi:10.1109/TCE.2008.4560107
- [9] H. Minn, V.K. Bhargava and K.B. Letaif, "A Combined Timing and Frequency Synchronization and Channel Estimation for OFDM Systems," *IEEE Trans. On Communications*, vol.54, 2006, pp. 416-422. doi:10.1109/TCOMM.2006.869860



Temper Protection For Live Video Using Digital Image Watermarking

Pratik Suresh Bang

*Department of Electronics Engineering
J.D. College of Engineering & Management
Nagpur, India*

E-mail address : prateek.bang@gmail.com

Contact No. : 9822701007

Abstract—With the rapid development and wide use of Internet, transmitting information faces a big challenge of security. So, people need a safe and secured way for transmission of information. Digital watermarking is a technique of data hiding, which provide security to the data. This paper presents a method to detect video tampering and distinguish it from common video processing operations, such as noise, and brightness increase, recompression using a practical watermarking scheme for real-time authentication to the digital video. In our method, the watermark represent the frame's indices and macro-blocks, are embedded into the non-zero quantized discrete cosine transform value of blocks, the last non-zero values enabling our method to detect temporal, spatial and spatio-temporal tampering. Our method can be easily configured to adjust robustness, transparency, and capacity of the system according to the specific application. In addition, our method takes advantage of content-based cryptography and increases the security of the system. While our method can be applied to all type of videos. Also, analyzing the detection error helps to distinguish malicious attacks from some common processing such as recompression. In our method a Spread Spectrum Watermarking algorithm is used for embedded watermarking into the video for authentication and contented based cryptography is used to provide security to the system. An Error Resilient technique using reversible data embedding in real time video aiming at high quality recovery under high loss rate is proposed. For compressed videos, predictive coding techniques increase the dependency between frames. When error occurs, it may propagate to other frames. In order to achieve higher compression ratio, it adopted prediction to further compress frames. Such technique also results in error propagation in frames. This paper proposes a new error resilient technique using reversible data embedding. The use of reversible data embedding technique is to provide better restoration and reduce noise ratio.

Keywords— *Digital images; Copyright Protection; Digital image watermarking.*

I. Introduction

Watermarking is a technique used to hide data or identifying information within digital multimedia. Our discussion will focus on the watermarking of digital video, though digital images and documents are also routinely watermarked. Digital watermarking is becoming very popular, especially for adding non-detectable identifying marks, such as copyright or author information. The digital watermarking process embeds a signal into the digital media without significantly degrading its visual (original) quality. Digital watermarking is a process to embed some information called watermark into different kinds of media called as Cover Work. Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the malicious or third party attacker. It is widely used in application for copyright protection for digital information. It is very different from the encryption in the sense that it allows the user to interpret, view and access the signal but protect the ownership of the original content. Digital watermarking involves embedding a structure in a host signal to “mark” its ownership. Digital watermarks are inside the information so that ownership of the information cannot be claimed by third party. While some watermarks are visible, most watermarks are invisible.

The fast growth of the Internet, sudden production of digital media, low-cost and reliable storage devices, and editing technologies have led to widespread forgeries and unauthorized sharing of digital media. Among these media, video is becoming increasingly important in a wide range of applications, such as video surveillance, video broadcast, DVDs, video conferencing, and video-on-demand applications, where authenticity and integrity of the video data is crucial. In surveillance applications, significant investments have been made in infrastructure, such as video cameras and networks installed in public facilities on a wide scale. However, current video editing software can be used to tamper

with such video, making them unreliable and defeating the purpose of such applications at the first place.

II. REVIEW OF RELATED RESEARCHES

My work has been motivated by a copious number of earlier works available in the literature that utilize digital image watermarking for protecting copyrights of digital images. A brief description of some recent important researches is presented below.

In earlier paper, a new rotation and scaling invariant image watermarking scheme is proposed by Dong Zheng, Sha Wang, and Jiying Zhao [1] based on rotation invariant feature and image normalization. Using maximum a posterior probability based image segmentation, the cover image is segmented into several homogeneous areas. Each region can be represented by a generalized Gaussian distribution, which is critical for the analysis of the watermarking processes mathematically. The advantage of this method a mathematical model is established to approximate the image based on the mixture generalized Gaussian distribution, which can facilitate the analysis of the watermarking processes. But the disadvantage of this technique is, when the image normalization was used to grant the rotation and scaling invariance to the disk regions, it was clearly shown in the experimental results that the performance of the watermarking scheme is not good against rotation. Through experiments, we find out that the feature points cannot be located accurately, if the watermarked image goes through distortions and geometrical transforms.

This paper by K. Ait Saadi, A. Bouridane, A. Gessoum [2] addresses the problem of ensuring the integrity and the authenticity of H.264/AVC video. It is achieved by authenticating each Group Of pictures (GOP) within the video separately. The proposed technique uses content based digital signature generated from robust features extracted from transform domain as fragile watermark and then embeds it in motion vectors belonging to the GOPs with the best partition mode in tree-structured motion compensation. Experimental results show that the proposed detects spatial cropping and temporal in a video. Fragile watermarking is used for tamper detection. It is highly sensitive to modification, making it difficult to distinguish malicious tampering from some common video processing operation such as Recompression. The method presented is designed to work in compressed domain, it is an extension and improvement of video authentication scheme developed in where cryptographic hash function has been used to ensure security by hashing the inherent features of the compressed H.264/AVC video to produce a compact size signature or watermark. But this technique cause more distortion in the image.

As technology grew up, a multibit, multiplicative, spread spectrum watermarking using the discrete multiwavelet (including unbalanced and balanced multiwavelet) transform was presented by Lihong Cui and Wenguo Li [3]. Performance improvement with respect to existing algorithm is obtained by means of a new just perceptual weighting (JPW) model. The new model incorporates various masking effects of human visual perception by taking into account the

eye's sensitivity to noise changes depending on spatial frequency, luminance and texture of all the image sub-bands. In contrast to conventional JND threshold model, JPW describing minimum perceptual sensitivity weighting to noise changes, is fitter for non-additive watermarking. Specifically, watermarking strength is adaptively adjusted to obtain minimum perceptual distortion by employing the JPW model. Correspondingly, an adaptive optimum decoding is derived using a statistic model based on generalized-Gaussian distribution (GGD) for multiwavelet coefficients of the cover-image. Furthermore, the impact of multiwavelet characteristics on proposed watermarking scheme is also analyzed.

Xiaoyu Feng, Hongting Zhang, Hsiao-Chun Wu [4] presented paper in which the digital imaging technology has grown explosively for multimedia applications in recent years. The need for the copyrighted digitalized media becomes urgent nowadays. An approach for the digital copyright protection is to employ advanced watermarking techniques, where watermarks can reveal the ownership identities. Generally speaking, the watermarks are embedded into an image or video signals. We will investigate digital watermarking techniques and propose a new optimal watermarking scheme. Efficient scale-factor optimization scheme is used, which can lead to the maximum overall SNR for both subject signal and watermarks. But this method has drawback that it detect the watermarked image, again shows as original as watermarked.

The method proposed by Satyendra N. Biswas [5] embeds several binary images decomposed from a single watermarked image into different scenes in a video sequence. The spatial spread spectrum watermark is embedded directly into the compressed bit streams by modifying the discrete cosine transform coefficients. Conventional watermarking techniques as available are not always competent enough to protect the authenticity of multimedia objects as they are usually applied in the uncompressed domain. In order to embed the watermark with minimum loss in image fidelity, a visual mask based on local image characteristics is incorporated. Simulation experiments demonstrate that the developed technique yields effective and robust protection against conventional spatial strikes, *viz.* Scaling and frame averaging besides temporal attacks.

III. Proposed Work

A watermark is a digital code permanently embedded into cover content into a video sequence. A watermark can carry any information you can imagine but the amount of the information is not limited. The more information a watermark carries the more vulnerable that information is. The amount is absolutely limited by the size of particular video sequence. Watermarking prefers robustness to capacity, thus a watermark typically carries tens to thousands of hidden information bits per one video frame.

Digital watermarking is a process for modifying physical or electronic media to embed a machine readable code into the media. The digital media may be modified such that the embedded code is imperceptible or nearly imperceptible to the user and may be detected through an automated detection

process. Most commonly, digital watermarking is applied to media signals such as audio signals, video signals, and images. However, it may also be applied to other types of media objects, including documents (e.g., through line, word or character shifting), multi-dimensional graphics models, and surface textures of objects and software.

Digital watermarking systems typically have two primary components first is an encoder that embeds the watermark in a host media signal, and second is a decoder that detects and reads the embedded watermark from a signal suspected of containing a watermark (a suspect signal). The encoder embeds a watermark by altering the host digital media signal. The reading component analyzes a suspect digital signal to detect whether a watermark is present or not. In applications where the watermark encodes information, the reader extracts this information from the detected watermarks in the video.

Nowadays, several particular watermarking techniques have been developed. The reader is presumed to be familiar with this field. There are particular techniques for embedding and detecting imperceptible watermarks in digital media. One particular problem in digital watermarking applications is synchronizing a detector to deal with geometric warping distortion of a watermarked image or video. A number of techniques have been developed for dealing with geometric distortion in watermarked images. One technique is to make the watermark more robust to geometric distortion by embedding it in attributes of the image that are relatively invariant to geometric distortion. While this improves detection in some cases, it typically does not address all forms of more complex, non-linear geometric distortion as well as geometric distortion. Another technique is to include geometric calibration features in the watermark signal that enable detection and estimation of the geometric distortion parameters, such as scaling and rotation. These features include, for example, calibration signal peaks in a particular transform domain, such as the auto-correlation domain and/or Fourier domain. These techniques use correlation techniques or other pattern matching methods to estimate affine geometric distortion parameters. For example, cross correlation of the received signal and the calibration signal in particular transform domains produce correlation peaks that correspond to affine distortion parameters, such as scale, rotation, translation, shear, and differential scale.

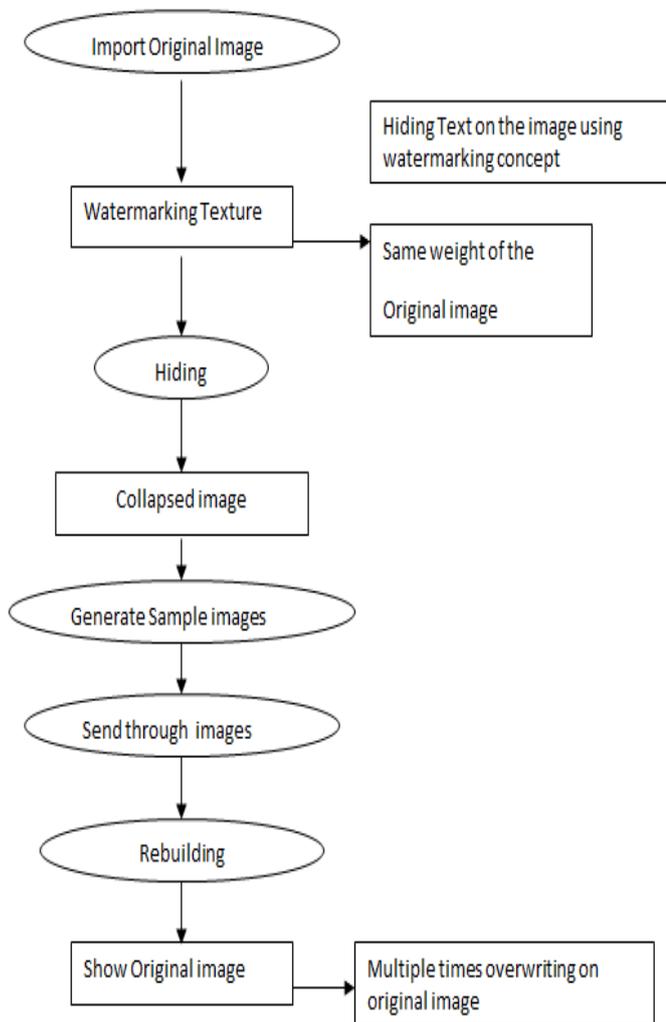
Such techniques do not provide error free estimation of geometric distortion. In some cases, even where the geometric distortion is linear, errors result from estimation. In addition, affine transform parameters can only approximate geometric distortion that is non-linear. For example, it can provide a piecewise linear estimate of affine distortion in sub-blocks of an image, but it cannot always accurately represent non-linear distortion in a manner that leads to error free recovery of the digital watermark message. The invention provides a method for synchronizing a watermark detector. One aspect of the invention is a method of synchronizing a digital watermark detector. The detector operates on a watermarked signal where a watermark signal has been distributed throughout the host media signal, and preferably, repeatedly embedded in segments of the host media signal (e.g., music, image or video signal). The method divides a watermarked signal into blocks, each block including a portion of a watermark signal. For example, in the case where the watermark is replicated in segments of the host signal, these blocks sub-divide each

segment into smaller parts. For each block, the method computes a local correlation space comprising a neighborhood of correlation values by correlating the watermarked data in the block with a known watermark signal at a neighborhood around the block. It then finds a correlation maxima in the local correlation space for each block, where the correlation maxima indicates a local offset used to align the watermarked data in the block before decoding a watermark message from the block.

This method applies to watermarked signals of varying media types. In addition, it may be used to synchronize watermark detection and message reading in various signal domains, such as a spatial domain, temporal domain, frequency domain, or some other transform domain (e.g., autocorrelation, wavelet, Fourier, etc.). For example, it can be applied in the spatial domain or spatial frequency domain for images and video frames, as well as the time or frequency domain for audio. It may also be applied in the time-frequency domain for audio and video signals. In one implementation, the method uses an estimate of affine geometric distortion parameters to transform an image block in the watermarked image to a position approximating an original orientation of the image block in the watermarked image. It then shifts the transformed image block to neighboring locations. The method then computes a correlation surface by finding the correlation between the watermark signal and the transformed block at its location and each of the neighboring locations. The method finds a correlation maximum in the correlation surface formed by the correlation values in the neighborhood. The location of the correlation maximum provides an offset value that further refines the orientation of the image data. A message decoder then decodes a watermark message from the watermarked image adjusted by the offset value.

In our proposed method, spread spectrum watermarking algorithm is used, in spread spectrum communications, one transmits a narrowband signal over a much larger bandwidth such that the signal energy present in any single frequency is not detectable. Similarly, the watermark is spread over very many frequency bins so that the energy in any one bin is very small and certainly undetectable. To insert a watermark in the frequency domain of an image we should first apply DCT (Discrete Cosine Transformation). This is a standard way to represent an image in frequency domain.

IV. Flow Chart



v. Methodology

Module Description:

1. Preprocessing

Color Enhancement, Improve the image quality, Size corrections, and noise removal.

Algorithm: Morphological Filters, Automatic Color Enhancement technique.

2. Resolution Hiding

Reduce the resolution or hide the original images using sample images.

3. Watermarking

Implementing multiple watermarking concepts to provide security for the original images. For that we are going to generate random sample images with the same pixels. Using these images we can overwrite on the original image and then we get a collapsed image.

4. Security providing

Multiple watermark process will generate random keys for each and every image.

Algorithm: Using these keys the reverse process will be done by receiver side.

References

- [1] Dong Zheng, Sha Wang, and Jiying Zhao, *Member, IEEE* "RST Invariant Image Watermarking Algorithm With Mathematical Modeling and Analysis of the Watermarking Processes" *IEEE Transactions On Image Processing*, Vol. 18, No. 5, May 2009.
- [2] K. Ait Saadi, A. Bouridane, A.Gessoum "H.264/AVC Video Authentication Based Video Content" *IEEE Transactions On Image and Signal Processing*, March 2010.
- [3] Lihong Cui and Wenguo Li" Adaptive Multiwavelet-Based Watermarking Through JPW Masking " *IEEE Transactions On Image Processing*, Vol. 20, No. 4, April 2011.
- [4] Xiaoyu Feng, Hongting Zhang, Hsiao-Chun Wu, Senior Member, IEEE, and Yiyang Wu, Fellow, IEEE "A New Approach for Optimal Multiple Watermarks Injection" *IEEE Signal Processing Letters*, Vol. 18, No. 10, October 2011.
- [5] Satyendra N. Biswas, Sabikun Nahar, Sunil R. Das, Emil M. Petriu, Mansour H. Assaf, and Voicu Groza "MPEG-2 Digital Video Watermarking Technique" 2012 IEEE conference.



DESIGN OF OPEN CORE PROTOCOL BUS BRIDGE INTERFACE USING VHDL

Sonam Fulwadhvani
M.tech. Student (VLSI)
Dept. of ETC
Jhulelal Institute Of Technology
Nagpur, Maharashtra
fulwadhvani.sonam@gmail.com

Abstract—System on Chip (SoC) design is becoming challenging due to its complexity and the necessity of Intellectual Properties (IP) reuse to shorten the design time. OCP (Open Core Protocol) is an efficient bus protocol for the core communication between IP blocks. Bus Bridge interconnects other bus standards to OCP. I2C is a simple bidirectional two wire bus for efficient inter IC control. This paper focuses on the implementation and design of Bus Bridge using OCP master and I2C slave protocol. Multi voltage design for power reduction is the important feature of the paper. The implementation of the developed FSMs for OCP and I2C was done in VHDL and was synthesized using Xilinx ISE 10.1 synthesis tool design compiler.

Keywords—I2C controller, OCP Bridge, OCP compliant, Master, Slave, Interface, Power reduction, Multi voltage Design.

I. INTRODUCTION

Current technology trends, scaling and with end users show a marked preference for the smaller geometries of deep sub micron processes force a design style where multiple independent circuit implementations are integrated together into a single System-On-Chip (SoC). However, contemporary SoC designs have their own share of issues and challenges. The major challenges faced by a design engineer include the ever increasing complexity in modern SoC designs, reusability, time-to-market, communication between Intellectual Property (IP) cores, integration of different clocked domain IP cores, and global clock distributions on a chip. The design of standard Network-on-Chip (NoC) interfaces to SoC is pivotal in addressing design reusability, time-to-market, and integration of IP cores employing different clock domains (synchronous, elastic, and asynchronous).

OCP is a standard core-centric protocol which addresses the IP cores reusability. This not only allows independent IP core development without IP core interconnect network but also allows IP core development in parallel with a system design, reducing design time, design risk, and manufacturing costs. OCP data communication models range from simple

request grant handshaking through pipelined request-response to complex out-of order transaction. OCP describes a point-to-point interface between two communication module, such as

IP cores and bus interface modules (bus wrappers).

II. OCP COMPLIANT SYSTEM

OCP's strength is the ability to configure an interface to match a core's communication requirements. At least one OCP interface must be included in the core for compliance. All aspects of the OCP interface specification must be complied by each OCP interface on the core. There are 3 major types of interfaces as specified by OCP. (i) Bus Bridge Interface (ii) Processor Interface (iii) Memory Interface. The Bus bridge interface includes an external bus like AXI or USB and the internal bus will be OCP. The Processor interface includes the interface between processors which include only the OCP master. These interfaces differ in protocol features or signals to optimize the needs of IP cores. Whereas, they follow the same OCP timing and validation rules, that simplifies the cost in and implementation verification.

III. OCP bridge interface system

To simplify the creation of bridges to other interface protocols, the bridging profiles of OCP are designed. The bridge has an OCP master or slave protocol. It is classified into two types (i) A simple H-bus profile which provides a connection through an external bridge for example an AMBA AHB protocol to a CPU (ii) The X-bus profile supports non-cacheable and cacheable instruction and data traffic between CPU and the memories and register interfaces of other targets.

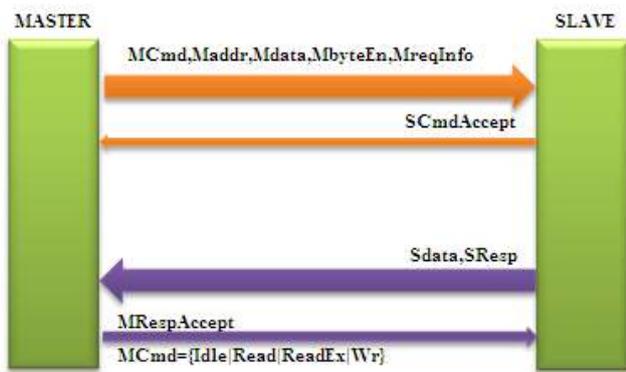


Figure1.Simple H bus signal Processing

IV. THE SYSTEM IMPLEMENTED

The need for a model to understand the OCP bus bridge compliant system and also a processor interface system, the scope of the research is extended. The design comprises the Bus Bridge system as the OCP Master and I2C controller as the OCP Slave. The Master accepts responses and gives requests whereas the Slave receives and responds to the requests provided by the master. Acknowledgments are indicated with the help of the Handshake Signals that are provided for both Master as well as the Slave. The Processor which is designed with OCP master is interfaced with the I2C controller which gives the output serial I2C buses.

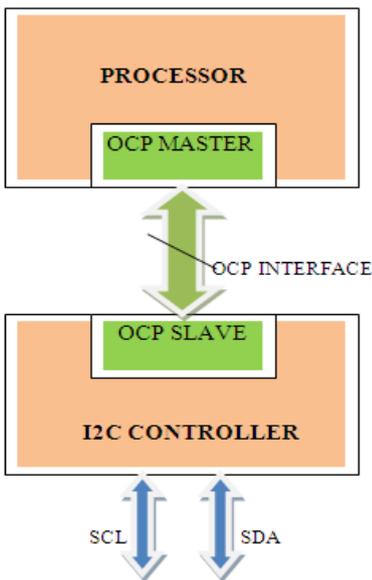


Figure2. Block Schematic of the Implemented Design

The I2C controller responds to the master signal from the processor and gives the serial two wire output SDA and SCL. By switching the command field to write the master starts its write operation and presents a valid data and address. According to the Design a write is performed when the Slave accepts the command and captures data and address. The

master initiates a read request by switching its command field to read. Thus it presents a valid address and the slave accepts the command. The data from the specified address is captured by the slave and is driven to the master. This proposed system is parameterizable for both address and data.

A. I2C Controller without OCP

In the Interface an I2C controller is designed as a Slave. The data is transferred in I2C bus synchronously to SCL on the SDA line on a byte by byte basis. For each data bit there is one SCL clock pulse with the MSB being transmitted first. Each transferred byte is followed by an acknowledgment bit. The master provides the slave address for I2C slave, the address and data to be written and read. According to the I2C bus protocol, these are the output of I2C serial buses SDA, SCL.

TABLE I. DESIGN PARAMETERS OF I2C CONTROLLER

Design Parameter	Size (in bits)
Address	8
Data	8

B. Processor without OCP

In the Interface, the Processor is the Master whose address and data are mapped to the I2C controller which gives the I2C bus protocol. A multicycle processor with 32-bit address and 32-bit data is designed as the Master that allows a functional unit to be used more than once per instruction.

TABLE II. DESIGN PARAMETERS OF PROCESSOR

Design Parameter	Size (in bits)
Address	32
Data	32
Instruction	32

C. OCP Compliant Processor

This processor is reconfigurable and is configured with OCP which contains the basic OCP signals and will serve as an OCP master. To transfer the command is OCP master command and this 3-bit signal indicates the type of OCP transfer the master is requesting. Depending on the direction of data flow, each non-idle command is either a read or write-type request. The slave will be either written into or read from, according to the Master command.

D. OCP Compliant Bus Bridge Interface

For the Interface, the entire system acts as an OCP-I2C bus bridge. This design presents the Peripheral profile with simple read and write whereas Generic profile with data handshaking.

E. OCP Compliant I2C Controller

The master provides the transfer requests to which the I2C controller, which acts as the slave, responds. The I2C controller is configured which contains the basic OCP signals

Quantity		Value
Minimum period	Without OCP	1.061ns
	With OCP	1.061ns
Minimum period	Without OCP	942.774MHz
	With OCP	942.774MHz

and will act as an OCP slave. The master receives the Sent back response signals.

V. OBSERVATIONS AND RESULTS ON EXPERIMENTATION

A. Design Setup

The Table below gives the test set up for the implementation of the Proposed design.

TABLE III. SETUP SUMMARY

Design method	VHDL based behavioral modeling
Synthesis platform	Xilinx ISE 10.1

B. Synthesis Results

Xilinx ISE 10.1 design compiler is used to synthesize the proposed design. Xilinx ISE is a complete ECAD application that helps to design, debug and test

Quantity		Value
Minimum period	Without OCP	2.001ns
	With OCP	1.900ns
Maximum frequency	Without OCP	499.725MHz
	With OCP	526.288MHz

the integrated circuits. In this design, the master, the slave and the interface were synthesized separately and then the interface without Burst transfer.

The table below shows the timing analysis of the I2C controller with and without OCP.

TABLE IV. TIMING ANALYSIS OF I2C CONTROLLER

The table below shows the timing analysis of the Processor.

TABLE VI. TIMING ANALYSIS OF PROCESSOR

TABLE VII. TIMING ANALYSIS OF BRIDGE INTERFACE

Quantity		Value
Minimum period	Without OCP	2.217ns
	With OCP	2.238ns
Maximum frequency	Without OCP	450.979MHz
	With OCP	446.867MHz

On comparing the timing analysis of the designs with and without wrapper it is found that there is a little variation in the speed of operation with the use of OCP. On synthesis, it can be obtained that the device utilization is better for OCP compliant designs.

C. Power Analysis

The modern day semi-conductor industries are focusing on the Power dissipation of the design. The components in the active area contribute the major part of power which is the Dynamic power. The advanced synthesis tools are ASIC as compared to the FPGA tools and are specific. These tools are available for different technologies. The table below shows the power consumption by various designs.

TABLE VIII. POWER ANALYSIS

Design	Dynamic power
Processor without OCP	843.383uW
Processor with OCP	876.514uW
I2C Controller without OCP	65.4895uW
I2C Controller with OCP	88.019uW
Bus Bridge Interface without OCP	919.810uW
Bus Bridge Interface with OCP	962.312uW

The operating voltage of the system is 5V. There is an increase in the amount of power used with the introduction of OCP interface. This increases the hardware complexity of the design and that might be the reason for the increased power.

D. Multi-Voltage Design-Power Reduction

In today's system-on-chip designs, Energy Efficiency has become a very important issue to be addressed. One way that lowers the power consumption is reducing the Supply Voltage. Thus, to provide flexibility in controlling the power and performance tradeoff, Multi Supply Voltage (MSV) is introduced. One of the latest ways for Power Optimization is by lowering the voltage supply and is one of the most effective ways. For dynamic power, a minor adjustment to voltage level can result in a significant reduction in power consumption, which is proportional to the square of the voltage.

VI. CONCLUSION

A parameterizable and reconfigurable OCP compliant bus bridge interface and processor interface system specifically targeted to use with high speed applications has been presented in this paper. The lack of availability of a common interface that can be used with the different IP cores in a SoC design, is the primary trigger to the development of such a design. The

complexity of the design is increased due to interfacing of different IP cores through different protocols in a SoC design. A common interface that supports all the needs of current day SoC design and it provides IP core reusability is required. That also would reduce the complexity of the system. OCP provides that common interface for IP core reusability.

In this paper, OCP for bus bridge is implemented. A comparison of the performance is being made of the bridge interface with and without OCP. In terms of speed and power consumption, the interface with OCP is preferable. The proposed design reduces the power consumption with a high speed and is a good alternative for any SoC design.

REFERENCES

- [1] Ramesh Bhakthavatchalu, Deepthy G R, Vidhya S and Nisha V, "Analysis of Low Power Open Core Protocol Bridge Interface Using VHDL", 978-1-4244-9477-4/11/\$26.00 ©2011 IEEE.
- [2] G. Geetha Reddy, K. Vanisree, David Solomon Raju. Y, "Implementation of Bus Bridge between AHB and OCP", Global Journal of Advanced Engineering Technologies, Vol1, Issue4-2012 ISSN: 2277-6370.
- [3] Nayab Rasool Shaik, Srikanth Pothula in "Design of Open Core Protocol", International Journal of Soft Computing and Engineering (IJSCIE) ISSN: 2231-2307, Volume-1, Issue-5, November 2011.
- [4] Chih-Wea Wang, Chi-Shao Lai, Chi-Feng Wu, Shih-Arn Hwang, and Ying-Hsi Lin, "On-chip Interconnection Design and SoC Integration with OCP", Proceedings of VLSI-DAT, 2008, pp. 25– 28, April 2008.
- [5] Naseer Rasool .T1 , Shaik Jaffar2, Shaik Saheb Basha3 Design and Analysis of Open Core Protocol for the on Chip Bus Using VHDL International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064.
- [6] Kun Tong and Jinian Bian, "Assertion-based Performance Analysis for OCP Systems." In Proc. *Circuits, Signals, and Systems (CSS 2007)*, Banff, Alberta, Canada, July 2007
- [7] T. Bjerregaard, S. Mahadevan, R. Olsen, and J. Sparso, An OCP compliant network adapter for GALS-based SoC design using the MANGO network-on-chip, In Proceedings of International Symposium on System on-Chip 2005. IEEE, 2005
- [8] V. S. Vij, R. P. Gudla, and K. S. Stevens, "Interfacing synchronous and asynchronous domains for open core protocol," in *27th International Conference on VLSI Design and 13th International Conference on Embedded Systems*, 2014, pp. 282–287.
- [9] Shihua Zhang, Asif Iqbal Ahmed and Otmane Ait Mohamed, "A Reusable verification Framework of Open Core Protocol", Circuits and Systems and TAISA Conference, 2009, pp. 1-4, June 28, 2009
- [10] Bhakthavatchalu R, DeepthyG.R., ShanoojaS, "Implementation of Reconfigurable Open Core Protocol compliant memory system using VHDL" Industrial and Information Systems (ICIIS), 2010, International Conference ,2010,pp.213-218 ,July 29,2011.

Design and Implementation of 128 bit Quadruple Precision Fused Multiply Add Unit for Many Core Processors

¹Ms. Mithilesh Mahendra,

Assistant Professor, Tulsiramji Gaikwad-Patil College of Engineering and Technology,
Nagpur, India.
mithileshmahendra@gmail.com

Abstract- Binary 128 arithmetic finds a hard in floating point application of Quadruple Precision. The major component of 128 bit Fused Multiply Add (FMA) unit with multimode operations are Alignment Shifter, Normalization shifter, Multiplier, Dual Adder by CLA. The main contribution of this paper is to reduce the latency. The technical challenges in existing FMA architectures are latency and higher precision. The precision gets affected by the repeated occurrence of fractional part. In order to reduce the latency the Multiplier is designed by using reduced complexity Wallace Multiplier and the latency of overall architecture gets reduced up to 15-25%. In this paper the total delay of multiplier designed using reduced complexity Wallace Multiplier is found to be 37.673 ns. Simultaneously to get higher precision we design namely Alignment Shifter and Normalization Shifter in the FMA unit by using Barrel Shifter as this Alignment Shifter and Normalization Shifter will have less precision, but since replacement of these blocks by Barrel Shifter will result into higher precision and the latency is further reduced by 25-30% and the total delay of Alignment Shifter and Normalization Shifter using Barrel Shifter is found to be 5.85 ns.

Keywords- Latency, Fused Multiply add, Computer Arithmetic, Multimode Operations, Floating Point Arithmetic

I. INTRODUCTION

IEEE-754 floating-point double precision (64-bit) or extended double precision (80-bit) arithmetic has been implemented in modern processors, but they are becoming insufficient for today's large-scale applications due to the accumulation of errors in computations, this errors increased gradually after many times of floating-point arithmetic operation, resulting in imprecise and incredible computation results and also increased latency. In order to improve the precision and latency of floating-point results, higher precision floating-point computation is required. The one promising approach to the precision problem is using the quadruple precision or QP floating-point data format also referred as binary128 as specified in the new IEEE-754-2008 standard [6], consisting

of three fields as the 1-bit sign (S), the 15-bit exponent (E) and 112-bit fraction (T) (Refer Figure 1). Another approach to increase the accuracy is using the fused multiply add (FMA). It combines improvements in performance (two operations in a single instruction) and improvements in accuracy (one single rounding) and is fundamental in many multimedia and scientific applications. The bias of exponent is 16383. The fraction of normalized data implies the integer bit as 1, which is not need to presented, so the precision is 113-bit in fact (Refer TABLE 1).

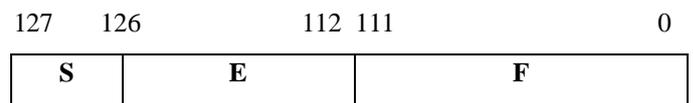


Figure 1: QP floating-point data format

TABLE I: IEEE 754-2008 FLOATING-POINT DATA TYPE

Floating Point Data Type	SP	DP	QP
Sign (S) width	1	1	1
Exponent(E) width	8	11	15
Fraction (T) width	23	52	112
Precision (p) width	24	53	113
Data width	32	64	128
Bias	127	1023	16383

II. RELATED WORK

A brief survey of the related work with reference to the requirements of high precision and high reliable floating-point arithmetic for technical computation shows the proposed architecture of a low-cost binary128 FMA design, which can perform a binary128 FMA operation with a latency of four cycles, or two binary64 FMAs fully pipelined operation with a latency of three cycles, or four binary32 FMAs fully pipelined

operation with a latency of three cycles [1]. Another research shows flexible multimode embedded Floating - point unit for FPGAs with dual-precision floating-point adder and multiplier each can perform one double-precision operation or two single-precision operations in parallel [2]. This paper also presented a novel design for a dual-precision floating-point multiplier to show that the FPGA with embedded multimode FPUs provide considerable performance and area benefits in single-precision, double-precision, fixed-point, and integer applications when implemented on the latest FPGAs, such as the Xilinx Virtex-5 FPGA. The paper [3] shows the high performance QPFMA with 7 stage pipeline satisfying the requirement of high performance processor. In this proposed work the complement of negative result by using the dual adder and the optimization LZA logic, reducing the data width of LZA and the level of normalization shifter, the hardware overhead and operation latency of the QPFMA is decrease. One more cascade design is proposed [4] which reduce the accumulation dependent latency by 2x over a fused design, at a cost of a 13% increase in non-accumulation dependent latency. For more latency sensitive applications, a cascade design provides a number of parameters that can be optimized, and in particular it allows one to create a design with very low effective latency between operations with sum dependence. The reduction in latency depends on two main optimizations: forwarding of unrounded results and tightening the accumulation bypass path by staggering the exponent and mantissa data path of the adder. The paper represents an architecture for the computation of the double-precision floating-point multiply-add fused operation to obtain the reduced latency floating-point addition, in which the alignment shifter, that is in parallel with the multiplier, is moved such that the multiplication can be bypassed, but this modification increases the critical path, a double-data path organization is implemented, in which the alignment shifter and normalization shifter are used in separate paths. [5]

III. PROPOSED WORK

Main optimization proposed is to design and simulate the reduced latency and high performance multi mode SOC quadruple precision (binary128) floating-point FMA architecture for the FPGA with the decreased latency and high precision. In this proposed work, the multiple mode computation such as multiply- add, multiply-sub, multiply-multiply and add-sub has been consider for the implementation. Figure 2 shows the overall architecture of QPFMA with the major components as Multiplier-113bit, 341bit Alignment Shifter, 342 bit Normalization Shifter, 342 bit Dual Adder, 228 bit Leading Zero Anticipator and the rounding block. This architecture is computing Quadruple Precision (QP) floating point data operation of $F = AB+C$. In which alignment shifter is used to align the value of C as per the exponent difference obtain from the exponent difference block, this difference value can vary and cannot be fixed depending on exponent value of A, B and C i.e E_A , E_B and E_C .

To make a synthesizable shifter block we design a shifter by using barrel shifter concept and power of 2.

The value of C will get shifted depending on the exponent calculation value. After every shifting the removed bits will generate sticky bit (st) as: If the operation is addition, then the st bit is produced by ORing all the bits of C which is shifted out beyond 341, but if the operation is subtraction, then the sticky bit is produced by ANDing all the bits of C which is shifted out beyond 341 after C bit is inverted.

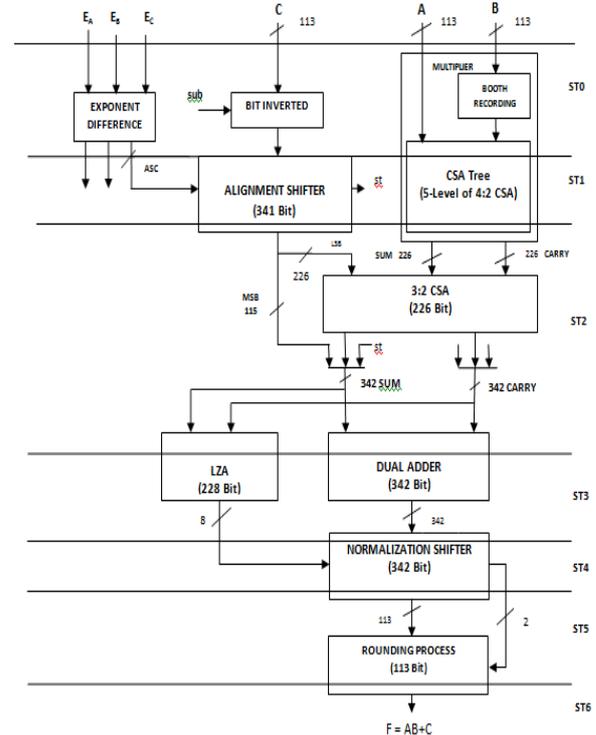


Figure 2. QPFMA Overall Architecture

After the generation of sticky bit it is jointed to the least significant bit (LSB) of the Sum` output from the 3:2 CSA as shown in figure 2, while a sticky bit produced from subtraction is jointed to the LSB of the Carry` output from the 3:2 CSA. Then both the correct sticky bit and complement of the addend C can be recognize when Sum` and Carry` are added. The output of 3:2 CSA is the A and B input to the dual adder which will add two numbers simultaneously and produce the sum output as the S0 and S1 and carry out (C_{out}). Considering the long latency of 342-bit adder, the dual adder is designed by using both the idea of end-around-carry adder and carry select adder.. As in paper [3] it is divided into 3 segments, including two parallel 114-bit adders with the same addends and carry in as 0 and 1 in each segment. The dual adder can calculate out the absolute of (Carry, Sum) directly, avoiding the complement of negative result and reducing the latency of a 342-bit adder. The latency of the dual adder is the latency of a 114-bit adder and a 2:1 multiplex. As the large area size will give very high delay and latency will get increased as observe in [3] the latency of the 342- bit adder is reduced to the latency of 114-bit adder and a 2:1 multiplex by

using the dual adder. Therefore in this proposed design the 113-bit multiplier is made up by using reduced complexity Wallace multiplier which will generate two products output simultaneously (Carry, Sum) by multiplying two inputs A and B. This product AB obtained after the multiplication is then added with the addend C which is available at the alignment shifter it will shift the addend C where as AB is fixed. This alignment shifter is designed by using the barrel shifter as shown in figure 3, where depending on the bit of addend C the select lines of MUX is activated and if the bit obtained is one it will shift the data otherwise it is kept as it is and forwarded for further operation to carry save adder and dual adder. Due to this the hardware overhead is reduced and thus the delay required is reduced and hence the latency will get reduced.

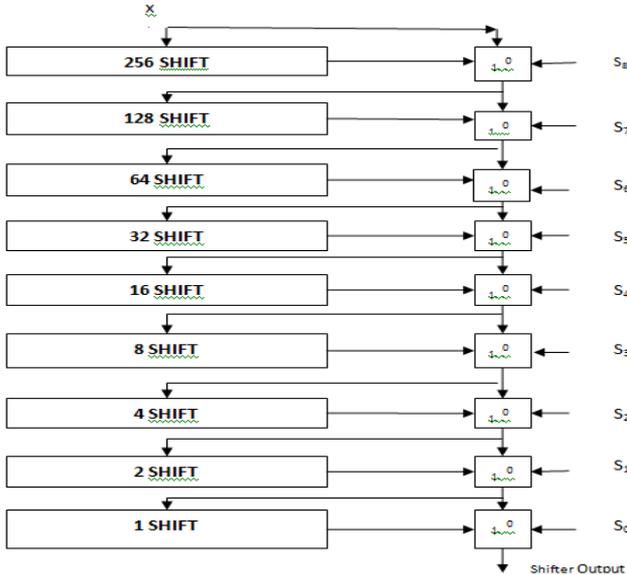


Figure 3: Block Diagram of Alignment Shifter Using Barrel Shifter

IV. SYNTHESIS AND SIMULATION

The Multiplier and Alignment shifter are the important part of the fused multiply add architecture in this paper multiplier is designed by using the reduced complexity Wallace Multiplier which has 114 bits input x (0:113) and 114 bits input y (0:113) and will generate product output of 226 bits p (0:225) at a time. The figure 4 shows the top view of reduced complexity Wallace multiplier. The figure 5 and figure 6 shows the internal structure of the multiplier design. The figure 8 shows the simulation waveform for the reduced complexity Wallace multiplier.

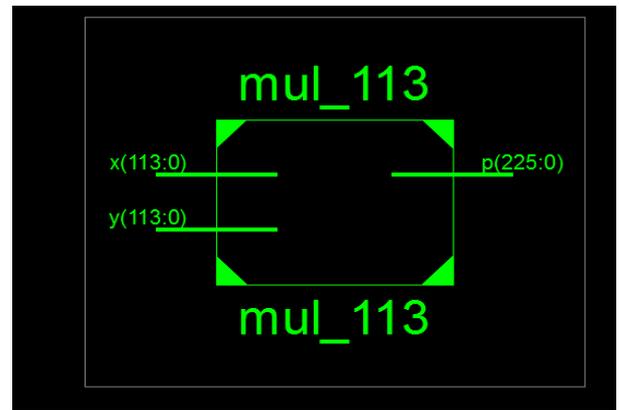


Figure 4: Top View of Reduced Complexity Wallace Multiplier

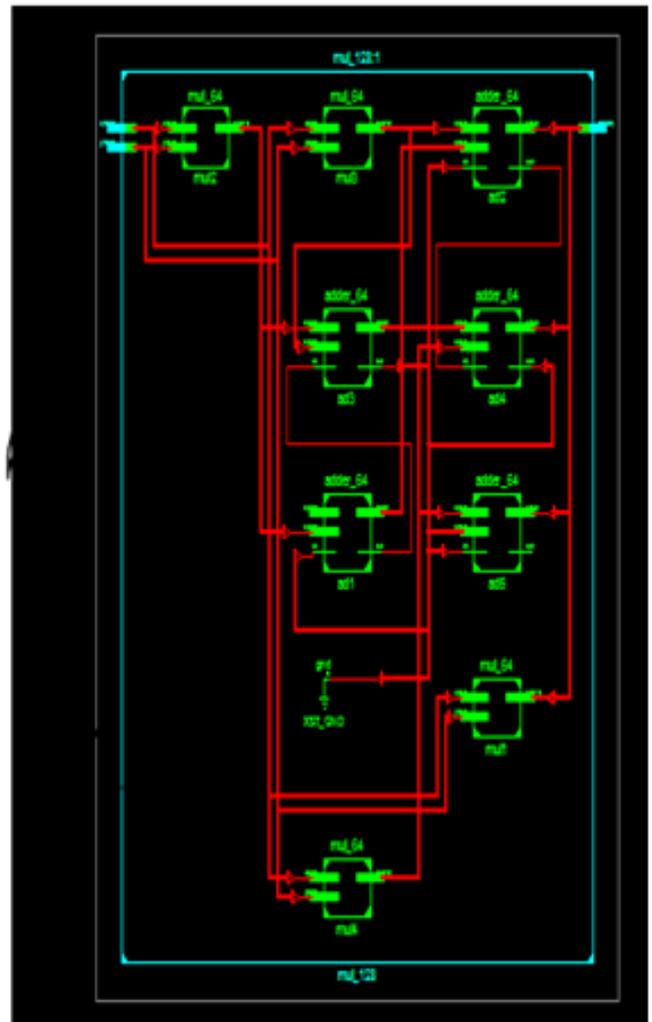


Figure 5: Simulation Result of Reduced Complexity Wallace Multiplier

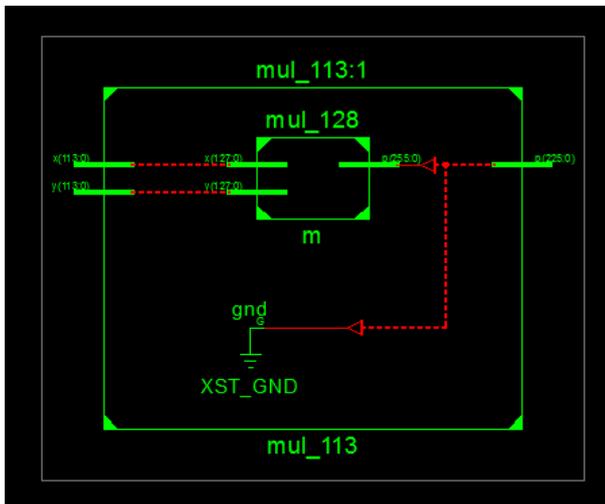


Figure 6: Internal design of 113 bit Wallace Multiplier

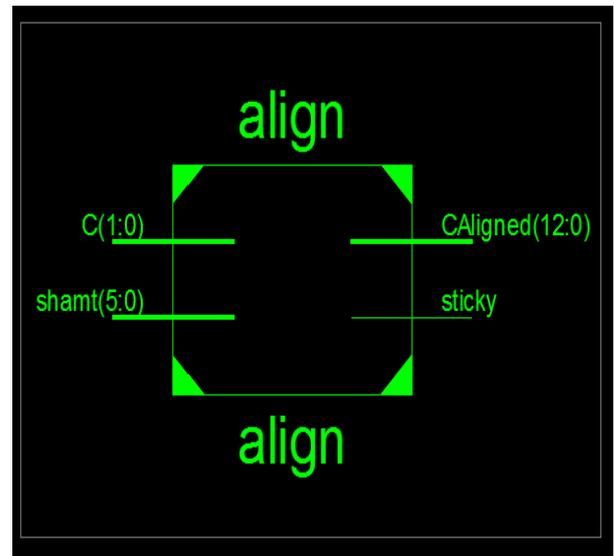


Figure 7: Top View of Alignment Shifter using Barrel Shifter

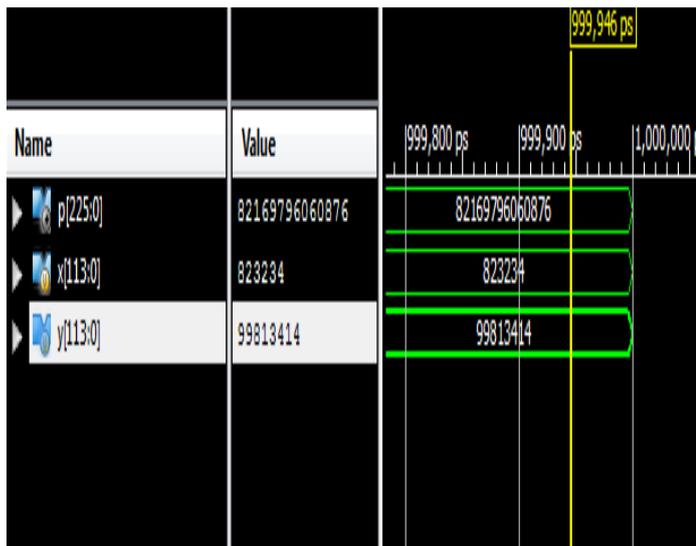


Figure 8: Simulation Result for Reduced Complexity Wallace Multiplier

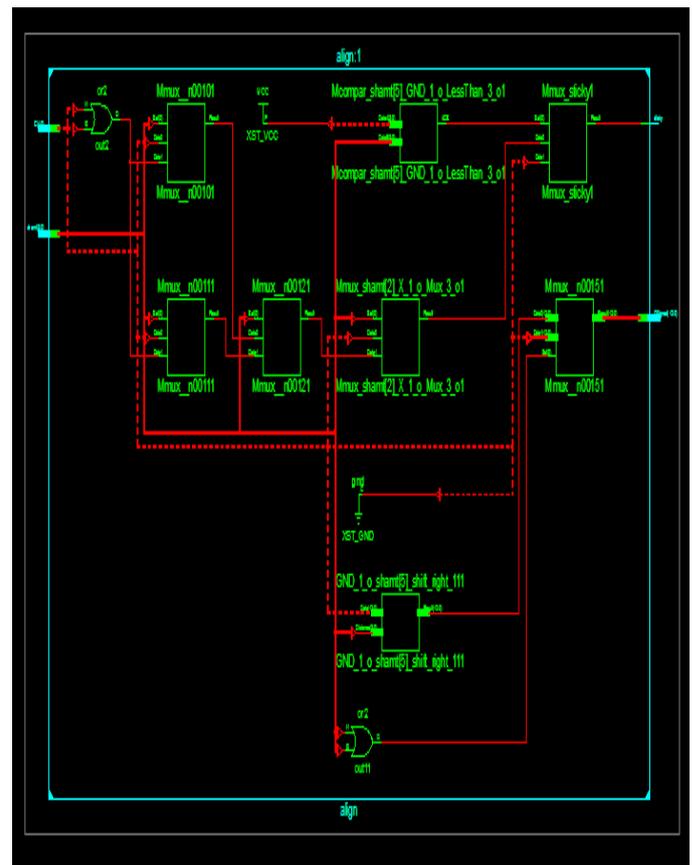


Figure 8: Internal Schematic of Alignment Shifter using Barrel Shifter

Whereas the Alignment shifter is designed by using the barrel shifter as shown in figure 7. in which the addend C is shifted left the position of 116 bit and then the C is shifted right according to the bit position of C if the bit is 0 then the C is not shifted, else if the bit is 1 then the C is shifted towards right and will generate the sticky bit as following: If the operation to be performed is the addition; then the sticky bit is generated by “OR”ing all the bits of addend C which are shifted out further than 341 and sticky bit thus generated is applied to the least significant bit (LSB) of the sum output from the 3:2 carry save adder. While if the operation is subtraction, then the C bit is inverted and the sticky bit is formed by “AND”ing all the bits of C shifted out beyond 341 and sticky bit thus generated is applied to the least significant bit (LSB) of the carry output from the 3:2 CSA. Then both the correct sticky bit and the addend C are applied to the dual adder for addition added

Figure 8 shows the internal schematic of the alignment shifter using barrel shifter. The figure 9 shows the simulation waveform for the alignment shifter using barrel shifter, which performs the shifting of addend C depending on the exponent bit.

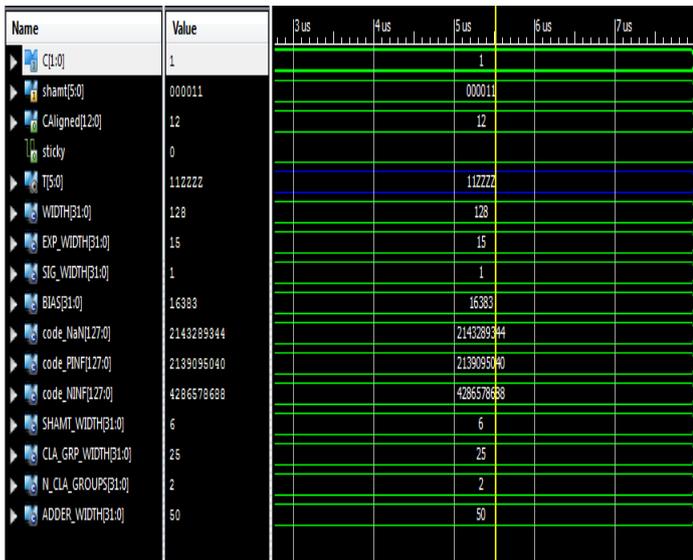


Figure 8: Simulation Waveform of Alignment Shifter using Barrel Shifter

V. RESULT

The synthesis result obtained from proposed design of multiplier by using the reduced complexity Wallace Multiplier and the Alignment shifter designed by using the barrel shifter for 128 bit Fused Multiply Add (FMA) unit is as (see Table 2)

TABLE II: COMPOUND ADDER SYNTHESIS RESULT

Designed Unit	Number of LUT uses as logic	Number of occupied Slices	Maximum Combinational path delay (ns)
Multiplier using Wallace Multiplier	18208	10168	37.673 ns
Alignment Shifter using Barrel Shifter	1236	469	5.845 ns

VI. CONCLUSION

In this paper, we have proposed the design of dual adder using compound adder and emphasize that the total delay of dual adder designed using compound adder is found to be 5.776 ns. The simulation and synthesis result indicates that the hardware overhead and the delay are reduced by this design. It will be further optimized by improvement in algorithm to decrease area and latency more.

ACKNOWLEDGMENT

The authors would like to propose a lot of thanks to the anonymous reviewers for their helpful feedback.

REFERENCES

- [1] Libo Huang, Sheng Ma, Li Shen, Zhiying Wang, Nong Xiao, "Low-Cost Binary128 Floating-Point FMA Unit Design with SIMD Support", IEEE TRANSACTIONS ON COMPUTERS, VOL.61, NO.5, 745-751, MAY 2012.
- [2] Yee Jern Chong and Sri Parameswaran, "Configurable Multimode Embedded Floating-Point Units for FPGAs", IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 19, NO. 11, NOVEMBER 2011, 1063-8210/\$26.00 © 2010 IEEE
- [3] He Jun, Zhu Ying, "Design and Implementation of a Quadruple Floating-point Fused Multiply-Add Unit", Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)
- [4] Sameh Galal, Mark Horowitz, "Latency Sensitive FMA Design", 2011 20th IEEE Symposium on Computer Arithmetic, 1063-6889/11 \$26.00 © 2011 IEEE DOI 10.1109/ARITH.2011.26
- [5] Bruguera, J.D.; Lang, T. "Floating-point fused multiply-add: reduced latency for floating-point addition", Proc. 17th IEEE Symp. Computer Arithmetic, Hyannis, 27-29 June, 2005.
- [6] IEEE Computer Society. IEEE Standard for Floating Point Arithmetic. IEEE Standard 754-2008, 3 Park Avenue New York, NY10016-5997, USA 29 August 2008.
- [7] T. Lang and J.D. Bruguera, "Floating-Point Multiply-Add-Fused with Reduced Latency," IEEE Trans. Computers, vol. 53, no. 8, pp. 988-1003, Aug. 2004.
- [8] Li Tie-jun, Li Qiu-liang, Xu Wei-xia, A High Performance Pipeline Architecture of 128bit Floating-point Fused Multiply-add Unit, JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY 2010, 32(2):56-60.
- [9] Seidel, P.M. Multiple path IEEE floating-point fused multiply-add, Proc. 46th Int. IEEE Midwest Symp. Circuits and Systems (MWSCAS), 2003.
- [10] Eric Quinnell, Floating-Point Fused Multiply-Add Architectures. Phd thesis, University of Texas at Austin, May 2007.
- [11] R. K. Montoye, E. Hokenek, and S. L. Runyon, "Design of the IBM RISC System/6000 Floating-Point Execution Unit," IBM J. Research & Development, vol. 34, pp. 59-70, 1990.
- [12] A. Akkas and M. Schulte, "A Quadruple Precision and Dual Double Precision Floating - Point Multiplier," Proc. Euromicro Symp. Digital System Design (DSD '03), pp. 76-81, 2003.
- [13] M.S. Schmoekler and K.J. Nowka, "Leading Zero Anticipation and Detection a Comparison of Methods," Proc. IEEE 15th Symp. Computer Arithmetic (ARITH), pp. 7-12, June 2001.
- [14] E. M. Schwarz, "Binary Floating - Point Unit Design: the fused Multiply - add dataflow", High - Performance Energy - Efficient Microprocessor, Edited by V. G. Oklobdzija and R. K. Krishnamurthy, Springer, Chapter 8, 2006.
- [15] G. Govindu, S. Choi, V. K. Prasanna, V. Daga, S. Gangadharpalli, and V. Sridhar, "A high-performance and energy efficient architecture for floating-point based LU decomposition on FPGAs," in Proc. 11th Reconfigurable Arch. Workshop (RAW), Santa Fe, NM, Apr. 2004, p. 149a.
- [16] Fousse L, Hanrot G, Lefevre V et al. Mpfr: A multiple-precision binary floating-point library with correct rounding. ACM Transactions on Mathematical Software (TOMS), 2007,33 (2):1-14.
- [17] M. J. Beauchamp, S. Hauck, and K. S. Hemmert, "Embedded floating point units in FPGAs," in Proc. IEEE Symp. Field Program. Gate Arrays (FPGA), 2006, pp. 12-20.
- [18] P. CDiniz and G. Govindu, "Design of a field-programmable dual-precision floating-point arithmetic unit," in Proc. Int. Conf. Field Program.Logic Appl. (FPL), 2006, pp. 1-4.



A Review on The Internet of Things

Deepak Fouzdar
Department of Electronics and Communication
TulsiramjiGaikwad-Patil College of Engineering and Technology
Nagpur

Abstract- Internet, the world-wise network of interconnected computer networks based on a standard communication protocol (TCP/IP). Thing, an object not precisely identifiable. Internet of Things (IoT), a world-wide network of interconnected objects uniquely addressable, based on standard communication protocol. Current internet is a collection of rather uniform devices, IoT exhibit much higher level of heterogeneity, as objects of totally different functionality, technology and application fields belongs to the same communication environment. Technological Trends-the identified five distinct macro-trends that will shape the future of technology, together with the explosion of ubiquitous devices that constitute the future of IoT like data deluge, decrease in energy required to operate intelligent devices, miniaturization of devices, autonomic management, IPv6 as an integration layer.

I. INTRODUCTION

Internet of Everything

The Internet of Things, also called The Internet of objects, refers to a wireless network between objects, usually the network will be wireless and self-configuring, such as household appliances.

Machine-to-Machine Era

Internet of Things refers to the concept that the internet is no longer just a global network for people to communicate with one another using computers, but it is also a platform for devices to communicate electronically with the world around them.

II. EVOLUTION OF INTERNET OF THINGS

Internet of boffins	<u>1965-1995</u>
Internet of geeks	<u>1995-2000</u>
Internet of masses	<u>2000-2007</u>
Mobile internet	<u>2007-2012</u>
Internet of things	<u>2012-bevond</u>

III. INTERNET USAGE AND POPULATION STATISTICS

World Population	6.3 Billion	6.8 Billion	7.2 Billion	7.6 Billion
Connected Devices	500 Million	12.5 Billion	25 Billion	50 Billion
Connected Devices Per Person	0.08	1.84	3.47	6.58
	2003	2010	2015	2020

IV. SALIENT FEATURES

A. Ambient Intelligence

The autonomous and intelligent entities will act in full interoperability & will be able to auto-organize themselves depending on the context, circumstances or environment.

B. Semantic Sharing

The machine can rend and send by it selves. No need to tell human beings.

C. Miniaturization

The devices become increasingly smaller.

D. Event Driven

Designing the scheme depending on the need.

V. ENABLING TECHNOLOGIES

A. RFID

To identify and track the data of things.

B. Sensor

To collect and process the data to detect the changes in the physical status of things.

C. *Smart Tech*

To enhance the power of the network by devolving processing capabilities to different part of the network.

D. *Nano Tech*

To make the smaller and smaller things have the ability to connect and interact.

VI. APPLICATIONS

A. *RFID*

Radio-frequency identification (RFID) is the wireless use of electromagnetic fields to transfer data, for the purpose of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by electromagnetic induction from magnetic fields produced near the reader. Some types collect energy from the interrogating radio waves and act as a passive transponder. These are widely used in transportation and logistics. Easy to deploy: RFID tags and RFID readers.

B. *WiFi*

WiFi is a local area wireless computer networking technology that allows electronic devices to connect to the network, mainly using the 2.4 gigahertz UHF and 5 gigahertz SHF ISM radio bands. Widely used both in indoor and outdoor environments. Highly interoperable.

C. *QR Code*

QR code (Quick Response Code). A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used.

D. *Sensors and Smartphones*

A sensor is a type of transducer whose purpose is to detect events or changes in its environment, and then provide a corresponding output. Sensors are used in everyday objects such as touch-sensitive elevators buttons (tactile sensor) and lamps which dims or brighten by touching the base, and smartphones.

E. *Smart wristband*

The Jawbone UP is a wearable wristband that has state of art sensors built into to track your health on the go. It has a built in heart health

sensor that can measure and track your resting heart rate while you are working or at home relaxing. It can automatically sync data of your workouts onto your phone to keep track of your daily and weekly workout regimen.

VII. WEB OF THINGS

To achieve IoT we need a universal protocol to combine several heterogeneous devices.

This protocol should be: simple, lightweight, loosely-coupled, scalable, flexible and standard.

- Several technologies and protocols are already available and widely accepted by the community:
 - HTTP, TCP, IPV6, XML, JSON, RSS, ATOM, REST, WS-*, URI, etc.
- URI to make the objects easily identifiable and addressable
- XML, WS-* and REST to allow the objects to expose their features and to communicate with external or centralized services.

VIII. ACKNOWLEDGMENT

I would like to mention my guide Prof. Supratim Saha who helped me in preparing the paper on this topic and guided me to understand the applications of IoT.

IX. REFERENCES

- [1] "*IEEE Xplore Full-Text PDF:*". Retrieved 26 June 2015
- [2] Kevin Ashton: That 'Internet of Things' Thing. In: RFID Journal, 22. Juli 2009. Abgerufen am 8. April 2011
- [3] Cisco: Over 50 billions of devices connected to Internet <http://blogs.cisco.com/news/the-internet-of-things-infographic/>
- [4] IoT - Visit the future: <http://www.iot-visitthefuture.eu/index.php?id=108>



Micro-controller Integrated Crop Management System

Diksha Rahangdale¹, Kalyani Gajpure²,
Pranjali Deshpande³

B.E. 8th sem, Electronics and Communication
Tulsiramji Gaikwad-Patil College of Engg. and Tech.
Nagpur, India

diksharah1994@gmail.com¹

gakalyani@gmail.com²

pranjali_16@yahoo.com³

Prof.. Gaurav Pohane

Electronics and Communication
Tulsiramji Gaikwad-Patil College of Engg. and Tech.
Nagpur, India

gauravpohane@gmail.com

Abstract—The recent trends in developing low cost techniques to support cost effective Agriculture in developing countries with large population has motivated the development of low cost sensing systems to provide for low cost irrigation facilities and also to provide for conservation of water at the same time. The current paper highlights the development of temperature and soil moisture sensor that can be placed on suitable locations on field for monitoring of temperature and moisture of soil, the two parameters to which the crops are susceptible. The sensing system is based on a feedback control mechanism with a centralized control unit which regulates the flow of water on to the field in the real time based on the instantaneous temperature and moisture values. Depending on the varied requirement of different crops, a lookup table has been prepared and referred to for ascertaining the amount of water needed by that crop.

Keywords—moisture sensor; temperature sensor; atmega16; solenoid valves;

I. INTRODUCTION

In the field of agriculture, use of proper method of irrigation is important and it is well known that irrigation by automatic crop manager using microcontroller is very economical and efficient. In the conventional crop manager irrigation system, the farmer has to keep watch on irrigation timetable, which is different for different crops. The project makes the irrigation automated. In a country like India, where the economy is mainly based on agriculture and the climatic conditions are isotropic, still we are not able to make full use of agricultural resources. The main reason is the lack of rains & scarcity of land reservoir water. The continuous extraction of water from earth is reducing the water level due to which lot of land is coming slowly in the zones of un-irrigated land. Another very important reason of this is due to unplanned use of water due to which a significant amount of water goes waste.

In the modern crop manager irrigation systems, the most significant advantage is that water is supplied near the root

zone of the plants drip by drip due to which a large quantity of water is saved. At the present era, the farmers have been using irrigation technique in India through the manual control in which the farmers irrigate the land at the regular interval. This process sometimes consumes more water or sometimes the water reaches late due to which the crops get dried growth rate, lighter weight fruit follows slight water deficiency. This problem can be perfectly rectified if we use automatic micro controller based drip irrigation system in which Slowed the irrigation will take place only when there will be intense requirement of water. Irrigation system uses valves to turn irrigation ON and OFF. These valves may be easily automated by using controllers and solenoids. Automating farm or nursery irrigation allows farmers to apply the right amount of water at the right time, regardless of the availability of labor to turn valves on and off.

Due to rapid climate change in recent decades, an increase in the severity of flood-related damages is observed. This causes serious destruction to residential properties and it also threatens public safety, particularly residents in the coastal regions or in the areas with heavy rain falls. The Federal Insurance and Mitigation Administration (FEMA)'s National Flood Insurance Program (NFIP) estimates that total losses due to six-inch flood are approximately \$20,000 per 1,000 square foot home [1]. Although several commercial flood warning systems are currently available, many of them are either expensive or unable to identify multiple water levels. In fact, some water detection devices are triggered by a single event and their alerts are broadcasted via a buzzer. However it is often too late for people to protect their belongings and evacuate to safe ground if their flood warning appliance is solely activated by a certain water level without pre-flood warning.

In addition, farmers using automation equipment are able to reduce runoff from over watering saturated soils, avoid irrigating at the wrong time of day, which will improve crop

performance by ensuring adequate water and nutrients when needed. Automatic Crop Manager Irrigation is a valuable tool for accurate soil moisture control in highly specialized greenhouse vegetable production and it is a simple, precise method for irrigation. It also helps in time saving, removal of human error in adjusting available soil moisture levels and to maximize their net profits.

II. AIMS AND OBJECTIVES

A. Aim

- The aim of the project is to mainly focus on automating the procedure of handling the agricultural equipment's in a traditional way.
- So various sensors like Moisture, Temperature, LDR has been used for automating purpose.
- Depending on moisture level the controller controls the flow of water using solenoid valves.
- The moisture sensors used are wireless to reduce the wiring and dig it in the soil.
- Apart from this as microcontroller is connected with water pump as well as humidity & temperature sensor, which check the requirement of water & can automatically turn on pump and feeds water to crops.

B. Objectives

- Modeling project covers the joint optimization of water-level detector and cropping system which operate on the basis of central well water level using solenoid valves.
- Different crops require different watering scheme, scheduling and different temperature conditions. So we are using ATmega-16 microcontroller to handle all this in a systematic way.
- The moisture sensors used are wireless so that the wirings are reduced and damage caused due to it can be prevented.
- Android application is used for system-user interface so that the messages can be delivered on the user's mobile directly.
- Infrared sensors are used for fencing purpose in order to prevent farm from the animals.

III. LITERATURE REVIEW

The micro-controller based automated real time Irrigation system will supply the following:

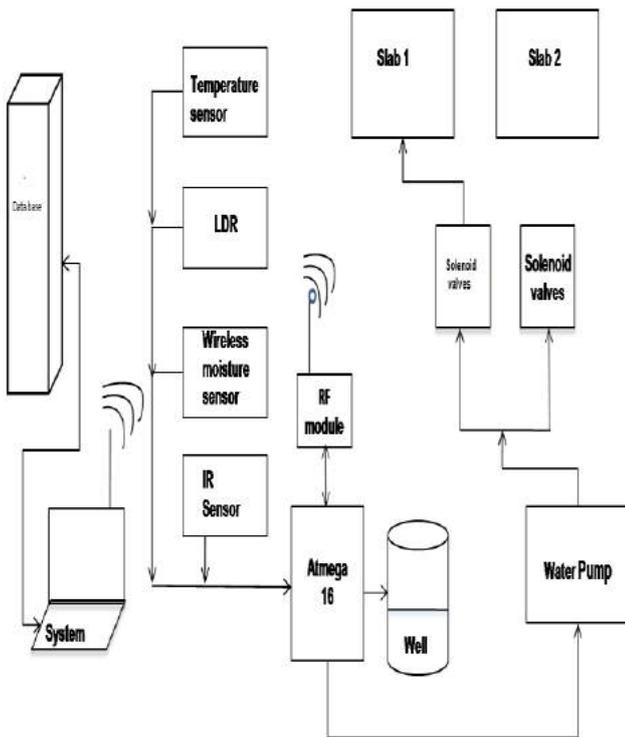
- As there is no unexpected usage of water, a lot of water is saved from being wasted.
- The irrigation system is use only when there is not sufficient moisture in the soil and the microcontroller decides when should the pump be turned on/off, saves a lot time and water for the farmers.
- As there is no unanticipated usage of water, a lot of water is saved from creature wasted. This also gives much wanted rest to the farmers, as they don't have to go and revolve the pump on/off automatically. The constant increasing command of the food provisions requires a rapid improvement in food production technology.

In an Automated Irrigation System using (AVR ATMEGA-16L), the most significant advantage is that water is supplied only when the moisture in soil goes below a determined threshold value. In current times, the farmers have been using irrigation system through the labour-intensive control in which the farmers irrigate the land at regular intervals by turning the water-pump on/off when essential. These procedures sometimes consume more water and sometimes the water supply to the land is delayed due to which the crops dry off. Water shortage deteriorate plants enlargement before visible wilting occurs. In addition to this slow development rate, lighter mass fruit follows water shortage. This problem can be absolutely rectified if we use Automated Irrigation System in which the irrigation will take place only when there will be strong requirement of water, as optional by the moisture in the soil. **Irrigation** is the artificial application of water to the soil usually for supporting in rising crops. In crop manufacture it is mostly used in waterless areas and in periods of rainfall shortfalls, but also to protect plants against hoarfrost.

The Microcontroller and soil moisture sensor based irrigation system proves to be a real time response control system which monitors and wheel all the activities of irrigation system. The present system is a model to modernize the agriculture industries at a mass scale with optimum expenditure. In this paper, an automated irrigation model is proposed using different circuits as demonstrated in different figures. We designed and implemented this model considering low cost, reliability, alternate source of electric power and automatic control. As the proposed model is automatically controlled it will help the farmers to properly irrigate their fields. The model always ensures the sufficient level of water in the paddy field avoiding the under-irrigation and over-irrigation they can provide irrigation to larger areas of plants with less water spending and inferior pressure. Using this system, one can save manpower, water to get better manufacture and eventually income. Advanced soil moisture level sensor will use in these we can measure different parameter that is pressure, temperature and humidity, of soil. Different amount of water requirements for different types of soil in this according to the type of crop, and water resistance capacity in different seasons, system provide definite amount of water to the plant hence, we can save large amount of water.

IV. WORKING

A. Block Diagram



B. Working

- When the power supply is on, the microcontroller is initiated and linked with the database system.
- The readings of moisture and temperature are received by AT-mega 16 from the respective sensors.
- The wireless moisture sensors are used so that the damage caused due to wiring can be prevented.
- If there occurs any insufficiency of moisture / water in any particular area; the water is supplied with the help of water pump through solenoid valves.
- The database is simultaneously updated as per the selected crop.
- LDR Sensor is used for automatic fencing lights in Night.
- Uploading all the above data to Online SQL Server for getting the updates on Android Mobile; else GSM text facility.
- Equipped Moisture Sensor is placed far from server without cabling, using WL CC2500 Module.

V. EXPECTED OUTCOME

This system is designed to eliminate the efforts of farmers as to check the moisture level of soil. This sensing of moisture sometimes becomes very difficult to do manually. Hence a Crop Management system is evolved which reduces these efforts and measure the moisture content of the soil. In an effort to increase agriculture's shares to the national economy serious measures need to be implemented to modernize present irrigation system. For modernization we

focused on this project and designed useful model for proper utilization of water and ensure maintaining required weather database of particular crop. This model report discusses a Crop Manager using micro-controller for remote operation of irrigation, this type of controller can save time as it can automatically control the farming without actually reaching the place.

Thus our aims in this way will get fulfilled which are stated below:-

- Reduce human efforts
- Efficient utilization of Water
- Proper feed to the crops sown
- Ensuring timely water supply according to respective season

VI. ADVANTAGES

- Crop Manager learns and adapts from every new input and will continually improve your new data asset for each growing area.
- Proper utilization of water using water level sensor.
- One time investment, providing the crops with required need.
- By applying innovative computational intelligence, Crop Manager merges the valuable historical data with the new data sets that are being delivered by all the emerging technologies within the agriculture industry.
- Creates a valuable asset in agriculture business.
- Crop Manager combines all of this data, expertise and implements it on the farm from the database. Crop Manager learns and adapts from every new input and will continually improve new data asset for each changing weather conditions

VII. APPLICATIONS

- This Module advice a farmer on how they can use the available water to their beneficial, in an attempt to save money & provide the crops with what they need to be healthy.
- As various sensors used this module helps the farmer decides the crops that the farm will grow to make most money, as well as be beneficial to the soil Crop Manager is a next generation, web-based decision support application, which delivers predictive information to the agriculture industry.
- By applying innovative computational intelligence, Crop Manager merges your valuable historical data with the new data sets that are being delivered by all the emerging technologies within the agriculture industry.
- Creates a valuable asset in your business. Applies enhanced data to any size growing area
- Crop Manager combines all of this data, expertise and knowledge for you. It allows you to link your

new data asset to your entire area of operation or any growing area.

VIII. CONCLUSIONS

- Multiple numbers of different crop's data can be pre-defined in the database.
- Can be implemented for greenhouse cultivation in projects.
- The system can be made flexible according to the farm land's requirements.
- Infrared automation technology can be implemented for pests, worm's etc. detection occurring on the crop to prevent further damage on a large scale.
- Continual nutrient monitoring to set parameters, including water top up, nutrient top up and water usage.
- Various feeding/watering/misting schedules, integrating real-time parameters such as air temperature and humidity.
- SMS and email alerts for deviations from parameters that may indicate a problem, for example burst pipe.
- Logging of key environmental variables including temperature, wind speed and direction, humidity and rainfall, for automated and management decision making secure off-site monitoring via the internet.
- Use of Solar cells to provide energy top the system.

IX. FUTURE SCOPES

- Multiple number of different crop's data can be pre-defined in the database.

- Can be implemented for greenhouse cultivation in projects.
- The system can be made flexible according to the farm land's requirements.
- Infrared automation technology can be implemented for pests, worms etc. detection occurring on the crop to prevent further damage on a large scale.

REFERENCES

- [1] Chaitali R. Fule¹, Pranjali K. Awachat², "International Journal of Advance Research in Computer Science and Management Studies" Volume 2, Issue 1, January 2014
- [2] Joaquin Gutierrez, Juan Francisco Villa-Medina, Alejandra Nieto-Garraway, and Miguel Ángel Porta-Gándara "Automated Irrigation System Using a Wireless Sensor Network and GPRS Module" IEEE 2013
- [3] Jia Uddin, S.M. Taslim Reza, Qader Newaz, Jamal Uddin, Touhidul Islam, and Jong-Myon Kim, "Automated Irrigation System Using Solar Power" ©2012 IEEE
- [4] Thomas J. Jackson, Fellow, IEEE, Michael H. Cosh, Rajat Bindlish, Senior Member, IEEE, Patric J. Starks, David D. Bosch, Mark Seyfried, David C. Goodrich, Mary Susan Moran, Senior Member, IEEE, and Jinyang Du, "Validation of Advanced Microwave Scanning Radiometer Soil Moisture Products", IEEE 2010
- [5] Andrew J. Skinner and Martin F. Lambert, "An Automatic Soil Pore-Water Salinity Sensor Based on a Wetting-Front Detector" 2010 IEEE
- [6] Samy Sadeky, Ayoub Al-Hamadiy, Bernd Michaelisy, Usama Sayedz, "An Acoustic Method for Soil Moisture Measurement", IEEE 2004.
- [7] G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)



Real Time Image Processing Using QT and Open CV

Aditya V. Wagh

Department of Electronics and Comm Engineering,
Tulsiram Gaikwad Patil College of Engg Nagpur
aditya.wagh2@gmail.com

Prof. Supratim Saha

Department of Electronics and Comm Engineering,
Tulsiram Gaikwad Patil College of Engg Nagpur

Abstract:

The rapid development of computer industry production and computer intelligence, as well as the corresponding developments in computer-aided image analysis, has made industrial image processing to be a very important branch of scientific image processing. Image processing is one of most growing research area these days and now it is very much integrated with the industrial production. Generally speaking, it is very difficult for us to distinguish the exact number of the copper core in the tiny wire, however, in order to ensure that the wire meets the requirements of production, we have to know the accurate number of copper core in the wire. Here the paper will introduce a method of image edge detection to determine the exact number of the copper core in the tiny wire based on OpenCV with rich computer vision and image processing algorithms and functions. The application (GUI) Graphical User Interface was designed using Qt and Linux gcc Integrated Development Environment (IDE) for implementing image processing algorithm using Open Source Computer Vision Library (OpenCV). This developed software integrated in mobiles by the cross compilation of Qt and the OpenCV software for Linux Operating system.

Keywords: *OpenCV, Linux Integrated Development Environment, Qt Creator, Image Processing*

either an image or one of the associated characteristics of that image. The image-processing techniques consider the image as a two-dimensional signal and apply some of the standard signal-processing methods on it.

At present, many dedicated software like MATLAB, Vivado, OpenCV, etc., are available for embedded system programming. Among these languages, OpenCV (Open Computer Vision) [5, 6], a well documented and vibrant open source C++ library growing with new computing technology applications, was designed and originally developed by Intel and now supported by Willow Garage, has a huge computational efficiency with a strong focus on real-time applications. It is a free source library for both commercial and non-commercial uses, which provides a simple-to-use computer vision infrastructure that helps build fairly sophisticated vision and real time image processing systems. OpenCV is written in optimized C and can take advantage of multi-core processors. Implementation of such useful library on an embedded processor like ARM makes it possible to achieve real-time image processing without any bottle necks in the software part. OpenCV is one of the most extended software libraries used in computer vision applications. OpenCV as an open source library .constituted by a series of C / C ++ functions and classes, offers many common algorithms to realize image processing and computer vision computing, which can be used to achieve powerful image processing, and to develop real-time applications system.

1. Introduction

Image processing is a multi-disciplinary subject, which has potential applications in many areas of science, engineering and technology, viz., biomedical, space, military, vision, biometrics, etc. Image processing helps to enhance an image or to extract hidden information from an image. In this paper, image conversion including C++ implementation, memory constraints and floating-point support to integrate with different embedded platforms like DSP, was carried out. In embedded system image processing, the input image, such as video frame or photograph, gives an output which can be

In the tiny wire industrial production process, it is very necessary for us to determine whether the wire meets specific quantity of copper. However due to the small size of the copper core and the defects, which to some extent increases the difficulty to distinguish. So we use the digital image processing to determine the exact quantity of the copper core. This paper describes how efficiently image processing applications can be used to check and judge the merits of the industrial product. In section 2 it describes previous work on the image before processing .In Section.3, the simulation environment and the experimental methodology to evaluate the dynamic library functions are presented. In Section.3, the

implementation of Embedded Device application using Qt is discussed in detailed. In Section 4, the extensive simulation results, analysis and the performance of the image quality are presented. Section 5 consists of the Flow Chart and Section 6 consists of Conclusion.

2. PREVIOUS WORKS ON IMAGE

A) Capture image

In OpenCV, the data type of image is usual IplImage. Comes from Intel Image Processing Library. Image Processing Library is inheritance from the actual OpenCV versions which may require IplImage data type is defined in CXCORE [3]. IplImage is the main image structure used in OpenCV. IplImage has been in OpenCV since the very beginning. It is a part of the C interface for OpenCV. You need to allocate and deallocate memory for IplImage structures yourself. OpenCV has many powerful image processing functions. In order to capture and show an image we should use cvLoadImage, cvNamedWindow, and cvShowImage functions. The function cvLoadImage loads the specified image file and return IplImage pointer to the file. CvName Window defines a window for displaying. The function cvShowImage display the image in the specified window. By using the above three functions, we can successfully display the image that we will deal with. The source image is as Fig. 1 which edge is not clear.

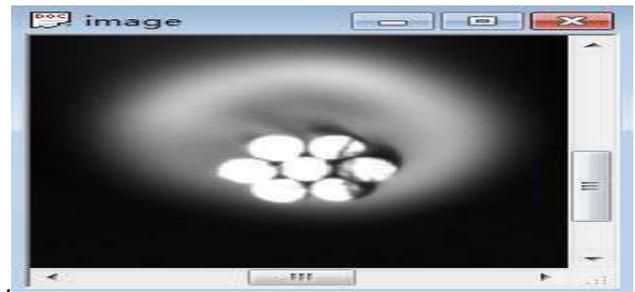


B) Color_to_Gray

Source images obtained are generally color but as we know grayscale images are very common and entirely sufficient for the task discussed in the paper. So there is no need to use more complicated and harder-to-process color images. For facilitating processing, color image will be usually converted to grayscale. A grayscale digital image is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest. Often, the gray scale intensity is stored as an 8-bit integer giving 256 possible different shades of gray from black to white. If the levels are evenly spaced then the difference between successive gray levels is significantly better than the gray level resolving power of the human eye. Opencv offers us cvCvtColor function to convert the color

image to grayscale image. The effect of RGB to Grayscale image is well demonstrated in the

Fig



C) Median Filter

At the same time, because of the noise interfering to the detection accuracy, it is necessary for us to do denoising for the captured images. Blurring image is the modest process in image processing. Blur, is a process done to reduce noise. As this can be achieved in different ways, this paper demonstrates a basic filter method-median filter. Median filtering method is a kind of nonlinear smoothing technique, and the gray value of its every pixel is set to a middle value of all the gray value of the pixel in a neighboring window. Median filtering is very effective to remove salt and pepper noise. OpenCV includes a Median filter that can be applied to an image by calling the cvSmooth function. The image after smooth processing is as Fig.



PREVIOUS WORKS ON EMBEDDED DEVICE

Since OpenCV library has many useful functions, which is widely used in many applications. Willow Garage's personal robot was developed using the OpenCV library with image Recognition n system. Stanley also used OpenCV library for his image processing engine. J.-P. Farrugia et al. uses GPUCV library, it needs additional computational resources, quick processing and with extra power consumption. Even though GPUCV library is group of OpenCV vision tasks, these can't use in embedded platforms such as mobiles, automotive and robots, which limits to thermal constraints. In Masayuki

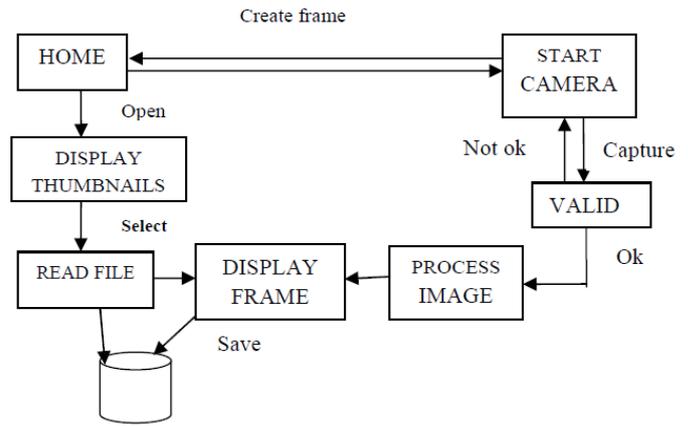
Hiromoto et al. paper gives embedded. applications includes mobile, robotics and etc. This also requires special embedded processors to achieve image recognition within the system's size and limited power. Clemens Arth et al. was developed the specialized DSP based enhanced system for image recognition. To overlay these issues on embedded applications, we propose optimized OpenCV implementation for image applications for mobile platforms.

3. METHODOLOGY AND SIMULATION ENVIRONMENT

In this section the tools and methodology to implement and evaluate the dynamically loading IPP with OpenCV libraries are detailed. The Intel Integrated Performance Primitives (IPP) was used to collect automatically OpenCV functions, to optimize the processors on the assembler level. So the task is to make those image processing libraries available on the development environment. This was performed with the image processing applications in real time. The computations on the processing are modeled as cycle accurate. The experimental results focused on the more complex comic images. We have used QT4.6.3 for the implementation of image application. This was developed by using OpenCV 2.0.0.CMAKE 2.8 GUI for cross compile OpenCV 2.0.0 for Ubuntu 12.04 LTS Express edition to get the image processing libraries. The simulation has done with Ubuntu 12.04 LTS on HP Laptop. HP Laptop built with Intel Duo Core CPU T5750 operated Linux OS, running at 2.0GHz with 32KB L1 D-Cache, 32KB L1 I-Cache 2MB L2 cache with 8-way set associative and 3GB RAM. Then using Qt, cross compiled images loads into ARM mini 2440 operated with Linux OS to display images without loss of quality of image..

4. IMPLEMENTATION OF EMBEDDED PLATFORM USING OpenCV

The image processing algorithms are implemented using OpenCV. OpenCV was designed for high computational efficiency with a strong focus on real time applications. OpenCV was written with optimized C, so it could yield benefit of multi-core processors.



The library was improved with C language according to mobile platform for image processing use on Windows. Fig. 1 shows the proposed implementation of image processing application on mobile.

5. Flow chart



6. Conclusions

In this paper, we presented a method to detect human upper body using Embedded Platform. ARM board is used to compilation of OpenCV image processing algorithm. The developed software was able to slice or chop the comics strip along border into individual units, stored on the permanent memory and displayed on the ARM Board. Human detection algorithm works on the basis of Haar like Features and this haar features are classify with using cascade classifier which is addition of weak classifier makes a strong classifier. This developed software can be easily integrated in ARM by the cross compilation of QT and the OpenCV software for an Operating system.

7. Acknowledgment

Here we are thanking to our collage to allow this research work and also to all Pre-Researchers

8. References

- [1] Khana, The future of Mobile Application Storefronts, Wireless Expertise market report, 2009
- [2] Fitzek and Reichert, Mobile Phone Programming and its Application to Wireless Networking, 2007
- [3] Jurgen Scheible and Ville Tuulos, Mobile Python: Rapid prototyping of applications on the mobile platform, 2007
- [4] <http://sourcefouge.net/projects/opencvlibrary>.
- [5] Willow Garage, Inc., Willow garage <http://www.willowgarage.com/> (August 2009).
- [6] J.-P. Farrugia, P. Horain, E. Guehenneux, Y. Alusse, GPUCV: a framework for image processing acceleration with graphics processors, in: Proceedings of the ICME, 2006.
- [7] Masayuki Hiromoto, Kentaro Nakahara, Hiroki Sugano, Yukihiko Nakamura, and Ryusuke Miyamoto, "Aspecialized processor suitable for adaboost-based detection with haar-like features," in Proc. of CVPR, 2007.
- [8] Clemens Arth, Florian Limberger, and Horst Bischof, "Real-time license plate recognition on an embedded DSP-platform," in Proc. of CVPR, June 2007.
- [9] S. Dikbas, T. Arici, and Y. Altunbasak, "Chrominance Edge preserving Grayscale Transformation with Approximate First Principal Component for Color Edge Detection", IEEE Proc. ICIP 2007, 11, 261-264, 2007.
- [10] K. Panetta, S. Qasi, and S. Aгаian, "Techniques for detection and classification of edges in color images", SPIE Proc., Volume 6982, pp. 69820W-69820W-11 (2008).
- [11] K. Panetta, S. Qasi, and S. Aгаian, "Techniques for detection and classification of edges in color images", SPIE Proc., Volume 6982, pp. 69820W-69820W-11 (2008).
- [12] H.M. Merklinger, "A Technical View of Bokeh," Photo Techniques, 1997
- [13] Linear Gaussian blur evolution for detection of blurry images E. Tsomkol H.J. Kim E. Izquierdo
- [14] X. Wang and J. Jian-Qiu, "An edge detection algorithm based on Canny operator". IEEE Proc. of the seventh International Conference on Intelligent Systems Design and Applications (ISDA2007), 623-628, 2007
- [15] E.J. Wharton, K. Panetta, and S. Aгаian, "Logarithmic edge detection with applications"., Journal of computers, 3(9), 2008.
- [16] S. Wesolkowski and Ed. Jernigan, "Color Edge Detection IN RGB using Jointly Euclidean Distance and Vector Angle". University of Waterloo, Waterloo Canada, Vision Interface 9-16, 1999
- [17] A. Koschan, "A Comparative Study on Color Edge Detecton", IEEE Proc. ACCV'95, Singapore, IIL 547-478, 1995
- [18] S. Dikbas, T. Arici, and Y. Altunbasak, " Chrominance Edge preserving Grayscale Transformation with Approximate First Principal Component for Color Edge Detection", IEEE Proc. ICIP 2007, 11, 261-264, 2007.
- [19] A. Koschan, "A Comparative Study on Color Edge Detecton", IEEE Proc. ACCV'95, Singapore, IIL 547-478, 1995.
- [20] JOHN CANNY "A Computational Approach to Edge Detection" IN IEEE Transactions on Pattern Analysis and Machine Intelligence, 679-698, 1986.



Automatic traffic red light detection system

¹Dolly Tambe, ²Roshani Dekate, ³Ankit Chauhan, ⁴Nikhil Sakhare, ⁵Sushma Raut

^{1, 2, 3, 4, 5}Department of Electronics Engineering,

^{1, 2, 3, 4, 5}Tulsiramji Gaikwad-Patil College of Engineering and Technology, Nagpur.

Abstract- Everyone is in a hurry these days and that is reflected in the erratic driving behavior we often see by drivers rushing to get somewhere. 'Red Light Runners' are on the rise and more alarming is the carnage that they are leaving behind in their haste.

Last year, 676 people were killed and an estimated 116,000 were injured in crashes involving drivers who ran red lights, stops signs and other traffic control devices. In Kentucky, there were 3,695 collisions resulting in 31 deaths from crashes caused by disregarding traffic signals.

Enforcement is the key to getting people to comply with the law, but communities don't have the resources to allow law enforcement to patrol intersections as often as is needed to ticket all motorists who run red lights. Many cities have installed cameras at large intersections and studies show that these cameras have been effective in reducing the number of citations written for disregarding traffic signals in these areas.

Keywords - Microcontroller Based System, Embedded System, Traffic Control Management.

1. INTRODUCTION

The obligation on the motorist is to stop, unless the light is green, in which case you may proceed only if it is clear and safe to do so. If the amber light is illuminated, a vehicle must stop, unless it has already passed the white stop line or the vehicle is so close to the stop line, that coming to a halt might cause an accident. If the red light is showing, then you must stop behind the stop line in all circumstances.

When approaching a traffic light that is illuminated on green, you may proceed if it is clear and safe to do so. If the light is amber, you must stop unless your wheels are already over the white line, or you do not have enough room to brake before the stop line without causing an accident. If the light is red, you are obligated to stop in all circumstances. If you do not stop when it is indicated that you should do so, you have committed a traffic light offence.

2. RELATED WORK

A. Intelligent Traffic Lights Based on RFID This paper states that the traffic management is the critical issue of the road. Traffic lights play an important role in the traffic management. The existing traffic lights follow the

predetermined sequence. So these lights are called static traffic lights. These traffic lights are not capable to count the number of vehicles and the priority of the vehicles on intersection point. As a result some vehicles have to wait even there is no traffic on the other side. The vehicles like Ambulance and Fire Brigade are also stuck in traffic and waste their valuable time. The proposed system provides quality of service to Emergency vehicles and improves the accuracy of Automatic Traffic Light Violation Detection system as well as helps to trace out the stolen vehicles using RFID.

D. Dynamic Traffic Light Sequence Using RFID It avoids problems that usually arise with standard traffic control systems, especially those related to image processing and beam interruption techniques. This RFID technique deals with a multi-vehicle, multilane, multi road junction area. It provides an efficient time management scheme, in which a dynamic time schedule is worked out in real time for the passage of each traffic column. The real time operation of the system emulates the judgment of a traffic policeman on duty. The number of vehicles in each column and the routing are proprieties, upon which the calculations and the judgments are based

3. PROPOSED SYSTEM

Radio Frequency Identification (RFID) devices consist of tags and readers that assist in the tracking of goods and vehicles. Tags are the devices that give identity to the vehicle and work like a wireless name plate. It transmits its identity to readers which are placed at strategic locations like RED light crossing of a premise, highway,. Readers pick up these signals and transmit them to the centralized data servers from where the information can be viewed or utilized any where. These readers can also trigger the other peripheral devices like an access control mechanism- boom barrier to operate as per the business logic. For. e.g on identifying a known vehicle, a reader can signal the boom barrier to open and allow the vehicle automatically. The read-range of the reader varies from 5m to 30 m depending upon the technology (Passive Vs Active) in place. The use of RFID technology also necessitates the purchase and utilization of either fixed or hand held readers which can help the guard to quickly access the vehicle information by bringing the device near the vehicle.

4. HARDWARE IMPLEMENTATION

A. Radio Frequency Identification (RFID) RFID is an acronym for radio frequency identification. Briefly the

RF stand for “radiofrequency” and ID means “identifier” that allows an item, for instance a library book, to be identified, accessed, stored, reprogrammed and communicated by using radio waves. Radio Frequency Identification (RFID) is a generic term for non-contacting technologies that use radio waves to automatically identify people or objects. There are several methods of identification, but the most common is to store a unique serial number that identifies a person or object on a microchip that is attached to an antenna. The combined antenna and microchip are called an "RFID transponder" or "RFID tag" and work in combination with an "RFID reader". An RFID system consists of a reader and one or more tags. The reader's antenna is used to transmit radio frequency (RF) energy. The tag will then modulate the electromagnetic waves generated by the reader in order to transmit its data back to the reader. The reader receives the modulated waves and converts them into digital data. There are two major types of tag technologies. "Passive tags" are tags that do not contain their own power source or transmitter. When radio waves from the reader reach the chip's antenna, the energy is converted by the antenna into electricity that can power up the microchip in the tag. The tag is then able to send back any information stored on the tag by reflecting the electromagnetic waves as described above. "Active tags" have their own power source and transmitter. The power source, usually a battery, is used to run the microchip's circuitry and to broadcast a signal to a reader. Due to the fact that passive tags do not have their own transmitter and must reflect their signal to the reader, the reading distance is much shorter than with active tags. However, active tags are typically larger, more expensive, and require occasional service.

Frequency refers to the size of the radio waves used to communicate between the RFID system components. Just as you tune your radio to different frequencies in order to hear different radio stations, RFID tags and readers must be tuned to the same frequency in order to communicate effectively. The read range of a tag ultimately depends on many factors: the frequency of RFID system operation, the power of the reader, environmental conditions, physical size of the tags antenna and interference from other RF devices. The Sunrom RFID Card Reader's antenna was designed with a RFID operation at a tag read distance of around 7 cm.

B. Global Position System (GPS) Global Positioning System (GPS) satellites broadcast signals from space that GPS receivers, use to provide three-dimensional location (latitude, longitude, and altitude) plus precise time. GPS receivers provides reliable positioning, navigation, and timing services to worldwide users on a continuous basis in all weather, day and night, anywhere on or near the Earth. The output is serial data of 9600 baud rate which is standard NMEA 0183 v3.0 protocol offering industry standard data messages and a command set for easy interface to mapping software and embedded devices.

The current GPS consists of three major segments. These are the space segment (SS), a control segment (CS), and a user segment (US).

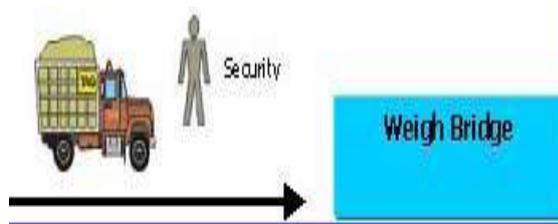
C. Global System for Mobile Communications (GSM) GSM uses Frequency Division Multiplexing AND Time Division Multiplexing. FDMA divides the frequency ranges for GSM, which are 890- 915, 935-960 and some others that the book didn't have. Each is divided into 200kHz wide channels. As far as TDMA goes, each time slot is 577 micro seconds long, 8 time slices is a frame, lasting for a grand total of 4.615ms. A multi frame consists of 51 frames, 51 multi frames make up a Super frame, and 2048 Super frames make a Hyper frame which is 2715648 frames. The GSM network can be divided into three parts to illustrate this, consider figure 1. i) Mobile station ii) Base station subsystem and iii) Network subsystem.

5. ADVANTAGES OF RFID IN VEHICLES

- Tamper proof
- Concealed installation of antennas
- Weather proof
- 100 % detection for two-wheelers / four-wheelers
- No height restrictions on vehicles as scanning is done from underneath
- RFID tags can be affixed to automobiles for activating hands-free access to communities and parking lots.
- The RFID reader can also trigger surveillance cameras or video recorders whenever a vehicle enters or exits the controlled area.
- Each access can be recorded in the RFID reader or host computer's database to maintain a history of access activities and administer billing of daily, weekly, or monthly fees.
- Gives automatic notification when a car enters or leaves the lot
- Eliminates manual record keeping, thereby increasing accuracy and staff productivity.

Tracking vehicles within the plant: The use of RFID in a vehicle assembly line ensures optimum operation, enhanced efficiency and eliminates the possibility of fraud and theft. Strategically positioned fixed RFID readers with multiple tag reading capability trace the newly finished cars as they leave the product line. In this way vehicles can be tracked throughout the plant.

Prevents manipulation of data: The security issues RFID tags to the trucks that are coming inside the premises. It is attached to the truck that carries the cane load and identification is done throughout its journey. The RFID antenna will be coupled to the PC and once the truck is over the weigh bridge the data is captured from the tag and this is passed on to the PC for processing. This can reduce your fraud activities drastically.



Better Fleet Management: RFID has enabled better fleet management. Now the transporters have a fix on reasons behind vehicular downtime. They know how long it takes to load raw materials and they can measure the performance of drivers. Transporters can plan availability of trucks based on the latest tracking data and make optimum use of their fleets.



Parking Lot Access Control: We also provide parking barrier drop-arm control systems to control authorized access into and out of the parking area. RFID based access control systems ensures that only authorized vehicles can get into and get out of the parking area. Parking barrier arms automatically lifts to let the vehicle pass through on success identification of the vehicle RFID tag. This can be done by fixing RFID tag to the windscreen of the vehicle. When the vehicle comes in range of the reader, the reader reads the card ID and authenticates the same. If ID is authenticated the relay for moving the boom barrier is fired and access to the parking lot is enabled. In this way there is no need for any guard to be monitoring the exit and entry of vehicles to the parking lot. The vehicles will be logged automatically and a total report of the usage of the parking lot can be generated.

6. CONCLUSION

This system will definitely help to traffic police to give the way to the ambulance when there is heavy traffic on the road. Also the condition of patient is monitored and this information is send to the respective doctor so that doctor can prepare for the next process before the patient reach to the hospital. The design and implementation of this technique is directly targeted for traffic management so that emergency vehicle on road get clear way to reach there destination in less time and without any human interruption. The main feature of this operation is the ability to communicate with purpose using GSM and GPS. It is very smart to find the location of emergency of VIP vehicle and get clear path to pass on.

7. REFERENCES

[1] Nor Azlina , Bt Abd Rahman , Mohsen Bafandehkar, Behzad Nazarbakhsh , Nurul Haniza Bt Mohtar , “Ubiquitous Computing For Security Enhancement Of Vehicles”, IEEE International Conference on Vehicular

Electronics and Safety (ICVES) ,Beijing, pp: 113- 118, 2011.

[2] Omidiora E.O, Fakolujo O.A, Arulogun O.T, Aborisade D.O, “A Prototype of a Fingerprint Based Ignition Systems in Vehicles”, European Journal of Scientific Research, pp: 164-171, 2011.

[3] Weiqi Yuan, Yonghua Tang, “The Driver Authentication Device Based on the Characteristics of Palm print and Palm Vein”, International Conference on Hand-Based Biometrics (ICHB), Hong kong, pp: 1-5, 2011.

[4] Hugo Silva, Andr’e Lourenc, O’Ana Fred, “In-Vehicle Driver Recognition Based on Hands ECG Signals”, International Conference on Intelligent User Interface , Lisbon, Portugal, pp: 25-28, 2012.

[5] Ronghua Chen, Mary Fenghua She, Xiangping Sun, Lingxue Kong, Yuchuan Wu , “Driver Recognition Based on Dynamic Handgrip Pattern on Stealing Wheel”, 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, Sydney NSW, pp: 108-112, 2011.

BER Calculation Using MATLAB Simulation for OFDM Transmission

Ashwin Shinde,

Asst Professor

Dr. Babasaheb Ambedkar College of
Engineering and Research, Nagpur

Sumedha Chokandre

Asst Professor

Dr. Babasaheb Ambedkar College of
Engineering and Research, Nagpur

Mayuri Marawar

Asst Professor

S.B. Jain Institute of Technology
Management and Research, Nagpur

II. OFDM SIMULATION

A. The Matlab source code

Abstract—Orthogonal frequency division multiplex (OFDM) modulation is being used more and more in telecommunication, wired and wireless. DVB and DAB already use this modulation technique and ADSL is based on it. The advantages of this modulation are the reason for its increasing usage. OFDM can be implemented easily, it is Spectrally efficient and can provide high data rates with sufficient robustness to channel imperfections. The purpose of this paper is to use a Matlab simulation of OFDM to see how the Bit Error Ratio (BER) of a transmission varies when Signal to Noise Ratio (S/N Ratio) and Multipropagation effects are changed on transmission channel.

Index Terms— BER, FFT, ISI, OFDM, S/N

I. INTRODUCTION

In an OFDM [4] scheme a large number of sub- channels or sub-carriers are used to transmit digital data. Each sub-channel is orthogonal to every other. They are closely spaced and narrow band. The separation of the sub-channels is as minimal as possible to obtain high spectral efficiency. OFDM is being used because of its capability to handle with multipath interference at the receiver.

These two are the main effects of multipropagation [3]. Frequency selective fading and Inter Symbolic Interference (ISI) [5]. In OFDM the large number of narrow band sub-carriers provides sufficiently “flat” channels. Therefore the fading can be handled by simple equalizing techniques for each channel. Furthermore the large amount of carriers can provide same data rates of a single carrier modulation at a lower symbol rate.

The symbol rate of each channel can be dropped to a point that makes each symbol longer than the channel’s impulse response. This eliminates ISI. The two main drawbacks of OFDM are the large dynamic range of the signals being transmitted and the sensitivity to frequency errors.

Using a Matlab simulation we can implement an OFDM transmission. Using the simulation we can easily change the values of S/N ratio [2] and change the multipropagation effects on the transmission. Then we can analyze the results of each transmission and see how the BER [1] is changed

The Matlab code used in this paper was developed by Alan C. Brooks and Stephan Hoelzer [8]. This implementation is used to transmit a computer file in binary data form modulated by OFDM and 16- QAM modulation. A scheme of every part of the implementation can be seen in Fig 1. As it can be seen in the figure channel imperfections are modeled in this implementation. In the end of the transmission, when the receiver receives the data, a comparison of the transmitted and the received messages is done in order to calculate the Bit Error Ratio (BER).

This paper does not explain in detail the simulation code. It uses it to create results and see the behavior of OFDM under different channel properties. Nevertheless some of the main variables of the code are described, because the choice of them has a critical effect on the results.

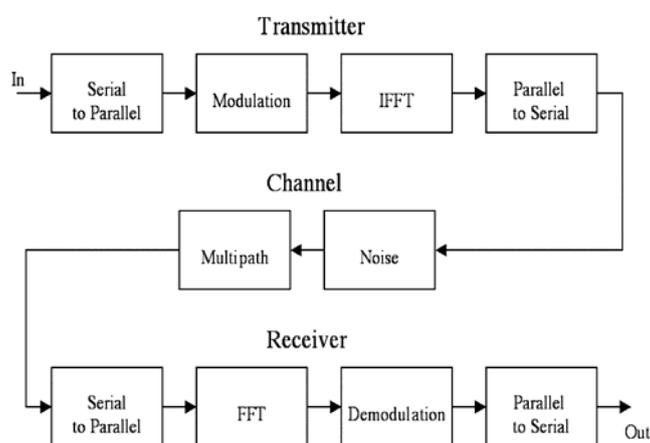


Figure 1: Matlab FlowChart

B. General Options in the Simulation

The general options of each transmission are in the *setup.m* file of the simulation. Two of the most important variables are analyzed.

One of the main characteristics of every simulation model of OFDM is the size of the fast Fourier transformation (FFT) used to generate the signal. In the simulation it is equal to the number of samples for the transmission signal. In the code this variable is named *fft_size*. The more the size of the FFT is increased the more samples there are for each signal. The more samples there are the smoother and more accurate the signal is.

Another very important variable is the number of the carriers (or the sub – channels) being used in every simulation. This variable is named *num_carriers*. According to the number of sub – carriers the data is cut into pieces, which are called chunks. Each carrier transmits 2 data bits. The first is coded in the real part of the Fourier transformation of signal and the second in the imaginary.

C. Variables which have an effect on S/N ratio

In this implementation noise is added to the transmission signal. In the *setup.m* file there is the variable called *noise_level*. This variable changes the level of the noise of the channel. The level of the noise is given by the following equation:

$$A_n = A_s \cdot \text{noise_level} \quad (1)$$

Where A_n is the level of the noise

A_s is the level of the signal

We know that the S/N ratio is given by the following equation [2]

$$S/N = (1/\text{noise_level}^2) \quad (2)$$

The noise produced is uniformly distributed in the closed space:

$$[-\text{noise_level} \cdot A_s, \text{noise_level} \cdot A_s]$$

The noise after being generated is added to the signal. This is done in the *ch_noise.m* file.

D. Variables which have an effect on multipropagation

Adding two delayed and attenuated copies of the signal to itself simulates multipath propagation. The copies are named echoes. The first echo is delayed less and has a higher level than the second.

The time of the delay of the two echoes are changed by the variables d_1 and d_2 . But it is also a function of the number of carriers. Actually the time of the delay for both echoes is analog to the number of carriers. So each time the number of carriers changed in the tests, to keep the time of delay stable, d_1 and d_2 variables were divided by the change. This is done in order to make the tests equivalents.

The level of the echoes is changed by the variables a_1 and a_2 and it is given by the following equation.

$$\begin{aligned} A_{\text{echo1}} &= a_1 A \\ A_{\text{echo2}} &= a_2 A_s \end{aligned} \quad (3)$$

Where A_{echo1} is the level of the first echo

A_{echo2} is the level of the second echo

III. PLOTS OF BER AS A FUNCTION OF S/N RATIO AND MULTI PROPAGATION

A. BER and S/N ratio

To make the plots of the BER as a function of the S/N ratio a file was transmitted for many S/N ratios. As mention before the S/N ratio can be changed by the *noise_level* variable, which changes the S/N ratio according to the equation(2).

Each time a transmission took place the *noise_level* variable changed. The lowest S/N ratio was decided to have the value 0.1 and the highest 10. Therefore, by solving the equation (2), the *noise_level* variable varies from 0.3162 to 3.162.

The transmission was simulated for 5 sets of carriers. 32, 64, 128, 256 and 512 carriers. For each set of carriers a BER curve as a function of S/N ratio was plotted.

There are two plots. In the first the echoes have high level and in the second low levels. To be exact, in the first plot the two echoes have a level of 0.50 and 0.40 times and in the second 0.10 and 0.05 times the level of the signal. The results can be seen in Fig 2. and Fig 3.

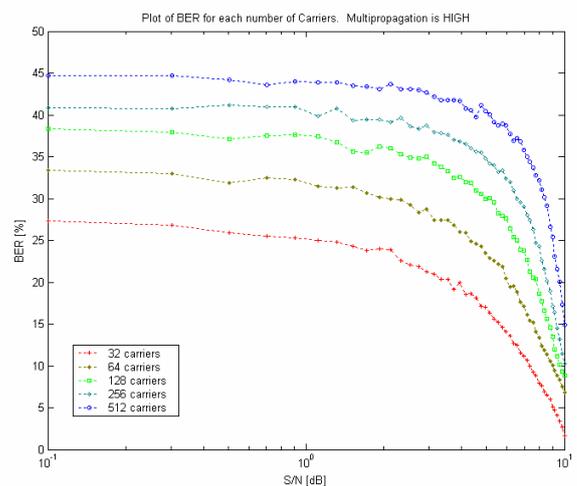


Figure 2: BER as a function of S/N ratio. Multipropagation effects are high

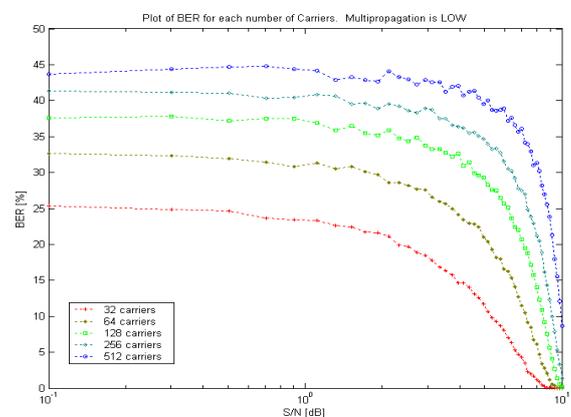


Figure 3: BER as a function of S/N ratio. Multipropagation effects are low

A. BER as a function of Multipropagation

In these plots the behavior of the BER of OFDM can be seen as a function of the level of the signals.

As before, a file was transmitted, each time with a different level for the echoes. The level of the echoes has a start value of 0.05 for the first and 0 for the second times the level of the signal. They have a final value of 0.50 and 0.40 times the level of the signal.

Again the transmission was simulated for 5 sets of carriers. 32, 64, 128, 256 and 512 carriers. For each set of carriers a BER curve was plotted. The x – axis of the plots represents the factor by which the level of the signal is to be multiplied to equal the first echo.

There are two plots. In the first the transmission takes place with a low S/N ratio - 0.1 - and in the second with a high – 10.

The results of the BER as a function of multipropagation for each set of carriers can be seen in the Fig 4. & Fig 5.

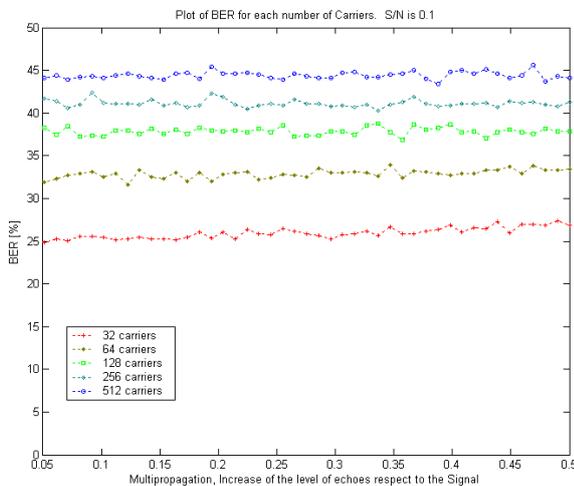


Figure 4: BER as a function of Multipropagation. S/N Ratio is 0.1

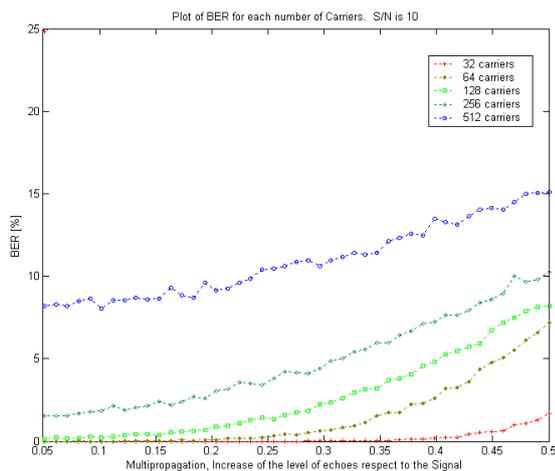


Figure 5: BER as a function of Multipropagation. S/N Ratio is 10

IV. CONCLUSION

The first and obvious thing we can notice from all the Plots is that the more we increase the number of carriers for certain S/N Ratio and Multipropagation effect the more the BER increases. This is to be expected, because the more we increase the number of carriers the more we increase the symbol rate and therefore the data rate.

From the plots of the BER as a function of the S/N ratio we can see that when the S/N ratio is very low (0.1) multipropagation does not have any impact on the BER. Furthermore, it has an impact when the S/N ratio has high values, for example 512 carriers have 15% BER when Multipropagation is low and the S/N ratio is 10 but it drops to 8% BER when Multipropagation is high and the S/N ratio is again 10.

This can be seen from the plot of BER as a function of Multipropagation when we have the S/N ratio is equal to 0.1. The BER by every set of carriers stays constant though the multipropagation effects are increased.

From the Plot of BER as a function of Multipropagation with a high S/N ratio we can notice that the less the number of carriers, the more immunity the transmission to the Multipropagation effects.

ACKNOWLEDGEMENT

This work was done in the VSLI design / DSP lab of MIT and it was supported by all the staff working in the lab and by the Senior Lecturer Mr. Srikanth Kamath

REFERENCES

- [1] B. Das ,S. Tiwari, S. Das, "Performance Study of Discrete Wavelet Packet Based MB-OFDM System for Short Range Indoor Wireless Environment", Devices and Communications (ICDeCom), 2011 International Conference on Feb. 2011.
- [2] M.Z. Win and R. A. Scholtz, "Ultra-wide bandwidth timehopping spread-spectrum impulse radio for wireless multipleaccess communications". IEEE Trans. Comm., Vol. 48, Issue 4, pp. 679-689, 2000.
- [3] L. Hanzo, M. Munster, B. J.Chol, and T. Keller, "OFDM and MC-CDMA for Broadband Multi-user Communications, WLANs and Broadcasting", John Wiley & Sons 2003.
- [4] Haitham J. Taha and M. F. M. Salleh, "Performance Comaparison of Wavelet Packet Transform(WPT) and FFT-OFDM System Based on QAM Modulation Parameters in Fading Channels," Wseas Transactions on Communications, Vol. 9, Issue 8, pp. 453-462,2010.
- [5] A.Batra, J. Balakrishnan, G. R. Aiello, J. R. Foerster and A. Dabak, "Design of a multiband OFDM system for realistic UWB channel environments", IEEE Transactions on Microwave Theory and Techniques, Vol. 52, Issue 9, pp. 2123- 2138, 2004.
- [6] Thesis of Eric Lawrey on OFDM modulation technique for wireless radio applications, submitted on October 1997
- [7] Paper of Guillermo Acosta on OFDM Simulation Using Matlab
- [8] A study by Alan C. Brooks and Stephen J. Hoelzer on OFDM Simulation using Matlab
- [9] *Wireless Digital Communications* by Molisch