TECH-CHRONICLE
AN INTERNATIONAL E-JOURNAL ON
EMERGING TRENDS IN SCIENCE, TECHNOLOGY AND MANAGEMENT

"Survey Paper On Improving Image Forgery Localization Using Contourlet Transform with Tampering Possibility Maps"

Sneha Bahadure[1], **Mukul Pande**[2]

[1]M.Tech (WCC) Student, TGPCET, Nagpur, Maharashtra, India

[2]Professor, Department of Information Technology, TGPCET, Nagpur, Maharashtra, India

***Abstract*—** During the previous decade, many work had been done on the image forensics while it is able to defect the tampered images at high accuracy rate by using many technologies and methods like designed mechanism, localization of tampered portion or region of the ordinary or fake image so it may causes many issues and problem, they can still present many challenges specially when the this type of tampering operation is unknown. Some researchers have realized that it is necessary to integrate different forensic techniques to obtain better localization performance. But some important issues have not been comprehensively studied, for example, how to select and improve/readjust proper forensic approaches, and how to fuse the detection results of different forensic approaches to obtain good localization results. In above proposed work we can use the comtourlet transform to obtain the better result other than the previous techniques.

Keywords - Image forensics, forgery localization , statistical feature, copy-move detection

I. INTRODUCTION

The image forensics leads to address authenticity and integrity of image. It may leads to security problems. Image tampering, splicing or cloning are techniques are used to create forged images. So that the integrity of the image is lost. The digitally forged images are sometimes seems to be so real and it cannot be distinguishable the differences from the original image is difficult and difficult to define changes from the tampered image. From that authenticity is also lost. Integrity and authenticity verification of digital images are one of the serious issue in the field of image processing. The term forgery is conventionally defined as the production of fraud copy of a document, signature or a work of art on original document. The change of photography from requiring chemicals and darkroom tricks to manipulate images has given way to the digital forensics. With the move to the world of Megapixels, a new door opens to the dark-side of image counterfeiting and forgeries. Gone are the days of needing to create "trick shots" with an analog camera or careful chemical preparation in the darkroom. Today, manipulating an image involves simply using tools available in the digital darkroom, such as Adobe Photoshop or Macromedia Fireworks. With these new techniques easily available to the masses via an inexpensive PC, the need exists to verify the authenticity of a digital image because of our increased reliance on digital media. Two examples of the importance of digital image authentication are witnessed in the news media we rely on to provide accurate information and the courtroom where someone's fate may depend on the authenticity of a digital image as evidence. This work is on the detection of digital image tampering for forged image.

Types to Detect Image Forgery:

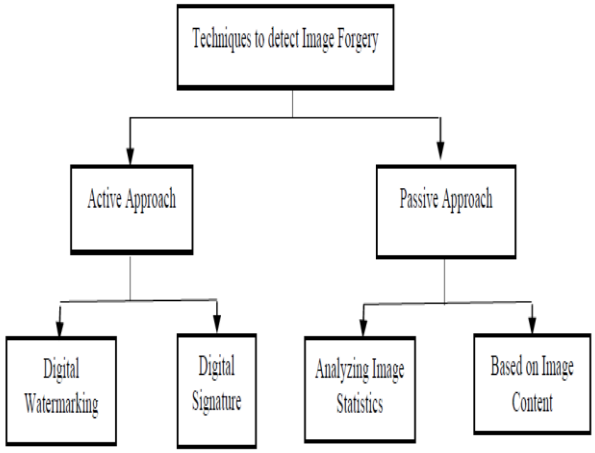

Image Retouching: changes in an image by adjusting contrast, brightness, noise level and also by edge sharpening. In this forgery the motive is to provide an image with better visualization than original one.

Fig. Image Retouching

Image Splicing: Original image joint or combined with two or more different images into one image to make a forged image. In this regions from different images are taken to change original image. To identify this kind of forgery the focus is on identifying and determining the incompatibilities in characteristics of image as region of different image are used for making forged image.

Fig. Image Splicing

Copy-Move Forgery: In this forgery a region is copied and move from original image then after applying some transformations region paste on the same image at some other location to hide an object in the given image or to add some additional information to change the original message conveyed by the image.

II. LITERATURE SURVEY

Image Forgery Localization

Over the past decade, many efforts have been made in passive image forensics. Although it is able to detect tampered images at high accuracies based on some carefully designed mechanisms, localization of the tampered regions in a fake image still presents many challenges, especially when the type of tampering operation is unknown. Some researchers have realized that it is necessary to integrate different forensic approaches in order to obtain better localization performance. However, several important issues have not been comprehensively studied, for example, how to select and improve/readjust proper forensic approaches, and how to fuse the detection results of different forensic approaches to obtain good localization results. In this paper, module is designed to improve the performance of forgery localization via integrating tampering possibility maps.

In the above paper, two existing forensic approaches can be first select and improve, that is statistical feature-based detector and copy-move forgery detector, and then adjust their results to obtain tampering possibility maps. After investigating the properties of possibility maps and comparing various fusion schemes, it is a simple yet very effective strategy to integrate the tampering possibility maps to obtain the final localization results. The extensive experiments show that the two improved approaches used in our framework significantly outperform the state-of-the-art techniques, and the experiment can achieve fusion results with the best F1-score in the IEEE IFS-TC Image Forensics Challenge.

Image forgery detection

This paper focuses on passive techniques for image forensics operates in the absence of any watermark or signature. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image.

The set of image forensic tools can be roughly grouped into five categories:

- pixel-based techniques that detect statistical anomalies introduced at the pixel level
- format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme
- camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip post-processing

- physically based techniques that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera

Geometric-based technique makes measurement of objects in the world and their positions relative to the camera.

Information Forensics

In recent decades, we have witnessed the evolution of information technologies from the development of VLSI technologies, to communication and networking infrastructure, to the standardization of multimedia compression and coding schemes, to effective multimedia content search and retrieval. As a result, multimedia devices and digital content have become ubiquitous. This path of technological evolution has naturally led to a critical issue that must be addressed next, namely, to ensure that content, devices, and intellectual property are being used by authorized users for legitimate purposes, and to be able to forensically prove with high confidence when otherwise. When security is compromised, intellectual rights are violated, or authenticity is forged, forensic methodologies and tools are employed to reconstruct what has happened to digital content in order to answer who has done what, when, where, and how. It provide an overview on what has been done over the last decade in the new and emerging field of information forensics regarding theories, methodologies, state-of-the-art techniques, major applications, and to provide an outlook of the future.

Robust detection of region-duplication forgery

This paper introduces Region duplication forgery, in which a part of a digital image is copied and then pasted to another portion of the same image in order to conceal an important object in the scene, is one of the common image forgery techniques. In this paper, we describe an efficient and robust algorithm for detecting and localizing this type of malicious tampering. We present experimental results which show that our method is robust and can successfully detect this type of tampering for images that have been subjected to various forms of post region duplication image processing, including blurring, noise contamination, severe lossy compression, and a mixture of these processing operations.

Region duplication detection

Region duplication is a simple and effective operation to create digital image forgeries, where a continuous portion of pixels in an image, after possible geometrical and illumination adjustments, are copied and pasted to a different location in the same image. Most existing region duplication detection methods are based on directly matching blocks of image pixels or transform coefficients, and are not effective when the duplicated regions have geometrical or illumination distortions. In this work, we describe a new region duplication detection method that is robust to distortions of the duplicated regions. Our method starts by estimating the transform between matched scale invariant feature transform (SIFT) key-points, which are insensitive to geometrical and illumination distortions, and then finds all pixels within the duplicated regions after discounting the estimated transforms. Method which can be used in this paper is shows effective detection on an automatically synthesized forgery image database with duplicated and distorted regions. We further demonstrate its practical performance with several challenging forgery images created with state-of-the-art tools.

Copy-move detection based approach: Copy-move detection tries to find the duplicate regions within an image. Many effective methods have been proposed previously, such as [3][10][11]. The three works mentioned above used the image editing technique Patch-Match [12] to find the similar patches, and then further determined the copy-move regions. As reported in their papers, copy move detection made major contributions to the overall localization performance. However, copy-move detection cannot differentiate between the original regions from the copied regions, and thus always gives some ambiguous results. On the other hand, such methods are very specific. If there is no copy-move operation involved in the tampering procedure or the tampered region comes from another image, copy-move detection probably produces some inaccurate tampered regions and thus confuses the localization results.

Sensor pattern noise based approach: As a reliable and unique fingerprint for a camera, sensor pattern noise can help to evaluate the integrity of an image taken by the same camera. By estimating the sensor pattern noise from the testing images, the tampered regions can be revealed by checking the compatibility of sensor pattern noise block by block [13], [14]. Although such a method can deal with many types of manipulations, its localization resolution1 is limited since it needs sufficient pixels for comparing the sensor pattern noise. Furthermore, for a given image in practice, it is hard to obtain the sensor pattern noise of its acquisition camera.

Statistical feature based approach: By adopting sliding window strategy to extract forensic features from each image patch and feed them into a pre-trained classifier, it is possible to identify some tampered regions, such as patches from different image sources or with different processing histories. In [15] and [13] features inspired by SRM are used as the forensic features. The statistical feature based approaches can be applied to any image under investigation. However, since it relies on machine learning techniques for training and testing, there would probably be some erroneous results. Thus, we should carefully select the features and the related parameters in order to control the error rates

Sr. No	Title	Author	Methodology	Advantage	Disadvantage
1.	Image Forgery Localization via Integrating Tampering Possibility Maps	Haodong Li, Weiqi Luo, Xiaoqing Qiu, and Jiwu Huang	Find out image forgery via copy move and statistical feature extraction technic	Detects forgerd region of the image	Computational load for no of blocks of the image
2.	Image forgery detection	H. Farid	Uses a pixel based method and camera based methods	Also detects the exact forged portion of the image	But sometimes gives a false positive result
3	Information forensics: An overview of the first decade	M. C. Stamm, M. Wu, and K. J. R. Liu	In this paper we understand about the image forensics	Forged image or fraud image analysis	-
4	Robust detection of region-duplication forgery in digital image	W. Luo, J. Huang, and G. Qiu	Detects duplication of the image	Detects duplication of the image	High time complexity
5.	Region duplication detection using image feature matching	X. Pan and S. Lyu	Detects feature matching of the image by using SIFT	Detects features on the basis of the color, features as well as texture	Ambiguity in result

SUMMARY

In above paper, methodology can be implemented by using DCT Transforms , JPEG transform , DWT transforms ,etc. but all these techniques does not work properly with and size and shape of the image. This methodology cannot give us exact result of the image tampering. So that it cannot be useful in image forensic. For that problem we are developing an contourlet transforms technique that can be work with size and shape of the image.

III. COMPARATIVE ANALYSIS

IV. RESEARCH METHODOLOGY

- After the literature survey following benefits has been noted that these techniques do not work with shape.
- In current work , wavelet transform is used with SVM for detection of image tampering.
- But this approach does not take into consideration on the shape verification of the image.
- This reduces accuracy of image tampering detection.
- Contourlet transform can use for shape analysis and to reduce the error in detection of forgery

V.CONCLUSIONS

In this paper, a new method to detect the forgery in digital images has been proposed, which can be used for image authentication. This method uses contourlet transform to transfer the image to the frequency domain. In order to enhance the security of the method, the

pseudorandom number generator based on cellular automata is used. In tamper detection step, for improving the detection and localization process of forged area Results obtained from tests performed on various images with various types of tampers display good visual quality and enough imperceptibility for the proposed method.

VI. REFERENCES

[1] Haodong Li, Weiqi Luo, Xiaoqing Qiu, and Jiwu Huang, "Image Forgery Localization via Integrating Tampering Possibility Maps", IEEE transactions on informetic forensics and security, VOL. 12, NO. 5, MAY 2017.

[2] H. Farid, "Image forgery detection", IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16–25, Mar. 2009.

[3] M. C. Stamm, M. Wu, and K. J. R. Liu, "Information forensics: An overview of the first decade", IEEE Access, vol. 1, pp. 167–200, May 2013.

[4] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image", in Proc. 18th Int. Conf. Pattern Recognition., vol. 4. Aug. 2006, pp. 746–749.

[5] X. Pan and S. Lyu, "Region duplication detection using image feature matching" ,IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 857–867, Dec. 2010.

[6] P. Korus and J. Huang, "Improved tampering localization in digital image forensics based on maximal entropy random walk", IEEE Signal Process. Lett., vol. 23, no. 1, pp. 169–173, Jan. 2016.

[7] J. Y.-F. Hsu, "Image tampering detection for forensics applications", Ph.D. dissertation, Graduate School Arts Sci., Columbia Univ., New York, NY, USA, 2009.

[8] J. Lukáš, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise", Proc. SPIE, vol. 6072, p. 60720Y, Feb. 2006.

[9] X. Qiu, H. Li, W. Luo, and J. Huang, "A universal image forensic strategy based on steganalytic model", in Proc. 2nd ACM Workshop Inf. Hiding Multimedia Secur., New York, NY, USA, 2014, pp. 165–170.

[10] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches", IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.

[11] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copy– move forgery detection", IEEE Trans. Inf. Forensics Security, vol. 10, no. 11, pp. 2284–2297, Nov. 2015.

[12] C. Barnes, E. Shechtman, A. Finkelstein, and D. Goldman, "PatchMatch: A randomized correspondence algorithm for structural image editing", ACM Trans. Graph., vol. 28, no. 3, pp. 24:1–24:11, Jul. 2009.

[13] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, "Image forgery localization through the fusion of camera-based, feature-based and pixelbased techniques", in Proc. IEEE Int. Conf. Image Process., Oct. 2014, pp. 5302–5306.

[14] L. Gaborini, P. Bestagini, S. Milani, M. Tagliasacchi, and S. Tubaro, "Multi-clue image tampering localization", in Proc. IEEE Int. Workshop Inf. Forensics Secur., Dec. 2014, pp. 125–130.

[15] L. Verdoliva, D. Cozzolino, and G. Poggi, "A feature-based approach for image tampering detection and localization", in Proc. IEEE Int. Workshop Inf. Forensics Secur., Dec. 2014, pp. 149–154.

[16] Milad Jafari Barani , Peyman Ayubi , Fooad Jalili , Milad Yousefi Valandar and Ehsan Azariyun, "Image forgery detection in contourlet transform domain based on new chaotic cellular automata" , Published online 11 September 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1365.

[17] ChitwanBhalla Surbhi Gupta , "A Review on Splicing Image Forgery Detection Techniques" , IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol.6, No.2, Mar-April 2016.

BIOGRAPHIES

Ms. Sneha Dilip Bahadure
Completed B.E
(InformationTechnology)
From TGPCET, Nagpur,
She is pursuing M.Tech (WCC)
From T.G.P.C.E.T., Nagpur