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

Review on Biometric Template Security Scheme

[1]Purva Rudrakumar Gabhane
Computer Science and Engg. KITS
Email: purva.gabhane2010@gmail.com

[2]Asst. Prof. Anisa Anjum
Computer Science and Engg.KITS, Ramtek.

Abstract: Now a day's security is very essential because the fords are increasing day by day. Everywhere we need security. To provide security and to give access to the right person authentication is very important. In the traditional time for authentication purpose we use password, pins but now a days theses authentication schemes are not sufficient. From this biometric is invented to provide the authentication. Biometrics deals with human's physical as well as behavioral characteristics. The biometric data which is extracted from the human's physical as well as behavioral characteristics is fingerprint, palm print, face, retina and so many. This biometric data is used for authentication and verification purpose and save in database as a biometric template. Mostly fingerprint is used as a biometric trait. To give access to the correct person is the great challenge to the biometric system. In this paper research is done on various biometric template security schemes. Initially the biometric is introduced in the paper later the working of biometric system in introduce. There are certain attack are possible on biometric system those attack of biometric system are introduced later. Attack on biometric system move this to study the existing biometric template attacks and the various techniques that are used for securing the biometric template. While storing the biometric template in the database increases the chance of compromising it. Security of the biometric system is the most challenging task. This paper proposed the review of various techniques that are used for securing the biometric template. Biometric is initially introduced in the paper later on preprocessing step are given. There are certain attacks are possible on the two phases of biometric system that are enrollment and authentication phase. One of the attack is possible during storing the template in the database. To secure from this attack various technique are used. Review is done on those techniques.

Keywords: Biometric, template, authentication.

I. INTRODUCTION

Biometrics deals with human's physical as well as behavioral characteristics. Fingerprint, iris, hand geometry, voice, palm print, face, handwritten signatures are the commonly used biometric traits.

Reliability, convenience, and universality are the desirable properties of biometric traits with respect to use of biometric token. Once the biometric template has been

comprised it cannot be reissued or revoked so for that biometric template protection is necessary. There are some problem in biometric system to overcome these problem there are certain methods to secure the integrity of biometric tempalte. Various attack on biometric system has been reviewed and then explore the biometric template attacks on database. In the proposed paper various biometric template protection scheme are studied. In section I the overview of biometric system is covered. Section II of paper focuses on various attacks and threats on biometric system. Section III include literature review of biometric template protection scheme, in section IV different biometric template protection scheme are covered and finally in section V conclusion of this paper is given.

I. OVERVIEW OF BIOMETRIC SYSTEME

Biometrics deals with human's physical as well as behavioral characteristics. Biometric system retrieves the biometric pattern and from those biometric traits biometric feature sets are extracted and then store as biometric template in a database. In a generic biometric system there are five major components they are sensor, feature extractor, template database, matcher and a decision module.

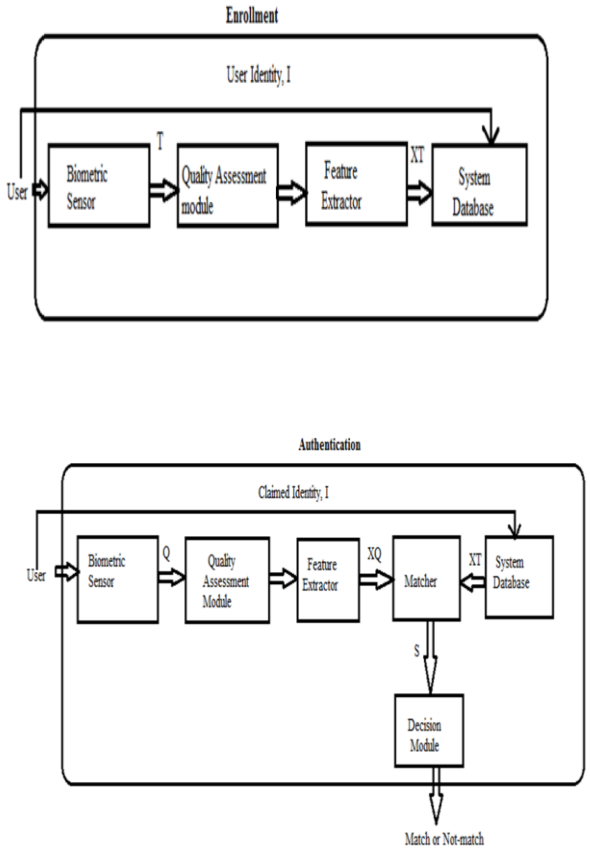

Fig. 1: Enrollment and Authentication system

Sensor is used in between the user and authentication system as an interface, it scans the biometric feature of the user. For distinguishing between the different users, features extractor module is used. It processes on scanned biometric data that is use for extracting the feature set. At the time of enrollment extracted feature data is stored in the database as a biometric template. The security of the template database is very important because it is geographically distributed. The matcher module is used for comparing two biometric feature sets that are from template and query and the match score is find out, on the basics of that match score decision module will decide and gives response to the query. If the match score met the certain threshold then it is declare a positive match. If the biometric feature of the query template is not match with the saved database template then it is declare as a negative match. Maintaining the Integrity of the Specifications.

In the proposed paper literature review of various attacks and threats that are possible on biometric template is documented. For securing the biometric template various template protection schemes and techniques are currently used that are determine.

II. BIOMETRIC SYSTEM ATTACK AND THREATS

Ratha et al in (Ratha, Connell, & Bolle, 2001) proposed the various attacks on the biometric system. Fig 2. Shows the graphical representation of various attack that are possible on biometric system. Ratha classified the biometric system attack as follows:

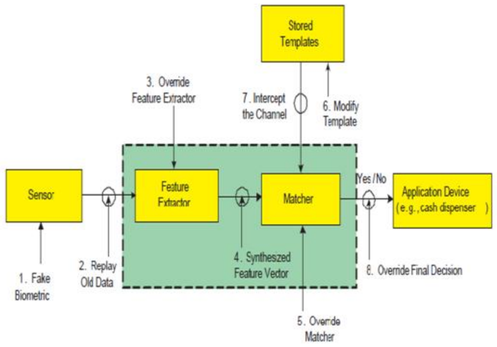

Fig. 2: Attacks on Biometric System

Attack at scanner

This attack is also called as “Type 1 attack”, in this attack the attacker physically destroy the recognition scanner and due to that denial of service is caused. At the sensor artificial fingerprint is presented.

Attack on channel between the scanner and the feature extractor

This attack is also called as “Type 2 attack” or replay attack, second type of attack include the resubmission of digitally stores biometric data. After scanning the biometric trait it will send to the feature extractor module for processing at that time attacker replace the fingerprint traits.

Attack on feature extractor module

In this type of attack the feature extractor could produce the feature values chosen by the attacker not the data that is obtain from the sensor.

Attack on the channel between the feature extractor and matcher

In this type 4 attack commutation channel between the feature extractor and the matcher is intercepted. A synthetic feature set is used to replace the data that is obtained from the sensor.

Attack on matcher

This is also known as “Type 5 Attack”. Matcher is replace with the Trojan horse by attacker and matcher will always produce the high matching score and allow application to pass the biometric authentication mechanism.

Attack on template store in database

This is also called as the “Type 6 Attack”. The attacker compromises the security of database where all the fingerprint are stored. The attacker can add new fingerprint template, delete the template or modify the existing template.

Attack on the channel between the system database and the matcher

The communication channel between the database and matcher is intercepted by the attacker to alter the data. This is also known as “Type 7 attack”.

Attack on the channel between the matcher and the application

The attacker intercepts the communication channel between the matcher and the application to replay previously submitted data or alter the data. This is also called as “Type 8 attack”.

BIOMETRIC TEMPLATE PROTECTION SCHEME

Biometric template protection schemes are classified into Feature Transformation and Biometric encryption, Jain et al in

(Jain, Nandakumar, & Nagar, 2008) classified the various biometric template protection technique that are Feature

Transformation and Biometric Encryption. The existing biometric template security technique are discuss in literature based on this classification. The graphical representation of biometric template protection techniques are given below.

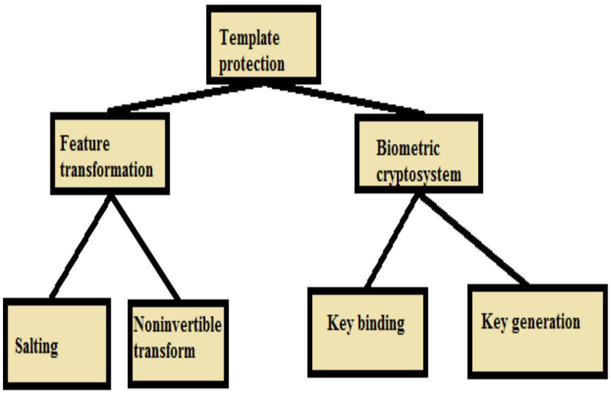

Fig. 3: Biometric Template scheme

.

Feature Transformation

In feature transformation, the transformation function (F) is applied to the template (T), and only the transformed template (F (T, K)) is stored in the database that is given below in figure. The parameters of the transformation function are typically derived from a random key (K) or password. The same transformation function is applied to query feature (Q) as that of the template (T) and then the transformed query (F (Q, K)) is matched directly against transformation function (F). The feature transformation schemes can be again classified as salting and non-invertible transformation. F is invertible in salting that is if an adversary gains access to the key and the transformed template, she can recover the original biometric template (or a close approximation of it). So that the security of the salting scheme is based on the secrecy of the key or password. While in non-invertible transformation schemes typically apply a one-way function on the template and it is computationally hard to invert a transformed template even if the key is known.

Biometric Cryptosystem

Traditional identity authentication based on simple passwords have always been easy to break using simple dictionary attacks proposed by Li & Hwang, 2010. To bypass these caveats cryptographic secret keys and passwords have been proposed. In an earlier research, Jain et al in (Jain, Nandakumar, &

Nagar, 2008) subdivided biometric cryptosystems into Key Generation and Key Binding.

Key generation: While exploring biometric cryptosystems, we observed from literature that in Key Generation a biometric key is derived directly from biometric data (Blanton & Aliasgari, 2013). Under Key Generation we explore and discuss secure sketches and fuzzy extractors.

Key Binding: In Biometric Cryptosystems, we learned that Key Binding is where a secret key and the biometric template are monolithically bound within a cryptographic framework

whilst it is computationally infeasible to decode the key or biometric template without prior knowledge of the user’s biometric data (Kannan & Thilaka, 2013). We explored Fuzzy vault cryptographic schemes which use key binding in our research to understand how key binding works.

2.1 Fuzzy vault: Fuzzy vault is cryptographic construct that was proposed by Jules and Sudan in 2002, in this fuzzy vault the secret information is encrypted and decrypted using unordered set of genuine points and chaff points. Deshpande and Joshi define fuzzy vault as a technique that is used for secure binding of randomly generated key with extracted biometric feature, while Geetika and Kaur describe a biometric fuzzy vault as a biometric cryptosystem used for protecting private keys and releasing them only when the legitimate user enter their biometric data.

OTHER BIOMETRIC TEMPLATE PROTECTION SCHEME

Other biometric template protection scheme include watermarking, steganography, visual cryptography.

Watermarking Technique: Watermarking scheme is the secure and robust for the biometric template security. Diffusion and digital watermarking techniques are used to improve the security and secrecy of the templates. Diffusion phase is done by chaotic sequence and Hessenberg decomposition. This phase essentially change

The pixel values of biometric template randomly. Finally, the watermark image, which is the face image of the owner of biometric template, is embedded in the diffused biometric template with the help of singular value decomposition..

Steganography Technique: Security is the most demanding feature in the computer's world. Steganography is one of the major techniques used for secret communication. Steganography is the art of sending secret messages over a public channel in such a way that only the intended recipient knows about the existence of the message. In steganography the secret message is hidden into the cover medium. In this, author proposes a new algorithm to hide the biometric template inside the cover image using steganography template protection technique. By using this algorithm an intruder cannot percept the existence of biometric template embedded in the image file [1].

Visual Cryptography Technique: Visual cryptography is a secret sharing scheme where a secret image is encrypted into the number of shares which independently disclose no information about the original image. The performance of iris template is comparatively higher than the other templates. So authors focused on iris template. In proposed paper, authors are storing the extracted image of the template and assigning a unique number to every template which is encrypted using Visual Cryptography. Visual cryptography provides an extra layer of authentication. The combination of biometrics and visual cryptography is a promising information security technique which offers an efficient way to protect the biometric template. In this technique two fold security to the iris template is provided.

III. CONCLUSION

In this paper we introduced biometric systems then progressed to identify biometric attacks and threats documented in existing literature. We found out from existing literature that most of the biometric attacks target biometric templates. We then determined vulnerabilities that biometric templates are exposed to as a result of these attacks and continued to explore the "Type 6" attack on biometric templates, which is the attack of biometric templates in databases. The various biometric template techniques which usually fall under feature transformation and cryptosystems were explored to identify their strengths and shortcomings.

This review gives a clear and precise understanding on the current status of biometric attacks, biometric template vulnerabilities arising as a result of these attacks and finally shows what researchers have been working on to stop these biometric template attacks. It was noted that there was no particular biometric template protection technique that proved satisfactory in all aspects of an ideal biometric template protection scheme and that there was still need for more research work to be done to establish secure, reliable, efficient and fool proof biometric template protection techniques. In future work, we will propose a two-step encryption & decryption approach for securing biometric fingerprint templates stored in a database.

References

[1] Rubal Jain and Dr. Chander Kant, "A Novel Approach for Securing Fingerprint Template using Steganography", International Journal of Innovations & Advancement in Computer Science, ISSN 2347 – 8616, Volume 4, Issue 6, pp. 503–512, June 2015.

[2] S.Usha and M.Karthik, "A Robust Digital Image Watermarking for Biometric Template Protection Applications", International Journal of Advanced Research in Electrical, Electronics, and Instrumentation Engineering, ISSN 2320-3765, Volume 4, Issue 4, pp. 2067-2072, 2015.

[3] V.Wagh and S.Sonvane, "Minutiae Point Extraction using Biometric Fingerprint Enhancement", Journal on International Research in Engineering and Advance Technology, ISSN 2320-8791 Volume 2, Issue 1, pp. 777-789 March 2014.

[4] N.Hajare, A.Borage, N.Kamble, and S.Shinde, "Biometric Template Security using Visual Cryptography", International Journal of Engineering Research and Application, ISSN 2248-9622, Volume 3, Issue 2, pp. 1320-1323, March 2013

[5] S.Sowakarthika and N.Radha, "Securing Iris and Fingerprint Templates using Fuzzy Vault and Symmetric Algorithm", International Conference on Intelligent System and Control (ISCO), pp. 189-193, 2013.

[6] Thi Hanh Nguyen, Yi Wang, "A Fingerprint Fuzzy Vault Scheme using a Fast ChaffPoint Generation Algorithm", Signal Processing, Communication and Coming(ICSPCC), IEEE International Conference, pp. 1-6, 2013.

[7] S. Ponnarasi and M.Rajaram, "Impact of Algorithm for Extraction of Minutiae Points in Fingerprint Image", Journal of Computer Science, Volume 8, Issue 9, pp. 1467-1672, 2012.

[8] R. Verma, A. Gole, " Wavelet Application in Fingerprint Recognition", International Journal of Soft Computing and Engineering, Volume 1, Issue 4, pp. 129-134, 2011.

[9] A. Nagar, K. Nandakumar, and A. Jain, "Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptor," International Conference on Pattern Recognition, Volume 6, pp. 822-825, 2008.

[10] K. Nandakumar, A. Jain, S. Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance", IEEE Transaction on Information Forensics and Security, Volume 2, Issue 4, pp. 744-754, 2007.

[11] N. Raha, S. Chikkerur, and J. Connell, "Generating Cancelable Fingerprint Template", IEEE Transaction on Pattern Analysis and Machine Intelligence, Volume 29, Issue 4, pp. 561-572, 2007.

[12] Geetika, & Kaur, M. (2013, April). Fuzzy Vault with Iris and Retina: A Review. International Journal of Advanced Research in Computer Science and Software Engineering, 3(4).

[13] Jain, A., Nandakumar, K., & Nagar, A. (2008). Biometric Template Security. EURASIP Journal on Advances in Signal Processing (2008).