ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

Enhancement of Biometric Cryptosystem Using Fuzzy Vault

[1] Ashish Vijayanand Chakole [2]Asst. Prof. A. Thomas
[1][2]Computer Science and Engg, G.H. Raisoni College of Engineering, Nagpur.

Abstract: **- Now a day's security is terribly essential as a result of the fords area unit increasing day by day. Everywhere we have a tendency to would like security. To provide security and to offer access to the correct person authentication is extremely vital. In the traditional time for authentication purpose we have a tendency to use secret, pins but currently a day's theses authentication schemes area unit not sufficient. From this biometric is invented to give the authentication. Biometrics deals with human are physical as well as activity characteristics. The biometric data that is extracted from the human's physical as well as activity characteristics is fingerprint, palm print, face, retina and thus several. This biometric data is used for authentication and verification purpose and save in info as a biometric templet. Mostly fingerprint is used as a biometric attribute. To give access to the proper person is that the nice challenge to the biometric system. In this paper research is finished on numerous biometric templet security schemes. Initially the biometric is introduced in the paper later the operating of biometric system in introduce. There area unit sure attack area unit doable on biometric system those attack of biometric system are introduced later. Attack on biometric system move this to study the prevailing biometric templet attacks and also the numerous techniques that area unit used for securing the biometric template. While storing the biometric templet in the info will increase the prospect of compromising it. Security of the biometric system is the most challenging task. This paper proposed the review of numerous techniques that area unit used for securing the biometric templet. Biometric is initially introduced in the paper presently preprocessing step area unit given. There area unit sure attacks area unit doable on the 2 sections of biometric system that are enrollment and authentication phase. One of the attack is feasible during storing the templet within the info. To secure from this attack various technique area unit used. Review is done on those techniques.**

Keywords:**--Biometric, template, authentication**

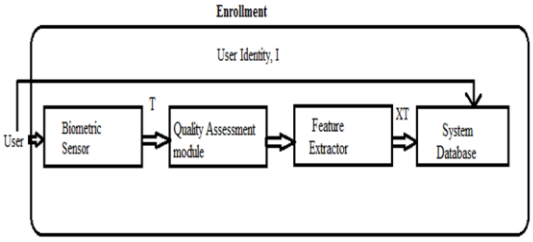
I. INTRODUCTION

Biometrics deals with human's physical as well as activity characteristics. Fingerprint, iris, hand geometry, voice, palm print, face, handwritten signatures area unit the ordinarily used biometric traits. Reliability, convenience, and universality area unit the fascinating properties of biometric traits with respect to use of biometric token. Once the biometric model has been comprised it cannot be reissued or revoked therefore for that biometric template protection is important. There area unit some drawback in biometric system to overcome these

drawback there are sure ways to secure the integrity of biometric tempalte. Various attack on biometric system has been reviewed and then explore the biometric model attacks on information. In the proposed paper numerous biometric model protection theme area unit studied. In section I the overview of biometric system is lined. Section II of paper focuses on various attacks and threats on biometric system. Section III include literature review of biometric model protection theme, in section IV different biometric model protection theme area unit lined and finally in section V conclusion of this paper is given.

II. 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.



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

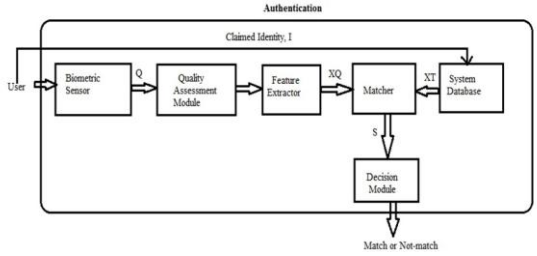


Fig. 1: Enrollment and Authentication system

Sensor is used in between the user associated authentication system as an interface, it scans the biometric feature of the user. For distinguishing between the totally 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 keep in the info as a biometric guide. The security of the template info is incredibly vital as a result of it's geographically distributed. The matcher module is used for scrutiny 2 biometric feature sets that square measure from guide and question and therefore the match score is locate out, on the basics of that match score decision module can decide and provides response to the question. If the match score met the certain threshold then it is declare a positive match. If the biometric feature of the query guide is not match with the saved info guide then it's declare as a negative match.

Maintaining the Integrity of the Specifications. In the proposed paper literature review of assorted attacks and threats that square measure potential on biometric guide is documented. For securing the biometric guide varied template protection schemes and techniques square measure presently used that square measure verify.

III. 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:

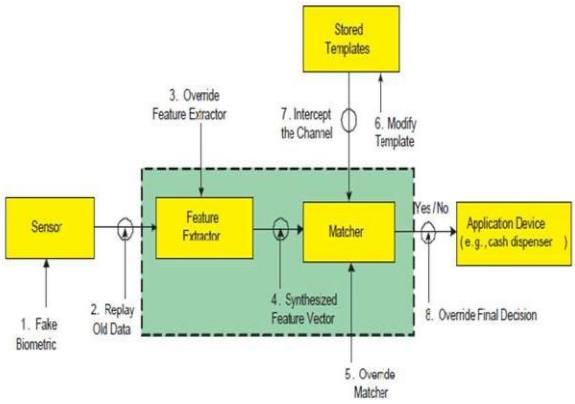


Fig. 2: Attacks on Biometric System

A. Attack at scanner

This attack is also referred to as as "Type one attack", in this attack the attacker physically destroy the popularity scanner and owing to that denial of service is caused. At the sensor artificial fingerprint is bestowed.

B. Attack on channel between the scanner and the feature extractor

This attack is also known as as "Type a pair of attack" or replay attack, second type of attack embody the resubmission of digitally stores biometric knowledge. After scanning the biometric attribute it can send to the feature extractor module for process at that point wrongdoer replace the fingerprint traits.

C. Attack on feature extractor module

In this variety of attack the feature extractor could manufacture the feature values chosen by the assailant not the information that's get from the device.

D. Attack on the channel between the feature extractor and matcher

In this type four attack commutation channel between the feature extractor and also the mediator is intercepted. A synthetic feature set is employed to exchange the information that's obtained from the detector.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

E. Attack on matcher

This is also called "Type five Attack". Matcher is replace with the Trojan horse by assailant and mediator can invariably turn out the high matching score and permit application to pass the identification mechanism.

F. Attack on template store in database

This is also referred to as because the "Type VI Attack". The attacker compromises the security of info wherever all the fingerprint square measure hold. The attacker wil add new fingerprint guide, delete the guide or modify the existing template.

G. 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".

H. 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".

IV. 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. schemes that use key binding in our analysis to perceive however key binding works.

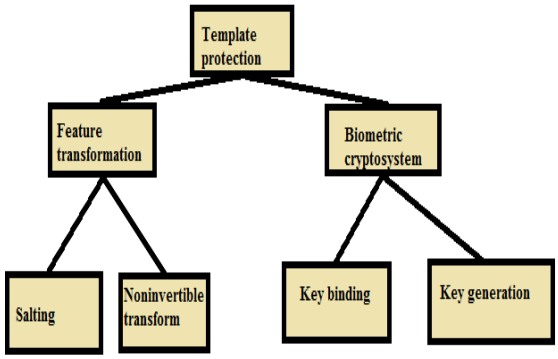


Fig. 3: Biometric Template scheme

A. Feature Transformation

In feature transformation, the transformation function (F) is applied to the templet (T), and only the remodeled templet (F (T, K)) is stored in the info that's given below in figure. The parameters of the transformation function ar usually derived from a random key (K) or arcanum. The same transformation function is applied question|to question |to question} feature (Q) as that of the templet (T) so the remodeled query (F (Q, K)) is matched directly against transformation function (F). The feature transformation schemes can be once more classified as seasoning and non-invertible transformation. F is invertible in seasoning that is if Associate in Nursing somebody gains access to the key and also the remodeled templet, she can recover the first biometric templet (or an in depth approximation of it). So that the safety of the seasoning theme is predicated on the secrecy of the key or Arcanum. 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.

B. Biometric Cryptosystem

Traditional identity authentication primarily based on easy passwords have perpetually been simple to interrupt victimisation easy lexicon attacks planned by Li & Hwang, 2010. To bypass these caveats cryptographic secret keys and passwords have been planned. In an earlier analysis, Jain et al in (Jain, Nandakumar, & Nagar, 2008) subdivided biometric

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

cryptosystems into Key Generation and Key Binding.

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

2) Key Binding: In Biometric Cryptosystems, we learned that Key Binding is wherever a secret key and the biometric example square measure monolithically certain at intervals a cryptological framework while it's computationally unworkable to rewrite the key or biometric example while not previous data of the user's biometric knowledge (Kannan & Thilaka, 2013). We explored Fuzzy vault cryptological

2.1 Fuzzy vault: Fuzzy vault is cryptological construct that was planned by Jules and Sudan in 2002, in this fuzzy vault the key information is encrypted and decrypted victimisation unordered set of real points and chaff points. Deshpande and Joshi define fuzzy vault as a technique that's used for secure binding of indiscriminately generated key with extracted biometric feature, while Geetika and Kaur describe a biometric fuzzy vault as a biometric cryptosystem used for protective personal keys and emotional them only the legitimate user enter their biometric knowledge.

V. OTHER BIOMETRIC TEMPLATE PROTECTION SCHEME

Other biometric templet protection theme embody watermarking, steganography, visual cryptography. Watermarking Technique: Watermarking scheme is the secure and strong for the biometric templet security. Diffusion and digital watermarking techniques are used to improve the safety and secrecy of the templates. Diffusion phase is done by chaotic sequence and Hessenberg decomposition. This phase primarily modification The pixel values of biometric templet willy-nilly. Finally, the watermark image, which is the face image of the owner of biometric templet, is embedded in the diffused biometric templet with the assistance of singular price decomposition..

Steganography Technique: Security is the most demanding feature within the computer's world. Steganography is one of the foremost techniques used for secret communication. Steganography is the art of sending secret messages over a public channel in such a way that solely the supposed recipient is aware of concerning the existence of the message. In steganography the secret message is hidden into the duvet medium. In this, author proposes a new algorithm to cover the biometric example within the duvet image victimisation steganography example protection technique. By using this algorithmic program associate degree unwelcome person cannot perceptual experience the existence of biometric example embedded in the image file [1].

Visual Cryptography Technique: Visual cryptography is a secret sharing scheme wherever a secret image is encrypted into the quantity of shares that severally disclose no data concerning the first image. The performance of iris template is relatively on top of the opposite templates. So authors centered on iris example. In proposed paper, authors are storing the extracted image of the example and distribution a distinctive range to each example that is encrypted exploitation Visual Cryptography. Visual cryptography provides an further layer of authentication. The combination of biometrics associate degreed visual cryptography could be a promising data security technique that offers an economical thanks to shield the biometric example. In this technique two fold security to the iris example is provided.

V. CONCLUSION

In this paper we introduced biometric systems then progressed to spot biometric attacks and threats documented in existing literature. We found out from existing literature that the majority of the biometric attacks target biometric templates. We then determined vulnerabilities that biometric templates area unit 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 model techniques that typically be feature transformation and cryptosystems were explored to spot their strengths and shortcomings. This review gives a clear and

precise understanding on this standing of biometric attacks, biometric model vulnerabilities arising as a result of these attacks and eventually shows what researchers are functioning on to prevent these biometric template attacks. It was noted that there was no particular biometric model protection technique that proven satisfactory altogether aspects of a perfect biometric model protection theme which there was still would like for a lot of analysis work to be done to ascertain secure, reliable, efficient and fool proof biometric model protection techniques. In future work, we can propose a ballroom dance coding & coding approach for securing biometric fingerprint templates hold on in a very information.

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).