A REVIEW ON BIOMETRIC CRYPTOSYSTEM USING FUZZY VAULT

V. Sujitha and D. Chitra

P. A. College of Engineering and Technology, Pollachi, Tamilnadu, India
sujithavpacet@gmail.com, chitrapacet@gmail.com

ABSTRACT

Biometric framework helps to gather statistics from individual and it's used to particularly find out the person with the physical-behavioral mechanism of the biometric qualities. The most challenge of biometric method is to provide the guarantee for storage space of the biometric templates without compromising the security and privacy. Biometric cryptosystem method is very helpful to secure traits from unauthorized access. The fuzzy vault is a famous and better biometric cryptography method to ensure the templates and its secret key in biometric frameworks. This paper reviews the various research work did in biometric cryptosystem using fuzzy vault.

Key words: Biometric, Cryptosystem, Fuzzy vault

INTRODUCTION

Biometrics is one of the technology that is used to determine human uniqueness for the purpose of authenticating or identifying the individuality of an object. It is classified the authorized or unauthorized users by their bio features such as fingerprint, facial features, retinal, palm veins and geometry of arms or some unique aspects of voice, gesture and hand writings [Pankanti, et al., 2000]. The biometric method incorporates image capturing, feature extraction then patterns matching modules as shown in Fig. 1.

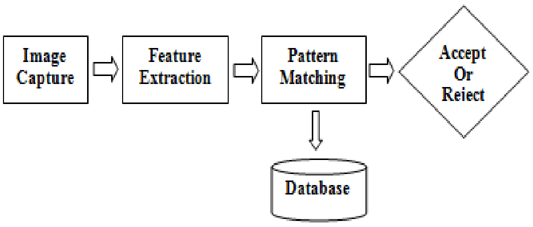

Figure 1: Biometric System

The primary work of biometric is to make sure about the storage of templates without degrades the privacy and security. Providing security of biometric templates are more important because potential mishandling of stolen templates. Two main concerns about a stolen template such as (i) spoofing process & (ii) privacy intrusion Process R. Cappelli, et al [2007]. of original images and use that incorrect image. Also, opponent can reconstruct the original image and misused those images. Due to lacking real time detection quantity of current biometric processing, spoofing is threatening susceptibility. The many number of security methods have been proposed to secure biometric templates. Figure 2 shows the classification of template protection methods.

BIOMETRIC CRYPTOSYSTEM

Biometric Cryptosystem is a template-based cryptography method that is used to secure biometric templates from mishandling. Biometric Cryptosystem based methods unify the scheme of both biometrics and cryptography. They are used to secure cryptographic key by using biometric features like palm, finger, iris etc. They are also used these features to protect templates.

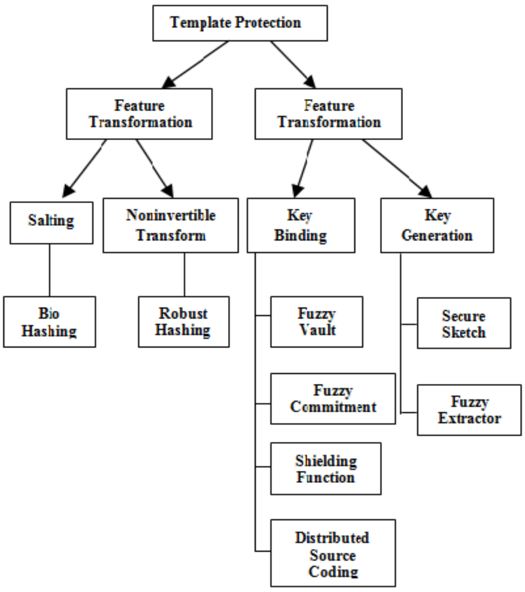

Figure 2: Category of Template Protection Methods

This method uses helper data about the stored templates. Helper data is stored with original template and that data does not leak any primary details of the original template. Biometric cryptosystem-based methods are also called Helper Data based methods. From the query image cryptographic key is extracted using helper data. Validity of the extracted key checked during verification. Intra-user variations are found using error correction coding techniques.

Biometric cryptosystem are further classified into key release, key binding and key generation based methods of Karthik Nandakumar, et al., [2007].

(i) Key Release Methods

The process of biometric-based key is that the biometric devices, which perform user authentication and a system of cryptography, can perform control over the other components. In that system, a cryptographic key is saved in user's database, enhanced with the user name, biometric template, authorized privileges which released ahead a successful biometric authentication process. Integrating biometric into cryptosystem is referred as biometric based key release method (Figure 2) [4].

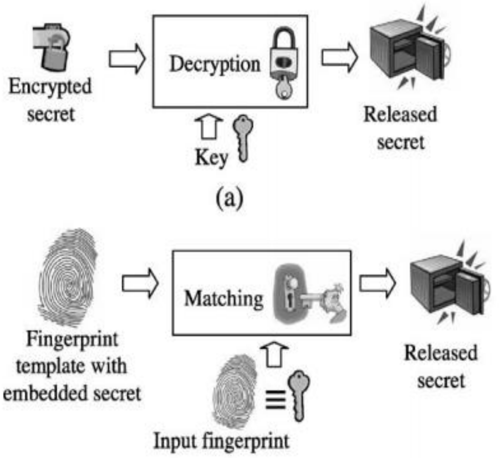

Figure: 2 Authentications Based on Key Release Method

The characteristics of the biometric system are:

- Require to- access biometric templates for matching
- User authentication and key release are fully decoupled

(ii) Key Binding Based Methods

Helper data is acquired through binding a key with the biometric pattern, this method is referred as a key-binding biometric cryptosystem. In this system, the biometric model is secured using bind template with a key.

Single units that combine both the key and the template. The helper data does not leak out any real values of key and fingerprint images. And we cannot decode the original biometric data without correct query imfage [Sarika Khandelwal, et al., 2013]. Regenerating the correct key gives a successful match (Figure 3).

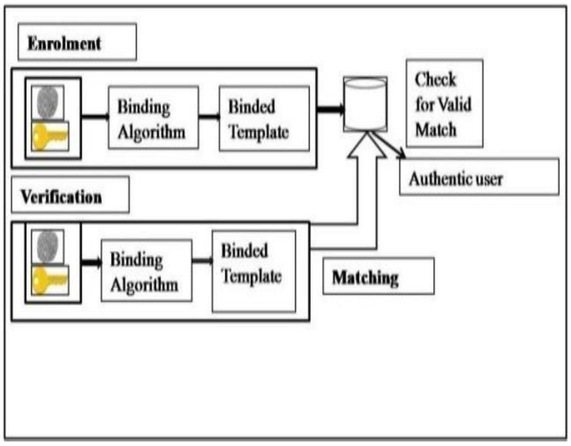

Figure: 3 Authentications Based on Key Binding Method

The following methods can be classified as the key binding- based methods;

a) Fuzzy Vault

b) Fuzzy Commitment

c) Shielding Function

d) Distributed Source Coding

(iii) Key Generation Based Methods

Helper data is derived only from the template and the cryptographic key process to produce from the data and the query features, which leads to a key production biometric cryptosystemic [Sarika Khandelwal, et al., 2013].

Direct key generation is one of the schemes from biometric. Based on user-specific quantization schemes early biometric key production schemes are engaged. Some information about (Quantization boundaries) is stored as helper data its helps during verification to consider for intra class variations (Figure 4).

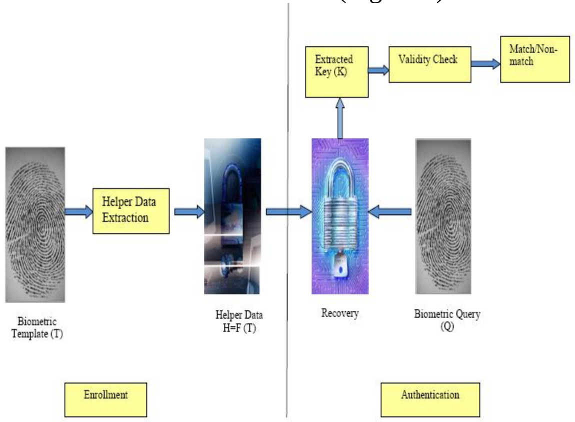

Figure: 4 Authentications Based on Key Generation Method

The following are the popular key generation-based schemes;

a) Fuzzy Extractors

b) Secure sketch

The fuzzy vault scheme for crytography proposed by Juels and Sudan,et al [2002] has become one of the most popular and used approaches for biometric pattern protection.

FUZZY VAULT SCHEME

The fuzzy vault structure links both the secret key and the template. A polynomial value P is generated using top secret key S. This polynomial is assessed by all the elements of the uneven set X. The client selects number of chaff points (C) that not lie down on the polynomial P. The genuine points (G) include uneven set X and its polynomial value [Juels and Sudan,et al., 2002].

$$V=G+C$$

The combination of chaff and genuine point set from that the attacker cannot recreate original template.

The consumer has to divide enough number of points from the vault V by correlating X' with V. By using RS code P can be recreated successfully when X' overlap with X and S can regenerated successfully. This construct is called fuzzy because the vault will obtain decoded for nearest values of X and X' and the secret key S can be retrieved. The schematic diagram showing the operations of fuzzy vault is shown in Figure. 5 [Juels and Sudan,et al., 2002].

(i) Attacks against Fuzzy Vault Scheme

During usual authentication system, the original biometric templates are stored in the database without encryption. It is very easy for an attacker to retrieve the original template.

LITERATURE SURVEY

The security of authorized key word on a server is well implicit and can give cryptographic security in broadly accepted models, Nonozisokhi Gea,et al [2017]. But secure passwords are tough to keep track and may results in a user choosing weak key words reduces the system protection. A potential solution to this well-known liability is biometrics. This can be used to produce better protection and also do not remember the passwords, Cavoukian et al [2009].

Enhanced version of fingerprint biometrics was done by Tomko et al., [1994]. Clancy et al., [2003] proposed the first realistic. Juels and Sudan et al., [2002] proposed the fuzzy vault scheme to secure the positions of fingerprint minutiae.

Karthik et al., [2007] proposed a fully automatic implementation method for fuzzy vault finger print system. In this process a indistinct version of the template, aligning the query fingerprint with the transformed template is a major task. Helper data not leak any primary information about the minutiae template and also contains sufficient information for aligning.

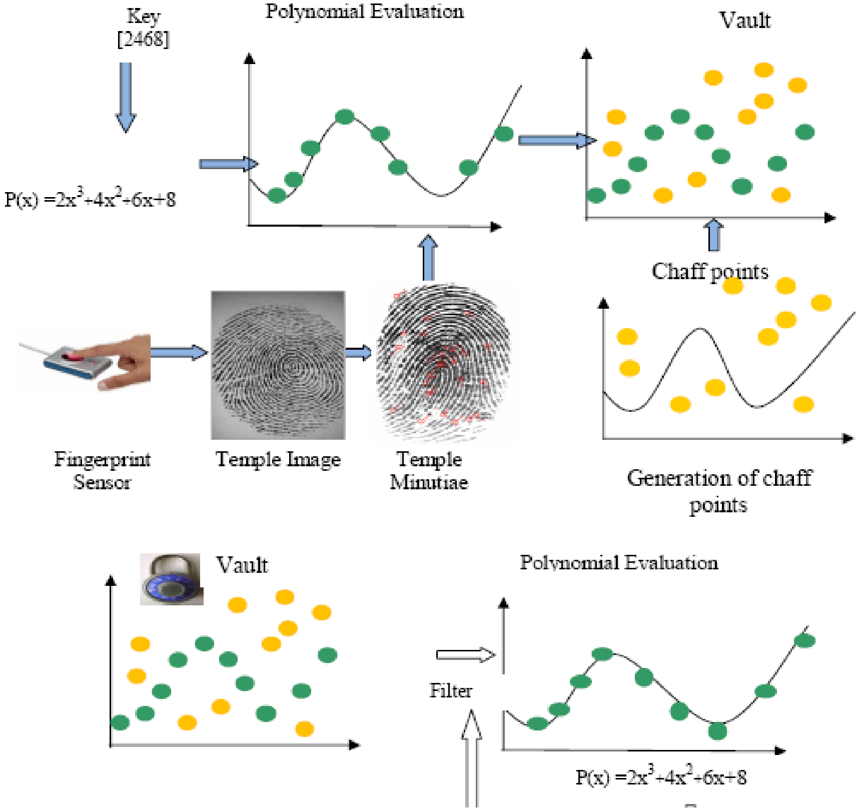

Fig.5. Fuzzy Vault Scheme

Mohamed et al., [2013] has proposed an appro-ach on the generation of chaff points for the protection of fuzzy vault. The fuzzy vault security is depending on the scale of polynomial value and included chaff points.

George et al., [2014] proposed signature images with the biometric cryptographic systems. Although fuzzy vault has proved with the physiological biometrics, but it has not been proved with the authentication system. Here Fuzzy vault encoding, and decoding is done with the offline signature images.

Devesh Harahan and Om Prakash [2017] proposed a new approach fuzzy cryptosystem with palm print. Usu-ally, confined with the help of fuzzy vault created by randomizing the palm print. Randomized palm features are found using the PCA and the polynomial construc-tion is agreed out. The proposed method defines and works well for the palm print than the finger print. The security of the fuzzy vault relies on the polynomial value, higher the degree higher the security.

As per Evelyn Brindha, et al., [2012] the authentication stage, the fuzzy vault decoding is carried out. Based on the result FMR reduces to 12% and FNMR improved to 88%. Hence the proposed method yields a good result.

Karthik et al., [2008] proposed a scheme for secu-ring multiple templates. The multibiometric vault provi-des better recognition performance and higher security compared to a unibiometric vault.

Abhisekh et al., [2012] proposed a method on multibiometric cryptosystem using the three popular biometrics finger print, face and iris. Here the various methodologies of a user are planned to use distinct secure design, for that two well known biometric cryptosystems Fuzzy Vault and Fuzzy Commitment scheme are used.

Archana et al., [2011] proposed a method to form a fuzzy vault to store the key, based on iris pseudo textu-res. The methodology has twin phases:

(i) To mine binary key from iris textures

(ii) To produce fuzzy vault by using Lagrange inter-polating polynomial projections.

Rethna et al., [2013] implemented multibiometric method and it increases the security and accuracy of multibiometric system by using fuzzy vault and fuzzy commitment schemes. Hackers cannot able to guess or reconstruct the template and also cannot be identified which biometric is used.

Li and Peng, [2014] implemented a new finger multi-biometric cryptosystem using feature-level fusion to concurrently protect multiple templates of fingerprint, finger vein, finger knuckle print and finger shape traits as a single secure sketch. For finger based multi-biometric cryptosystem analyze the feature level fusion with respect to their collision on security and recognition accuracy.

Meenakshi and Padmavathi, [2010] proposed a met-hod related to password hardened fuzzy vault with iris, retina and finger print. The protection of the password hardened scheme is evaluated with the min-entropy. Extraction of feature points from finger print, iris and retina are performed. The canny edge detection is used to subtract the iris and Hough transformation is then used first to iris boundary and then to the iris boundary. The image contrast is increased using histogram equa-lization technique. Then the password toughened fuzzy vault is implemented by the transformation of biometric features with the user defined password. Various pass-words are used for different metrics and transformed into new features. Then fuzzy vault encoding, and deco-ding are conceded out. Min entropy is used to calculate the password security of the hardened fuzzy vault. Also, the security of the scheme depends on the chaff points are added and also if the degree of polynomial is higher, higher the security.

5. CONCLUSION

Biometrics is a significant feature of any unique character-based security system and it identify the auth-orized or unauthorized person based on their unique traits. For better user identification the biometrics feat-ures are integrated with cryptographic method. There are number of defy involved in merging biometrics into a cryptographic system, because of significant variations in the representations of a biometric identifier and due to defective nature of biometric feature extraction and mat-ching algorithms. Fuzzy vault is an efficient method for biometric cryptosystems, because it not requires ordered representation of a biometric and it can abide variations with in biometric up to some level. Here various imple-mentations of the biometric cryptosystem using fuzzy vault have been discussed. Provision of safety to the prototype is much vital nowadays. Fuzzy vault is effi-cient technique for encryption that can give better security to the stored template for a high-quality degree since it can capable overcomes the key management problem. This paper also gives the different attacks that can be reduced to make a biometric template more safe and secure.

REFERENCES

Pankanti, S., R.M. Bolle, and A. K. Jain, Biometrics: The Future of Identification. IEEE Computer 33 (2): 46 –49 (2000).

Cappelli, R., A. Lumini, D. Maio, and D. Maltoni. Fing-erprint Image Reconstruction From Standard Tem-plates. IEEE Trans. PAMI 29(9):1489–1503 2007.

Karthik N. and A.K. Jain and S. Pankanti, Fingerprint-Based Fuzzy Vault: Implementation and Performa-nce. IEEE Transactions on Information Forensics and Security (2007)

Sarika K., P.C. Gupta and K. Mantri, Survey of Threats to the Biometric Authentication Systems and Solu-tions. International Journal of Computer Applica-tions 61(17): (2013)

Juels and M. Sudan, A Fuzzy Vault Scheme, Proc. IEEE International Symposium on Information Theory, Lausanne, Switzerland Pp. 408 (2002).

Nonozisokhi G., Suharsono, G.A., W.U, Widyastuti, Int-roduction of Hd3a gene in IPB CP1 potato cultivar through Agrobacterium tumefaciens-mediated tra-nsformation under the control of use 35S CaMV promoter. Pak.J. Biotechnol. 14(2):129-134 (2017)

Cavoukian and A. Stoianov, Biometrics: theory, methods and applications. Hoboken, NJ, USA: John Wiley & Sons, Inc., Biometric Encryption: The New Breed of Untraceable Biometrics Ch. 26 (2009).

Tomko, G.J., C. Soutar, and G. J. Schmidt, Fingerprint controlled public key cryptographic system. US Patent 5, 541, 994 (1994).

Clancy, T.C., N. Kiyavash, and D.J. Lin, Secure smart card-based fingerprint authentication, Proc. ACM SIGMM workshop on Biometrics methods and applications, ser. WBMA-'03. New York, NY, USA: ACM Pp. 45–52 (2003).

A fuzzy vault scheme, Des. Codes Cryptography 38(2): 237–257 (2006).

Mohamed K.H., M.N. Marsono, R. Bakhteri, Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm‖. Feature generation computer, Systems (2013).

George S. Eskander, Robert Soberin, Eric Granger, A bio-cryptographic system based on offline signature images‖, Information sciences (2014).

Natthakorn W., K. Nakkanong and C. Nualsri, Express-ion responses of pathogenesis-related proteins in tolerant and susceptible hevea brasiliensis clones to the white root disease. Pak. J. Biotechnol. 14(2): 141- 148 (2017)

V Evelyn B. and A.M Natarajan, Fingerprint and palm print based fuzzy vault‖. Journal of Biometrics and Biostatistics (2012).

Karthik N. anil K. Jain, Multibiometric Template Security Using Fuzzy Vault. Biometrics: Theory, Appl-ications and Systems, BTAS-08. 2nd IEEE International Conference on 29 Sept.-1 Oct. (2008)

Abhisekh N., K.N. Kumar and A.A.K. Jain, Multibiometric cryptosystem based on feature-level fusion‖, IEEE Transaction on information Forensics and Security (2012).

Archana K.C., Biometric Cryptosystem Using Fuzzy Vault For Iris. International J.of Multidispl. Research & Advcs. in Engg. (IJMRAE) 3(3): 187-192 (2011)

Rethna J., Virgil J. and C.J. Jangid, Multibiometric Cryptosystem with Fuzzy Vault and Fuzzy Commitment by Feature-Level Fusion. International Journal of Emerging Technology and Advanced Engineering 3(3): (2013)

Li L. and J. Peng, Finger Multi biometric Cryptosystem using Feature-Level Fusion International Journal of Signal Processing, Image Processing and Pattern Recognition 7(3): 223-236 (2014)

Meenakshi V.S. and G. Padmavathi, Security analysis of Password Hardened multimodal biometric fuzzy vault with combined feature point extracted from finger print, iris and retina for high security applications‖, science direct (2010).