Fuzzy Vault: A Review

C.B.Vasantha laxmi
Department of EEE, Bannari Amman Institute of Technology, India.

C.Keerthana
Department of EEE, Bannari Amman Institute of Technology, India.

Abstract – This paper is a brief evaluation of fuzzy vault which is a biometric template security technique. Biometric based authentication has more benefit over traditional method such as password due to their uniqueness and necessary physical attendance at the time of verification. But there are large concerns about the safety and confidentiality of biometric technology. Fingerprint Identification is the most usually used biometric systems and fuzzy vault is a new method to secure the template. The purpose of this paper is to review all the important progresses in fuzzy vault till now.

Index Terms – Biometric systems, template security, types of verification system, fuzzy vault.

1. INTRODUCTION

The first biometric system of this gentle was considered by Juels and Wattenberg it was called as "Fuzzy assurance", where the cryptographic key is given by biometric data. "Fuzzy", in that context, indicates that the value close to the original can extract the committed value. Future, Juels and Sudan came up with Fuzzy vault schemes which are instruction invariant for the fuzzy commitment scheme but it uses a Reed–Solomon code. Code word is evaluated by polynomial and the secret message is introduced as the amounts of the polynomial. The polynomial is estimated for unlike values of a set of structures of biometric data. Thus Fuzzy commitment and Fuzzy Vault remained pre-cursor to Fuzzy extractors. Fuzzy extractor is a biometric instrument to authenticate a user by its personal biometric template as a key. In today's world use of biometric authentication system is growing in several applications so it is significant to secure the user data from attackers.[1]

Advantages of Fuzzy Vault:

- Fuzzy vault is protected in the sense that it does not leakage information about minutiae.
- Skill to handle intra-class differences in biometric data. Not like cryptography, it may let a match to arise if the difference between the query biometric data and the template is minor.
- The fuzzy vault scheme stocks only a transformed version of the template, which makes it applicable to many modalities also fingerprints [2,3,4].

Disadvantages of Fuzzy Vault:

- Arrangement of query with transformed version of biometric is quite problematic.
- The chaff ideas created later in the method tend to have a lesser amount of degree of freedom. A point with less degree of freedom has extra neighboring points and it becomes little easy to spot them.[5].
- Given two or other such fuzzy vault orders generated from the same point, but by different keys and various random chaff, the minutiae are probable recoverable by matching the two templates. [6]
- If an attacker is able to still reveal the top-secret by means of newer technology then the template converts trivial to further improve biometric data. After secret, polynomial is directly recreated and hence biometric can be realised.[7]

2. CLASSIFICATION OF BIOMETRICS

A. Fingerprint verification

Fingerprint authentication discusses about the automatic method of proving a match between double human fingerprints. Fingerprints are of several forms of biometrics used to identify persons and prove their identity.

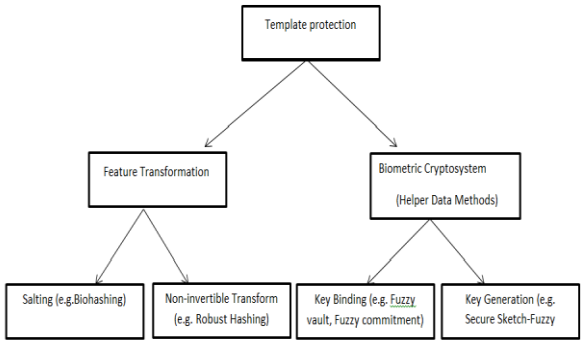

Fig.1: Classification of Template Protection schemes

Radha Narayanan and S.karthikeyan [8] has described an approach of double encryption based secure fuzzy vault using fingerprint biometric. In this method it combines of methods of

symmetric and asymmetric crypto system. It decreases the drawbacks regarding both the techniques.

There are two types one is locking of the vault and unlocking of the vault. The main purpose is to check for the use of fingerprint biometric in the construction of a cryptographic fuzzy vault system.

The popular existing techniques are based on remark core points of fingerprint but exact estimate continues to be a intricate difficulty and faults in the reference core points may run to false reject. To overcome this, a minutiae-cantered region encoding, MinuCode is used to mistreatment the reference core point purpose and grip with the noise of fingerprint biometrics. The position and position attributes of a minutia are combined and these attributes are measured as a 3-tuple (x, y, θ). Once the process for the locking and unlocking of vault is identified, the conditions for the authentic users to effectively unlock the vault can be fixed while rejecting the unauthenticated users.

The vault is supposed to unlock effectively, if the codes obtained from grid F (generated by R-S codes) with the help of query fingerprint features will be identically similar to the codes utilized at the time of locking. The inverse R-S codes can be utilized to the achieved codes to get the unique symmetric decryption key. At last, this decryption key can effectively decrypt the secret private RSA key.

The features obtained from this biometrics are used for encryption. Reed-Solomon encoding technique is used to tolerate the errors in decryption. The investigational results display that the proposed security scheme results in better security than the existing techniques.

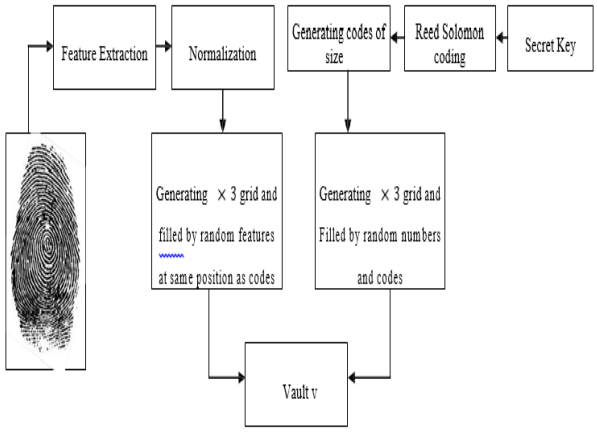

Fig 1.1: Block Diagram for Locking of the Vault

This paper offers better security scheme by using fingerprint biometric features. Since the thefts are increasing continuously, the need for improved security scheme is also increasing. The proposed scheme can be enhanced by incorporating multimodal biometric features to prevent the security attacks from the unauthorized users.

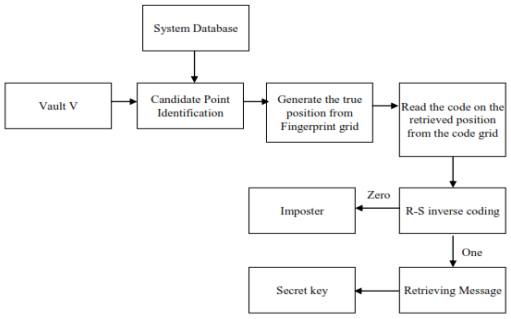

Fig 1.2: Block Diagram for Unlocking of the Vault

V.S.Meenakshi and G.Padmavathi [9], designed the technique called password hardened multimodal biometrics fuzzy vault. The scheme is examined on the iris and retina biometric traits. Unique Feature points are extracted from the iris and retina. Salting technique based on password is applied to feature points. These transformed points are used to create a fuzzy vault. The hardening of fuzzy vault using password drives the additional layer of security and provides cancellability feature in fuzzy vault. The loophole of the technique is as it is using the invertible function for transforming the feature points, if the attacker acquires the vault and password, he will be able to redeem the original minutiae points . Another pitfall is if an attacker gains an access to template before transformed and template after transformed, he can easily acquires password which was used in template transformation function.

Ki Young Moon et al [10] outlined the scheme using fingerprint trait. It provides efficient fuzzy vault with automatic alignment and solution to the co-relation problem of the fuzzy vault. For the automatic alignment, geometric hash function is applied and to conquer the co-relation problem, the chaff points are added on the basis of information of the genuine point instead of adding randomly. Since the comparison of keys is done in the hash domain for high security. It adds computational cost to the scheme.

Wencheng Yang Jiankun Hu et al [11], developed a scheme called a delaunay triangle group based fuzzy vault with cancellability. Polar transformation is used with fuzzy vault to provide revocability. Rather than applying the transformation function on the single minutiae, unit of transformation is triangle called delaunay triangle group. This transformed unit is more stable and intensive to non-linear distortion to biometric trait's image. Implementation of this scheme on the public database manifests that the performance decreased slightly but security of biometric traits enhanced. Other combinations of bio-crypto system and feature transformation based technique are also

proposed in literature on fingerprint trait.

B. Iris Verification

Hao et al[12] presented a realistic and secure way to include the irisbiometric into cryptographic applications.They thought on the error patterns within iris codes and established a two layered error correction codes that combines Hadamard and the Reed solomn codes.The key was made from the iris image of the person through the auxiliary error correction data that do not reveal the key and can be saved in a tamper resistant token like smart card. The estimation of the procedures was done with the aid of examples from 70 different eyes, l/O samples being obtained from every eye. It was recognized that an error free key can be replicated dependably from genuine iris codes with a achievement rate of 99.5%. It is possible to get the output up to 140 bits of biometric key, more than adequate for 128- bit AES.

Clancy et al. [13] planned a smart card based fuzzy vault that employed fingerprints for locking and unlocking. The assumption that developed fingerprint images are pre-aligned is not realistic and could be the possible reason for high false rejection rate (30.0%) has been reported.

Development of a new cryptographic construct using palm print based fuzzy vault has been examined by Amjoy kumar and Ajay kumar[14] by presenting a new approach to construct the cryptographic vault using palm print features. An experimental result illustrates that EER is about 0.3% while achieving the FRR of 0% at 0.35%.

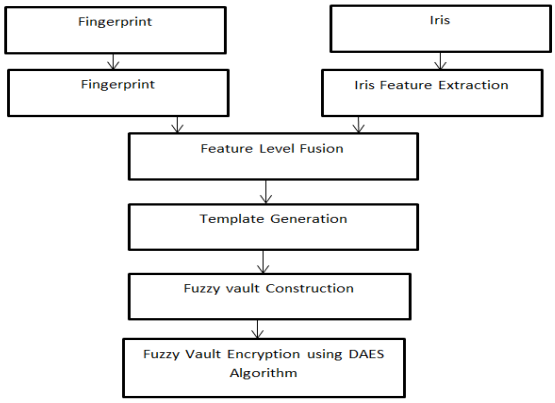

Fig: 2.1 Construction Multimode Fuzzy Vault

Three issue scheme for biometric created cryptography key regeneration using iris was proposed by Sanjay Kanade et al.[15] They used three issue (smart card, iris code and password) scheme for cryptographic key regeneration based on fuzzy drawings idea which handles biometric unpredictability with error correcting codes. Their FAR rate is 0.055% and FRR is 1.04%.

Karthik Nandakumar and Anil Jain presented multibiometric Template security using fuzzy vault.[18] Multibiometric vault delivers better recognition presentation and higher security compared to aunibiometric vault. The multibiometric vault created on fingerprint and iris reaches a GAR of 98.2% at FAR of 0.01%, while corresponding GAR values of the individual iris and fingerprint are 88% and 78.8%.

Securing Fingerprint Template: Fuzzy vault with helper data proposed by Umut Uludag and Anil Jain[19]. They present an implementation of fuzzy vault based on orientation field based helper data that is automatically extracted from the fingerprints. Initially, two impressions per finger (impression owner 1 for locking the vault, and impression owner 2 for unlocking the vault) are used. The Genuine Accept Rate (GAR) is found to be 72.6% at FAR 0%. Note that 16 fingers out of 100 were ignored since they did not contain a sufficient number (24) of minutiae for locking or unlocking the vault. Using two impresses per finger (impression number2 and number 7) for decoding the vault increases the GAR to 84.5% at 0% FAR.

Iris based hard fuzzy vault proposed by Srinivasa Reddy applies a order of morphological operations to abstract minutiae points from the iris texture. This idea is utilized for mining the locking or unlocking part from the retina. To identify the bifurcation feature point on the retinal texture the method proposed by Li Chen is used.

Biometric fuzzy extractors scheme for iris templates was proposed by F. Hernandez Alverz .Their aim is to measure how it deals with the intra user and inter user variability. For Intra operator GAR is 88.9% and FRR is 11% and for inter operator FAR is 1. 35%.

C. Hand Vein pattern

Hand vein pattern verification is the latest technology in biometric. It have lot of advantages than other methods. There are three methods used the palm vein recognition, hand vein recognition and finger vein recognition. Xiangping Zeng and Weidong Jin [20],described in this paper about the vein recogination.They have used the vein image pre-processing method. The pre-processing is actually the image enhancement process including normalization of the vein image size and gray, threshold processing, filtering algorithm to remove noise and refine the vein image.

Figure 3.1. Preprocessing of finger vein image: (a) original image; (b) normalization image; (c) binary image; (d) filtering image; (e) thinning image

First, vein acquisition device collects vein infrared image after image preprocessing, we will get a clear refinement

single pixel vein image. Then, extract the features of the single pixel vein image. Finally, match the features of the vein image with the sample database, and by matching algorithm we will make the identification come true.

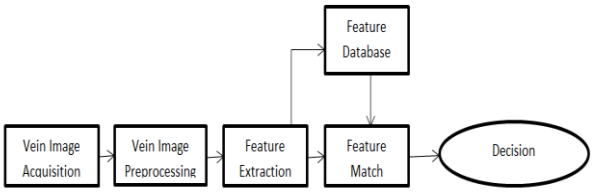

Figure 3.2. Diagram of vein recognition system

Sanchit, Maurício Ramalho et al. [21],this paper uses two types of hand vein that is palm and dorsal for verification purpose. An additional issue addressed in this paper has to do with the top way together dorsal and palm veins to develop a multimodal system. The remainder of the paper is planned as follows. The general architecture of the proposed biometric identification system.

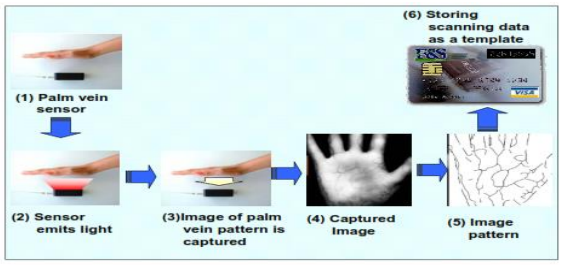

Figure3.3. Biometric Palm Vein Authentication System

This paper describe a multimodal biometric identification system that is created on a score equal mixture of palm and dorsal veins distance scores. Working results clearly show that the planned multimodal system offers very good results when related to the corresponding unimodal systems.

3. CONCLUSION

The fingerprint identification is one of the most common used form biometric identification. Fuzzy vault is an emerging area for template protection and has the potential for next generation security systems. Latest development in biometric is hand vein. When compared to other biometric it have lot of advantages. In is paper I have discussed about the fuzzy vault and biometric application.

REFERENCES

[1] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric Template Security," in Journal on Advances in Signal Processing, Michigan State University; pp. 1-17, 2007.
[2] Kai Xi and Jiankum HO, "Bio-Cryptography",pp.139-148,2009.
[3] T Clancy, D Lin and N Kiyavash, " Secure smartcard-based fingerprint authentication" in Proceedings of ACM SIGMM Workshop on Biometric Methods and Applications, Berkley, CA, pp. 45-52, 2003.
[4] Cengiz Orencik, "Fuzzy Vault Scheme for Fingerprint Verification: Implementation, Analysis and Improvements",Sabanci University, pp. 1-50, 2008.
[5] Mohammad Khalil-Hani, Rabia Bakhteri, "Securing Cryptographic Key with Fuzzy Vault based on a new Chaff Generation Method," in proceedings of IEEE, pp. 259-265, 2010.
[6] Hoi Ting Poon and Ali Miri, "A Collusion Attack on the Fuzzy Vault Scheme", University of Ottawa, ISC, pp. 27 -34, 2009.
[7] Sumin Hong, Woongryul Jeon, Seungjoo Ki, Dongho Won, Choonsik Park, "The Vulnerabilities Anal ysis of Fuzzy Vault using Password", in proceedings of IEEE, Vol. 3, pp.76-83, 2008.
[8] Radha Narayanan and S.Karthikeyan "Double Encryption based Secure Fuzzy Vault Construction using Fingerprint Biometric Features," Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering , March 21-23, 2012.
[9] Suriza Ahmad Zabidi, and Momoh-Jimoh E. Salami, "Design and Development of Intelligent Fingerprint-Based Security System," Knowledge-Based Intelligent Information and Engineering Systems, Book Chapter on Springer link, vol. 3214, pp. 312-318, 2004.
[10] T. A. Albert, and S. Ganesan, "Applications of Principal Component Analysis in Multimodal Biometric Fusion System," European Journal of Scientific Research, Vol. 67, No. 2, pp. 248-259, 2012.
[11] Xuebing Zhou, Stephen D. Wolthusen, Christoph Busch, and Arjan Kuijper, "A Security Analysis of Biometric Template Protection Schemes," Image Analysis and Recognition, Springer link, pp. 429-438,2009.
[12] F. Hao, R. Anderson and 1. Daughrnan, "Combining crypto biometrics effectively" IEEE Transaction on computers, vol.5, pp. 1081-1088,2006.
[13] T. Charles Clancy and Negar Kiyavash, Dennis J. Lin, "Secure Smartcard Based fingerprint authentication" In WBMA'03: Proceedings of the the 2003.ACM SIGMM workshop on Biometrics methods and applications,page45-52,New York,NY,USA, 2003 ACM press.
[14] Amjoy Kumar and Ajay Kumar "Development of new cryptographic construct using palm print based fuzzy vault"Indian Institute of Technology, EURASIP Journal on Advances in signal processing 2009
[15] Sanjay Kanade, Danielle Camara, Emine Krichen, Dijana Petrovska-Delacretz and Bernadette Dorizzi "Three factor scheme for biometrics based cryptographic key regeration using iris" Telecom & Management SudParis Evry,France.
[16] Karthik Nandakumar and Anil K. Jain "Multibiometric template security using fuzzy vault" BTAS 2008.
[17] Umut Uludag and Anil Jain "Securing fingerprint template: Fuzzy vault with helper data" Michigan State University.
[18] S. Sowkarthika and N. Radha "Securing Iris and Fingerprint Templates Using Fuzzy Vault and Symmetric Algorithm".
[19] F. Hernandez Alvarez, L. Hernandez Encinas and C.Sanchez Avila, "Biometric Fuzzy extractor scheme for iris templates",Spain.
[20] Xiangping Zeng and Weidong Jin" Research of Hand Vein Patterns Recognition for Biometric Identification," International Conference on Biomedical Engineering and Biotechnology 2012.
[21] Sanchit, Maurício Ramalho ,Paulo Lobato Correia, Luís Ducla Soares "Biometric Identification through Palm and Dosal Hand Vein Patterns".

Author

C.B.VASANTHA LAXMI received her B.E degree in Electrical And Electronic Engineering from Sathyamangalam Bannari Amman Institute of Technology (Autonomous) Anna University, Chennai. She is currently pursuing her M.E Degree in Power Electronic And Deives at Bannari Amman Institute of Technology, Anna University, Chennai. Her areas of interest are power electronic and Image Processing.