Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Fingerprint Fuzzy Vault: A Review

Rahul Hooda
CSE, PEC University of Technology
India.

Sahil Gupta
CSE, PEC University of Technology
India.

Abstract---- This paper is a brief review of fuzzy vault which is a biometric template security technique. The advent of technology over the last decade has established biometric identification as an electronic equivalent to physical verification. Biometric traits offer a reliable solution to the problem of user authentication in identity management systems. Biometric based authentication has more advantage over traditional method such as password due to their uniqueness and required physical attendance at the time of authentication. But there are increasing concerns about the security and privacy of biometric technology. Fingerprint Identification is the most commonly used in biometric systems and fuzzy vault is a new technique to secure the template. The aim of this paper is to review all the important developments in fuzzy vault till.

Keywords---- Biometric systems, template security, fingerprint verification system, fuzzy vault, chaff generation methods.

I. Introduction

In today's world use of biometric traits as authentication system is increasing in various applications so it is important to secure the user data from attackers. As for each user a template is stored, focus should be there to provide biometric template protection because once it is compromised it cannot be revoked and reissued. Template protection scheme is broadly classified into two main categories namely feature transformed approach and biometric cryptosystem (Fig. 1). In feature transformed approach a transformed scheme is applied to the biometric template and only transformed template is stored in the database. Depending on the characteristics of the transformation function, the feature transform scheme can be further categorized into salting and noninvertible transformation scheme. In Salting, transformation function is invertible, that is, if an adversary gains access to the key and the transformed template, he can recover the original biometric template (or a close approximation of it) whereas in noninvertible transformation scheme, a one way function is applied on the template and it is computationally hard to invert a transformed template even if the key is known [1, 2, and 3].

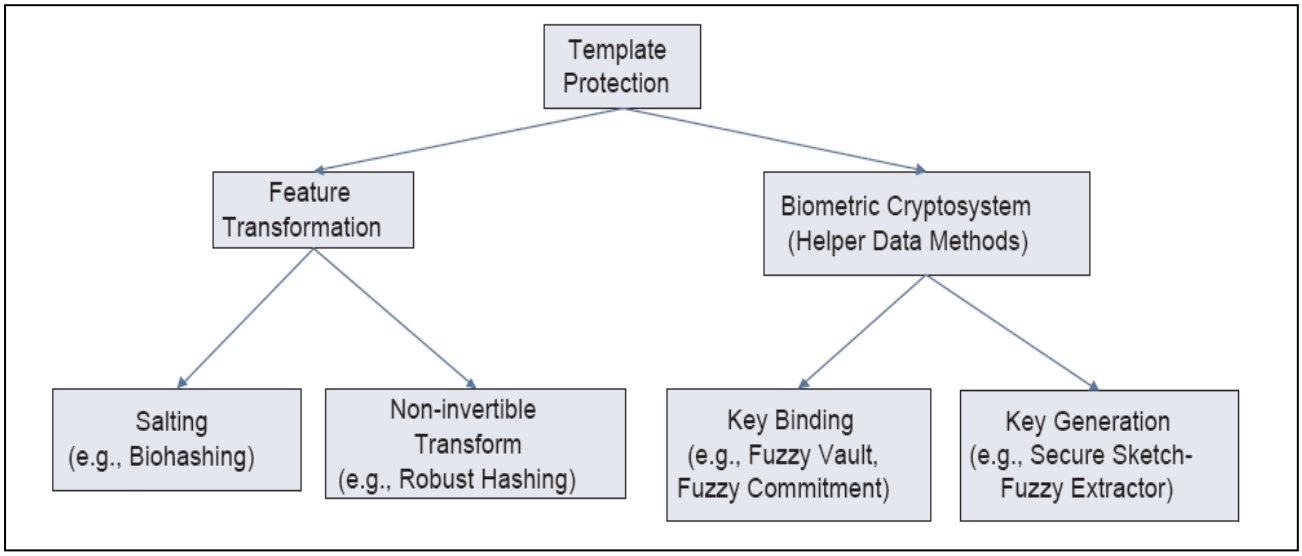

Fig.1 Classification of Template Protection Schemes

In biometric cryptosystem, some public information called helper data about the biometric template is stored. While the helper data does not reveal any significant information about the original biometric template, it is needed to extract a cryptographic key from the query biometric features. Depending on how the helper data is obtained biometric cryptosystems can be further classified into key generating and key binding biometric cryptosystems. In key generating

biometric cryptosystem the helper data is derived only from the biometric template and the cryptographic key is directly generated from the helper data and the query biometric features whereas in key binding biometric cryptosystem the helper data is obtained by binding a key that is independent of the biometric features with the biometric template [1, 2, and 3]. Fuzzy vault is an example of key binding biometric cryptosystem. In this paper an overview of the work done in the field of fuzzy vault is provided and fuzzy vault scheme is also explained briefly.

The rest parts of the paper are organized as follows: Section II introduces the fuzzy vault scheme. A review of the work done in the field of fuzzy vault is presented in section III. Conclusions are drawn in the last section.

II. Fuzzy Vault Scheme

Juels and Sudan [4] originally proposed Fuzzy vault scheme using the example of Alice and Bob. The security of fuzzy vault scheme is based on the infeasibility of the polynomial reconstruction problem. Alice hides secret k using an unordered set A. A polynomial p is selected which encodes k in some way. Elements of set A are plotted by evaluating the polynomial on each value. Then large numbers of random chaff points are added to the computed values to form the fuzzy vault V. All the chaff points should fulfil the condition of not lying on the polynomial p. Chaff points are used to hide the genuine points from an attacker.

Bob can only found out the secret key k only if provides sufficient number of points equal to that in set A. For that Bob will provide an unordered set B. If the points in set B substantially overlap with points in set A then polynomial can be recreated and secret key k will be given to the user. But if A and B does not overlaps enough then it will not be able to reconstruct the polynomial and hence user will be denied having secret key. This scheme is called fuzzy vault since it will work even when set A and B are not completely similar.

Advantages of Fuzzy Vault:

- Fuzzy vault is secure in the sense that it does not leak information about minutiae since it uses one-way hash function for encryption like 'Cancellable' biometrics.
- Ability to handle intra-class variations in biometric data. Unlike cryptography, it may allow a match to occur if the difference between the query biometric data and the template is small.
- The fuzzy vault scheme stores only a transformed version of the template, which makes it applicable to various modalities besides fingerprints.[2,5,6]

Issues in Fuzzy Vault:

- Alignment of query with transformed version of biometric is quite difficult.
- The chaff points generated later in the process tend to have less degree of freedom. A point with less degree of freedom has more neighbouring points and it becomes little easy to detect them. [7]
- Given two or more such fuzzy vault instances generated from the same point, but with different keys and different random chaff, the minutiae are likely recoverable by matching the two templates. [8]
- If an attacker is able to recover the secret k through means other than attack against the template it becomes trivial to recover biometric data. From secret, polynomial is directly reconstructed and hence biometric can be achieved. [9]

III. Related Work

Fuzzy vault is quite a new area of research and great amount of research in this area is going on. Clancy et al [5] proposed a fingerprint vault based on fuzzy vault of Juels and Sudan. They used multiple minutiae locations as elements of locking set. This method assumed that fingerprints required to form vault and for query are pre-aligned. In their scheme Reed Solomon technique is used to reconstruct polynomial and decode the secret. Yang and Verbauwhede [10] introduce alignment in fuzzy vault system for fingerprints by proposing the use of reference minutiae, which are extracted during vault encoding and decoding. The alignment is established if these two references are same and thus the origins of coordinate frames to be used. Uludag et al [11] proposed a method for fuzzy vault for fingerprints using simple translation and rotation for alignment because reference minutiae may not be same in number or in position during enrolment and verification. This algorithm used cyclic redundancy check and Lagrange interpolation instead of Reed Solomon decoding. The main drawback of Reed Solomon coding scheme are that the input data set only contain integer within limited range and vault may leak some information because it is stored without transformation.

In 2006, Anil K Jain and Uludag [12] enhanced performance of fuzzy vault by introducing helper data. In this proposed method template is stored after transforming to other set of coordinates to provide security but it then becomes difficult to align query with stored template. With the use of helper data, the stored template in transformed domain is used for alignment and comparison with the query data. It does not leak minutiae information while aligning the query template. Karthik Nandkumar and Anil K Jain [13] further improved fuzzy vault by using minutiae matcher to compensate for non-linear distortion in fingerprints and considering orientation in addition to the location of the minutiae point. They also used local image quality index estimated from fingerprint to select the most reliable minutiae. Abhishek Nagar et al [14] proposed a technique of evaluating the polynomial using helper data using encryption. Orientation and ridge frequency information in minutiae neighbourhoods are the two attributes used for minutiae description for securing polynomial evaluations. Seira Hidano et al [15] proposed a scheme which stores the user template after encryption and this scheme is used to generate the secret data from the user template and the query biometric data. In this paper, a fingerprint authentication system is simulated to evaluate template security of the proposed technique. The research of Jason Jeffers and Arathi Arakala [16] is directed to methods of realizing the fuzzy vault for the fingerprint biometric using minutiae points described in a translation and rotation invariant manner. The variation in different samples of the same biometric makes it difficult to replace passwords directly with biometrics in a cryptographic scheme**.** Hoi Ting

Poon and Ali Miri [17] discussed that CRC decoders are most commonly used decoders in fuzzy vault but they have some flaws. They proposed a new decoder which is based on Euclidean algorithm and origins from Reed Solomon(RS) codes. This new scheme has considerably decreased the decoding time as compared to CRC decoders and also maintains security. Zhang et al [18] implemented a modified fuzzy vault scheme which requires less memory for storing the templates and also leads to less entropy loss. In this paper, a new interpolation method is also proposed and implemented which reduces the computation complexity of the verification process and also the latency. In the next three subparts developments in the important areas of alignment between template and query, chaff placement methods and vulnerabilities of the fuzzy vault.

A. Alignment between Template and Query

Template and Query needs to be aligned to have a good fingerprint matching system. Daesung Moon et al [19] were first to include alignment in their method. All previous methods assumed that fingerprint features were pre-aligned. They added automatic alignment of fingerprint features in the matching stage using the geometric hashing technique. Yongwha Chung et al [20] were first to implement alignment approach in fuzzy vault. It was important since alignment was performed in a non-invertible transformed domain. Jason Jeffers and Arathi Arakala [21] propose pre-alignment algorithm that uses properties intrinsic to minutiae sets instead of using hash tables. For properties of minutiae sets Five nearest neighbour, Vornoi neighbour and Triangle based structures are used as three structures. Peng Li et al [22] were of the view that alignment method based on high curvature points may reduce the security level of fuzzy vault system. They developed effective implementation which took the minutiae descriptor into consideration

B. Chaff Placements Methods

Placing of chaff points is the most time critical operation in the fuzzy vault scheme. Time taken during this operation mainly decides the performance of system. Alper Kanak and Ibrahim Sogukpinar [23] used the Clancy method to add chaff points but in different way. This method enhances the security by combining the fingerprint minutiae with the user specific pseudo random data. At each acquisition a subset is selected from the set of user specific randomly selected chaff minutiae features which is stored for each user. Predefined chaff minutiae are used in these vaults as it reduces the time to calculate chaff points each time for enrolment. Orencik et al [24] suggests that the location of chaff points may leak information about the genuine points and proposes a new technique that makes it difficult to distinguish genuine points from chaff points. The distance between a chaff point and a genuine point or two chaff points is 't' but the distance between two genuine points is not fixed and can be less than 't' which makes the detection of minutiae easy. So chaff points should be placed at distance t' which is less than t. To create the false impression of genuine image points, chaff points are generated such that they lie on fake polynomial. This improves the security of chaff generation scheme. Mohamed Khalil-Hani, Rabia Bakhteri [7] proved that the most time consuming and thus critical operation in the fuzzy vault scheme is generation of the chaff points. The proposed a new chaff generation algorithm for the fuzzy vault in a bio-cryptosystem which is based on a circle packing theorem, requires less computation power than existing methods. Experimental results of the proposed algorithm show that algorithm is about 100 times quicker than existing methods for 200 or more number of chaff points.

C. Vulnerabilities in Fuzzy Vault

Although fuzzy vault is intended to secure template but there are still some vulnerabilities which need to be addressed. Qiong Li, Zhaoqing liu and Xiamu Niu [25] provides an analysis of fuzzy vault scheme and explained the problem existed in the UNLOCK algorithm. It is suggested that the use of the Reed- Solomon code in the UNLOCK algorithm is not suitable and its computation complexity analysis also needs reconsideration. A new UNLOCK algorithm and computation complexity analysis which solves the discussed problems are also presented. Hoi Ting Poon and Ali Miri [27] describe various algorithms of collusion attacks on the fuzzy vault scheme. Collusion attack is an attack where the attacker is assumed to have access to multiple vaults locked by the same key. The attack can be used effectively to reduce the vault size by identifying and removing chaff points. The vault size depends on the rate at which chaff points are identified and the vault size decreases as it increases. Sumin Hong et al [9] analyze the vulnerabilities in the scheme proposed by K. Nandakumar for hardening a fingerprint minutiae-based fuzzy vault using password and propose a new scheme which is secure against various attacks to fuzzy vaults. Walter J. Scheirer and Terrance E. Boult [26] provide a analysis of various attacks against the database in major privacy enhanced technologies (PETs) which includes attack via surreptitious key-inversion attack, record multiplicity and novel blended substitution attacks. All the known attacks against Biometric Fuzzy Vault (BFV) and Biometric Encryption (BE) are discussed and new attacks are also explained. Woo Yong Choi et al [27] proposes a new attack called Fast Polynomial Reconstruction (FPR) attack. In this if the fuzzy vault contains two more genuine points then the degree of the polynomial then the original polynomial can be reconstructed. Experiments results are also shown which proves that the new attack is better than both the correlation attack and brute force attack.

IV. Conclusion

The fingerprint identification is one of the oldest and most common form of biometric identification. Fuzzy vault is an emerging area for template protection and has the potential for next generation security systems. Literature review consists of work done in the area of fuzzy vault, improvements in image alignment and different chaff generation methods. Work has been done in this field but still some scope is there for improvement. Issues related to vulnerabilities of fuzzy vault, image alignment and chaff generation time can be the basis on which future work be possible.

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 Jiankun Ho, "*Bio-cryptography*", pp. 139-148, 2009.
[3] Anil K. Jain, Arun Ross and Patrick Flynn, "*Handbook of Biometrics*", pp. 1-10, 2008.
[4] Ari Juels and Madhu Sudan, "A Fuzzy Vault Scheme," *in IEEE International Symposium Information Theory*, Lausanne, Switzerland, pp. 408, 2002.
[5] 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.
[6] Cengiz Orencik, "Fuzzy Vault Scheme for Fingerprint Verification: Implementation, Analysis and Improvements", Sabanci University, pp. 1-50, 2008.
[7] 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.
[8] Hoi Ting Poon and Ali Miri, "A Collusion Attack on the Fuzzy Vault Scheme", University of Ottawa, ISC, pp. 27-34, 2009.
[9] Sumin Hong, Woongryul Jeon, Seungjoo Ki, Dongho Won, Choonsik Park, "The Vulnerabilities Analysis of Fuzzy Vault using Password", *in proceedings of IEEE*, Vol. 3, pp.76-83, 2008.
[10] S Yang and I Verbauwhede, "Automatic secure fingerprint verification system based on fuzzy vault scheme*" in Proceedings of IEEE ICASSP*, Philadelphia, PA, Vol. 5, pp. 609-612, , 2005.
[11] Umut Uludag, Sharath Pankanti and Anil K. Jain, "Fuzzy vault for fingerprints," *in Proceedings of Audio- and Video- based Biometric Person Authentication*, Rye Town, NY, 2005.
[12] Umut Uludag and Anil K. Jain, "Securing fingerprint template: Fuzzy vault with Helper Data," *in Proceedings of CVPR Workshop Privacy Research Vision*, New York, pp. 163, 2006.
[13] Karthik Nandakumar, Anil K. Jain and Sharath Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance," *IEEE Transition for Information Forensics & Security*, pp. 744-757, 2007.
[14] Abhishek Nagar, Karthik Nandakumar and Anil K. Jain, "Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptors," *in International Conference for Pattern Recognition*, Tampa, pp. 1-4, 2008.
[15] Seira Hidano, Tetsushi Ohki, Naohisa Komatsu and Masao Kasahara, "On Biometric Encryprtion using Fingerprint and It's Secirity Evaluation," *in 10th International Conference on Control, Automation and Robotics and Vision*, pp. 950-956, 2008.
[16] Jason Jeffers and Arathi Arakala, "Minutiae Based Structures for a Fuzzy Vault," *in Biometric Symposium IEEE*, RMIT University, Melbourne, pp. 1-6, 2006.
[17] Hoi Ting Poon and Ali Miri, "On Efficient Decoding of the Fuzzy Vault Scheme", *in 11th International Conference on Information Sciences, Signal Processing and their Applications: Main Tracks*, pp.454-459, 2012.
[18] Xinmiao Zhang, Richard Shi and James Ritcey, "On the Implementation of Modified Fuzzy Vault for Biometric Encryption", *in Information Theory and Applications Workshop (ITA)*, pp. 56-61, 2012.
[19] Daesung Moon, Sungju Lee, Yonghwa Chung, Sung Bumpan and Kiyoung Moon, "Implementation of Automatic Fuzzy Fingerprint Vault," *Seventh International Conference on Machine Learning and Cybernetics*, Kunming Korea, Vol. 7, pp. 3781- 3786, 2008.
[20] Yonghwa Chung, Daesung Moon, Sungju Lee, Seungwan Jung, Taehae Kim and Dosung Aho, "Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault," *in proceedings of Springer*, Korea, pp. 358-369, 2005.
[21] Jason Jeffers and Arathi Arakala, "Fingerprint Alignment for a Minutiae-Based Fuzzy Vault," *in Biometric Symposium IEEE*, pp. 1-6, 2007.
[22] Peng Li, Xin Yang, Kai Cao, Xuniang Tao, Ruifang Wang and Jie Tian, "An Alignment-free Fingerprint Cryptosystem based on Fuzzy Vault Scheme," *Journal of Network and Computer Applications*, Beijing, Vol. 33, pp. 207-220, 2009.
[23] Alper Kanak and Ibrahim Sogukpinar, "Fingerprint hardening with Randomly Selected Chaff Minutiae," *in CAIP Springer*, pp. 383-390, 2007.
[24] Cengiz Orencik, Thomas Brochmann Pederson, Erkay Savas and Mehmet Keskinoz, "Improved Fuzzy Vault Scheme for Fingerprint Verification," *in International Conference on Security and Cryptography SECRYPT*, Porto, pp. 37-43, 2008.
[25] Qiong Li, Zhaoqing liu and Xiamu Niu, "Analysis and Problems of Fuzzy Vault Scheme," *in proceedings of IEEE*, pp. 244-250, 2006.
[26] Walter J. Scheirer and Terrance E. Boult, "Cracking Fuzzy Vaults and Biometric Encryption," *in proceedings of IEEE*, Securics Inc. and University of Colorado, pp. 1-6, 2007.
[27] Woo Yong Choi, Sung Bum Pan, Joo-Man Kim, Yongwha Chung and Dowon Hong, "Fast Polynomial Reconstruction Attack against Fuzzy Fingerprint Vault", *in 5th International Conference on New Trends in Information and Service Science*, pp.299-302, 2011.

