Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Enhancement Techniques of The Fuzzy Vault: A Review

Ismeet Kaur
CSE, PEC University of Technology
India

Ajay Mittal
CSE, PEC University of Technology
India

Manvjeet Kaur
CSE, PEC University of Technology
India

Abstract— Security of a biometric system is of paramount importance considering increased commercial use for allowing access to sensitive areas. In this context protection of stored biometric templates is of particular interest as these templates are irrevocable once leaked. Fuzzy vault has emerged as a novel cryptographic construct for the protection of biometric templates. But like every other technique this scheme is rife with loopholes. To overcome these issues several security enhancement techniques have been introduced for the fuzzy vault. This paper discusses these security issues and the various enhancement techniques currently available for fuzzy fingerprint vault.

Keywords— fuzzy vault, biometrics, security, security enhancement.

I. INTRODUCTION

Biometric systems are gaining popularity as they eliminate the possibility of stealing of passwords and tokens. But irrevocability in case of leaking of biometric data is a major issue. This calls for increased protection of biometric templates. Template protection schemes can be classified into the following categories [1]: feature transformation approach and biometric cryptosystem. In feature transformation, a transformation function is applied on the biometric template and the transformed template is stored in the database. The same function is also applied on the query feature and then this is cross-matched with the stored template. The feature transform approach can be further categorized as (i) *salting* in which the transform can be inverted using a secret key, and (ii) *non-invertible transform* in which the template once inverted cannot be changed back even if the key is known.

In a biometric cryptosystem, the biometric template stores some public information. It can be further categorized as (i) *key-binding biometric cryptosystems* in which template is generated by binding a random key to the helper data and (ii) *key-generation biometric cryptosystem* in which the key is derived from the helper data. Matching is performed by decoding the key from the template and verifying it by matching it with the original key.

Fuzzy vault is a key-binding biometric cryptosystem proposed by Juels and Sudan[2]. In this scheme genuine points are hidden among a large number of chaff points to make it computationally difficult for the attacker to identify the genuine points.

Fuzzy vault has certain limitations:

(i) Once the vault is compromised, the biometric data cannot be reused to create another vault. [3]
(ii) An attacker may also be able to exploit the fuzzy vault on the basis of statistical analysis of the distribution of minutiae points. [4]
(iii) An attacker may replace chaff points with his own features. This may lead to denial of service to the user or access to both the user and the attacker.[1,5]
(iv) Aligning of stored template and query minutiae by using helper data may leak some information about the template to the attacker. [5]
(v) Fuzzy vault is vulnerable to correlation attack if the attacker has access to two templates of the same user.[6]

The paper proceeds with analysis of enhancement techniques of the fuzzy vault in some specific areas (Section II). The final section (Section III) recapitulates the essence of the biometric scenario regarding the fuzzy vault.

II. SECURITY ENHANCING TECHNIQUES OF THE FUZZY VAULT

Fuzzy vault has certain ambiguous areas that make it susceptible to some adversaries. An attacker may be able to exploit user data by extracting information leaked during alignment or by hacking into the biometric database and retrieving user templates. It is anticipated that even if an adversary is able to intercept a fuzzy vault, he should not be able to decode it successfully [1]. Some of the techniques proposed so far to enhance the security of the fuzzy vault are discussed as follows:

A. Multimodal fuzzy vault

Unimodal fuzzy vault is vulnerable to noisy data, spoofing, inter class similarities and intra class variations [7]. Multimodal systems employ multiple impressions of the same trait or use of multiple traits as shown in Fig 1. It may be a combination of fingerprint and other traits or multiple fingers[8] etc. Security is measured in terms of average min-entropy of the biometric template given the vault. The proposed scheme [9] shows a higher min-entropy value than single fingerprint indicating greater security of the fuzzy vault. But there may be some degradation in.

GAR.

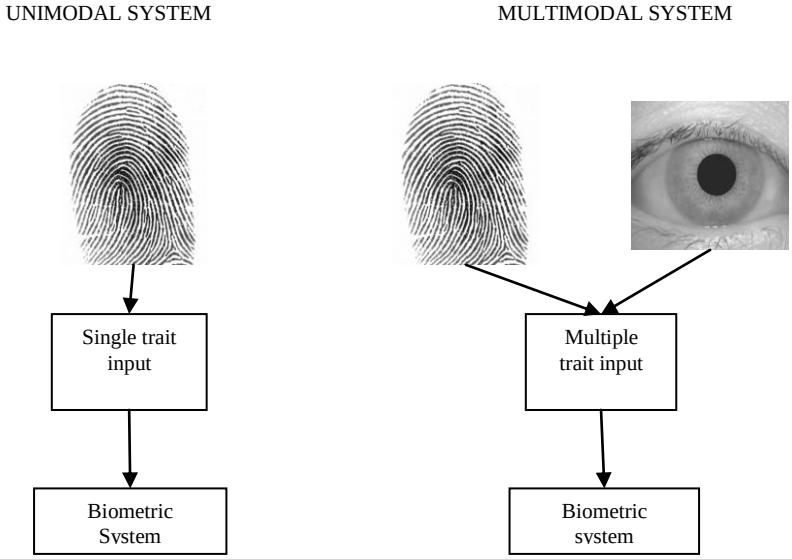

Fig 1: Unimodal and multimodal biometric systems

B. Hardening fingerprint fuzzy vault using password

In proposed scheme [10] first the fuzzy vault is constructed, then the vault is encrypted with a key that may be derived from the secret stored in the vault or may be a totally different key. This way password adds another layer of security to the vault as it is difficult for the attacker to decode both the password and the fuzzy vault.

But passwords may be stolen through socialization as people find it hard to remember difficult passwords and usually assign a password related to their personal life. Even if the password is not known an adversary may be able to compute the encrypted template through cross-matching and derive the original template from which the password of the user can be figured out. Sumin Hong [11] proposes an improvement to the above scheme by using hashed password.

C. Fuzzy fingerprint vault using Minutiae Descriptors to encrypt ordinate points

A minutiae descriptor consists of ridge orientation and frequency information of points in the space around a minutia. In the proposed scheme the ordinate values of the vault are encrypted with the minutiae descriptors. Fuzzy commitment scheme [12] is used for this. Non-matching descriptors will not be able to decrypt the ordinate values so an attacker will not be able to decode the vault and guessing the ordinate values and minutiae descriptors simultaneously is hard.[13]

D. Fuzzy vault using multi-polynomials

Fuzzy vaults use a single polynomial, the coefficients of which store the secret key and on which the minutiae points are traced. The proposed scheme [14] uses varying degrees of polynomial depending on the number of minutiae points extracted from a user biometric and has tried to provide protection in case of few minutiae points. It also uses multiple polynomials to maintain the security of the system. Proposed scheme claims to make an attack 2^{192} more difficult than using low degree polynomial.

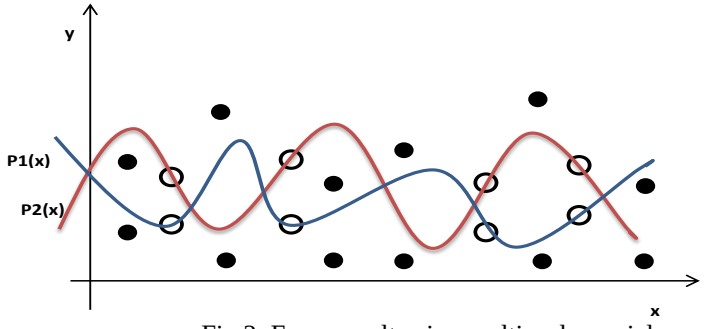

Fig 2: Fuzzy vault using multi-polynomials

E. Encrypted Fuzzy vault

Feng Quan [15] proposes performing encryption and decryption twice. The secret key consisting of the coefficients of the polynomial is encrypted. Besides this the minutiae points are also decrypted using a private list derived from a secret key or the minutiae points. This technique does not use chaff points for the encrypted vault. Chaff points are added after the encrypted vault is decrypted.

Brute force attack is not feasible; it becomes susceptible if an attacker is able to guess the private list derived from a PIN or password.

F. Increasing Degree Of The Polynomial

Peng Li [16] proposes that if the minutiae points are kept constant, then by increasing the degree of the polynomial the security level can be increased. This increases the complexity of the unlocking phase which will make it computationally difficult for the attacker to decode.

But increasing degree of the polynomial leads to high error rates (FAR, FRR). Further, it will also lead to increased computation time for polynomial reconstruction in the decoding phase [17]. So, the authors suggest that a tradeoff between security and matching accuracy should be reached.

G. Secure Alignment

During alignment of stored template and query minutiae information about the data may leak out [5]. To overcome this problem several new alignment free cryptosystems have been proposed. Ki Young [18] proposes an automatic alignment for fingerprints using geometric hash tables. Yang [19] has also proposed automatic system for fuzzy vault.

H. One-Time Template

In this scheme [18] a new template is created every time a user is successfully authenticated. Some new minutiae points have to be added every time otherwise an attacker will be able to correlate two previously created vaults. This scheme will not work if the size of image is small as the chaff points added will start repeating after all permutation are applied on a limited domain. A larger size of image will allow more number of minutiae points and greater range for chaff points.

I. Chaff Point Placement

Ki Young [18] proposes to add chaff points based on information of minutiae instead of randomly generating them. The proposed works also shows to be resistant to correlation attack. Besides that it gives better GAR values without degradation of FAR.

III. CONCLUSION

Biometric authentication systems are gradually replacing traditional authentication systems as a user does not have to worry about losing password or token. Emerging security concerns of protecting biometric template has made the fuzzy vault cryptosystem a viable option as it accommodates variations in user input. With increased interest in fuzzy vault efforts have been made to plug gaps that have surfaced so far. This paper has attempted to encompass some of the security enhancement techniques to address the security issue of the fuzzy vault. As the security level of the fuzzy vault increases, it will find increased deployment in biometric systems.

REFERENCES

[1] Anil K. Jain, Karthik Nandakumar and Abhishek Nagar, "Biometric Template Security", in Journal on Advances in Signal Processing. Michigan State University, Vol. 2008, pp. 1-17, 2008.

[2] Ari Juels and Madhu Sudan, "A Fuzzy Vault Scheme", in proceedings of IEEE International Symposium Information Theory, Lausanne, Switzerland,pp.408, 2002.

[3] Karthik Nandakumar, Anil K. Jain and Sharath Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance", in proceedings of IEEE Transactions on Information Forensics & Security, Vol. 2, pp. 744-757, 2007.

[4] Ee-Chien Chang, Ren Shen, Francis Weijian Teo, " Finding the Original Point Set Hidden among Chaff", in Proceedings of ACM Symposium on Information, Computer and Communications Security, pp. 182-188, 2006.

[5] Walter J. Scheirer and Terrance E. Boult, "Cracking Fuzzy Vaults and Biometric Encryption", Securics Inc. and University of Colorado, in proceedings of IEEE, pp. 1-6, 2007.

[6] Alisher Kholmatov and Berrin Yanikoglu, "Realization of Correlation Attack Against the Fuzzy Vault Scheme", Sabanci University, Istanbul.

[7] Arun Ross And Anil K. Jain, "Multimodal Biometrics: An Overview", in proceedings of EUSIPCO, pp. 1221-1224, 2004.

[8] Marianne Hirschbichler, Colin Boyd and Wageeh Boles, "A scheme for enhancing security using multiple fingerprints and the fuzzy vault", in proceedings of IEEE DICTA, pp.540-547, 2008.

[9] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in proceedings of IEEE Second International Conference on Biometrics: Theory, Applications and Systems, 2008.

[10] Karthik Nandkumar, Abhishek Nagar, Anil K. Jain, "Hardening Fingerprint Fuzzy Vault using Password", in proceedings of ICB, Michigan State University, 2007.

[11] Sumin Hong, Woongryul Jeon, Seungjoo Ki, Dongho Won, Choonsik Park, "The Vunerabilities Analysis of Fuzzy Vault using Password", in proceedings of IEEE, Vol. 3, pp.76-83, 2008.

[12] Ari Juels and Martin Wattenberg, " A Fuzzy Commitment Scheme", in proceedings of ACM CCS, pp. 28-36, 1999.

[13] Abhishek Nagar, Karthik Nandkumar, Anil K. Jain, "Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptors", in proceedings of IEEE ICPR, Tampa, pp. 1-4, 2008.

[14] Daesung Moon, Woo-Yong Choi, Kiyoung Moon, "Fuzzy Fingerprint Using Multiple Polynomials", in proceedings of IEEE, pp. 290-293, 2009.

[15] Feng Quan, Su Fei and Cai Anni, "Encrypted Fuzzy Vault Based on Fingerprint", China, International Conference on Information Assurance and Security, Beijing, Vol. 1, pp.137-140, 2009.

[16] 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.

[17] Woo Yong Choi, Jin-Won Park and Yongwha Chung, " Protection of the Fingerprint Minutiae", Recent Application in Biometrics, 2011.

[18] Ki Young Moon, Daesung Moon, Jang-Hee Yoo, Hyun-Suk Cho, "Biometrics Information Protection Using Fuzzy Vault Scheme", in proceedings of IEEE SITIS, pp. 124-128, 2012.

[19] Shenglin Yang and Ingrid Verbauwhede, " Automatic Secure Fingerprint Verification System Based On Fuzzy Vault Scheme", in proceedings of IEEE ICASSP, Philadelphia, Vol. 5, pp. 609-612, 2005.

