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

Fuzzy Vault with Iris and Retina: A Review

Geetika
Department of Computer Science and Engineering
PEC University of Technology, Chandigarh, India

Manavjeet Kaur
Department of Computer Science and Engineering
PEC University of Technology, Chandigarh, India

Abstract-Biometric systems play an important role in authenticating the identity of an individual. Such authenticated systems are still prone to attacks and securing them is an important issue. To overcome this, biometric based authentication is blended with cryptography resulting in a framework called fuzzy vault which provides a high level of security. Fuzzy vault is a biometric cryptosystem used for protecting private keys and releasing them only when the legitimate users enter their biometric data. Fuzzy vault provides better security with iris and retina, because of their higher stability and template longevity as compared to other biometric traits. This paper reviews the basic concept of biometric security, operations in fuzzy vault along with its advantages, limitations and its implementation with iris and retinal biometric traits.

Keywords-Biometric security, Fuzzy Vault, Crypto biometric system, independent component analysis, chaff point

I. Introduction

Biometric security is an automated measurement of Physiological and/or behavioral characteristics, such as DNA, fingerprints, retinas and irises, voice patterns, facial patterns to determine or authenticate the identity of an individual. Biometric traits cannot be lost or forgotten and they are inherently more reliable. It is very difficult to copy, share and distribute a biometric trait. Biometric system requires the person to be present at the time and point of authentication. There is typically an enrolment process in which the biological information is taken and stored in a database for future identification or verification purposes.

A. Iris

Iris is the elastic, pigmented, connective tissue that surrounds the pupil of the eye. Iris biometric is more reliable and accurate as compared to other biometric trait such as finger print. Iris texture is stable throughout life and is highly secure. Iris is less prone to attacks. Iris of the eye has different pattern for left and right eye. They are even unique for the identical twins. Iris is used for various authentication and security applications that include identity cards and passports, prison security, database access and computer login, border control and Government programmes etc.

B. Retina

These are the blood vessels at the back of the eye with a unique pattern. As compared to other biometric traits, Retina is highly secure and accurate. Retinal patterns are very difficult to spoof. These patterns vary for right and left eye. They are even unique for identical twins. Retinal patterns do not change with age as they are stable in nature. Retinal pattern is highly unlikely to be altered by any environmental or temporal conditions and is located deep within one's eyes. Because of this stability nature, retina is best suited biometric trait for high security system applications such as power plants and military applications. In cryptographic systems, key plays an important role. But the storage and secure generation of cryptographic keys is the main problem with the system. To overcome this, these systems have stored keys in storage devices such as smartcards, computers or servers, to be released only by password-based authentication [1]. The passwords may be shared, lost or forgotten. This problem can be solved by Biometric based authentication as biometric features are difficult to be copied, shared and distributed. Biometric system ensures access to the secret keys only to the legitimate user, but still there remains the risk of the keys and biometric templates being compromised by physical attacks. To overcome the above problems, Biometric based key generation method is needed in which cryptographic keys are blended with user's biometric data using cryptography to provide a high level security [2]. Here the secret key is extracted from the combined key and biometric template. Therefore, it becomes difficult for the attackers to obtain keys without knowing the specific user's biometric data. Hence the keys and biometric templates can remain secure. This Biometric based key generation construct is known as crypto-biometric system or Fuzzy Vault.

II. Fuzzy Vault

Fuzzy vault is a crypto-biometric system that utilizes the advantages of both cryptography and biometrics. It was first proposed by Juels and Sudan [3] in which secret information is encrypted and decrypted securely using a fuzzy unordered set of genuine points and chaff points. The basis for the security provided by Fuzzy Vault is Polynomial reconstruction problem which is a special case of Reed-Solomon list decoding problem. Fuzzy vault eliminates the key management problem as the key is release only when a legitimate user enters their biometric data. There are two operations in fuzzy vault i.e. Encoding and Decoding.

A. Locking the Vault-

While encoding, a secret key is locked by an unordered set G from the biometric sample. A polynomial P is then constructed by encoding the secret key and evaluated by all the elements of the unordered set. A random chaff point set C, which is 10 times the genuine points is taken. Then the union of the chaff point set C which do not lie on polynomial and the unordered set G is performed to create a vault V i.e. V = G U C

This union of the chaff point set hides the genuine point set from the attacker and thus securing the secret data and user biometric template simultaneously.

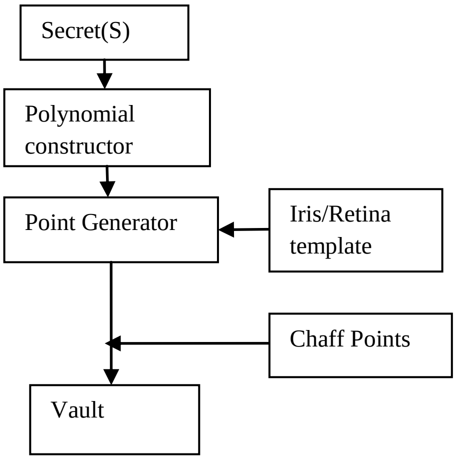

Fig. 1 Fuzzy vault scheme for locking the vault

B. Unlocking the Vault-

While decoding, the secret key S can be retrieved from the vault by providing query template which is represented by another unordered set G'. The set G' had to be almost equal to set G. If the difference between set *G* and set *G'* was very small i.e. substantial overlap, then the user can identify many points in V that lie on P. If sufficient number of points can be identified then the polynomial P can be exactly reconstructed by using an error correction scheme and thus generating the secret data securely/decoding the secret keys securely. If G' does not overlap substantially with G, it is infeasible to reconstruct P and the authentication is unsuccessful. This crypto-biometric system is known as fuzzy because the vault will get decoded even for very near values of G and G**'** and the secret key S can be retrieved. Therefore fuzzy vault is more suitable for biometric data which show inherent fuzziness as biometric data contain the intra-variations of the same person. Also, the fuzzy vault scheme requires pre-aligned biometric templates that are properly aligned with the input biometric data [1].

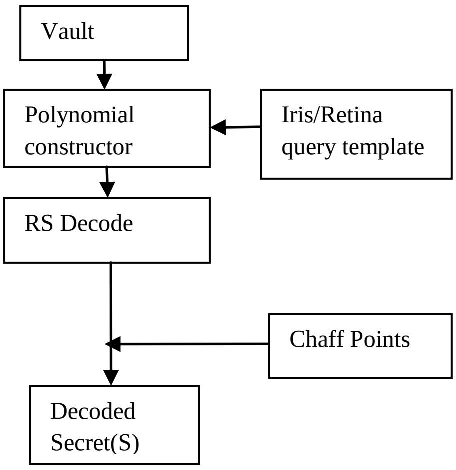

Fig. 2 Fuzzy vault scheme for unlocking the vault

C. Performance of Fuzzy Vault:

The parameters that affect the performance of fuzzy vault are:

1) *Parameter G:* it denotes the number of points in the vault that lie on the polynomial P and it depends on the number of features extracted from the template.

2) *Parameter C:* it denotes the number of chaff points that are added. It influences the security of the vault. If chaff points are not added then the vault reveals the information about the template and the secret key. With the increase in the number of chaff points, the degree of security for the vault increases.

3) *Parameter D:* it denotes the degree of polynomial and controls the tolerance of the system to errors in biometric data.

D. Advantages of Fuzzy Vault:

1) Fuzzy vault is secure in the sense that it does not leak information about minutiae since it uses one-way hash function or encryption like 'Cancellable' biometrics.

2) 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.
3) The fuzzy vault scheme stores only a transformed version of the template, which makes it applicable to various modalities besides fingerprints.

E. Limitations of Fuzzy Vault:

Fuzzy vault being a proven scheme has its own limitations [4].

1) If the vault is compromised, then the same biometric data cannot be used to construct a new vault with different key, polynomials and random chaff points. Fuzzy vault is prone to cross- matching of templates across various databases and cannot be revoked.
2) As the biometric features are of non uniform nature, it becomes easy for an attacker to exploit them and develop attacks based on statistical analysis of the points in the vault.
3) As the chaff points are more in number than the genuine points, it becomes possible for the attacker to substitute few points using his own biometric feature. Therefore both the genuine user and the attacker are authenticated by the vault using the same biometric identity. This results in the increase of false acceptance ratio.
4) As the original template of the genuine user being authenticated is temporarily exposed. The attacker can glean the template during this exposure.

To overcome the above limitations of fuzzy vault, password is used as an additional level of security and enhances the user-privacy.

III. Implementation With Different Traits

A. Fuzzy vault with iris:

In 2007, Youn Joo Lee [5] proposed a new method of applying iris data to the fuzzy vault with two advantages and contributions:

(i)First, a pattern clustering method and local shift-matching method were introduced to solve the intra variation problem of the extracted iris features.

(ii)Second, in order to produce unordered sets for fuzzy vault, multiple iris features were extracted from multiple local iris patches by using the iris feature extraction algorithm based on ICA (Independent Component Analysis).

The results of above method showed that 128-bit cryptographic keys as well as the iris templates were secure with the fuzzy vault scheme without requiring pre-alignment. In 2008, Srinivasa Reddy [6], proposed a scheme for hardening of both fuzzy vault and secret key by using password which provides an additional layer of security. The work was done in three stages:

(i) First, the biometric template is transformed randomly using the password. This transformation enhances the privacy by enabling the creation of revocable templates and preventing cross matching of templates across different applications.

(ii) Second, fuzzy vault was used to protect the transformed template. The key used for the fuzzy vault construction that secures the transformed template is derived from the iris textures and transformed by using same password.

(iii) Finally, the vault is encrypted using the key that was derived from the password.

The above method results in False Rejection Rate (FRR) of 0.08 i.e. genuine acceptance ratio of 92%which is higher as compared to other biometric templates such as fingerprints. Mrunal Fatangare and K.N.Honwadkar [7] blend cryptography and biometric as a security tool. Using unique biometric identity of a person the keys for cryptosystem can be made secure. This paper presents a biometric solution to cryptographic key management problem using iris based fuzzy vault by elaborating it on the basis of statistical analysis of colour iris. With this it becomes easy to capture locking and unlocking elements and also improves the FAR of system. In 2010, V. S. Meenakshi [8], proposed a method for generating Revocable Iris templates. This paper constitutes three steps which are as follows:

(i) Initially, the iris texture with highlighted minutiae feature points are subjected to permutation and translation. This results in the transformation of original minutiae points into new points.

(ii)Then, a new password of 64 bit is obtained by combining the soft biometric password with the user password.

(iii) Finally, by using password the iris templates are randomly transformed. This results in enhancing the user privacy and facilitating the generation of revocable templates. It also resists cross matching. With this, the similarity between the original and transformed template is reduced. Fuzzy vault construct was then used for securing the transformed templates. The proposed method solves the non revocability problem by using cancellable biometrics with password.

The security of these cancellable templates comes to be 18 to 30 bits in strength. Fuzzy vault was further used to secure the revocable biometric template. With this, the security of the iris templates increases to 52 to 64 bits.

B. Fuzzy vault with retina:

In 2009, V.S.Meenakshi and Dr. G. Padmavathi [9] proposed a fuzzy vault framework to secure retinal templates. The proposed unimodal fuzzy vault is constructed with feature points extracted from retina. This work measures the security of the resultant vault by using min-entropy. The idea of fuzzy vault secures the biometric template as well as the secret data at the same time. In the above study single template and query minutiae are used for encoding and decoding. The work also showed that it is computationally hard for an attacker to identify the genuine points.

C. Fuzzy vault with iris and retina:

In 2010, V.S.Meenakshi and Dr. G. Padmavathi [10] proposed a fuzzy vault framework to secure both retina and iris template. The proposed multimodal fuzzy vault is constructed with feature points extracted from retina and iris. This work measures the security of the resultant vault by using min-entropy. The idea of fuzzy vault secures the biometric template as well as the secret data at the same time. In the above study single template and query minutiae are used for encoding and decoding. The work also showed that multi biometric fuzzy vault is more secure as compared to single biometric fuzzy vault as it becomes difficult for an attacker to compromise it.

IV. Discussion And Conclusion

For a secure biometric authentication and cryptographic key protection, Fuzzy vault has been proved to be one of the most comprehensive mechanisms. Its implementation with iris and retina has provided better results in comparison to other biometric traits. Till now, the researchers have worked for enhancing the performance of fuzzy vault with the use of either passwords or cancellable biometrics with password which makes it difficult for the intruder to forge the genuine points.

References

[1] Uludag, U., Pankanti, S., Jain, A.K.: “Fuzzy Vault for Fingerprints”, Proceedings of Audio- and Video-based Biometrics, December 4, 2006 DRAFT 31 Person Authentication, Rye Town, USA, July 2005, pp. 310–319 (2005).

[2] J.Daugman, “Combining Cryptography and Biometrics,” Technical Report No.640, University of Cambridge Computer Laboratory, 2000.

[3] Ari Juels and Madhu Sudan, “A Fuzzy Vault Scheme”, IEEE International Symposium Information Theory, Lausanne, Switzerland, 2002, pp. 408.

[4] Karthik Nandakumar, Abhishek Nagar and Anil K.Jain,“Hardening Fingerprint Fuzzy Vault using Password”, International conference on Biometrics, 2007.

[5] Youn Joo Lee, Kwanghyuk Bae, Sung Joo Lee, Kang Ryoung Park, and Jaihie Kim, “Biometric Key Binding: Fuzzy Vault Based on Iris Images”, S.-W. Lee and S.Z. Li (Eds.): ICB 2007, LNCS 4642, pp. 800–808, 2007.

[6] E. Srinivasa Reddy, I. Ramesh Babu, “Performance of Iris Based Hard Fuzzy Vault”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008.

[7] P.U. Lahane, and Prof. S.R. Ganorkar, “Efficient Iris and Fingerprint Fusion for Person Identification”, International Journal of Computer Applications (0975 – 8887) Volume 50– No.17, July 2012

[8] V.S.Meenakshi, Dr. G. Padmavathi, “ Securing Iris Templates using Combined User and Soft Biometric based Password Hardened Fuzzy Vault”, (*IJCSIS) International Journal of Computer Science and Information Security,* Vol. 7, No. 2, February 2010.

[9] V.S.Meenakshi, Dr. G. Padmavathi, “Security Analysis of Hardened Retina Based Fuzzy Vault”, *International Conference on Advances in Recent Technologies in Communication and Computing*, 2009

[10] V.S.Meenakshi, Dr. G. Padmavathi, “Retina and Iris Based Multimodal Biometric Fuzzy Vault”, *International Journal of Computer Applications (0975 - 8887)* Volume 1 – No. 29, 2010

[11] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, “Biometric Template Security”, *Journal on Advances in Signal Processing, Michigan State University,* 2007, pp. 1-17.

[12] Anil K. Jain, Arun Ross and Patrick Flynn, “Handbook of Biometrics”, 2008, pp. 1-10.

[13] V.S.Meenakshi, Dr. G. Padmavathi, “ Securing Iris Templates using Combined User and Soft Biometric based Password Hardened Fuzzy Vault”, *(IJCSIS) International Journal of Computer Science and Information Security,* Vol. 7, No. 2, February 2010.

[14] Khin Sint Sint Kyaw, “Iris recognition system using statistical features for Biometric identification”, *International conference on electronic computer technology*, pp 554 – 556, 2009.

[15] U.Uludag, S. Pankanti, S.Prabhakar, and A.K.Jain, “Biometric Cryptosystems: issues and challenges”, *Proceedings of the IEEE*, June 2004.

[16] E.Srinivasa Reddy, Ramesh Babu; “Authentication using fuzzy vault based on iris texture” *Second Asia International Conference on Modelling & Simulation* 2008, pp 361-368.