Volume 2, Issue 11, November 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Securing Iris Templates using Double Encryption Method

Sowkarthika.S [1], Radha.N . [2]

[1]M.Phil Research Scholar, PSGR Krishnammal College for Women, Coimbatore-641004.

[2]Assistant Professor, G.R. Govindarajalu School of Applied Computer Technology. Coimbatore.

Abstract: The important aspect of all verification system is authentication and security. This aspect necessitates the development of a method that ensures user security and privacy. The traditional methods such as tokens and passwords provide security to the users. Uncertainly, the attackers can easily compromise these techniques. In recent years, the combination of biometrics and cryptography techniques has been proved as a efficient way to achieve security. The important feature of using biometric template is that it cannot be revoked by an unauthorized user. Most commonly used biometric features are iris, retina, fingerprint, face, palmprint, hand geometry, voice and so on. Fuzzy vault is the framework which comprises the combination of biometrics and cryptographic key generation technique. This fuzzy vault act as a additional layer of security. This paper proposes a biometric verification system investigating the usage of multibiometric features and fuzzy vault scheme.The fuzzy vault is again encoded using DAES algorithm. This concept is referred as double encryption in this paper. This approach uses multiple impressions of iris in order to provide higher accuracy rate. Experiments were conducted to investigate the performance of the proposed system in ensuring the user security and privacy.

Keywords-Authentication, Cryptography, Fuzzy Vault Scheme, Iris Extraction.

1. Introduction

The increasing popularity of biometrics, cryptography and a secret protection is driven by a common demand on information security. Biometric authentication is considered as one of the important secured system but these biometric authentication itself follows some procedural algorithms like feature extraction, matching, classification etc. There is a possibility of intrusion at any step so it requires additional security management. Cryptography is one of the most effective method to enhance the security of the system. The security level is based on the associated secret key. The simple memorized key can be easily intercepted, while the long and complex key requires extra storage management like tokens, smart cards etc. As a solution secure encryption key can be associated with biometrics. The limitations in the password and token based encryption scheme can be reduced by using the biometrics. The biometrics based encryption requires physical presence of person to be authenticated, so it is reliable and efficient.

The encryption keys can be generated using combination of biometric features and cryptology. Fuzzy vault is a system proposed by Juels and Sudan, which is designed to secure biometric features that are represented as an unordered set, Let X denote a biometric template with r elements. The user selects a key K , encodes it in a form of a polynomial P of degree n and evaluates the polynomial P on all the elements in X. This points lying on P are hidden among a large number of chaff points that do not lie on P. The Vault is construted using the Union of genuine and the chaff points. In the absence of user's biometric data it is computationally hard to identify the genuine points in V, and hence the template is secure. The error correction code such as reed and solomn code is used to provide the tolerance in the input biometric templates, while the decryption phase.

Iris is the most unique biometric identifier and also has a high identification security. Biometric methods based on spatial pattern of iris are believed to allow very high accuracy. This paper is intended to provide a review of use of the Iris in the template protection scheme. Iris recognition system follow step wise procedural algorithms like feature extraction, matching, classification and so on for authentication and verification purposes. Fuzzy vault is introduced to secure these templates.

This paper proposes a biometric verification systems, exploring the usage of multibiometric with fuzzy vault scheme and DAES. This proposed system will have enhanced security on comparision with traditional systems. The biometric feature uses in this system is iris, since it has been reported to provide better results. Experiments were conducted to examine the performance of the proposed system in ensuring security and privacy.

The remainder of this paper is organized as follows. Section 2 discusses the related work proposed earlier in literature for biometric authentication system using Iris and Cryptography. Section 3 explains our proposed system for

providing authentication using iris based multibiometric system using fuzzy vault and DAES scheme. Section 4 illustrates the experimental results with nessary explanations and section 5 concludes the paper.

2. Related Work

The most important part of the biometric authentication is secure storage of the biometric templates. Iris recognition plays a major role in the security application. There are numerous work with the combination of Iris biometrics and the cryptography.

Xiangqian Wu et al [1] had developed a Novel Cryptosystem based on Iris Key Generation . This paper proposes a novel biometric cryptosystem based on the most accurate biometric feature iris. In encryption phase, a quantified 256-dimension textural feature vector is firstly extracted from the preprocessed iris image using a set of 2-D Gabor filters. At the same time, an error-correct-code (ECC) is generated using Reed-Solomon algorithm. Then the feature vector is translated to a cipher key using Hash function. Some general encryption algorithms use this cipher key to encrypt the secret information. In decryption phase, a feature vector extracted from the input iris is firstly corrected using the ECC. Then it is translated to the cipher key using the same Hash function. Finally, the corresponding general decryption algorithms use the key to decrypt the information. FAR is 0% and FRR is 5.5%.

Bodo [2] first proposed to use the data derived from the biometrics templates as the cryptographic key directly in his German patent. Juels and Wattenberg proposed a fuzzy commitment scheme to combine CRC of Polynomial and Key. Error correction coding methods are used to tolerate variations of biometrics features. Juels and Sudan introduced the basic fuzzy vault scheme. This scheme is based on the difficulty of polynomial reconstruction problem. During enrollment, a user selects a polynomial and encodes his cryptographic key into the polynomial's coefficients. The encoding of key can be achieved by dividing key into non-overlapping chunks and mapping to the coefficients. This system can compensate for intraclass variations in the biometric data. It is based on fingerprint minutiae extraction.

Hao et al [3] presented a realistic and secure way to incorporate the iris biometric into cryptographic applications. They deliberated on the error patterns within iris codes and developed a two layered error correction codes that merges Hadamard and the Reed solomn codes. The key was produced from the iris image of the subject through the auxiliary error correction data that do not disclose the key and can be saved in a tamper resistant token like smart card. The evaluation of the methodologies was performed with the aid of samples from 70 different eyes, 10 samples being obtained from every eye. It was estsblished that an error free key can be reproduced reliably from genuine iris codes with a success rate of 99.5%. It is possible to produce upto 140 bits of biometric key, more than adequate for 128- bit AES.

Three factor scheme for biometric based cryptography key regeneration using iris was proposed by Sanjay Kanade et al.[4] They used three factor (smart card, iris code and password) scheme for cryptographic key regeneration based on fuzzy sketches idea which handles biometric variability with error correcting codes. Their FAR rate is 0.055% and FRR is 1.04%.

Karthik Nandakumar and Anil Jain introduced multibiometric Template security using fuzzy vault.[5] Multibiometric vault provides better recognition performance and higher security compared to a unibiometric vault. The multibiometric vault based on fingerprint and iris achieves 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%.

Iris based hard fuzzy vault proposed by Srinivasa Reddy[6] applies a sequence of morphological operations to extract minutiae points from the iris texture. This idea is utilized for extracting the locking/unlocking unit from the retina. To identify the bifurcation feature point on the retinal texture the method proposed by Li Chen is utilized.

Biometric fuzzy extractors scheme for iris templates was proposed by F. Hernandez Alvarez et al.[7] Their aim is to measure how it deals with the intra user and inter user variability. For Intra user GAR is 88.9% and FRR is 11% and for inter user FAR is 1.35%.

3. Proposed Work

The proposed work constructs the Iris template protection using double encryption method. The first encryption is done in the fuzzy vault and the second level of encryption is done using the double AES algorithm. Here in this system we use multiple impressions of the same iris to reduce the FAR rate. Fig shows the basic frame work for the iris template protection using double encryption.

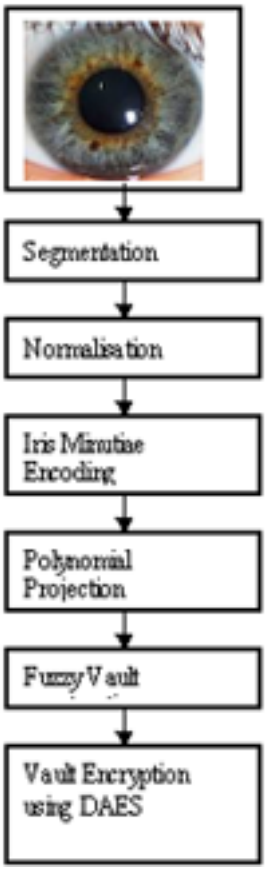

fig 1. Iris Double Encryption Scheme

3.1 Feature point Extraction of Minutiae from Iris

The idea proposed by Srinivasa Reddy [6] is utilized to extract the minutiae feature point from the iris texture. The following operations are applied to the iris images to extract lock and unlock data. Canny edge detection is applied on the iris images to deduct iris. Hough Transform is applied on iris image. Then thresholding is done to isolate eyelashes. Histogram equalization is performed on iris to enhance the contrast. Finally thinning is done to get structures as a collection of pixels. Now the (x,y) coordinates of the nodes and end points of the iris minutiae is extracted

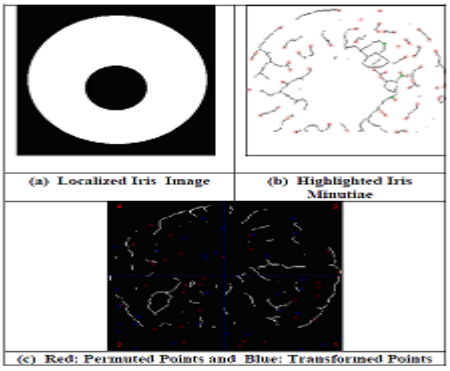

fig 2. Iris Transformation

3.2 Implementation of Multimodal Fuzzy vault.

The proposed method is implemented using Matlab 7.0. The iris samples are taken from CUBS database. This implementation identifies the lock/unlock data by highlighting the iris minutiae structures. The (x,y) attributes of the iris minutiae , where 'x' and 'y' represents the row and column indices of the biometric images are found out. Permutation and transalation is applied to the iris minutiaes. The transformed features are protected in a fuzzy vault. In this implementation 128 bit is generated. The feature point highlighted in fingerprint template and iris template id divided into 4 quadrants. Permutation is applied in such a way that the relative position of a feature point does not change. Fig 3 shows the locking scheme of the fuzzy vault whereas the fig 3.1 shows the unlock scheme of the fuzzy vault.

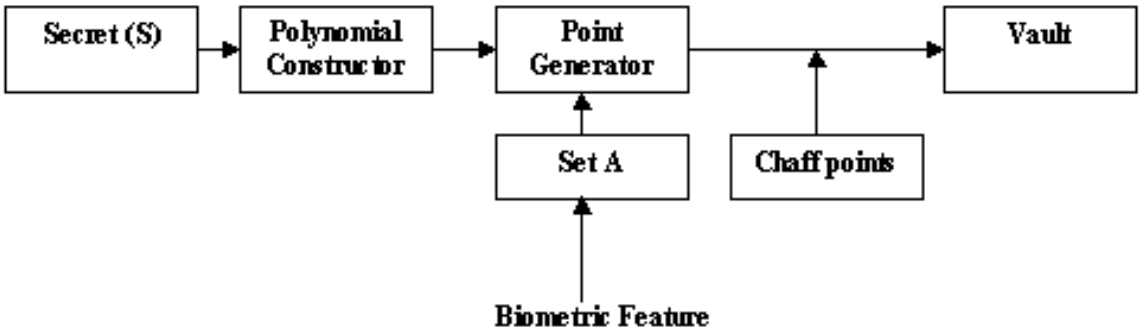

Fig 3. Fuzzy vault scheme to Lock the vault

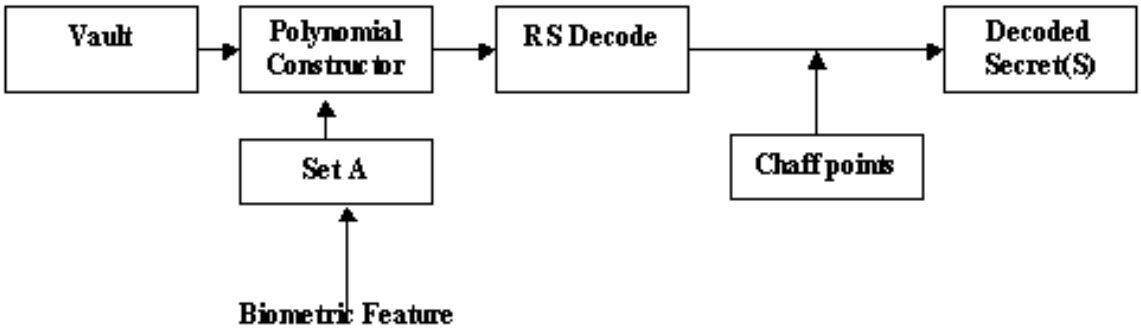

Fig 3. Fuzzy vault scheme to Unlock the vault

3.3 DAES Algorithm

AES gives the implementers a great flexibility. AES uses same key for both encryption and the decryption phase. It is much faster and it is easiest to implement. Given a message block P and the key block K, encryption function E returns an encrypted block C

C=E(p,k)

For Decryption

D(E(p,k),k)=P

C is Encrypted block
E is Encryption Function
P is orginal message
K is cryptographic key
D is Decryption function

Double AES

In Double AES two independent key blocks k1 and k2 are used in succession, first k1 and then k2.

$C=E(E(p,k_1),k_2)$

To enhace the security of the proposed system the key is encrypted twice.

3.4 Double Encryption Encoding Steps

The Double encryption vault encoding scheme has the following steps

Step1: The Reed solomn error correction encoding process is deployed on key to generate $K_{er.}$

Step2: Create a polynomial by segmenting K_{er} as its coefficients with the form of $K_{er=}c_{m-1}| c_{m-2}|\ldots| c_0$, where m is degree of the polynomial.

Step3: Project each real points onto the polynomial to generate real points set G, so that K_{er} is bound with real point set T through the polynomial.

Step 4: Randomly generate chaff points set C, it must be 10times greater than the real points.

Step5: The final vault V is constructed by taking union of two sets, i.e. GUC, and pass through the scrambler so that it is difficult to distinguish real points from chaff points.

Step6: The constructed fuzzy vault is again encoded with the AES to enhance security of the templates

3.5 Double Encryption Decoding Steps

In the decoding phase, the encrypted vault and burification feature point are decrypted using AES. This module has the following steps.

Step1: Project its own real points set to the vault and search for matchings. The candidate point set is then collected.

Step2: The polynomial is reconstructed based on the candidate set using Lagrange theorem.

Step3: An error-correction decoding process is deployed on K_{er} to derive key.

4. Experimental Results and Security Analysis

The implementation of the system consists of generation of double encryption. The biometric template is double encrypted using fuzzy vault and symmetric key. The Reed Solomn code is used to provide error tolerance. The evaluation is based on varying tolerance value over the range, and corresponding false acceptance rate (FAR) and false rejection rate (FRR) are then computed. Our experimental results illustrated the FRR of 0% at FAR of 0.35%. Our system is considered as more reliable and robust as far as attacks on secret key is concerned. Finally, a multibiometric based double encryption scheme is created to secure the iris templates.

5. Conclusion

Biometrics, cryptography and the fuzzy vault provide effective solution to information security from different perspectives.This paper has investigated a new approach to construct the cryptographic vault using iris features. In order to combine cryptography with multibiometric features we also incorporated the implementation of double encryption. The templates is first encoded using the fuzzy vault concept. In order to enhance the security of the proposed system we have used the symmetric key to encode the vault. This concept is referred as a double encryption in this work. The multiple feature representation offers more reliable characterization of features.

References

[1] Xiangqian Wu, Ning Qi, Kuanquan Wang, David Zhang, A Novel Cryptosystem based on Iris key Generation. 2008 IEEE Computer Society. Fourth international conference on natural computation. Oct 18
[2]. A. Bodo, Method for producing a digital signature with aid
of biometric feature, German Patent DE 42 43 908 Al, 1994
[3]F. Hao, R. Anderson and J. Daughman"Combining crypto biometrics effectively" IEEE Transaction on computers, vol. 5, pp.1081-1088,2006
[4] 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

5] Karthik Nandakumar and Anil K. Jain "Multibiometric template security using fuzzy vault" BTAS 2008

[6] E. Srinivasa Reddy, I. Ramesh Babu. "Performance of Iris based hard fuzzy vault", Proceedings of IEEE 8th International conference on computers and information technology workshops, 2008.

[7] F. Hernandez Alvarez, L. Hernandez Encinas, and C. Sanchez Avila " Biometric Fuzzy extractor scheme for iris templates" Spain.

[8]. N. K. Ratha, J. H. Connell, and R. M. Bolle, "An Analysis of Minutiae Matching Strength," in Proceedings of Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), Halmstad, Sweden, June 2001,pp. 223–228.
[9]. Jules and M. Sudan, "A fuzzy vault scheme", in Proc. IEEE Int. Symp. Inform. Theory, Lausanne, Switzerland, 2002, p. 408.
[10]. U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," Proc. IEEE (Special Issue Multimedia Security for Digital Rights Management), vol. 92, no. 6, pp. 948–960, Jun. 2004
[11]. Y J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation", Proc. of IEEE Int. conf. On Multi-media and Expo, pp. 2203-2206, 2004
[12]. Anil K.Jain, Sharath Pankanti,Umut Uludag Department of Computer Science and Engineering, "Fuzzy vault for fingerprint", Michigan State University, East Lansing, MI, 48824 2.Exploratory Computer Vision Group, IBM T.J. Watson Research Center, Yorktown Heights, NY, 10598
[13]. Ari Juels RSA laboratories, 174 middlesex turnpike, bedford, ma 01730, USA ,Madhu Sudan Massachusetts Institute of Technology, 32 Vassar street, Cambridge, MA 02139, USA, "A Fuzzy Vault Scheme" , RSA Lab, *International Journal of Computer Applications (0975 – 8887) Volume 15– No.5, February 2011*
[14] Y.H. Doh, J.S. Yoon, K.H. Choi, and M.S. Alam, " Optical security system for the protection of personel identification information", Applied optics .2005.
[15] P. W. Dent, "Cryptographic method and system for double encryption of messages", US Patent No. 6904150, Jun. 2005 Optics Communications, vol. 275, pp. 324–329, Jul. 2007.

