Authentication : A Survey on Biometric Approaches

Ms. V Gourisree
M.Tech Scholar
Computer Networks and Security
Government Engineering College Wayanad
Kerala, India-670 644
Email: vgourisree@gmail.com

Mr. K P Shabeer
Assistant Professor
Computer Science Engineering
Government Engineering College Wayanad
Kerala, India-670 644
Email: shabeerkp@gecwyd.ac.in

***Abstract*—Authentication is a technique adopted to limit the data access from intruders and attackers. There are many traditional approaches for authenticating a user/ system/ entity. Traditional authentication was based on password/tokens. These approaches have their own merits and demerits. The survey focus on different biometric approaches to authenticate a user/ system. The methods considered here are Biometric authentication using Elliptic Curve Cryptography(ECC), authentication using multiple biometric modalities, authentication using fused biometric traits where fusion is performed at cryptographic level. The fourth method is a type of cryptographic level fusion, which considers homogeneous biometric traits for fusion and cryptographic keys are generated from these biometric templates. Any biometric system which is used for authentication purpose need to meet the general standards which are low False Acceptance Ratio(FAR), low False Rejection Ratio(FRR), low cost and high security. All the mentioned methods are analyzed in terms of security, cost and accuracy. In biometric authentication using Elliptic Curve Cryptography(ECC) and authentication using multiple biometric modalities, we require multiple acquisition devices to obtain the corresponding biometric templates. While considering cryptographic level fusion and decision level fusion, both the methods have higher advantages compared to other 2 models. In MBCD, we consider homogeneous traits from which the key is generated. Both FAR and FRR are very low and therefore its security is high.**

Index terms : Authentication, Biometric cryptosystem, Multibiometric cryptosystem, MBCD.

I. Introduction

In basic cryptosystems used till date, authentication of the user is based on secret keys. These keys can be lost, forgotten or stolen. In this work, authentication is based on unique characteristics of a person, known as biometrics. These features can be finger- print, iris, palmvein etc. These traits provide a novel solution for key generation, en- cryption and decryption. It imparts high authentication accuracy. Biometric cryptosys- tems can be broadly classified into 2 categories: Single biometric Cryptosystem(SBC) and Multi biometric Cryptosystem (MBC). The work propose a noval architecture of multibiometric cryptosystem using decision level fusion. In order to protect each single biometric trait, we employ a hash function. Compared to single biometric cryptosystems, multibiometric cryptosystems can provide more accuracy and security.

The next few sections of the paper is organized as follows. Section II gives an introduction to biometric cryptosystems, which familiarizes 3 biometric models namely multimodal cryptosystems, multibiometric cryptosystem based on feature level fusion and multibiometric cryptosystem based on decision level fusion.

II. Biometric Cryptosystems

Biometrics can be classifed into 2 categories: Physical biometrics and behavioral biometrics. Physical biometrics make use of features such as fingerprint, palmvein etc., whereas behavioural biometrics make use of features like voice, signature etc,. The paper analyses different biometric cryptosystems mainly, single biometric cryptosystem, multimodal cryptosystems and multibiometric cryptosystem.

A. Biometric authentication using ECC[7]

- From the biometric template, generate the encryption and decryption keys.
- Cryptographic keys are obtained from the biometric images.
- ECC is used along with the biometric template to provide authentication securely.
- Steps
  - Fusion of multi-biometric template
  - Generation of ECC parameters from the biometric template
  - Generation of EC from the obtained parameters.

Generation of Elliptic curve cryptographic parameters:

1) Prime P
   - From the fused biometric template, obtain 10 values and store it in a variable f_p.
   - Calculate the sum of these obtained values and store the sum in a variable s = sum(f_p).
   - Identify the prime numbers associated with the obtained s, and store the primes in a variable PS = primes(s)
   - Find maximum of the prime numbers: P = max(PS).
2) ECC Parameter a and b
   - Find the difference between sum of 10 values and Prime number PS
     a = s - PS

- Find 1(rand (1)).
- Multiply two above calculated numbers to obtain b.

Encryption Procedure :

1) Let the message m be encoded as P_m = (x,y). This is done by user A.
2) Let the private key of user A be K_a.
3) K_a*G is computed by user A.
4) User A compute the P_m+K_a*$P_u b$.
5) User A take the C_m=(K_a*G, P_m+K_a*$P_u b$)as a cipher text.
6) User A can send this cipher text to User B.

Decryption Procedure :

1) Compute d B *K a *G.
2) Perform subtraction operations on the obtained values.
3) Thus user B compute P m := m+K a*P u b-d B *K a *G =P m -K A (P r b *G)+K P ub = P m -K P ub+K P ub =Pm.

B. Multimodal biometric system[2]

Multimodl biometrics offer better accuracy and security compared to that of single biometrics. Multimodal biometrics posseses more than one trait in the system. After analysis, it is concluded that the multimodal biometrics offer low False Acceptance Ratio(FAR). The reason why it offers less FAR is that, it is difficult for an attacker to extract multiple biometric features of a user.Example of the biometric modalities used can be face, fingerprint and palm vein. After the image of the modalities is obtained,image pre-processing is done and extraction of features are performed and fusion is performed at feature level.

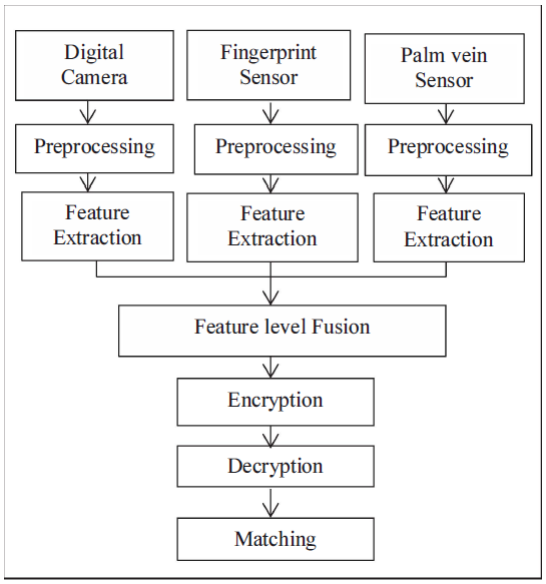

Fig. 1. Multimodal fusion

Inorder to perform encryption and decryption, we make use of RSA algorithm, which is a public key cryptosystem.

The steps are:

Key Generation:

1. Choose two integers p and q which are prime numbers.
2. Compute a variable n which is a obtained by performing multiplication operation on p and q.
3. Compute another variable m, by performing multiplication operation on p-1 and q-l.
4. Choose an integer e less than m, such that m and e are coprimes.
5. Calculate d using the equation d = e-1 mod m.
6. Public Key is (e,n) and Private key is (d,n).

C = pemod n.

P = Cdmod n.

C. Multibiometric cryptosystem based on decision level fusion[3]

In multibiometric cryptosystem based on decision level fusion,we consider homogeneous biometric features. Homogeneous biometric features are those features having the same characteristics. These can include multiple fingerprint images or multiple iris images and so on. Here we perform basic encryption operations on eachof the biometric template and then encryption operation is performed. The methodology can be described as follows.

1) Minutiae extraction:

- In biometrics and forensic science, minutiae are major features of a fingerprint, using which comparisons of one print with another can be made.
- Minutiae include:
  - Ridge ending : the ending of a ridge
  - Ridge bifurcation : Bifurcation is formed when a ridge is again divided into 2 ridges.
  - Short ridge : It is a ridge which spans only for a short distance and then ends.

Fig. 2. Minutiae points in a fingerprint

2) Delaunay triangulation: The process of dividing a portion of area into multiple triangles is called triangulation. Let the fingerprint image consists of n minutiae,denoted by M =m_i ni=1 . The next step is to perform the process ofDelaunay triangulation of M. This step is composed of two steps.

First,for the minutiae set M, a Voronoi diagram is constructed, which partitions the whole image into n regions such that all the points in the ith region are closer to m_i than to any other minutiae.
Second, the delaunay triangulation net is obtained from the minutiae after connecting the points.

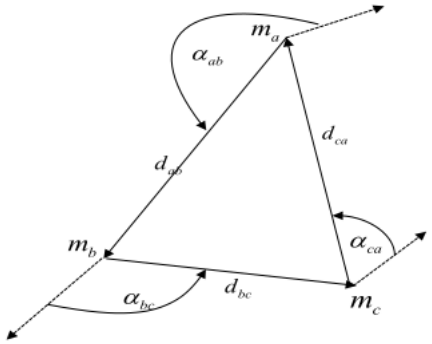

Fig. 3. Triangle and local features

3) Feature extraction: The features are extracted from the delaunay triangulation net using the following equations.

- $FV_i = (d_{ab}, d_{bc}, d_{ca}, \alpha_{ab}, \alpha_{bc}, \alpha_{ca})$
- $d_{ab} = \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2)}$
- $d_{bc} = \sqrt{(x_b - x_c)^2 + (y_b - y_c)^2)}$
- $d_{ca} = \sqrt{(x_c - x_a)^2 + (y_c - y_a)^2)}$
- $\alpha_{ab} = \tan^{-1}(\frac{y_a - y_b}{x_a - x_b}) - \theta_a$
- $\alpha_{bc} = \tan^{-1}(\frac{y_b - y_c}{x_b - x_c}) - \theta_b$
- $\alpha_{ca} = \tan^{-1}(\frac{y_c - y_a}{x_c - x_a}) - \theta_c$

4) Encryption: There are 2 levels of encryption. The first level of encryption uses a hash function to each feature vector and form a transformed template. We then use the fuzzy vault to bind the transformed template. The second level of encryption is the Shamir's secret sharing scheme. Here the secret is divided into parts, ie, the key is divided into n segments and each of these segments are used to perform encryption on each of the biometric templates separately. Let the parts be k_0 , k_1 , . . . k_n1 and then we encode them into a polynomial p, i.e. p(x)

5) Decryption: To perform decryption, the same methodology is adopted as that of encryption. The fingerprint images are obtained and we perform delaunay triangulation and features are extracted. Once the features are extracted we transform this into a transformed vector using MD5 algorithm. While performing encryption, in the second phase shamir's secret

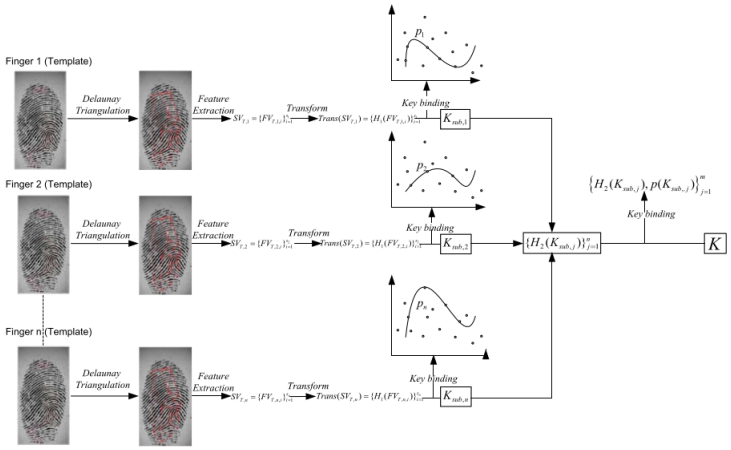

Fig. 4. Encryption procedure

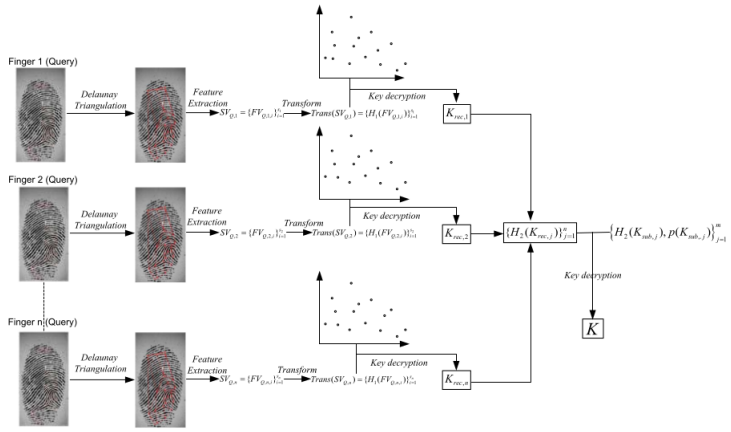

Fig. 5. Decryption procedure

sharing is done and we obtain a polynomial. In the decryption phase, we choose one point from this set and after key decryption, the same key is decrypted.

III. Conclusion

The work mainly focus on improving the security and accuracy of authentication and verfication procedures. Biometric cryptosystems overcome the disadvantages of traditional authentication systems, which make use of passwords or tokens for authentication. The method implemented also overcomes the limitations of single biometric cryptosystems, by fusing templates at the decision level. The method uses multiple fingerprints of the same user to encrypt the cryptographic key. The performance of the system is analyzed in terms of False Acceptance Ratio(FAR) and False Rejection Ratio(FRR).

IV. Acknowledgements

It is with great enthusiasm and the learning spirit that I bring out this paper. I also feel that it is the right opportunity to acknowledge the support and guidance that came in from various quarters.I am extremely grateful to the Principal Dr. K M

Abdul Hameed ,Government Engineering College Wayanad, for providing the necessary facilities. I take this opportunity to express my sincere thanks to Dr. V S Anitha ,Associate Professor and Head of the Computer Science and Engineering Department, for her valuable suggestions and guidance. I am extremely thankful to my guide Mr. K P Shabeer, Assistant Professor in Computer Science and Engineering Department for the inevitable guidance which lead me to the fulfilment of the work. My acknowledgement would not be complete without acknowledging my gratitude to my beloved parents who have been the pillars of support and constant encouragement through out the course of this work.

REFERENCES

[1] IEEE transactions on information forensics and security, volume 10, no. 6, June 2015,*A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion* Cai Li, Student Member, IEEE, Jiankun Hu, Josef Pieprzyk, and Willy Susilo, Senior Member, IEEE.

[2] International Conference on Industrial Instrumentation and Control (ICIC),2015 *Fusion Based Multimodal Biometric Cryptosystem* Saj eeda.R.Inamdar Post Graduate Student, Yogesh.H.Dandawate Professor,Vishwakarma Institute of Information Technology, Pune.

[3] IEEE transactions on information forensics and security, volume 4, no. 4, December 2009,*Multibiometric Cryptosystem: Model Structure and Performance Analysis* Bo Fu, Simon X. Yang, Senior Member, IEEE, Jianping Li, and Dekun Hu.

[4] IEEE transactions on information forensics and security, volume 7, no. 1, February 2012 *Multibiometric Cryptosystems Based on Feature-Level Fusion* ,Abhishek Nagar, Student Member, IEEE, Karthik Nandakumar, Member, IEEE, and AnilK. Jain, Fellow, IEEE.

[5] Proc. IEEE, vol. 92, no. 6,pp. 948960, Jun. 2004, *"Biometric cryptosystems: Issues and challenges"*, U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain.

[6] A. Juels and M. Wattenberg, A fuzzy commitment scheme, in Proc. 6th ACM Conf. Comput. Commun. Secur., Singapore, 1999, pp. 2836.

[7] Bharti Kashyap, K. J. Satao, Computer Science and Engg, Rungta College of Engineering and Technology,Bhilai, Chhattisgarh,India *Implementation of Multi-Biometric Cryptosystem for Information Security using Elliptic Curve Cryptography* , International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015.