FEATURE LEVEL FUSION BASED MULTI-BIOMETRIC CRYPTOSYSTEM USING FUZZY VAULT FOR WIRED NETWORK

Ms. Ketaki N. Bhoyar[1], Mrs. Manasi K. Kulkarni[2]

[1]Department of Computer Engineering, Progressive Education Society's Modern College of Engg., Shivajinagar, Pune,(India)

[2]Asst. Prof., Department of Computer Engineering, Progressive Education Society's Modern College of Engg., Shivajinagar, Pune, (India.)

ABSTRACT

User authentication is necessary these days to prevent the unauthorized access by the malicious users. Multi-biometric systems accumulate evidence from more than one biometric trait (e.g., face, fingerprint and iris) in order to recognize a person. They provide higher recognition accuracy and larger population coverage. Multi-biometric systems require storage of multiple biometric templates for each user, which results in increased risk to user privacy and system security. The method to secure the individual biometric template by using the fusion method to store the data in the fuzzy vault is proposed. Now the same multi-biometric cryptosystem should be reliably used over the internet and other networks. This paper proposes a multi-biometric cryptosystem over wired network to support various applications where user authentication is necessary. The Server side encoding and client side decoding with more complex fusion module is also proposed in this paper.

Keywords: Feature Level Fusion, Fuzzy Vault, Multi-biometric Cryptosystem, Template Security, Wired Network.

I. INTRODUCTION

In today's modern society, all types of public and private services are dependent on computer networks supporting them. The two best examples are electronic voting and electronic commerce. The role of authentication techniques to prevent unauthorized access by malicious users becomes more significant, because crimes and incidents over networks are increasing rapidly [1].

Biometrics authentication depends on biological individuality of human characteristics such as fingerprint, iris, retina, face, and voice. A biometrics authentication technology is to extract the identification data from human characteristics automatically and to compare it with already registered and stored data to authenticate a person, but the method to implement is different according to the characteristics it focuses. Due to the disadvantages of single biometrics authentication technology, it cannot satisfy a required reliability level. Thus multi-biometrics is useful to improve reliability of biometrics authentication. For example, fingerprint authentication at the entrance of a building may be combined with iris authentication at the entrance of a secured room in that building. [1]

Multi-biometrics authentication will be more popular over networks in the future especially for wired networks. It is useful to build a network based multi-biometric cryptosystem which can be used by many applications and commonly applicable to different types of biometrics authentication technologies. This paper proposes a multi-biometric cryptosystem using network authentication to support various applications where user authentication is necessary. In particular, it provides secured services to individual biometric data and to the data to be secured.

II. RELATED WORK

Abhishek Nagar, Karthik Nandakumar and Anil K. Jain in their paper Multibiometric Cryptosystem based on feature level fusion, explained the multi-biometric cryptosystem using both fuzzy vault and fuzzy Commitment. Also they proposed different embedding algorithms for transforming biometric representations. [2]

Umut Uludag, Sharath Pankanti, Anil K. Jain in their paper Fuzzy Vault for Fingerprints, explained the unibiometric authentication system using fingerprint minutiae as the single biometric trait. For the encoding and decoding to work they used the new cryptographic construct called Fuzzy Vault [7].

Haiping Lu, Karl Martin, Francis Bui, K. N. Plataniotis, Dimitris Hatzinakos in their paper Face Recognition with biometric encryption for privacy enhancing, explained a combination of face recognition and simple biometric encryption using helper data system. Their main objective was to address the privacy concern in a self exclusion scenario of face recognition [12].

Ae-Young Kim, Sang-Ho Lee in their paper Authentication Protocol using Fuzzy Eigenface Vault based on MOC, proposed a fuzzy vault based on the eigenfaces. For this scheme, they use a feature vector, which is called an eigenface, from a face image. The eigenface is calculated by the principle component analysis method [14].

Jules and Sudan in their paper A fuzzy vault scheme, proposed the concept of fuzzy vault. It is a logical constraint which is used to store the transformed data. It acts as the locking agent viz. whenever the fuzzy vault is created the data is considered to be locked [9].

III. THE PROPOSED FRAMEWORK

In this section the implementation for multi-biometric cryptosystem based on feature level fusion using fuzzy vault is explained. It works in three stages. At the registration stage all the biometric templates are accepted as input. For which the real time video of user's face is captured. Then the thumb print and the iris are captured further. Edge segmentation for the face is done using Canny Edge Detection Algorithm (CED). Feature Extraction for iris is done using Independent Component Analysis (ICA) [6] and that for thumb print is done by finding the coordinates of the minutiae points. The extracted features are then quantized and mapped to binary representation for feature points matching. The produced binary features and the key entered by the user are bound using the fuzzy vault. The key will be correctly retrieved if the presented face features have substantial overlap with the enrolled ones along with matching of iris and thumb print. The details of the proposed methods are presented in this section.

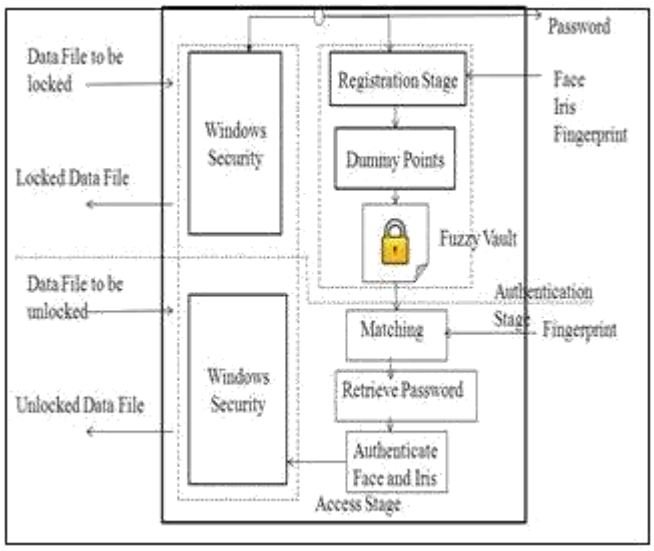

Figure 1. System Overview of Feature Level based Multibiometric Cryptosystem

Overview of the system as shown in figure 1 consists of three stages. The first stage is the registration stage. This stage will take place at the server side of the wired network. The registration stage will accept all three biometric templates viz. iris, face and thumb print and a textual password. Then the facial features are extracted using the Canny Edge Detection Algorithm in which edge segmentation is performed. Then features from iris are extracted using ICA also the thumb print features are extracted using the angle method in which angle Θ is found. After this step binary mapping is performed and all the data including the textual string will be converted into binary format. Using the binary format the biometric templates are fused with the entered textual string and they are stored in the Fuzzy Vault. Once the fuzzy vault is created at the server side the data is locked.

Now at the client side while accessing the same locked data authentication stage is performed. In this stage user trying to access the data is authenticated. At this stage he needs to enter only thumb print. From which the features are extracted and the password is retrieved. Using the password the other biometric templates are also retrieved and thus if they all are matched then the user is authenticated. Then the system enters the access stage. At this stage using the retrieved password and the features of the biometric templates data is accessed at the client side. For this system to work two things should be ready viz. Client Server Configuration and the Network Protocols.

3.1 Encoding at Server Side

On the server side, initially the user should register. For the registration purpose the user will provide his face, iris and the fingerprints. Then for each of the biometric feature the feature extraction will take place. While doing feature extraction the Canny Edge Detection algorithm will be used, the result of which is the edged map of the respected biometric feature. The same edged map is divided into subparts to go in detail with the image. Then according to the presence of the edge in the subpart, the binary value is extracted. If edge is present then 1 otherwise 0. The output is the binary valued string. The binary valued string is known as the feature vector for each biometric template. Now the feature vector for face and the feature vector for iris are concatenated. The

formed biometric string is reversed and it is converted into decimal number. The value we will get will be the coefficient of the polynomial being formed i.e. $P(u) = C_8u^8 + C_7u^7 + C_6u^6 + ... + Cu + C_0$ [3][4].

Now the feature vector for the fingerprint is considered. The length of the feature vector is too long to perform the calculation. So the Finite Field Arithmetic Algorithm (FFA) is used. In that algorithm the standard polynomial stated by Galois is considered. The polynomial is $C_{16}u^{16} + C_5u^5 + C_2u^2 + 1$. The standard value for the polynomial is 40961. Applying the FFA algorithm will reduce the normal value and make the calculations easier. This will give the variable of the polynomial. The constant of the polynomial is calculated by calculating the Cyclic Redundancy Check (CRC) of the feature vector of the fingerprint. Thus the complete value of the polynomial for one feature is obtained. In order to store all the values of the polynomials in the vault which is stored at the server side, some security measures are necessary. So we are including the chaff points here in order to confuse the hackers. The chaff will be scrambled with the original genuine points viz. is the combination of the value of the polynomial and the variable of the polynomial and hence the value will be stored on the server. The vault will be created and the user's registration is now complete. The complete process is illustrated in the following figure 2.

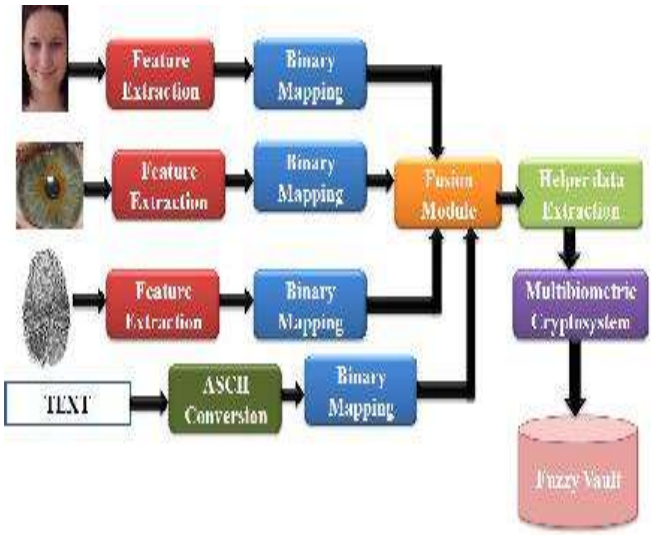

Figure 2. Encoding at Server Side

3.2 Decoding at client side

On the client side, the client will try to access the data so it will request the server to give him the access. For the decoding purpose, user needs to provide only fingerprint. No need to provide the face and the iris. The same procedure will be implemented. Features will be extracted. The binary mapping will be carried out. Thus the feature vector will be formed. Now from this feature vector the CRC is calculated. The calculated CRC is encrypted by the symmetric key algorithm to send over the network. Then at the server side, the vault is accessed. The data read from the vault will be the combination of the chaff points and the genuine points. Genuine points are extracted. Using them the Polynomial is reconstructed. Polynomial Interpolation is performed to find out all the coefficients of the Polynomial. The polynomial interpolation is done using the LaGrange's Interpolation formula as followed [3].

$$P^*(u) = \frac{(u-v_2)(u-v_3)...(u-v_{D+1})}{(v_1-v_2)(v_1-v_3)...(v_1-v_{D+1})} w_1 + \frac{(u-v_1)(u-v_3)...(u-v_{D+1})}{(v_2-v_1)(v_2-v_3)...(v_2-v_{D+1})} w_2 + ... + \frac{(u-v_1)(u-v_2)...(u-v_D)}{(v_{D+1}-v_2)(v_{D+1}-v_3)...(v_{D+1}-v_D)} w_{D+1}$$

One last coefficient among the polynomial is the constant which is the CRC. Thus the decrypted CRC and this CRC are matched. If they are matched then the access is given to the client otherwise user is stated to be invalid. The process is explained in the following figure 3.

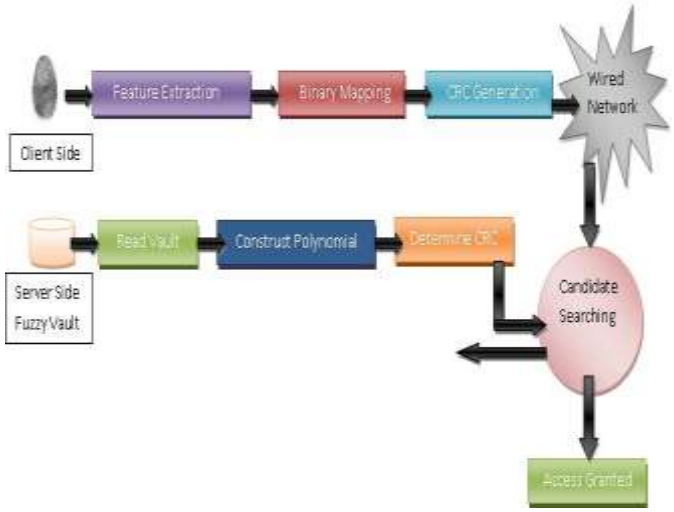

Figure 3. Decoding at client side

3.3 Algorithmic Approach

1. **Encoding Algorithm**
2. Step 1: Extract facial features (A)
3. Step 2: Extract iris features (B)
4. Step 3: S = Secret key (Textual String)
5. Step 4: Extract fingerprint features (C)
6. Step 5: A|B = Coefficient of P(u)
7. Step 6: S|C = Variable of P(u)
8. Step 7: Generate 16-bit CRC
9. Step 8: P(u) = Polynomial Constructed
10. Step 9: Generate Genuine Set $G = \{(u_1, P(u_1)), (u_2, P(u_2)),..., (u_n, P(u_n))\}$
11. Step 10: Generate Chaff points $C = \{c_1, c_2, ..., c_m\}$
12. Step 11: Generate Random points $D = \{d_1, d_2, ..., d_m\}$
13. Step 12: Generate constant pairs (c_j, d_j) where j=1,2,…,2m and its should be distinct from P(u)

14. Step 13: Generate the chaff set $C = \{(c_1, d_1), (c_2, d_2), ..., (c_m, d_m)\}$
15. Step 14: $G \cup C$
16. Step 15: Scramble the list generated
17. Step 16: The final vault set generated is $VS = \{(v_1, w_1), (v_2, w_2), ..., (v_{n+m}, w_{n+m})\}$
18. Step 17: Save vault [4].

2. Decoding Algorithm

Step 1: Extract fingerprint $(GS^{'})$ features

Step 2: Form Genuine Set

Step 3: Let V_l be the Vault points where $l = 1,2,3,..., m+n$

Step 4: Genuine Set from encoding is $GS = \{u_1, u_2, ..., u_n\}$

Step 5: Genuine Set from decoding is $GS^{*} = \{u_1^{*}, u_2^{*}, ..., u_n^{*}\}$

u_1^{*} and V_l

Step 6: Match $K <= n$

Step 7: Form K such that

Step 8: Matched points (v_l, w_l) are added to the list of K

Step 9: $D =$ Degree of Polynomial and unique projections are $D+1$

Step 10: Form set $C = \{K, D+1\}$

Step 11: Apply LaGrange's Interpolation polynomial for each combination

$L = \{(v_1, w_1), (v_2, w_2), ..., (v_{D+1}, w_{D+!})\}$

Step 12: Calculate CRC for $L_1, L_2, ..., L_D$

Step 13: Compare with CRC from encoding and if matched, key will be retrieved

3.4 Implementation Results

Data transfer over the client server configuration takes place securely maintaining data integrity, confidentiality and authenticity. This system secures individual biometric template data along with the data stored at specific location. It decodes with less response time.

Figure 4.1. Locking at server side

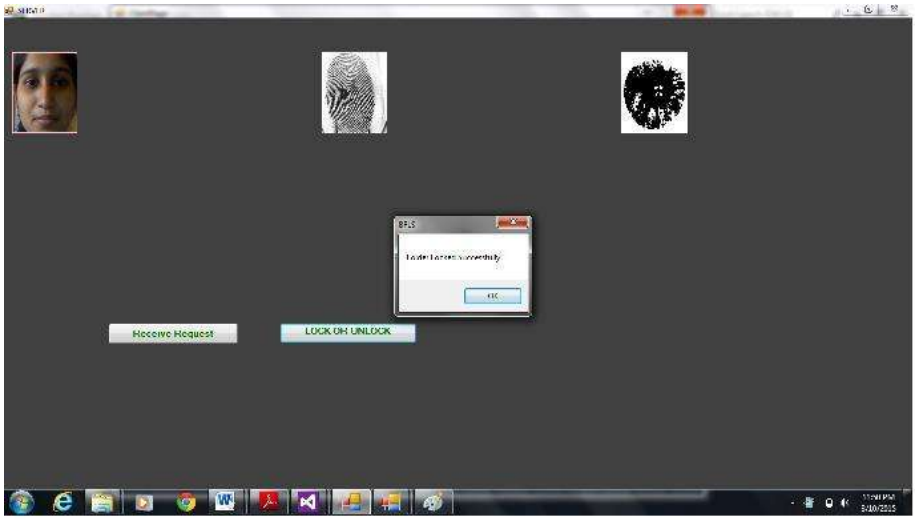

Figure 4.2. Locking at server side

3.5 Future Work

In future the same security system can be designed which will work for mobiles and secure mobile data on wireless mode.

IV. CONCLUSION

Thus a feature-level fusion framework for the design of Multi-biometric cryptosystems that simultaneously protects the multiple templates of a user using a single secure sketch is proposed. The Multi-biometric cryptosystem and the feature level fusion model on wired network based on Client Server Configuration are also proposed.

V. ACKNOWLEDGEMENT

A large measure of any credit for the "Feature Level Fusion based Multi-biometric Cryptosystem using Fuzzy Vault for Wired Network" must go to our guide Mrs. Manasi Kulkarni, Asst. Prof., and our ME coordinator Ms. Deipali Gore who with the author has assisted in the preparation of this paper. We admire their infinite patience and understanding that they guided us in field we had no previous experience. We are grateful to them for having faith in us.

REFERENCES

[1] Shoichiro Seno, Tetsuo Sadakane, Yoshimasa Baba, Toshihiro Shikama, "A Network Authentication System with Multi-Biometrics", 2003, vol no.03.

[2] Abhishek Nagar, Karthik Nandakumar, Anil K. Jain, "Multibiometric Cyptosystems based on Feature Level Fusion", IEEE, Feb 2012.

[3] Ketaki N. Bhoyar, "Biometric Folder Locking System using Fuzzy Vault for Face ",IJCA, Vol No. 57, Nov 2012.

[4] Lifang Wua,b, Songlong Yuana, "A face based fuzzy vault scheme for online authentication", Second International Symposium on data, privacy and e-commerce, 2010.

[5] Bo Fu, Simon X. Yang, Senior Member, IEEE, Jianping Li, and Dekun Hu, "Multi-biometric Cryptosystem: Model structure and Performance Analysis", IEEE Transactions on Information Forensics and security, Vol. 4, No. 4, Dec 2009.

[6] Youn Joo Lee, Kang Ryoung Park, Kwanghyuk Bae and Jaihi Kim, "A New Method for Generating Invariant Iris Private Key based on Fuzzy Vault System", IEEE Transactions on System, MAN and Cybernetics art B: Cybernetics, Vol. 58, no. 5, Oct. 2008.

[7] Umut Uludag, Sharath Pankanti, Anil K. Jain, "Fuzzy Vault for Fingerprints", Exploratory Computer Vision Group, IBM T.J. Watson Research Centre, Yorktown Heights, NY, 10598.

[8] A. Ross, K. Nandakumar, and A. K. Jain, "Handbook of Multi-biometrics", Springer, 2006.

[9] A. Juels and M. Sudan, "A Fuzzy Vault Scheme", in Proc. IEEE International symposium on Information Theory, Lausanne, Switzerland, 2002, P. 408.