ISSN:0975-9646

Review for Multibiometric Cryptosystem using Fuzzy Vault for Wired Network

Ms. **Ketaki N. Bhoyar**
Department of Computer Engineering
Progressive Education Society's Modern College of Engg., Shivajinagar,Pune, India

Mrs. **Manasi K. Kulkarni**
Asst. Prof. (Department of Computer Engineering)
Progressive Education Society's Modern College of Engg., Shivajinagar,Pune, India

Abstract— **For creating multi-biometric cryptosystem, multiple theories proposed by different authors in their papers published must be referred. 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 could be implemented using fuzzy vault as well as fuzzy commitment. The feature level fusion could be implemented using different embedding algorithms. The online authentication is implemented using the unibiometric fingerprint authentication system. Iris can also be extracted using the Independent Component Analysis. The fuzzy vault scheme proposed by jules and sudan helps to increase more complexity. Multi-biometric systems can be implemented on the network. This paper propose the survey of different theories that help the final multi-biometric system to be more secure and complex.**

IndexTerms— **Multi-biometric Cryptosystem, Fuzzy Vault, Feature Level Fusion, Independent Component Analysis, 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]

They propose a feature level fusion framework to simultaneously secure multiple templates of user using biometric cryptosystems. They proposed simple algorithms for three tasks:

1) Different biometric representations are converted into a common representation space using different embedding algorithms viz. binary strings to point-sets, point-sets to binary strings and fixed length real valued vectors to binary strings.
2) Different features are fused into a single multi-biometric template that can be secured using an appropriate biometric cryptosystem such as fuzzy vault and fuzzy commitment. They also proposed efficient decoding strategies for these biometric cryptosystems.
3) A minimum matching constraint for each trait is incorporated in order to encounter the possibility of an attacker gaining illegitimate access to the secure system by simply guessing/knowing only a subset of biometric traits.

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].

This paper explains how to extract the fingerprint features. These features are the abrupt changes in the regular ridge structure on the fingertip, characterized by either ending or bifurcation of the ridges. They are typically represented as (x, y, ϴ) triplets, where x, y and ϴ denotes the row indices, column indices and angle of the associated ridge respectively. This paper also represents the working of the unibiometric system using fuzzy vault. This system works in two stages viz. encoding stage and decoding stage. In encoding stage, features of the biometric template are extracted and then they are quantized and mapped into binary form. Then fusion of password and the extracted features takes place and is then stored into the fuzzy vault. When the fuzzy vault is created the data is secured. In the decoding stage another biometric template is accepted as the input. The accepted biometric template and the stored biometric template are matched; if they are matched the user is authenticated otherwise the user is declared as invalid.

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].

Kim and Lee proposed the authentication protocol based fuzzy eigenface vault scheme. For the calculation of fuzzy eigenface vault sets, we need the eigenface E as the feature vector, secret information or a cryptographic key S and a cyclic redundancy check value (CRC) for construction of a polynomial and checking the valid polynomial. The secret value S and the cyclic redundancy check value CRC are formed by 16-bit units which will be coefficients and used to construction of the D-degree polynomial P. In the experiment [10], D is 8. Using the polynomial P and the eigenface components Wpca, we calculate a genuine set, a chaff point set, and a final vault set. The s is locked in the final vault set.

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].

They explained the concept by giving the example of Alice and Bob. Alice may place a secret value k in a fuzzy vault and lock it using a set A of elements from some public universe U. If Bob tries to unlock the vault using the set B of similar length , he obtains k only if B is close to A. i.e. only if A and B overlap substantially.

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.

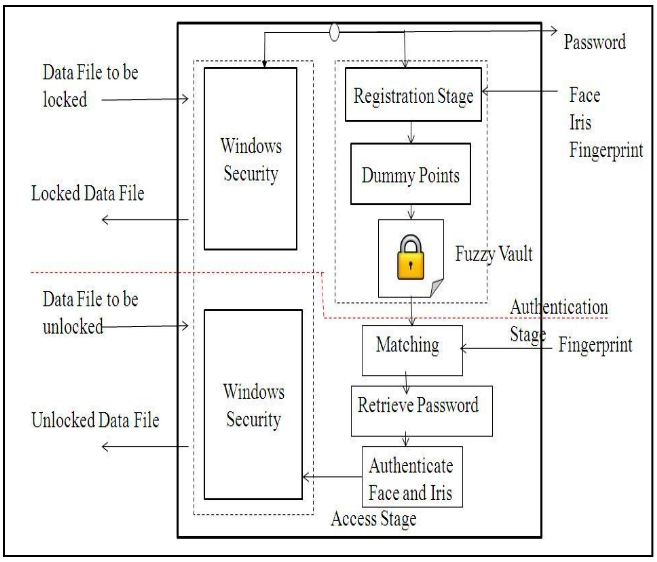

Figure 1. System Overview of Feature Level based Multibiometric Cryptosystem

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.

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 after the analysis of different theories proposed by different authors.

ACKNOWLWDGEMENT

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.

[10] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data”, Cryptology ePrint Archive, Tech. Rep. 235, Feb. 2006, A preliminary version of this work appeared in EUROCRYPT 2004.

[11] Marwa Fouad, Abdulmotaleb El Saddik, Jiying Zhao, Emil Petriu, “A Fuzzy Vault Implementation for Securing Revocable Iris Templates”, IEEE 2011.

[12] Haiping Lu, Karl Martin, Francis Bui, K. N. Plataniotis, Dimitris Hatzinakos, “Face Recognition with biometric encryption for privacy enhancing”, 2008.

[13] DAO Vu Hiep, TRAN Quang Duc, NGUYEN Thi Hoang Lan, “A Multi-biometric Encryption key Algorithm using Fuzzy vault to protect private key in bioPKI based security system”, 2010.

[14] Ae-Young Kim, Sang-Ho Lee, “Authentication Protocol using Fuzzy Eigenface Vault based on MOC”, ICACT 2007, pp 12-14, Feb. 2007.