International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Humming Bird (01st March 2014)

RESEARCH ARTICLE OPEN ACCESS

Multi-Biometric Cryptosystem on Fusion Level Distinctiveness

M.Sindhu
M.E Software Engineering
Rajalakshmi Engineering College
Thandalam, Chennai.
sindhutarani@gmail.com

N.Radhakrishnan
Professor
Dept of Information Technology
Rajalakshmi Engineering College
director.tifac@rajalakshmi.edu.in

Abstract –
Multi-biometric systems are being increasingly deployed in many large biometric applications, because they have several advantages such as lower error rates. Multi-biometric systems require storage of multiple biometric templates (e.g., fingerprint, iris and face) for each user, which results in increased user privacy and system security. The features of fingerprint, iris and face are obtained. The features are compared with database and values are generated. These templates are protected from attackers using two biometric cryptosystems such as fuzzy vault and fuzzy commitment and matching performance is done.
Keywords – Biometric Cryptosystem, Feature level, Fuzzy Vault and Fuzzy Commitment.

1. INTRODUCTION

Multi-Biometric system collects evidence from more than one biometric characteristic, in order to recognize the person. Multi-Biometric system is a combination of more than two biometric cryptosystems. Multi-Biometric Cryptosystem are used to increase the reliability, accuracy, higher recognition and cover large population. The error rates can be reduced. It has received more attention for more security. The biological characteristics are used as password for security. Compared to uni-biometric cryptosystem multi-biometric cryptosystem has many advantages. Multi-biometric system requires storage of multiple biometric templates which result in increased risk. Multi-biometric Cryptosystem includes fingerprint recognition, iris scan, hand geometry, palm print, face recognition, DNA and vascular pattern recognition. Behavioral biometrics also known as dynamic biometrics. While Multi-biometric systems have improved the accuracy and reliability of biometric systems, sufficient attention has not paid to security of templates. In multi-biometric cryptosystem if any one of the biometric templates is wrong the person will be unauthorized, due to this the user privacy is increased and attacks can be reduced.

Biometric Cryptosystem suffer from various attacks such as,

A .dishonestly interchanged data is submitted to the system,

B. the matcher program is replaced by attacks,

C. already stored database in the system is changed or replaced with other data,

D. final output may be overridden.

The key target of multi-algorithmic systems is to increase identification reliability. In this paper, the multi-algorithmic system includes fingerprint, iris and face. Cryptosystem includes three algorithm such as key generation, encryption and for decryption. Here only if the finger print and iris features are authorized the face features are extracted and identification is derived. The finger print and iris features are extracted using equivalent distance and for fingerprint linear sparse representation is used. There will be three different databases for all three biometrics. Using same database will have many disadvantages. Advantage of using different database includes memory space, easy comparison to the images, efficiency.

The required input biometric template is given and this biometric template compares with all image in the database. When comparing with each template in the database the algorithm generates values for each. The values are generated using matrix and mean of mean is calculated and value is generated. This is same for both iris and fingerprint.

Fingerprint and iris will have separate mean values and this both values are compared and equivalent distance is found. When the equivalent distance is zero the person is authenticated and face feature extraction takes place otherwise the person is unauthenticated, which shows the person is and attacker. Attacks can be done in two forms such as intrusion attack and function creep. Fingerprint extraction is done using linear sparse representation which calculates the value at different finite angles and value is generated and recognition is done.

The main aim of this paper is to provide security, this can be achieved using fuzzy vault and

fuzzy commitment. Fuzzy vault takes biometric input as key and used to recognize. It mainly focuses on fingerprint details. Fuzzy commitment represents the biometric traits as binary codes. The fundamental challenge in designing a biometric template protection scheme is to overcome the large variability among multiple acquisitions of the same biometric trait. There are two techniques such as biometric cryptosystem and template transformation.

Multi-biometric cryptosystems are used in distributed system applications like e-commerce transactions, e-banking and ATM. The fingerprint biometrics operates in two modes namely, enrollment and authentication. The features are extracted using singular point detection and minutiae extraction. Singular point makes use of core and delta and minutiae extraction is done with ridge endings and ridge bifurcation [8]. Matching scores of iris and face traits can be fused via triangular norm [9].

Communication channels between various modules of a biometric system are not secured properly, an adversary can potentially attack by using man-in-the middle attack to replace the information [7]. Fusion in biometric system is categorized into feature level fusion, score level fusion, decision level fusion [2].

The advantage of using is that it cannot guess how many biometrics is used and what type of biometrics is used [8]. Databases such as CASIA-Iris-Thousand database with noisy samples and the NVIE face database with visible and thermal face images is very complex [9].

II.SYSTEM OVERVIEW

The system architecture shown in Fig.1 is a three tier structure. The first layer, called fingerprint feature extraction. The second layer called iris feature extraction and the third layer face feature extraction. Embedding algorithms are used for feature transformations. The various embedding algorithms include point set into a binary string, real valued vector into a binary string and binary string into a point set.

Fusing different features into a single multi-biometric template that can be secured using an appropriate biometric cryptosystem such as fuzzy vault and fuzzy commitment. The system architecture consists of three databases for all three inputs such as fingerprint, face and iris. The fingerprint and iris are preprocessed and resized to control the flow of operation and features are extracted. A value will be generated for the input image. This input image will be compared with each image in the database and during comparison each fingerprint will have a value. Iris image are also preprocessed and features are extracted and comparison is done with the database and values are generated. Using a matcher both the iris value and fingerprint generated values are checked. When both the values are equal it indicates a authorized and proceed with face feature extraction, otherwise the person is not authorized and indicates a unauthorization. The face input is also preprocessed which resizes and features are extracted.

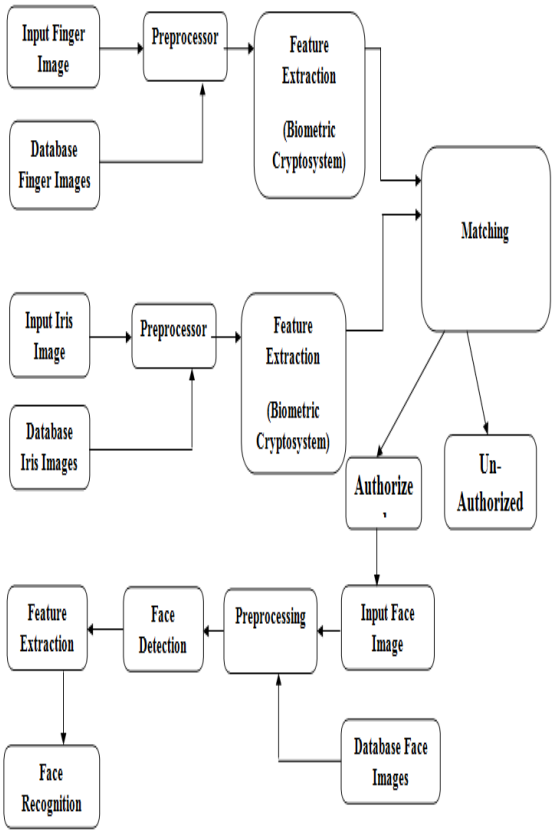

Fig. 1 System Architecture Of Multi-Biometric Cryptosystem On Fusion Level Distinctiveness

The face is detected at different angles using a linear sparse representation and features are extracted and recognized.

A. Fingerprint Feature Extraction

In this process, Fingerprint minutiae are extracted and they obtain the binary representation from the minutiae set. First the user has to upload all the images in the fingerprint database. Then the specified person will give his fingerprint minutiae as the input. Extractions are performed for the input fingerprint and mean value is calculated using matrix calculation and a value will be generated. The extracted fingerprint minutiae contain edges, ridges, bifurcation. The input image is then compared with the database mean value is calculated for each and equivalent distance is found using input fingerprint value and comparison done with the database.

B. Iris Feature Extraction

In this process, Iris features are extracted. The user has to upload and select the iris image from the sample database. Then the iris features are loaded into the system. In order to reduce the dimensionality of the iris code and remove the redundancy present equivalent distance is applied to the iris code features. Then the binary iris code features are extracted. The equivalent distance is calculated which is the score level.

C. Face Feature Extraction

Alignment of face image is essential prior to feature extraction. The face images should be processed in all different directions and angles to perform this in a efficient manner, linear sparse representation is used. This algorithm preprocesses the face, which takes the image alignment or region of interest identification. The face is detected and face features are extracted using the shape, color, locations etc. The face is recognized from the features.

D. Biometric Cryptosystem

In biometric cryptosystem, secure sketch is derived from the enrolled biometric template and stored in the system database instead of the original template. A key is associated with the biometric data which is called secure sketch that does not reveal information about the biometric template. The main advantage of biometric cryptosystem is the exact recovery of original biometric data which allows to use as encryption key. The main aim of the biometric cryptosystem is to provide security. This can be achieved using fuzzy vault and fuzzy commitment.

i.Fuzzy Vault

In fuzzy vault encoder, the biometric template will be given with a random secret key. It takes biometric input as key. It authenticates and encrypts the records. The secret key is then converted into polynomial degree. The set of genuine points along with polynomial evaluation constitute the sketch or vault. Fuzzy vault is mainly used to secure fingerprint details.

ii. Fuzzy Commitment

Fuzzy commitment is represented in the form of binary vectors. Here the cryptographic key is decommitted using biometric data. The binary string is divided into a number of segments and each segment is separately secured using commitment scheme. The keys associated with these segments are then used as additional points in fuzzy vault.

D. Matching Constraints

Matching constraints indicates the authorization and unauthorization of a person. There will be a score value which is used to identify. The values will be generated for each biometric input and a constraint should be initialized which makes the decision.

When the constraint satisfies, the person is authorized otherwise he is an attacker. All the three biometric should be of the same person. All user will have different score level, which identifies and recognize the specified user. A maximum and minimum value can be set. When the value is equivalent to zero the person is authorized and can enter into the system. When the value is not equivalent to zero the person is unauthorized, which means there is an attack from the hacker.

III.EVALUATION

Performance can be evaluated by getting the best recognition. Proper recognition help to defend from forgery attacks. Performance can be evaluated separately for fingerprint, iris and face. All three combines into a fusion and provides higher performance. The genuine authentication shows the efficiency of the system. The performance of fuzzy vault and fuzzy commitment depends upon the security. When all three biometric inputs can be attacked, then the performance is very low. When any one biometric can be hacked then the performance is moderate, but fuzzy scheme provides a very high security and secure the multi-biometric system.

Preprocessing, image segmentation, image binarization and image minutiae increases the performance of the system. The biometric features are extracted and the perfect value should be obtained which improves the system performance. Performance can be evaluated at various levels. The performance should be always high which results in proper recognition of the individual.

IV.DEMONSTRATION

The entire system is implemented in MATLAB. It includes a large library of precoded solutions to common programming problems and manages the execution of programs written specifically for this framework. The class library is used by programmers, who combine it with their own code to produce applications.

The demo of multi-biometric cryptosystem on fusion level distinctiveness contains databases for storing fingerprint, iris and face. The fingerprint, iris is preprocessed and feature is extracted and compared with the database separately. The value is generated from the extracted feature. The value is then used for detecting and the recognition which indicates the authorization and un-authorization of the individual. These indicate the degree of security.

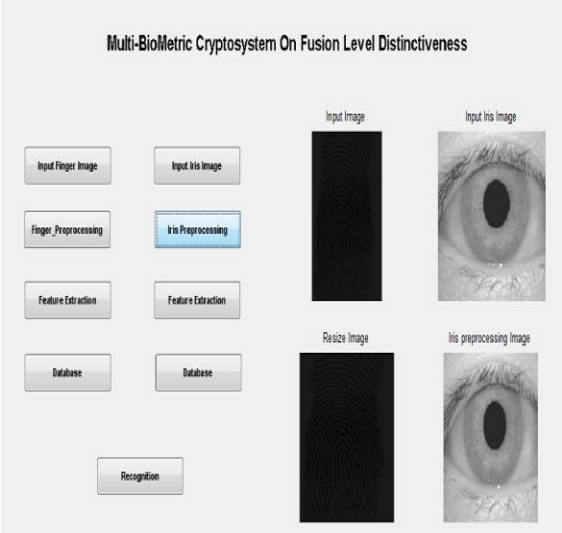

Fig.2 Demo on Multi-Biometric Cryptosystem on Fusion Level Distinctiveness

V.CONCLUSION

The proposal of multi-biometric cryptosystem on fusion level distinctiveness protects multiple templates of a user using multi-biometric cryptosystem. The features of the biometric are extracted and the score level value is generated. The security to the template which protects from attacks is done by two biometric cryptosystem called fuzzy vault and fuzzy commitment. To improve the efficiency of the system the matching constraint should be evaluated with a high degree.

In future work, multi-biometric cryptosystem
can be implemented by using many biometrics to enhance the security. To overcome the failure of anyone of the biometrics another biometric can be used as replacement. The biometrics should not be guessed how many it is used and what is used such the hackers find very difficult to use the template

REFERENCES

[1] A.Ross, K.Nandakumar , and A.K.Jain, Handbook multibiometrics. New York: Springer, 2006.

[2] A.Juels and M.Sudan, A fuzzy vault scheme, in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, 2002, p. 408.

[3] Christian Rathgeb and Christoph Busch, Multi , biometric template protection: Issues and challenges, *Biometrics and Internet Security Research Group, Center for Advanced Security Research Darmstadt,* Nov. 2012.

[4] D.Rhodes, Methods for binary multidimensional scaling, *Neural Computation*, vol. 14, pp.1195-1232.

[5] F.Hao, R.Anderson, and J.Daugman, Combining crypto with biometrics effectively, *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081-108, Sep. 2006.

[6] J.Rethna Virgil Jeny, Chanda J. Jangid, Multi Biometric cryptosystem with fuzzy vault and fuzzy commitment by feature level fusion, *International Journal of Emerging Technology and Advanced Engineering.*, vol. 3, issue 3, March 2013.

[7] M.Sujimangalam, M.Karnan, R.Sivakumar, Generating cryptosystem for multimodal biometrics based on feature level fusion, *International Journal of Computer Science and Management Research*, vol. 2, ISSN 2278-733X, May 2013.

[8] N.Geethanjali, K.Thamaraiselvi, R.Priyadharshini, Feature level fusion of multibiometric cryptosystem in distributed system, *International Journal Of. Modern Engineering Research IJMER*, vol. 2, no. 6, pp-4643-4647, Nov-Dec-2012.

[9] Niang Wang, Qiong Li, Ahmed A. Abd El-Latif, Jialiang Peng and Xiamu Niu, Multibiometrics Fusion for identity authentication: Dual iris, visible And thermal face imagery, International Journal of Security and Application, vol. 7, May 2013.

[10] Y.Sutcu, Q. Li, and N.Memon, Secure biometric templates from fingerprint-face features, in *Proc. CVPR Workshop Biometrics*, June. 2007.