ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Refining Multibiometrics System by Exhausting Multiple feature Extraction

Chanda J. Jangid[1], Dipak R. Patil[2]

M. E. Information Technology, AVCOE Sangamner, India[1]

Assistant Professor, Dept. of IT, AVCOE Sangamner, India[2]

Abstract: Multibiometrics system is the combination of two or more biometric systems. These systems are more trustworthy due to the occurrence of multiple independent evidences. Multibiometric systems are very popularly deployed in many large-scale biometric applications like FBI, UID in India and banking etc. The problems due to unimodal biometrics are tried to resolve by multibiometric system. The main objective is to secure the biometric template by producing a secure sketch with the use of multibiometric cryptosystem and then put in a database. Investigators are concentrating on "How to offer security to the organization". To protect the system template should be secure. If the multibiometric template is stolen it should be a serious issue for the safety of the organization and also for operator privacy. In this paper, present a feature-level fusion framework to defend multiple templates of a user as single secure sketch and compress the secure sketch to generate a compact multibiometric template that contain most of the information fulfilled in the individual template.

Keywords: Biometric cryptosystem, Multibiometrics, fuzzy commitment, fuzzy vault, fusion, secure sketch, template security.

1. INTRODUCTION

The latest research shows that use of combined biometric traits for any person's identification is more effective and more challenging. Now days the use of multibiometric system in many large scale applications like in FBI, User ID cards in India is going to be increased. Because they are providing some advantages over unibiometric system like lower error rate, large population coverage, it also given that a certain degree of elasticity for some unusable biometric traits and also face spoofing attack [1].

The term Multibiometrics denotes the combination of different types of information together like face, fingerprint and iris biometric traits. Multibiometric system combines any types of and any number of data.Multibiometric systems is efficient for removing various weaknesses of the unibiometric systems by counting the multiple sources of information. And it is only imaginable by fusing various biometric traits of a person, or multiple feature extraction on the same biometric [2].

To secure biometric templates number of techniques has been proposed.These techniques can be characterized into two main classes:

1.1 Biometric cryptosystems:

In a biometric cryptosystem, protected sketch is derived from the registered biometric template and put in storage in the system database in its place of the unique template. In the absence of the real user's biometric data, it must be difficult to rebuild the template from the sketch.Instead, specified an authentication query which is sufficiently closer to the registered template, it should be easy to decode the sketch and improve the template [9].

1.2 Template transformation:

In template transformation techniques the biometric template modified with a user definite key such that it is hard to improve the original template from the altered template. At the time of authentication, the similar transformation is applied to the biometric query and the similar is performed in the converted domain to avoid exposure of the new biometric template [10].

2. LITERATURE SURVEY

A number of efforts have been made to expand the secure biometric recognition framework to participate multiple biometric traits [3]. It combined faces and fingerprint templates that are collectedconverted into binary strings. Then these binary strings are added and then given as the input to a fuzzy commitment system. And bind multiple biometrics to cryptography, and produce multibiometric cryptosystem.Ending the unambiguous integration techniques of altered biometrics, the impacts of fusion at biometric levels on the biometric security, privacy and accuracy are demanding to increase.

Nandhakumar and Jain [4] were tried for a multibiometric cryptosystem in which biometric templates constructed on binary strings and point-sets are jointed. The binary string is distributed into a number of sections and each section is independently protected using a fuzzy commitment scheme. The secrets related with these section-wise fuzzy commitment systems are then used as additionalfeatures in the fuzzy vault built using the point-set-based features.

In [5] improved the accuracy and security of Multibiometric system by code-based cryptosystem.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

In accumulation of randomness cryptosystem also probabilistic, and provide more vulnerability of template towards brute force attacks. It usages a public key cryptosystem to construct, an assurance to achieve non-reputability and authentication. The stored template is easily hacked by attackers.

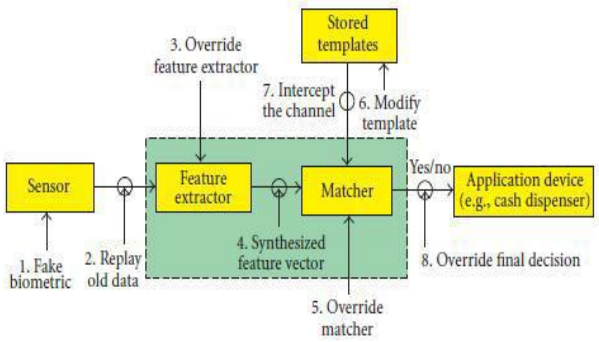

Fig. 1: Vulnerabilities in systems

There are some attacks [6] on various levels of multibiometric system, as shown in Fig. 1:

1. A fake biometric trait is specified as input to the biometric system, like an artificial finger.
2. An attacker may exchange the old data with new data of the user.
3. The feature extractor may be overruled and it will show the features whichare replaced by the attacker.
4. The authentic feature vector may be replaced by the unauthorized feature vector.
5. Matching machine may be replaced by the other machine, which gives predefined output.
6. The final template stored into the database may be modified by the intruder.
7. Channel from stored template to matcher may be intercept with the attacker channel and attackers given template is forwarded to the matcher.
8. The final decision may be override and prefixed result may be displayed.

3. PROPOSED SYSTEM

Existing multibiometric system combines three biometric traits and provide single secure sketch. That is stored into the system database. But it is needed to improve the both system performance and template security. Proposed system should be able to provide high security secure sketch with minimum size.

Proposed feature level fusion framework consists of five basic modules: (i) feature extraction, (ii) embedding algorithm, (iii) fusion module, (iv) biometric cryptosystem and (v) compression module. The framework of multibiometric cryptosystem is as shown in Figure 2.

3.1 Feature extraction:

Biometric images are captured and given to the feature extractor. It is able to extract maximum point of the images, which improve security of template.

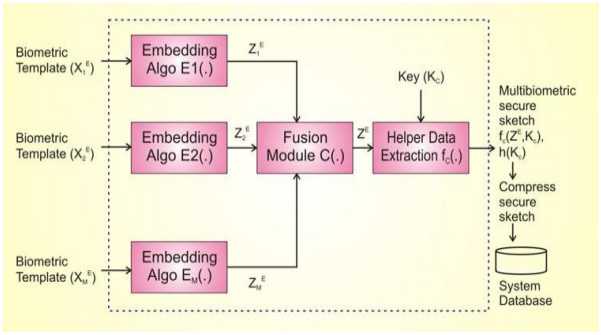

Fig. 2: Framework for Multibiometric cryptosystems with feature level fusion

3.2 Embedding algorithm (E):

The embedding algorithms are used to transform a biometric representation x_m into new common representation z_m, where $z_m = E_m(x_m)$, for all m = 1; 2; :::;M. The input can be a point-set, real valued feature vector or a binary string. The output could be a point-set or a binary string and by using fuzzy vault and fuzzy commitment they are secured.

3.3 Fusion module (C):

In fusion module all the biometric feature sets are combine $Z = z_1; z_2; :::; z_M$ to form a fused feature set Z.

3.4 Biometric cryptosystem (fc):

At the time of enrollment, the biometric cryptosystem create a secure sketch y_c by using the fused feature set and key kc. At the time of authentication, the biometric cryptosystem regenerate key k_c from secure sketch y_c and feature set.

3.5 Compression module:

The compression module, compress the size of secure sketch y_c then store into the database. This compressed secure sketch requires less space for storage in database.

There are some algorithms used to implement the given multibiometric system. Embedding algorithms [1] convert feature representation into common representation. Fuzzy vault encoding and decoding algorithms are used for securing point set based biometric features [1] [7]. Fuzzy commitment encoding and decoding algorithms are used to secure the biometric features in binary vector format [1] [8]. Compression algorithm is

1. Generate a matrix.
2. Invert that matrix.
3. For common block replace block from matrix
4. Return replaced block.

4. MATHEMATICAL MODEL

Mathematical model for "Refining biometric system by exhausting multiple feature extraction" It includes four sets as mentioned below:

S = (F, A, I, M)
Set (A) = Represents feature extraction points of face
Set (F) = Represents feature extraction points of fingerprint
Set (I) = Represents feature extraction points of iris

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Set (M) = Represents feature extraction points of master
Where, A = (a_0; a_1;:::; a_n) ΦA,
F = (f_0; f_1; :::; f_n)ΦF,
I = (i_0; i_1; :::; i_n) ΦI and
M = (m_0; m_1; :::;m_n)ΦM.

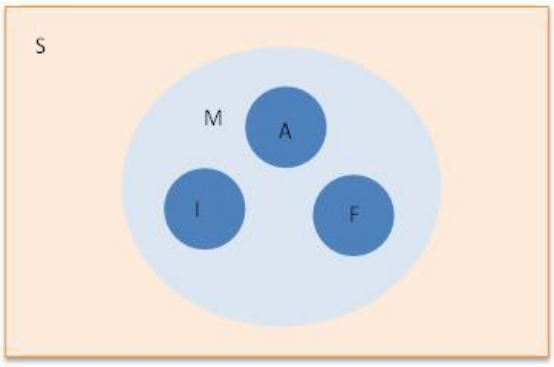

Fig. 3 vein diagram

4.1 State Transition Diagram:-

Step I:
A Finite set of states (Q) = {q_0; q_1; q_2; q_3; q_4} where
1. q_0 denotes initial state and q_4 denotes final state q_1, q_2, q_3 are internal states
2. A set of final or accepting states (F) = {q_4}
Step II:
State diagram:
q_0 = Feature extraction
q_1 = Fusion
q_2 = Secure data forwarding
q_3 = Performance evaluation
q_4 =Compression

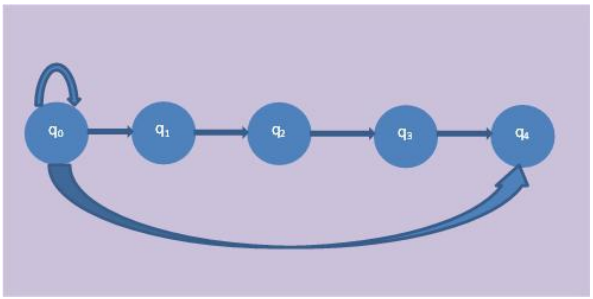

Fig. 4 State transition diagram

5. RESULT ANALYSIS

5.1 Datasets:
The virtual datasets used for the system have fingerprint database from FVC2002- DB-2, iris database from MMU1 Iris database and face database from XM2VTS. Sample database of face, fingerprint and iris real database is taken randomly from free available source.

5.2 Performance:
Performance of the system is measured with parameter GAR (Genuine Accept Rate) and FAR (False Accept Rate). As the threshold value changes these rates also changes for Virtual datasets and Real datasets. For virtual database, at the threshold value of 95.00 the GAR is 99% and FAR is very small. For virtual and real database increase in threshold value decrease the GAR.

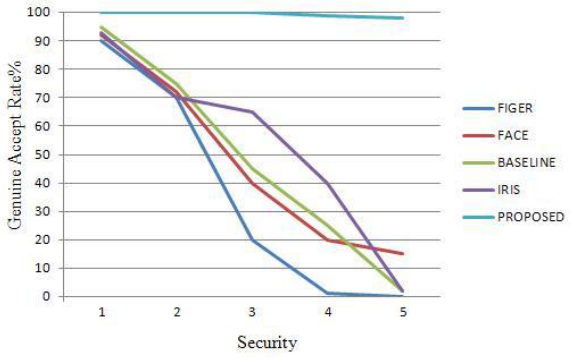

Fig. 5: For virtual database GAR

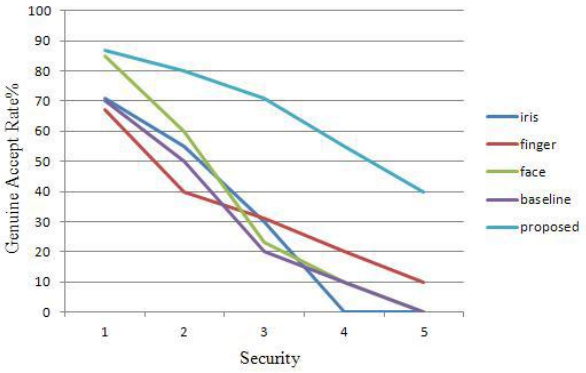

Fig. 6: For real database GAR

5.3 Size Analysis:
The Column chart depicts the performance graph regarding different user data that have been used. As per the graph the size of final image variation is shown, secure sketch image size in proposed system is smaller than the size of old system.

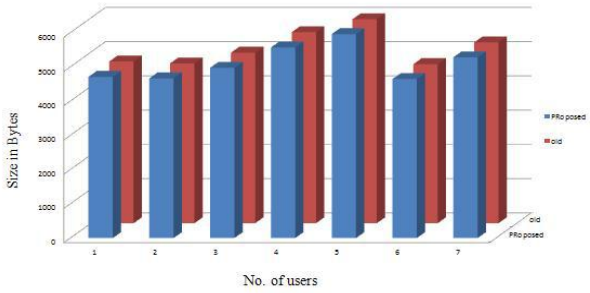

Fig. 7: Image size analysis

6. CONCLUSION

The proposed feature level fusion framework for multibiometric cryptosystem, protect multiple templates of user by using single secure sketch. The possibility of such a framework has been confirmed using both fuzzy vault

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

and fuzzy commitment, which are two of the supreme well-known biometric cryptosystems. Also proposed systems have embedding algorithm to convert biometric representation and compression to minimize the size of final sketch, this give better result.

REFERENCES

1) Abhishek Nagar, Karthick Nandhakumar, and AnilK. Jain, "Multibiometrics Cryptosystems Based on Feature-Level Fusion", IEEE Transactions on Information Forensics And Security, Vol. 7, No. 1, February 2012, pp 255-268
2) Anil Jain, Karthik Nandhakumar, and Arun Ross, "Score normalization in multimodal biometric systems", Pattern Recognition 38 (2005) 22702285, 18 January 2005
3) Fu, S. Yang, J. Li, and D. Hu, "Multibiometric cryptosystem: Model structure and performance analysis," IEEE, vol. 4, no. 4, Dec. 2009.
4) K. Nandhakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in Proc. IEEE 2nd Int. Conf. Biometrics: Theory, Applications, and Systems, Washington, DC, Sep. 2008
5) Ajay Sharma, Deo Brat Ojha "A Multi-Biometric Template Security: An Application of Code-Based Cryptosystem", IJCIM Vol. 19. No.1 (January-April, 2011) pp 14 -24
6) V. Evelyn Brindha, A. M. Natarajan, \Palm Print Based Fuzzy Vault for Unibiometric Template Security", European Journal of Scientific Research ISSN 1450-216X Vol.76 No.1 (2012), pp. 5-19
7) Juels and M. Sudan, "A fuzzy vault scheme," in Proc. IEEE Int. Symp. Information Theory, Lausanne, Switzerland, 2002, p. 408.
8) Juels and M. Wattenberg, "A fuzzy commitment scheme," in Proc. Sixth ACM Conf. Computer and Communications Security, Singapore,Nov. 1999, pp. 28–36.
9) J. Rethna Virgil Jeny, Chanda Jagdish Jangid , "Enhancing Security of Multibiometric Cryptosystem Using RSA" , International Journal for Advance Research In Engineering and Technology, Volume 1, Issue II Mar. 2013 ISSN 2320-680, pp.1-4
10) J. Rethna Virgil Jeny , Chanda Jagdish Jangid ,"Multi biometric Cryptosystem with Fuzzy Vault and Fuzzy Commitment by Feature-Level Fusion", International Journal of Emerging Technology and Advanced Engineering ,ISSN 2250-2459, Volume 3, Issue 3, March 2013, pp.359-365.

BIOGRAPHY

Chanda J. Jangid perceiving M. E. in Information Technology and received B. E. degree in Information Technology, from Amrutvahini college of Engineering, Sangamner.