Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Review of Multi-biometric Cryptosystem using Feature level Fusion

Ashish P. Palandurkar*
Department of Wireless Communication & Computing
AGPCE, RTMNU, Nagpur, India

Vinod Nayyar
Department of Computer Science & Engineering
AGPCE, RTMNU, Nagpur, India

R. D. Wagh
Department of Information Technology
DBCER, RTMNU, Nagpur, India

Abstract*— The basic concepts and methods on performance and effectiveness evaluations at the feature-level fusion model of multi-biometric cryptosystem are concentrated on in this paper. Single biometric cryptosystems were developed to obtain win-win scenarios for security and privacy. They are seriously threatened by spoof attacks, in which a forged biometric copy or artificially recreated biometric data of a legitimate user may be used to spoof a system. By using cryptographic theory, firstly, the formal definitions related to multi-biometric cryptosystems are formulated. Then we see under some extreme conditions, the security and privacy of multi-biometric cryptosystems at the feature level are analyzed and rigorously proved. Finally, a close relationship between security and privacy and the fundamental trade off between the accuracy and security are also studied.*

Keywords*— Biometrics; Security; Encryption; Fusion; Fuzzy Commitment; Fuzzy Vault*

I. INTRODUCTION

Biometric recognition refers to the automatic recognition of individuals based on their physiological and/or behavioural characteristics. Jain et al. [1] formally defined biometric recognition. For enhancing the privacy in biometric recognition, cancellable biometrics was developed to avoid storing the biometric data in clear. A transformed biometric using a one-way function, either in the signal domain or in the feature domain, substitutes the original biometric. The non-invertible transformation preserves the statistical properties of the original biometric data, while simultaneously enhancing the privacy of biometrics since it is hard to exactly reconstruct biometric data from the transformed data. Biometric encryption or biometric cryptosystem, as a new security technology, focuses on generation and binding of secret keys from/to biometric data. Neither the key nor the biometric can be retrieved from the stored template except the correct live biometric sample is presented [2]. Biometric cryptosystems aim to obtain a win-win scenario of security and privacy, especially a higher security. Unlike a password, the variability of the biometric data sampled in different environments makes it hard to generate identical biometric keys. Meanwhile, it is still a huge challenge because spoof attacks are also commonly encountered in biometric cryptosystems. Therefore, many researchers are inspired to distract goals from uni-biometric cryptosystems to multi-biometric cryptosystems.

In this paper, we will extend and further complete the theoretical analysis from [5], especially in the methodologies of the feature-fusion model. Under some extreme conditions, such as leakage of side information about biometrics, the security and privacy of multi-biometric cryptosystems, compared with those in uni-biometric cryptosystems, are rigorously shown at the feature-level. Furthermore, a close relationship between security and privacy is discussed. Based on an analysis of the accuracy in multibiometric cryptosystems, the fundamental trade off between the accuracy and security is studied from an information-theoretical prospective. To overcome from all these disadvantages of biometric system, we use multibiometric cryptosystem. Multibiometric is combination of more than one biometric, and fusion of multibiometric indicate the improvement in security and reliability of the system. Multibiometric systems fusion is categorized in three levels namely [3]:

A. Feature Level Fusion:

In feature level fusion new feature vector is constructed with high dimensionality. The newly formed vector is more discriminative than individuals.

B. Score Level Fusion:

In this level matching scores are collected from every individual and then combine together.

C. Decision Level Fusion:

In decision level fusion final results are combined together.

We use feature level fusion for multibiometric cryptosystem. Unlike passwords and tokens, compromised multibiometric templates are not recoverable. Because of this, multibiometric template security is very necessary thing. In this paper, we propose a scheme to protect all the templates of user in multibiometric system. The remaining part of the paper is preplanned as follows. Section II provides Fuzzy Vault and Fuzzy Commitment in background. Previous Research is given in section III. Proposed system with Fuzzy Vault and Fuzzy Commitment is presented in section IV. Section V describes the performance evaluation module of sytem Section VI describes conclusion and future work.

II. **BACKGROUND**

To secure biometric templates many techniques are there. These techniques are categorized into two classes:

A. Template transformation:

These techniques modify the biometric template with a user specific key so that it is complicated to recover the original template from the transformed template throughout authentication, the same transformation is applied to the biometric query and the matching is performed in the transformed domain to evade exposure of the original biometric template. Generally the secure template should satisfy the properties like:

(i) It must be computationally not easy to find a biometric feature set that will match with the particular template.
(ii) It must be computationally tough to identify that they are consequent from the same data or obtain the original biometric data.

B. Biometric cryptosystems:

In this technique secure sketch is obtained from given biometric template and stored in database as an alternative of original template. The helper data is usually obtained by binding a key with the template. So such techniques are also known as key binding biometric cryptosystems. To handle intra-user variations error correction coding techniques are typically used. Fuzzy vault [4] is well known example of biometric cryptosystem. And which is very useful in protecting point-set-based features. It is design to secure multibiometric features which are represented as a point set. Main advantage of fuzzy vault is, it has ability to secure fingerprint details.

Fuzzy Commitment is a biometric cryptosystem which is used to secure biometrics traits represented in binary vector. Main advantage of this technique is its compact size of the sketch. Assume that the enrolled biometric template is an -bit binary string. In fuzzy commitment, a uniformly random key of length l bits is generated and used to exclusively index an n-bit codeword of suitable error correcting code. The sketch is then extracted from the template. At the end sketch is stored in the database.

III. **PREVIOUS RESEARCH**

A number of attempts have been made to enlarge the secure biometric recognition framework to integrate multiple biometric traits [6]. It joint faces and fingerprint templates that are both altered into binary strings. These binary strings are concatenated and then used as the input to a fuzzy commitment scheme. Fu *et al.* Hypothetically analyzed the template security and recognition accuracy imparted by a multibiometric cryptosystem, which is operated in 4 different ways: no-split, MN-split, package,and biometric model. The first three models keep up a correspondence to decision-level fusion, where the biometric templates are secured separately. The biometric model is based on feature-level fusion of standardized templates. However, no system implementation was reported.

Nandakumar and Jain [7] wished-for a multibiometric cryptosystem in which biometric templates based on binary strings and point-sets are united. The binary string is separated into a number of segments and each segment is independently secured using a fuzzy commitment scheme. The keys related with these segment-wise fuzzy commitment schemes are then used as supplementary points in the fuzzy vault constructed using the point-set- based features. Fu and Yang [6] bind multiple biometrics to cryptography, and form multibiometric cryptosystem. Abandoning the unambiguous integration techniques of different biometrics, the impacts of fusion at biometric and cryptographic levels on the biometric security, privacy and accuracy are trying to increase. In this paper, we propose the design of a multibiometric cryptosystem with various templates and try to provide security with biometric cryptosystem techniques.

Lai et al. [9-11] studied a fundamental trade off between privacy and security, which are measured by the biometric measurement and key respectively, from an information theoretic perspective. They demonstrated the privacy-security trade-off in the single and multiple use case.

IV. **PROPOSED WORK**

Multibiometrics system is a collection of one or more biometrics, which is taken as a reflection in this paper we use fingerprint and Iris. In this project, we propose a Cryptosystem based feature-level fusion framework to simultaneously protect multiple templates of a user as a single secure sketch. It include,

1) Practical implementation of the proposed cryptosystem multimodal biometric system feature-level fusion framework uses two well-known biometric cryptosystems, namely, fuzzy vault and fuzzy commitment
2) Detailed analysis between matching accuracy and security is the proposed multibiometric cryptosystems based on two different databases (one real and one virtual mutimodal database), each containing the most popular biometric modalities.
3) Fuzzy commitment is a biometric cryptosystem that can be used to secure biometric traits represented in the form of binary vectors (e.g., iriscodes).Fuzzy vault is useful for securing point-set-based biometric features such as fingerprint minutiae.

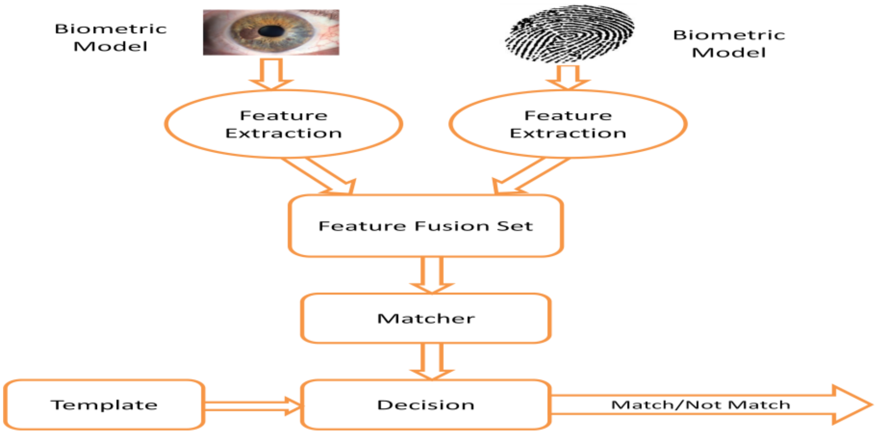

Fig. 1 Fusion of Two biometric Model

Fig 1 show the feature level fusion of two biometric models. Sensor collect biometric model as an input. Features are exacted from each biometric model individually and form feature vector. These features are collected together to form a single new vector. Feature level fusion can use similar feature extraction algorithm or different feature extraction algorithm. The combined feature vector is then used for classification process. Separately extracted templates are fused with the random key and it is given as input with the help of ECC and stored in the database. At the time of verification, the merged single vector is compared with the vector which is stored in the database and key is regenerated. Matching concert of a biometric system is calculated with the help of false acceptance rate (FAR) and genuine acceptance rate (GAR). The biometric cryptosystem fuzzy vault and fuzzy commitment do not produce revocable templates.

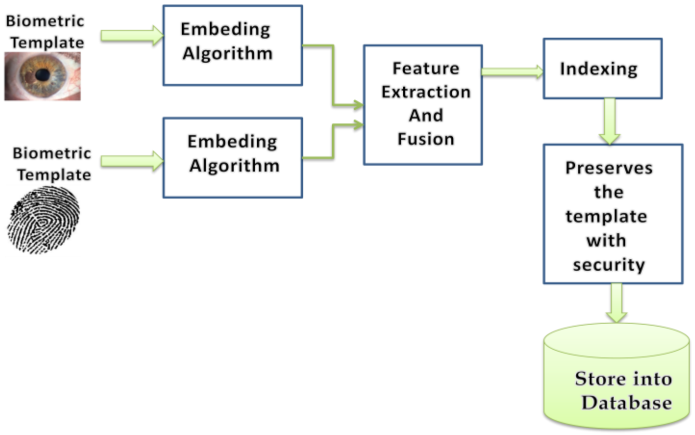

Fig. 2 Block Diagram of Multibiometric Cryptosystem

Fig. 2 shows block diagram of multibiometric cryptosystem with feature level fusion to protect template with fuzzy vault and fuzzy commitment techniques. Sensor collect biometric template as an input. By applying various feature extraction methods for individual biometric vector set is formed. All vectors combine together to form single feature set which is nothing but the feature level fusion. That fused secure sketch is protected with fuzzy vault and fuzzy commitment cryptosystem. In fuzzy vault encoder, the biometric template will be given alongside random secret key which is transformed to a polynomial degree then polynomial is evaluated in a graph. The set of points is secured by trouncing them with chaff points. The set of actual points along with polynomial evaluations together with chaff points represent the sketch or vault. In fuzzy vault decoder, the biometric will be specified and then by using the filter the vault points and the query are compared. In multibiometric vault the feature level fusion is used to join the biometrics and then fuzzy vault scheme is addressed. Fuzzy commitment is represented as binary vectors. The binary string is separated into a number of segments and each segment is independently secured using a fuzzy commitment scheme. The keys related with these segment wise fuzzy commitment schemes are then used as further points in the fuzzy vault constructed using the point-set based features. At the end final sketch is stored in database.Different Modules that is to be implemented in project.

A. Fingerprint feature Module

In this module, Fingerprint minutiae are extracted obtain the binary string representation from the minutiae set. First the user has to upload and select the fingerprint images from the sample database. Then the Finger print feature are loaded into the system. Then this module, extracts the fingerprint features.

B. IRIS feature Module

In this module, the binary Iris Code features are extracted. The user has to upload and select the IRIS images from the sample database. Then the IRIS feature are loaded into the system. In order to reduce the dimensionality of the iris code and remove the redundancy present in the code, LDA is applied to the IRIS code features. Then the binary IRIS code features are extracted.

C. Feature-Level Fusion Module

We propose a feature-level fusion framework to simultaneously secure multiple templates of a user using biometric cryptosystems. To demonstrate the viability of this framework, we propose simple algorithms for the following three tasks:

1. Converting different biometric representations into a common representation space using various embedding algorithms:
   (a) Binary strings to point-sets,
   (b) Point-sets to binary strings, and
   (c) Fixed-length real-valued vectors to binary strings.
2. 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; efficient decoding strategies for these biometric cryptosystems are also proposed.
3. Incorporating a minimum matching constraint for each trait, in order to counter the possibility of an attacker gaining illegitimate access to the secure system by simply guessing/knowing only a subset of the biometric traits.

V. **PERFORMANCE EVALUATION MODULE**

We evaluate the trade-off between recognition accuracy and security of the proposed multibiometric cryptosystems using To validate the constrained multibiometric cryptosystem, we implemented a system consisting of iris and fingerprint modalities, where minimum matching constraints are imposed for the fingerprint modality. We further assume that the adversary has knowledge about the iris biometric, i.e., he has access to some iris image of the enrolled user. In this experiment, a multibiometric fuzzy commitment is implemented and a *secondary* representation of fingerprints is obtained using minutiae aggregates. Minutiae are employed as the *primary* fingerprint representation, and hence a fuzzy vault is used in the second stage. Comparison with the Unimodal and Multimodal System.

VI. **CONCLUSION AND FUTURE WORK**

Proposed technique existing here provides security to the multibiometric cryptosystem with feature level fusion framework. Fuzzy vault and fuzzy commitment also help in accuracy and security of multibiometric template. It cannot be guessed by any hacker that how many biometrics is used and what type of biometrics are used. There are some critical issues that need to be investigated further is to improved feature fusion scheme to generate a compact multibiometric template that retains most of the information content in the individual templates and the methods to progress the security analysis by exactly modelling the biometric feature distributions.

REFERENCES

[1] P. S. Sanjekar and J. B. Patil, An Overview Of Multimodal Biometrics Department of Computer Engineering, RCPIT, Shirpur ,Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, February 2013,DOI :

[2] Kulwinder Singh, Kiranbir Kaur, Ashok Sardana,Gulzar Group of Institutes, Khanna, Punjab, India Global Institute of Engineering and Technology, Punjab, India IET Bhaddal, Ropar, Punjab, India,"Fingerprint Feature Extraction", IJCST Vol. 2, Issue 3, September 2011

[3] Abhishek Nagar, Student Member, IEEE, Karthik Nandakumar, Member, IEEE, and AnilK. Jain, Fellow, IEEE, Multibiometric Cryptosystems Based on Feature-Level Fusion, IEEE Transactions On Information Forensics And Security, Vol. 7, No. 1, February 2012,Page No255

[4] R.N. Kankrale, Prof. S. D. Sapkal. Template Level Fusion of Iris and Fingerprint in Multimodal Biometric Identification Systems, Department of Information Technology SRES

[5] A. Jagadeesan, Dr. K. Duraiswamy. Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion Of Fingerprint And Iris, (IJCSIS) International Journal of Computer Science and Information Security,Vol. 7, No. 2, February 2010

[6] Ai-hong Zhu ,Lian Li. Improving for Chaotic Image Encryption Algorithm Based on Logistic Map ,2nd Conference on Environmental Science and Information Application Technology ,2010,Page No:211 -214

[7] Sangram Bana1 and Dr. Davinder Kaur2.Fingerprint Recognition using Image Segmentation, Sangram Bana, et al. / (Ijaest) International Journal Of Advanced Engineering Sciences And Technologies Vol No. 5, Issue No. 1, 012 – 023

[8] S. Arun Vivek, J. Aravinth, S. Valarmathy_Professor "Feature Extraction for Multimodal Biometric and Study of Fusion Using Gaussian Mixture Model".

[9] L. Lai, S. W. Ho and H. V. Poor, "Privacy-Security Tradeoffs in Biometric Security Systems", in Forty-Sixth Annual Allerton Conference, Allerton House, UIUC, Illinois, USA, pp268-273, Sep. 2008.

[10] L. Lai, S. W. Ho, H. V. Poor, "Privacy-security Trade-off in Biometric Security Systems – Part I: Single Use Case", IEEE Trans. on In-formation Forensics and Security, Vol. 6, No.1, pp 122-139, Mar. 2011.

[11] L. Lai, S. W. Ho, H. V. Poor, "Privacy-security Trade-off in Biometric Security Systems-part II: Multiple Use Case", IEEE Trans. on Information Forensics and Security, Vol. 6, No. 1, pp140-151, Mar. 2011.