IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

A Review on Different Multi Biometric Cryptosystems

Sreemol R[1], Kavitha N[2]

Dept of Computer Science and Engineering, Rajiv Gandhi Institute of Technology, Kottayam, Kerala, India [1]

Professor, Dept of Computer Science and Engineering, Rajiv Gandhi Institute of Technology, Kottayam, Kerala, India[2]

Abstract: Biometric Identification is one of the area related to person recognition by means of physiological and behavioral features like iris, fingerprints, voice, face, etc. Biometric cryptosystems can be used to protect the biometric template. It provides a better solution for the cryptographic key generation, encryption and decryption. Single Biometric cryptosystems use a single biometric feature to protect the data, while multi biometric cryptosystems uses two or biometric features. Multi biometric cryptosystem uses different fusion techniques. In this paper, a survey of different kinds of multi biometric cryptosystem is done.

Keywords: biometric; fusion; cryptosystem.

I. INTRODUCTION

Identity recognition has become an important factor in the field of security applications from the past few decades. But nowadays applications of biometrics have many new security challenges. If the data in the biometric template is lost, it cannot be reset or reissued unlike the simple traditional passwords. So, a multi biometric cryptosystem can be used to protect the biometric template.Previous works are based on the entropy definition to measure the security of the system. But it measures the probability values rather than the actual values. Single Biometric Cryptosystem (SBC) uses a single feature for the identification purposes. Multi biometric cryptosystems (MBC) uses two or more biometric features for the identification purposes and it provides more security than SBC.MBC are of different types. MBC of feature level (MBCF) combines biometric features from multiple sources into a single template for identification and verification. But it mainly suffers the curse-of dimensionality problem. MBC of decision level fusion (MBCD) performs authentication in each SBC separately and outputs final decisions based on specific rules. But the common criticism on the latter is that it has very less information content. Hybrid fusion is a combination of score level and decision level fusion. In the case of score level fusion each biometric user provides a similarity score indicating the nearness of the template feature vector with the input feature vector.These scores can be combined together to claim an identity of a particular user.

II. LITERATURE REVIEW

Abhishek Nagar et.al [1] implemented a feature level fusion framework using fuzzy vault and fuzzy commitment. Multi biometric cryptosystem needs two or more biometric templates. But the storage of this templates may create risks to the user data. The biometric templates can be protected in many ways. One method is to store the secure sketch generated from the correspondingtemplate using a biometric cryptosystem. But the problem is the storage of multiple sketches. The proposed feature-level fusion framework simultaneously protect multiple templates

of a user as a single secure sketch. Also, they analyzed the accuracy and security of the proposed system based on a real and a virtual multimodal database containing the three biometric features such as face,iris and fingerprint.

Li Yuan [2] proposed a template protection method for multimodal biometric template using fuzzy commitment. After feature extraction using principal component analysis apply the feature level fusion on it. In the second step, the face and ear fused real-valued template is converted to binary template using noninvertible transformation. Finally, by means of fuzzy commitment, the binary template is encrypted.

In the fuzzy vault scheme proposed by ThiHanh Nguyen[3], the coefficients of a polynomial equation represents the encoded biometric features.It is then used to lock and unlock the secret key. The security of the given system depends onthe infeasibility of the polynomial reconstruction problem.Also, the performance of the fuzzy vault can be enhanced by addingmore chaff points to the vault. For a real-time implementation of the bio-cryptosystem, as would be required intoday's information security system, existing methods for chaffgeneration is not applicable.

Ahmed ShayerAndalib et al. [4] proposed a novel key generationscheme from fingerprint minutiae using a graph traversal basedapproach which is simple to implement and efficient in performance. Here,gabor filter is used to identify the fingerprint minutiae. From the template matrix, two directed acyclic graphs (DAG) are constructed where the minutiae coordinates represents the edges. After

DOI10.17148/IJARCCE.2017.63232

certain operations, from the two DAG's, two strings are generated. Also, on the two strings, simple rotation and combination operation are performed and generates four cryptographic keys. This method has a strong irreversible property.

Chi Chen et.al [5] proposed a multi biometric cryptosystem based on secret share technology with the help of fuzzy extractor. Each of the biometric featuregenerates a feature vector.Then the feature vector is put into a fuzzy extractor. It will generate a stable codeword called bit-string.Based on a secret share method,all the code words are used to bind a random key.This key can be used to encrypt user's secret data.Only a part of the enrolled biometric modalities are required to recover the random key during the verification phase.So the user can use the same biometric key on different devices. Fuzzy extractors can be used to bind a cryptographic key to biometricfeatures. But most of the fuzzy extractor needs fingerprint registration. Also, to rectify the uncertainty in biometric features, it needs some error correction codes. So, Wencheng Yanget.al[6] proposed a registration free fuzzy extractor with the help of Delaunay triangulation method. During the authentication of fingerprint, it avoid the feature pre alignment process. But the above systems which operates on the basis of feature level fusion mainly suffers the curse-of-dimensionality problem. To avoid that, cryptosystem based on decision level fusion can be used.
Cai Li et al.[7] proposed a Multibiometric Cryptosystem Based on Decision Level Fusion. They used hash function to protect each of the biometric features. Delaunay triangle-based matching algorithm was used to extract the features from the fingerprints. It provides better result. Also, the use of hash functions improve the security of each of the biometric feature.
Delaunay quadrangulation[8] is one another method which can be used for the feature extraction of fingerprint. The feature sets and similarity measures
utilized in the delaunay triangulation based systems are not suitable for existing templateprotection techniques. Moreover, local structural change caused by nonlinear distortion is not considered well in these systems. Fixed-length and alignment-freefeature vectors extracted from Delaunay quadrangles are less sensitive to nonlinear distortion.so, it works better than the triangulation based systems. In a work , Bian Yang et al. [9] showed that compared to feature level fusion , decision level fusion has not only the least fusion complexity, butalso the maximum interoperability across different biometric features, template protection and recognition algorithms, template formats and comparison score rule.
Amioy Kumar et al. [10] proposed a Cell-Array-Based Multibiometric Cryptosystem. They implemented a new framework for a biometric cryptosystem in which a cryptographic key is concealed with biometric modalities. The candidate biometric module is secured using two functions: BCH encoding and Hash function. These methods mainly uses the decision level fusion. However, performance improvement via decision level fusion is not clear. Decision level fusion has small and rigid information content. Score levelfusion uses a biometric score which represents the nearness of feature vector value with that of the template value. Hybrid fusion which is a combination of score level and decision level fusion can be used to protect the biometric template since it has the advantages of both the fusion techniques.

III.CONCLUSION

Multi biometric cryptosystems can effectively protect the biometric templates. In this study, we tried to give a brief introduction about various multi biometric cryptosystem and different fusion techniques. At last, we conclude that feature at fusion level is better for single biometric cryptosystems. But for multi biometric systems, feature-level fusion suffers the curse-of-dimensionality problem. Decision level fusion evaluates each biometric feature separately and outputs the results based on certain rules. But, it has small and rigid information content. Score level fusion uses a biometric score for authentication purposes. Hybrid fusion which is a combination of decision level and score level fusion can be used o protect the biometric cryptosystem.

REFERENCES

[1] AbhishekNagar, Karthik Nandakumar and Anil K. Jain," Multi biometric Cryptosystems Based on Feature-Level Fusion", IEEE Transactions On Information Forensics And Security, Feb. 2012, Vol. 7, No. 1,255-268.

[2] Li Yuan," Multimodal Cryptosystem Based on Fuzzy Commitment", IEEE 17th International Conference on Computational Science and Engineering ,2014,1545-1549.

[3] ThiHanh Nguyen, Yi Wang, TrungNhan Nguyen and Renfa Li, " A Fingerprint Fuzzy Vault Scheme Using A Fast Chaff Point Generation Algorithm", IEEE,2013

[4] Ahmed ShayerAndalib and Md. Abdulla-Al-Shami," A Novel Key Generation Scheme for Biometric Cryptosystems Using Fingerprint Minutiae", IEEE,2013.

[5] Chi Chen, Chaogang Wang, Tengfei, Yang, Song Wang and Jiankun Hu, "Multimodal Cryptosystem Based on Fuzzy Commitment", International Conference on Fuzzy Systems and Knowledge DiscoveryIEEE,2014 ,989-994.

[6] Wencheng Yang, Jiankun Hu, and Song Wang," A Delaunay Quadrangle-Based Fingerprint Authentication System With Template Protection Using Topology Code for Local Registrationand Security Enhancement",IEEE Transactions On Information Forensics And Security, July 2014,Vol. 9, No. 7, 1179-1191.

[7] Cai Li, Jiankun Hu, Josef Pieprzyk, and Willy Susilo, "A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of MultibiometricCryptosystems Based on Decision Level Fusion", IEEE Transactions On Information Forensics And Security

[8] Wencheng Yang, Jiankun Hu, and Song Wang," A Delaunay Quadrangle-Based Fingerprint Authentication System With Template Protection Using Topology Code for Local Registrationand Security Enhancement",IEEE Transactions On Information Forensics And Security, July 2014,Vol. 9, No. 7, 1179-1191

[9] Bian Yang , Christoph Busch , Koen de Groot , HaiyunXu and Raymond N. J. Veldhuis,"Performance Evaluation of Fusing Protected Fingerprint Minutiae Templates on the Decision Level", Sensors **2012**, 12, 5246-5272

[10] Amioy Kumar and Ajay kumar, "A Cell-Array-Based Multibiometric Cryptosystem", IEEE,2015,Vol.4,15-25

DOI10.17148/IJARCCE.2017.63232