iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** XII **Month of publication:** December 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Multibiometric Cryptosystem- Review

Shilpa Shrivastava[1], Sanjivani Shantaiya[2]
[1]M.Tech Student, DIMAT, CSVTU, Bhilai, [2]Professor, DIMAT, CSVTU, Bhilai

Abstract— Biometrics is the science of establishing the identity of an individual based on the physical or behavioural attributes of the person. A biometric system can be either an 'identification' system or a 'verification' system. Cryptography is very important for network security and features of a computer system. Biometric cryptosystems provides an innovative solution for cryptographic key generation, encryption as well as biometric template protection. Multibiometric cryptosystem offer higher authentication accuracy and flexibility. In this paper many techniques are surveyed for multibiometric cryptosystem, which provide security to the biometric data.

Keywords — Biometric, Biometric cryptosystem, Multibiometric cryptosystem, fusion, security.

I. INTRODUCTION

Biometrics is the science of establishing the identity of an individual based on the physical or behavioural attributes of the person. [1] Physiological aspect includes fingerprint, hand, iris, face and D.N.A and behavioural includes speech, keyboard typing, and signature. [2]

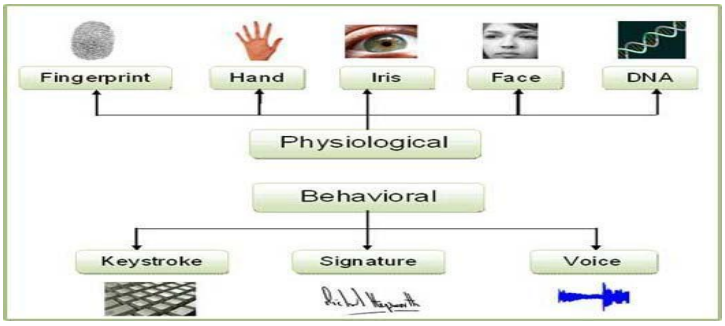


Fig. 1 Biometric Classification

A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

A. Identification

One to Many: Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database.

B. Verification

One to One: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

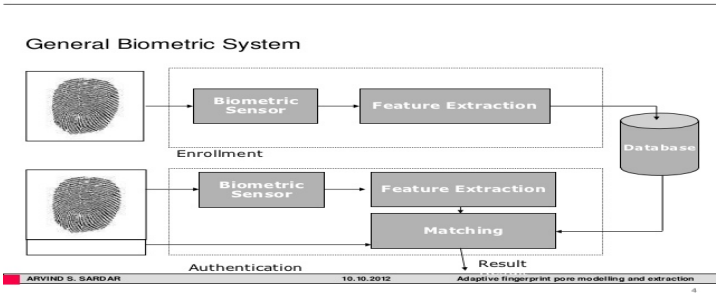


Fig. 2 Biometric System

Cryptography is very important for network security and features of a computer system. Cryptography comes from the Greek words

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

for "secret writing." Cryptography is the practice of secure data communication in the presence of third party. Cryptography encrypt the data at the transmitter end to protect it from stolen and from errors. [3].

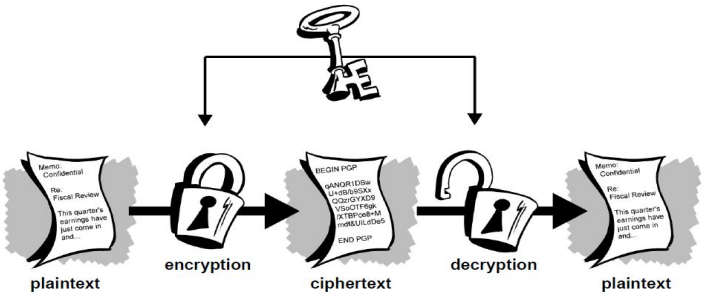


Fig. 3 Cryptography Example

Biometric cryptography is the combination of features of biometric as well as cryptography. Cryptography basically deals with keys that is public key and private key whereas biometric deals with physiological and behavioural characteristics of human being.

II. PROBLEM DYNAMIC

A. *Biometric Cryptosystem*

Biometric cryptosystems provide an innovative solution for cryptographic key generation, encryption as well as biometric template protection. In biometric cryptosystems, original templates are replaced by biometric-dependent information (referred to as helper data), which assists in recovering cryptographic keys. Matching is performed indirectly by verifying the validity of recovered keys. [4.] To derive the data biometric cryptosystem can be divided into two broad categories:

1) *Key-Binding Systems:* In this system binding of cryptographic key with a biometric template is done.
2) *Key-Generating Systems:* In this biometric template derives helper data and the cryptographic key is generated from the helper data and the biometric query.

B. *Multibiometric Cryptosystem*

Biometric system working on single biometric feature has certain limitations such as [5]

1) *Spoof Attack:* System gets fooled by fake biometric data.
2) *Data Sensed Error:* Captured data which contains some noise.
3) *Non Universality:* system may be able to read data from restricted people not from all.

The success of multibiometric cryptosystem is due to information fusion. Fusion can be done in following ways i.e. prior to matching and after matching.

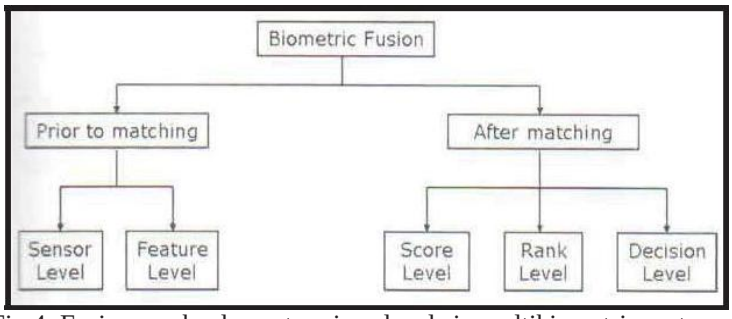


Fig 4: Fusion can be done at various levels in multibiometric systems

Multibiometric cryptosystem offer higher authentication accuracy and flexibility, wider population coverage and stronger security. Multibiometric cryptosystem can be classified into two categories based on different fusion modes:
Fusion at the feature level (also known as biometric level)
Fusion at the decision level (also known as cryptographic level)

III. SURVEY OF TECHNIQUES USED IN MULTIBIOMETRIC CRYPTOSYSTEM

Over the past several years, there have been a number of researches done dealing with the issues related to merging of biometrics into cryptosystems [1].

Chi Chen et al. [6] In this paper, An optional multi biometric cryptosystem based on fuzzy extractor and secret share technology is proposed. Each of the enrolled biometric modality generates a feature vector, and then the feature vector is put into a fuzzy extractor to get a stable codeword, namely a bit-string. All the code words are used to bind a random key based on a secret share method, and the key can be used to encrypt users' privacy data. During the verification phase, parts of the enrolled biometric modalities are enough to recover the random key. Therefore, the proposed scheme can provide a user the same biometric key on different devices.

Problem defined: Security and uncertainty (variation) in biometric data.

Method: Fuzzy (Commitment, vault, extractor) algorithm for biometric key generation.

End Discussion: The proposed scheme could recover a key with a subset of the enrolment traits. Experiment on a virtual multi-modal database shows the feasibility and efficiency. The virtual multi-biometric database shows that the novel concept of optional multi-biometric cryptosystem is better than the corresponding uni biometric cryptosystem both in matching accuracy and key entropy.

Madhavi et al. [7] A biometric is permanently associated with a user and cannot be changed. Hence, if a biometric identifier is compromised, it is lost forever and possibly for every application where the biometric is used. Moreover, if the same biometric is used in multiple applications, a user can potentially be tracked from one application to the next by cross-matching biometric databases. Biometrics also leaks personal information to the attacker. The stored biometric template attack is the most severe of all the attacks. Biometric templates cannot be reissued on spoofing. Therefore, apart from security; biometric templates should be imparted with revocability.

Problem defined: How to provide diversity, revocability, security and performance in single system?

Method: Extraction of Feature point from Fingerprint, Palm print, Iris and Retina has done by Feature Level Fusion, Random Tiling and Equal Probable 2^N Discretisation.

End Discussion: In this paper author has proposed a theoretical approach of biometric template protection method which is evaluated using multimodal biometrics – the fusion of fingerprint, palm print, iris and retina at feature level. Biometrics traits like iris and retina are internal parts of human and are less prone to damage. The evaluation of fusion models being developed for different fingerprint, palm print, iris and retina databases in terms of false accept rates, false reject rates and equal error rates under controlled and uncontrolled environments.

Manmohan Lakhera et al. [8] In this paper, a general architecture with the help of Digital Signature that guarantees privacy protection of biometric data. We specifically focus on secure a biometric data at the time of authentication and storage.

Problem defined: How to secure user's biometric data.

Method: Digital signature is used.

End Discussion: The author has proposed how to secure stored biometric data. We have specifically highlighted techniques that can secure biometric feature from attacker or unauthorized person. He has discussed the importance of public key cryptography and AES principles to enhance the confidentiality of biometric data. Security for stored biometrics may be used to protect the stored biometric data when the user's biometric data is compromised.

Eslam Hamouda et al.[9] In this paper, a novel method that employs Genetic Algorithm (GA) to generate a binarization scheme which used to transform the real-valued templates into robust binary ones. The main role of GA is to search for the optimal quantization and encoding parameters to generate the binarization scheme. Experiments were conducted with ORL face database for recognition. Our results demonstrated that binary templates achieved promising performance in terms of equal error rate for face recognition using a simple hamming distance classifier.

Problem defined: How to convert the real-valued templates into corresponding binary representation which retains the original information?

Method: Novel method is used by Genetic Algorithm and Quantization and Coding.

End Discussion: Experimental results with the generated binary encoded templates and a hamming distance classifier show superior performance in terms of equal error rate comparing to the real-valued templates. Moreover, the generated binary template is dramatically different from the original image, and it is impractical to reverse engineer to gain the original face image.

Bo Fu et al. [10] The basic concepts and methods on performance and effectiveness evaluations at the feature-level fusion model of multi-biometric encryption are concentrated on in this paper. From the cryptographic theory point of view, firstly, the formal

definitions related to multi-biometric cryptosystems are formulated. Under some extreme conditions, the security and privacy of multi-biometric cryptosystems at the feature level are analysed and rigorously proved. Finally, a close relationship between security and privacy and the fundamental trade-off between the accuracy and security are studied.

Problem defined: How to enhance the privacy in biometric recognition?

Method: Fuzzy vault framework is used in it. By using cancellable biometric which avoid storing the biometric data in clear Multibiometric cryptosystem based on feature level fusion.

End Discussion: In this paper, the author has investigated the basic feature level fusion model and its performance including the security, privacy, and accuracy. Moreover, we have not only showed the relationship between the security and privacy but also demonstrated how the security may be affected by the accuracy. We have presented the achievability proofs in this paper. The proposed methodologies may serve as guideline for designing application systems with the near optimal performance.

IV. CONCLUSIONS

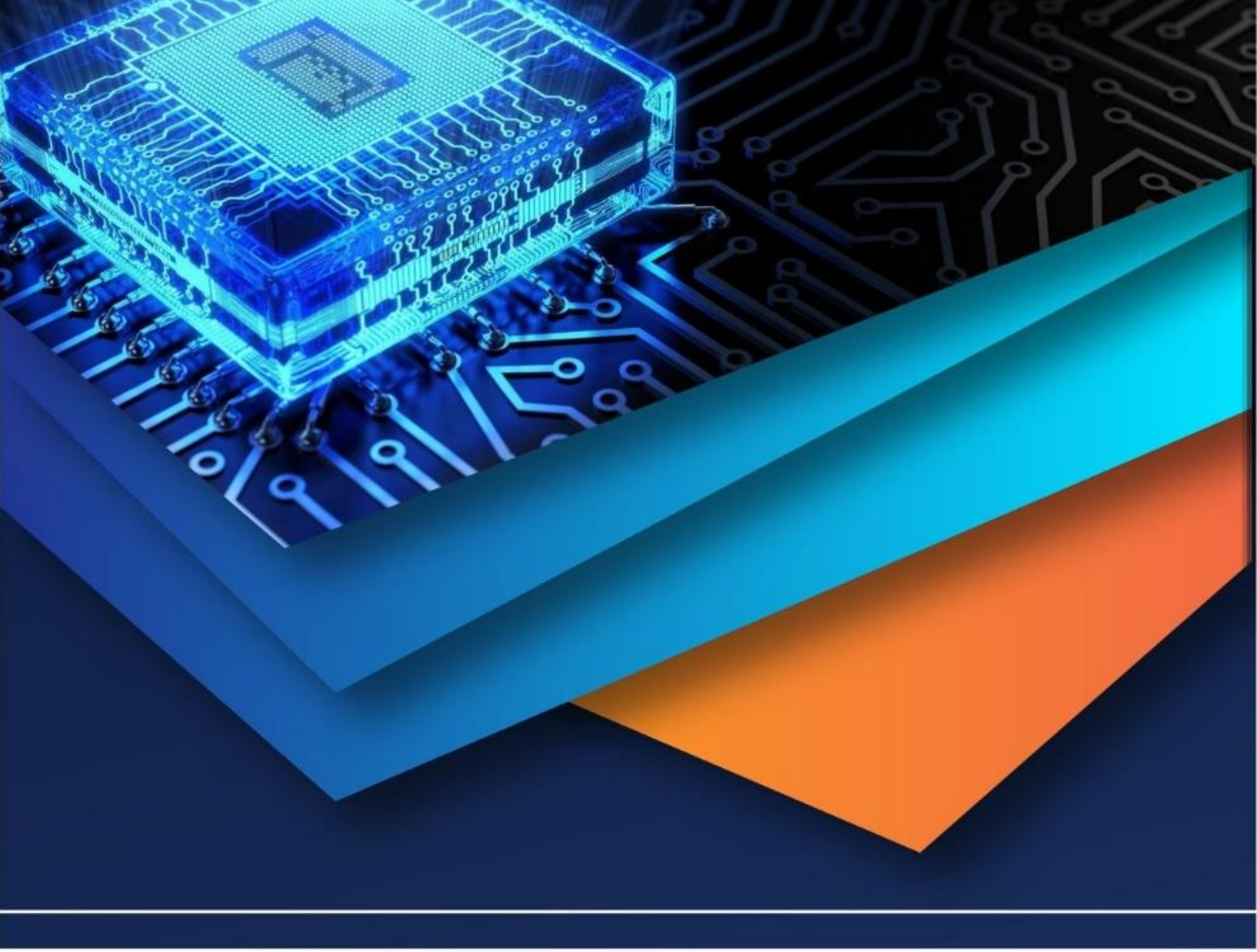
The virtual multibiometric database shows that the novel concept of optimal multibiometric cryptosystem is better than the corresponding unibiometric cryptosystem both n matching accuracy and key entropy. Some theoretical approach of biometric template protection method is evaluated using multimodal biometrics may be used to protect the stored biometric data when the user's biometric data is compromised, the basic feature level fusion model and its performance including the security, privacy and accuracy are investigated.

V. ACKNOWLEDGMENT

A large measure of any credit for the "Multibiometric Cryptosystem - Review" must go to our guide Mrs. Sanjivani Shantaiya, Prof who has assisted in the preparation of this paper. I admire her infinite patience and understanding that she guided me in the field I had no previous experience. I am grateful to her for having faith in me.

REFERENCES

[1] Jisha Nair.B.J. Ranjitha Kumari.S , A Review On Biometric Cryptosystems International Journal Of Latest Trends In Engineering And Technology (Ijltet) Vol. 6 Issue 1 September 2015.
[2] Bharti Kashyap, K.J. Satao, A Review on Multi-Biometric Cryptosystem for Information Security, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 5, May 2015.
[3] Pranab Garg, Jaswinder Singh Dilawari, A Review Paper on Cryptography and Significance of Key Length, International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012
[4] Cai Li, Jiankun Hu, Josef Pieprzyk, Willy Susilo, A New Bio-cryptosystem-oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion, 2015 IEEE.
[5] T.S. Sasikala, Dr. J. Jeya A Celin, Enhancement of Security Using Multimodal Biometrics, International Conference on Circuit, Power and Computing Technologies [ICCPCT] , 2014.
[6] Chi Chen, Chaogang Wang, Tengfei Yang, Song Wang, Jiankun Hu, Optional Multi-biometric Cryptosystem Based on Fuzzy Extractor, International Conference On Fuzzy System And Knowledge Discovery, IEEE 2014.
[7] Madhavi Gudavalli, S.Viswanadha Raju, K S M V KUMAR, A Template Protection Scheme for Multimodal Biometric System with Fingerprint, Palmprint, Iris and Retinal Traits, CUBE, Pune, India 2012.
[8] Manmohan Lakhera, Enhancing security of stored biometric data, International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with their Impact on Humanity (CIPECH14) 28 & 29 November 2014
[9] Eslam Hamouda, Xiaohui Yuan†, Osama Ouda Taher Hamza , and Lei Chen, Binary biometric template generation towards security and class separability, 5th ICCCNT, Hefei, China 2014.
[10] Bo Fu, Jie Lin and Guiduo Duan, Analysis of Multi biometric Encryption at Feature level Fusion, Proceedings of the 10th World Congress on Intelligent Control and Automation , Beijing, China , July 6-8, 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY