International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.6, Nov-Dec. 2012 pp-4643-4647 ISSN: 2249-6645

Feature Level Fusion of Multibiometric Cryptosystem in Distributed System

N. Geethanjali [1], Assistant.Prof. K.Thamaraiselvi [2], R. Priyadharshini[3]
[1, 2, 3] *Department of Information Technology, SNS College of Technology, INDIA.*

ABSTRACT: *Multibiometrics is the combination of one or more biometrics (e.g., Fingerprint, Iris, and Face). Researchers are focusing on how to provide security to the system, the template which was generated from the biometric need to be protected. The problems of unimodal biometrics are solved by multibiometrics. The main objective is to provide a security to the biometric template by generating a secure sketch by making use of multibiometric cryptosystem and which is stored in a database. Once the biometric template is stolen it becomes a serious issue for the security of the system and also for user privacy. In the existing approach, feature level fusion is used to combine the features securely with well-known biometric cryptosystems namely fuzzy vault and fuzzy commitment. The drawbacks of existing system include accuracy of the biometric need to be improved and the noises in the biometrics also need to be reduced. The proposed work is to enhance the security using multibiometric cryptosystem in distributed system applications like e-commerce transactions, e-banking and ATM.*

Keywords: *Biometric Cryptosystem, Error correcting code, Fingerprint, Iris, Multibiometrics, Unimodal biometrics.*

I. INTRODUCTION

The term "biometrics" is derived from the Greek words "Bio" (life) and "Metrics"(to measure). Biometrics refers to the physiological or behavioural characteristics of a person to authenticate his/her identity [1] [2]. Biometric system is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological or/and behavioural characteristics possessed by the person. Physiological biometrics also known as physical biometrics or static biometrics is based on data derived from the measurement of a part of an individual's anatomy. It includes fingerprint recognition, Iris scan, Retina scan, Hand Geometry; Palm print, Face recognition, DNA and Vascular Pattern Recognition. Among all fingerprint recognition is the olden technology.

Behavioural biometrics also known as dynamic biometrics is based on data derived from measurements of an action performed by an individual and distinctively incorporating time as a metric; the measures action has a beginning, middle and end. It includes Signature, Keystroke, Handwriting, Voice recognition and Gait. Soft biometrics is a human characteristic that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals. Examples of soft biometrics include scars, marks and tattoos, color of sys and hair color [3]. Trustable authentication plays an important role in secure communication systems. Traditionally, passwords (knowledge-based security) and smartcards (token-based security) are used as the first step towards identity proof in the system. However, security can be breached since dynamic passwords are easily divulged and guessed by means of social engineering or by dictionary attacks. Token-based authentication may in pat compensate the limitation of knowledge-based authentication; however, it is not reliable and easily stolen. If passwords and smartcards are shared or stolen form of an individual authentication based on the certain physiological or behavioural traits associated with the individual, overcomes the disadvantages of passwords and smartcards, but it is known that the sensed single biometric data is always noisy and distorted.

Multibiometrics overcomes the limitations imposed by unimodal biometrics by using multiple biometric modalities [4]. These systems are expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence. Multibiometric systems address the problem of non-universality and provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. The variety of factors should be considered when designing a multibiometric system. These include the choice and number of biometric traits; the level in the biometric system at which information provided by multiple traits should be integrated.

II. PROBLEM DEFINITION

If an attacker can hack into a biometric database, he can easily obtain the stored biometric information of a user. Biometric information can be used to gain unauthorized access to the system by either reverse engineering the template to create a physical spoof or replaying the stolen template. Biometric template information for unintended purposes (e.g., covertly track a user across different applications by cross-matching the templates from the associated databases) leading to violation of user privacy. The challenge in designing a biometric template protection scheme [15] is to overcome the large intra user variability among multiple acquisitions of the same biometric trait.

III. LITERATURE SURVEY

The earlier work in the fingerprint recognition was done by Moses and Ignatius [16]. They have used the fingerprint recognition in ATM for security purpose. Minutiae based technique was introduced by Jain et.al [17] presented among current fingerprint matching algorithms like minutiae based matching, correlation filters based matching, transform feature based matching, graph based matching and generic algorithm based matching; minutiae based fingerprint matching is

dominant. Abhishek and K.Jain provided security to the biometric template using biometric template using biometric cryptosystem and feature level fusion is used to combine multibiometrics [5]. To overcome the cancelable biometrics, by not storing the original template in the database is given by N.K.Ratna [6]. The biometrics authentication systems are done with two stages of enrollment and authentication. The problems of hacking a biometric template and usage of ECC (Error Correcting Code) and feature extraction of Iris biometrics is given by Emanuele and Chiara [7].Multibiometrics can be applied to distributed system using biometric cryptosystem is given by Manish et.Al [18].

IV. ENROLLMENT AND VERIFICATION OF UNIMODAL BIOMETRICS

Unimodal biometrics makes use of single source of biometrics for personal identification. The biometrics which is taken under consideration is fingerprint biometrics [14]. The biometric system 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 [15] and minutiae extraction is done with ridge endings and ridge bifurcations.

In the enrollment stage, the fingerprint images were collected using optical fingerprint sensor. Once fingerprint is acquired, next stage is to preprocess the fingerprint and to extract the feature using minutiae extraction and it is stored in the database. In authentication stage, the fingerprint query is given which undergoes image segmentation, image binarization and image minutiae shown in figure1, which either accepts or rejects the user's identity by matching against an existing fingerprint database.

1. Image Segmentation

The original image is given and the image undergoes image segmentation [13]. The fingerprint enhancement algorithm is image segmentation. Segmentation is the process of partitioning a digital image into multiple segments and typically used to locate objects and boundaries in images. In segmentation only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information.

2. Image Binarization

After performing segmentation the noisy area will be removed. In the image binarization, the gray scale image is transformed into a binary image by computing the mean value of each 32-by-32 input block matrix and transferring the pixel value to 1 if larger than the mean or to 0 if smaller. This improves the contrast between the ridges and valleys in a fingerprint image and consequently facilitates the extraction of minutiae.

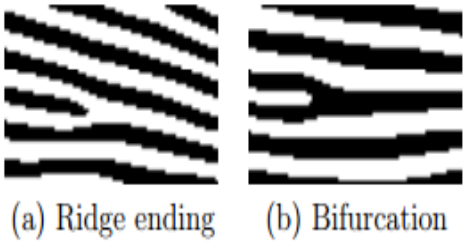


Fig.1 Ridge ending and bifurcation

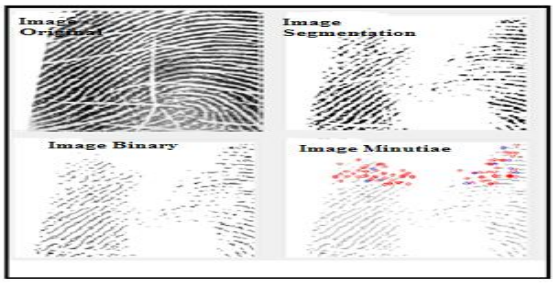


Fig.2 Fingerprint Feature Extraction

3. Image Minutiae

Most minutiae extraction algorithms operate on binary images where the black pixels that represent ridges, and the white pixels that represent valleys. Minutiae-based fingerprint representation [11] can also assist privacy issues since one cannot reconstruct the original image from using only minutiae information. The minutiae are relatively stable and robust to contrast; image resolutions and global distortion are compared to other fingerprint representations. Two fingerprint match if their minutiae points match. Most minutiae extraction algorithms operate on binary images where the black pixels that represent ridges, and the white pixels that represent valleys.

V. FEATURE LEVEL FUSION USING MULTIBIOMETRICS

Multibiometrics is a combination of one or more biometrics, which is taken into consideration in this paper are fingerprint and Iris. Using feature level fusion the features are extracted separately and combined into a single biometric feature set. Instead of storing the original template in the database, secure sketch is generated and stored in the database to provide protection to the template [8], which is achieved by two well known biometric cryptosystem fuzzy vault and fuzzy commitment.

The most important thing in an information fusion system is to determine the type of information that should be consolidated by the fusion module [19]. In feature level fusion which is shown in figure 3, the data or feature set originating from multiple sensors are first pre-processed and features are extracted separately from each sensor, form a feature vector. These features are then concatenated to form a single new vector. Feature level fusion can use same feature extraction algorithm or different feature extraction algorithm on different modalities whose feature has to be fused. The composite feature vector is then used for classification process. The fingerprint features are extracted using fingerprint minutiae and iris

features are extracted using binary strings. The fingerprint image will undergo processes of image segmentation, filtering of image using Gabor filter, noise removal and image binarization to extract the fingerprint features. Likewise the iris image will undergo processes of image segmentation, filtering of image using Gabor filter and at last the iris binary vector is obtained is shown in figure 5.

The templates which are extracted separately are fused with the random key which is given as input using ECC and stored in the database. In the verification stage, the fused single vector is compared with the vector which is stored in the database and key is regenerated. If the key which is not public matches, then the user is valid or it is decided that user is invalid.

Matching performance of a biometric system is measured with the help of false acceptance rate (FAR) and genuine acceptance rate (GAR). The biometric cryptosystem fuzzy vault and fuzzy commitment do not generate revocable templates. The step by step process followed to extract features from the biometrics is shown in figure 4, to achieve the goal of providing accuracy and security is given by:

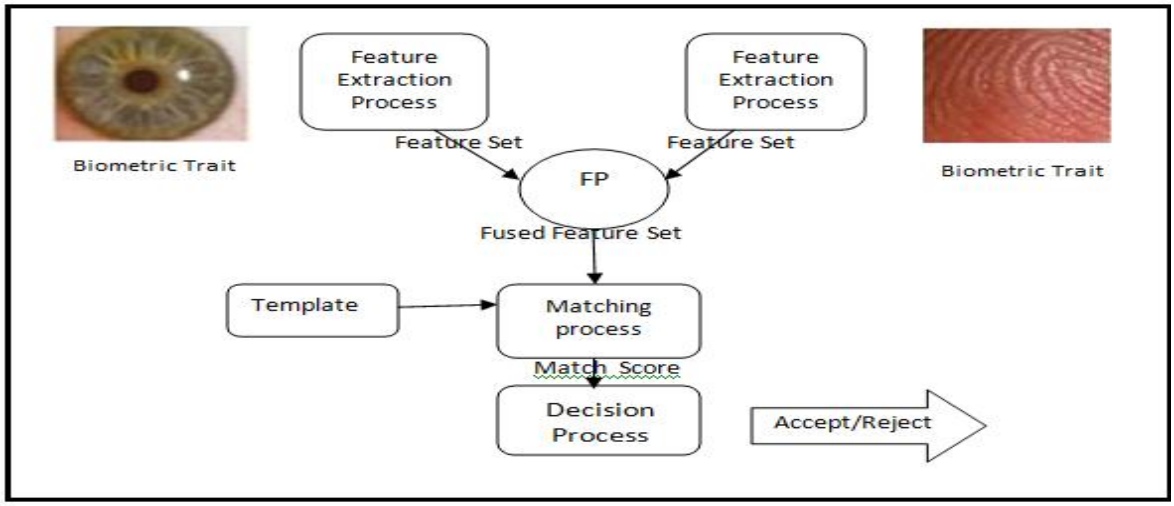


Fig.3 Feature Level Fusion

Data Acquisition – Images are collected using sensor. The optical sensors are most popular and are inexpensive.
Pre-processing - Tasks like image alignment or region of interest (ROI) identification take place in pre-processing.
Feature Extraction – To extract the features from the segmented image, resulting in a feature vector.
Feature Vector Binarization – To generate a binary string b of length T represents the feature vector. Additional information about interval boundaries is necessary.
ECC - In the enrollment stage, an error correcting code (ECC) is applied to b, to extract a set of parity-check bits. In the verification stage, the new binary feature vector b' is considered as a noisy version of the enrolled one. The stored parity-check bits are used to attempt the correction of b'.
XOR- In order to provide the system with revocable templates, this module computes bitwise exclusive OR between a binary feature vector and a randomly generated binary string b.

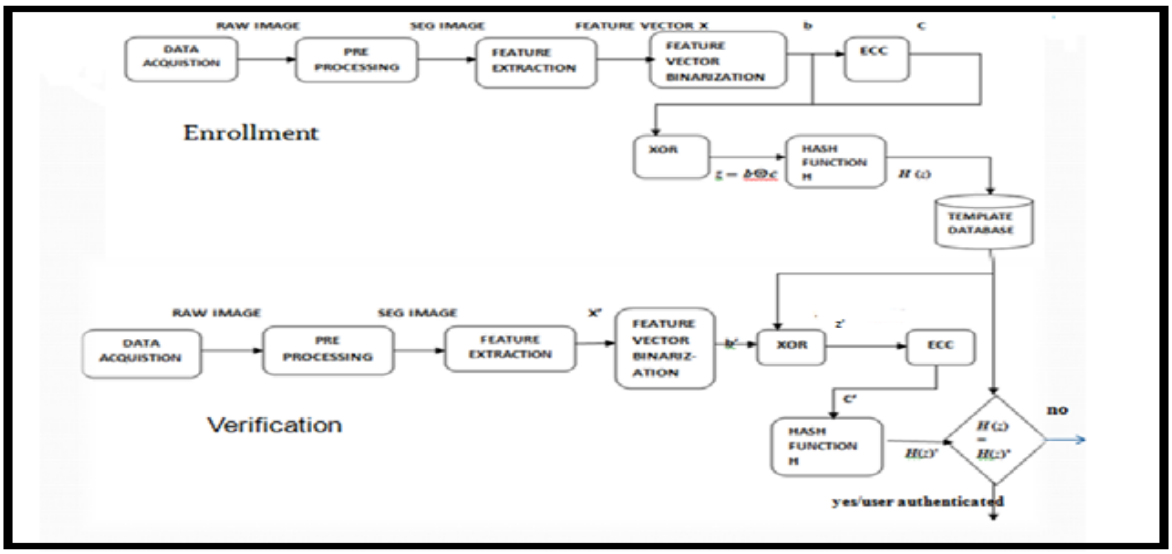
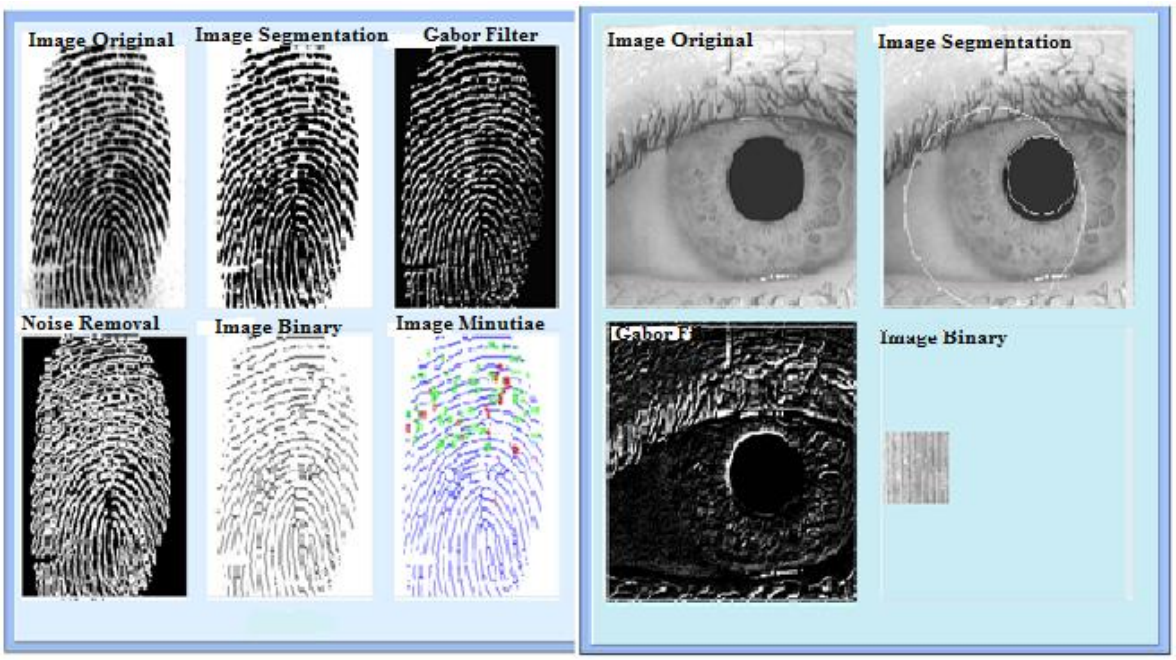


Fig.4 Block Diagram for Feature Level Fusion using Multibiometric Cryptosystem



a) Fingerprint Feature Extraction b) Iris Feature Extraction

Fig.5 Level By Level Feature Extraction of Fingerprint and Iris

Hash Function – When an individual is enrolled in the system, a hash function H, is applied to z= c ⊕ b. The output is stored in the system database, ensuring the privacy of b. In the verification stage, H is applied to corrected binary string z'= c ⊕ b", so that the output can be corrected to the stored hash.

Decision – If the stored hash H(z) and H(z') matches, then the user is successfully verified and the key will be regenerated, which is responsible for decision making.

VI. BIOMETRIC CRYPTOSYSTEM IN DISTRIBUTED SYSTEM

In distributed system, multibiometrics is used to provide security to the system and biometric cryptosystem for providing protection to the templates. ATM system is designed and users register their details and face image is captured and encrypted and stored in the binary format in the database and using feature level fusion fingerprint and iris templates are fused and stored in database. Fuzzy vault and fuzzy commitment build the biometric cryptosystem [10]. They do not generate revocable templates. Fuzzy Commitment is a biometric system that can be used to secure biometric traits represented in the form of binary vectors and fuzzy vault is represented in the form of point set.

1. Fuzzy Vault and Fuzzy Commitment

In fuzzy vault encoder, the biometric template will be given along with random secret key which is converted to a polynomial degree and polynomial is evaluated in a graph. The set of points is then secured by hiding them with chaff points [9]. The set of genuine points along with polynomial evaluations together with chaff points constitute the sketch or vault. In fuzzy vault decoder, the biometric will be given and then by using the filter the vault points and the query are compared. If the biometric query set is sufficiently close to many genuine points and it can be correctly identified and polynomial is reconstructed successfully and key is generated which is used for validity check. In multibiometric vault the feature level fusion is used to combine the biometrics and then fuzzy vault scheme is addressed.

Fuzzy commitment is represented in the form of binary vectors. The binary string is divided into a number of segments and each segment is separately secured using a fuzzy commitment scheme [12]. The keys associated with these segment wise fuzzy commitment schemes are then used as additional points in the fuzzy vault constructed using the point-set based features.

VII. CONCLUSION

Biometrics is not only a fascinating pattern recognition research problem but, if carefully used, could also be an embedding technology with the potential to make our society safer, reduce fraud and lead to user convenience. The proposed methodology presented here provides security to the distributed system and feature level fusion framework is provided. Likewise, it cannot be guessed it out how many biometrics is used and what type of biometrics are used. As secure sketch is generated from the template and stored in the database, the hackers cannot be able to use the template, unless and until they know the secret key. In future, the work is to overcome the failure of biometrics, which can be addressed by using multimodal model which gain the advantage of other biometrics in case of failure of one biometrics.

REFERENCES

[1] A.Ross , K.Nandakumar and A.K. Jain, "Handbook of Multibiometrics*",* New York: Springer,2006.
[2] Jain A.K, Ross A. and Prabhakar S, IEEE Transactions on Circuits and Systems for Video Technology,14, 4-20, 2009.
[3] Jain A.K, Dass SC and Nandakumar K, "Soft Biometric Traits for Personal Recognition Systems". Proc of International Conference on Biometric Authentication, Hong Kong: 731-738, 2004.
[4] Brunelli, R., and Falavigna, D. "Person Identification Using Multiple Cues", IEEE Trans. on Pattern Analysis and Machine Intelligence (Oct. 1995). IEEE, NY, 955–966.
[5] Abhishek Nagar, Karthik Nandakumar and AnilK. Jain, "Multibiometric Cryptosystems Based on Feature-Level Fusion", IEEE transactions on information forensics and security, vol. 7, no. 1255-268, 2012
[6] N. K. Ratha, S. Chikkerur, J. H. Connell, and R.M. Bolle, "Generating Cancelable Fingerprint Templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–572, Apr. 2007.
[7] Emanuele Maiorana, Chiara Ercole, "Secure Biometric Authentication System Architecture using Error Correcting Codes and Distributed Cryptography", 2007.
[8] A. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security," *EURASIP J. Adv. Signal Process.*, 2008.
[9] K. Nandakumar 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.
[10] A. Nagar, K. Nandakumar, and A. K. Jain, "Adapting Biometric Representations For Cryptosystems" Department of Computer Science and Engineering, Michigan State University,2011.
[11] Raymond Thai, "Fingerprint Image Enhancement and Minutiae Extraction", 2003.
[12] Juels and Wattenberg, "A Fuzzy Commitment Scheme", in proc, 6th ACM conf, Computer and Communication Security, 1999.
[13] Sangram Bana and Dr.Davinder Kaur, "Fingerprint Recognition using Image Segmentation", IJAEST, Volume no.5, 012-023, 2011.
[14] Ing. Martin Drahansky, "Biometric Security Systems Fingerprint Recognition Technology", 2005.
[15] D. Maltoni, D. Maio, A.K.Jain and S.Prabhakar, "Handbook of Fingerprint Recognition" , Springer, Berlin, Germany,2003.
[16] Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani, " ATM Security Using Fingerprint Biometric Identifier: An Investigate Study", IJACSA Vol.3,No.4,2012.
[17] Jain et.al. "On-line Fingerprint Verification", IEEE Transactions on Pattern Analysis.
[18] Manish Manoria , Ajit Kumar, Satyendra Singh and Debu Sinha, " Secure Biometric Cryptosystem for Distributed System", IJCNS, Vol 1, 2011.
[19] Mini Singh Ahuja and Sumit Chabbra, " A Survey of Multimodal Biometrics", IJCSA,2250-3765,2011.