Multi-Biometric Cryptosystem using the Features of Fingerprint and Palmprint for Securing Biometric Templates

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

Abstract— – Securing the privacy of biometric data has become a critical issue. This paper gives a multi biometrics cryptosystem that combines features of fingerprint and palmprint to overcome several drawbacks of uni biometrics cryptosystem. Preprocessing is a soul of an image processing in which feature enhancement is first step, in this system feature enhancement of input image that is fingerprint and palmprint are performed by applying a series of preprocessing techniques. Gaussian filter is used to independently extract a fingerprint feature which provides accuracy. Then we have extracted the features of both fingerprint and palmprint, in the later step the resultant images are combined in feature level fusion method using fuzzy commitment. After that codeword is generated with the help of Hamming Distance codeword generation method and then hashing is done with the help of MD5 algorithm which generates key. This key is stored and prior matching of the templates is done. We conclude that proposed methodology has better performance as compared to uni biometric cryptosystem approaches using individually only a fingerprint or a palmprint. The multiple biometrics helps to reduce the system error rate.

Key words: Biometric, Multi-biometric, Cryptosystem, Security, Features

I. INTRODUCTION

Human identification is one of the most important tasks when it comes to provide security. In earlier days identification system uses are token based system or knowledge based system. In token based system passports, keys, ID cards etc. Are used whereas knowledge based system uses password which is a combination of different words. But this token based and knowledge based system faces many problems such as password can be guessed, keys can be stolen hence they could not provide proper protection where higher level of security is needed [1] [2]. Biometrics is the science of establishing the identity of an individual based on the physical or behavioral attributes of the person.

Physiological aspect includes fingerprint, palmprint, hand, iris, face and D.N.A and behavioral includes speech, keyboard typing, and signature [3].

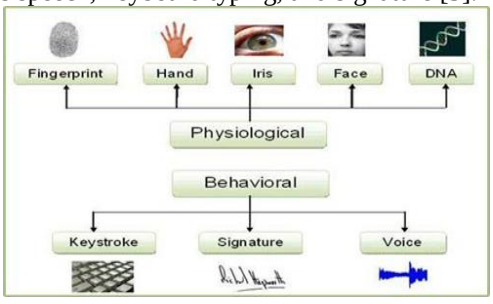


Fig. 1: Biometric Classification

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.

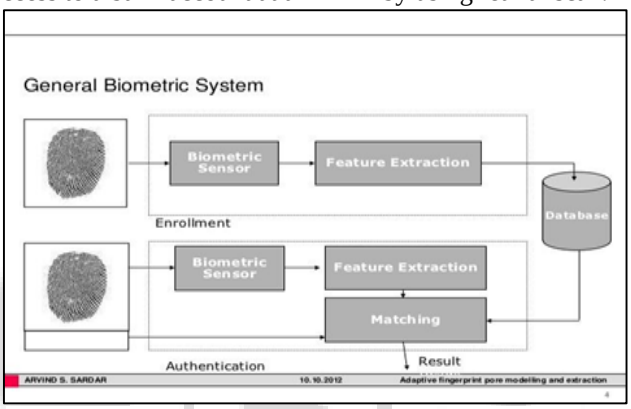


Fig. 2: Biometric System

Cryptography is the art of obtaining security by encoding message to make them unreadable. It is a technique in which plan text or clear text is converted into cipher text or non-readable text. The basic two techniques which are used to convert plain text into cipher text are Substitution technique and Transposition technique [4].

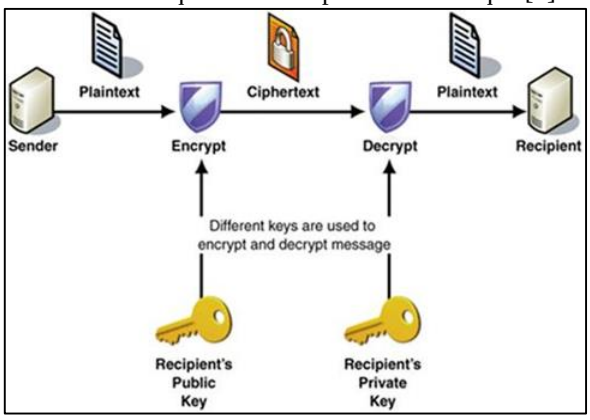


Fig. 3: Cryptography Example

The paper is organized as follows. Introduction section is followed by problem dynamics in which we define what problem we are dealing with. Next to that, we have included methodology section in which we will show which methodology we are using to reach our goals. After that result and discussion section is there in which we have discussed about our result and finally we have concluded with the limitation of work and future scope.

II. PROBLEM DYNAMICS

A. Biometric Cryptosystem:

The Biometric identification or recognition is basically based on the automatically identification or recognition of any individual on the basis of their physical and behavioral characteristics [5][6]. Though biometric recognition can authenticate, identify and provide privacy but this only cannot provide the level of security. 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. From Biometric encryption or Biometric cryptosystem which involves generation and binding of secrete keys from biometric data, key and biometric cannot be retrieved from the stored template only the proper and correct live sample is presented [7]. Up till now we were discussing about Biometric cryptosystem that too single but in the next section we will deal with Multibiometric Cryptosystem.

B. Multibiometric Cryptosystem:

Template security in Multibiometric cryptosystem is more critical than in single Biometric because it is easy to collect single biometric template of a single user than to collect multiple template of the same user [8].A Multi Biometric system is a biometric system that uses more than one biometric identifier like a combination of face, fingerprint, palmprint, iris, ear etc. In making a decision about personal identification. Multimodal biometrics systems are expected to be more reliable due to the presence of multiple traits. In this paper we are dealing with fingerprint and palmprint as a multibiometric and providing security to the templates of the same.

C. Fusion Based on Feature Level:

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 [2].

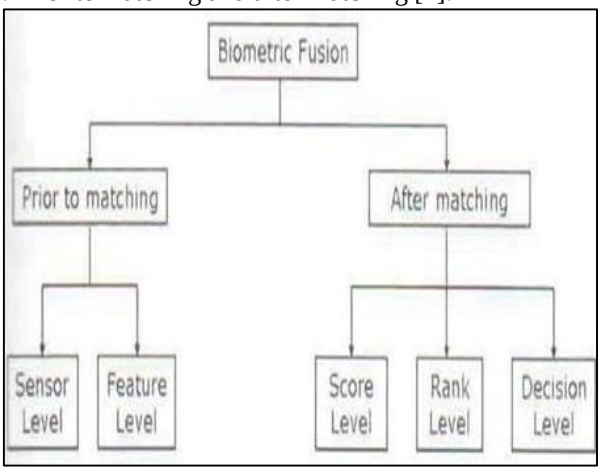


Fig. 4: Fusion can be done at various levels in multibiometric systems.

D. Fuzzy Commitment:

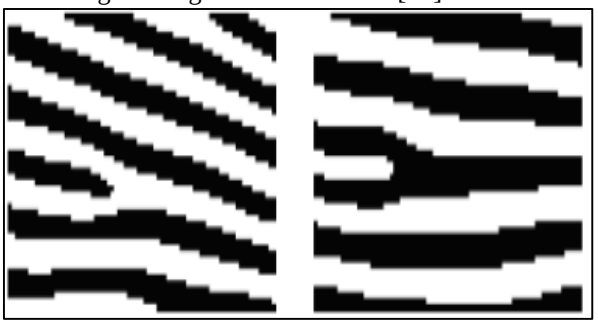
The feature level fusion framework can be implemented by the use of two famous Biometric Cryptosystem Fuzzy Vault and Fuzzy Commitment. The fuzzy commitment scheme assumes a binary string representation, where the difference between template and query is measured in terms of the hamming distance. To decode a fuzzy commitment sketch, one has to calculate the bits in binary templates [9].

III. METHODOLOGY

Extraction of feature point from Fingerprint and palmprint

A. Fingerprint:

A fingerprint is defined as a unique Pattern of ridge and valley on the surface of a finger of any person. A ridge can be defined as a single curved segment, whereas valley is dependent on ridge as it is the region between two adjacent ridges. Minutiae points are basically known as the local ridge discontinuities, hence the two types of which are as follows: ridge endings and bifurcations [10].



(a) (b)

Fig. 5: Minutiae Points (a) ridge ending (b) bifurcation

1) Fingerprint Features:

In our system we have calculated two basic features of finger which is known as ridge and bifurcation. As we know ridge is a single curve segment whereas bifurcations are points at which single ridge splits into two ridges.

2) What is fingerprint Recognition:

The fingerprint recognition problem can be categorized into three types: fingerprint enrollment, verification and fingerprint identification. Verification is used for positive recognition; it is the process that aim is to prevent multiple people from using the same identity. Fingerprint verification is to verify the authenticity of one -person by his fingerprint. There is one-to-one comparison in this case. In identification the system acknowledge an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one to-many comparison to establish an individual's identity [11].

3) Minutiae Extraction:

In all the fingerprint features, minutiae point features with respect to orientation maps are unique enough to differentiate amongst fingerprints robustly; the minutiae feature representation reduces the complex fingerprint recognition problem to a point pattern matching problem.

There are a lot of minutiae extraction methods available in the literature. We can classify these methods broadly into two categories (fig. 6):

- Those that work on binarized fingerprint images
- Those that work directly on gray-scale fingerprint images.

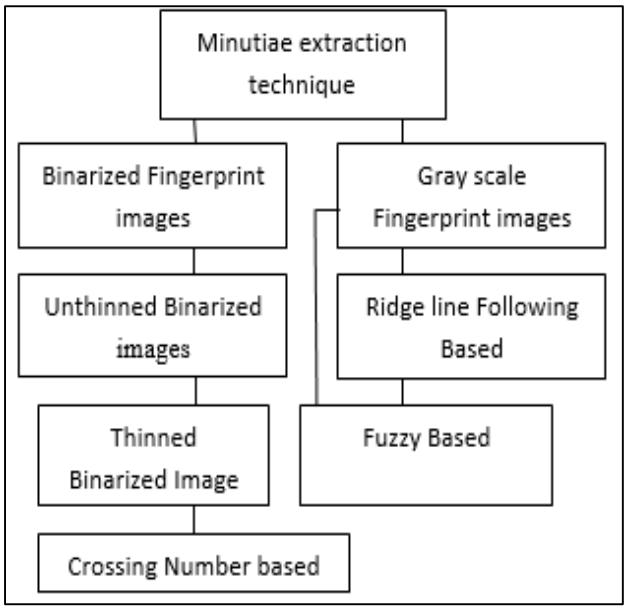


Fig. 6: Classification of Minutiae Extraction Techniques [10]

Here we are dealing with binarized fingerprint images.

The thinning algorithm removes pixels from ridges until the ridges are one pixel wide. Then the minutiae are extracted from the enhanced, binarized and thinned image.

Following the extraction of minutiae, a final image post processing stage is performed to eliminate false minutiae.

Most of the techniques in this category are based on the concept of crossing number.

3.1) Crossing Number: Crossing Number (CN) concept is the most commonly employed method of minutiae extraction [12].

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Fig. 7: 3×3 neighborhood

This method uses the skeleton image where the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3X3 window (fig. 7). The CN value is then computed as follows:

$$CN = 0.5 \sum |Pi - Pi+1| \qquad (1.1)$$

Where, P9=P1. It is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood. Using the properties of the CN as shown in fig. 8, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point.

CN	Property
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

Fig. 8: Properties of crossing number

B. Palmprint:

Palmprints are being used for recognition in a number of applications. Using Fingerprint fused with palmprint helps in increasing the robustness of the system.

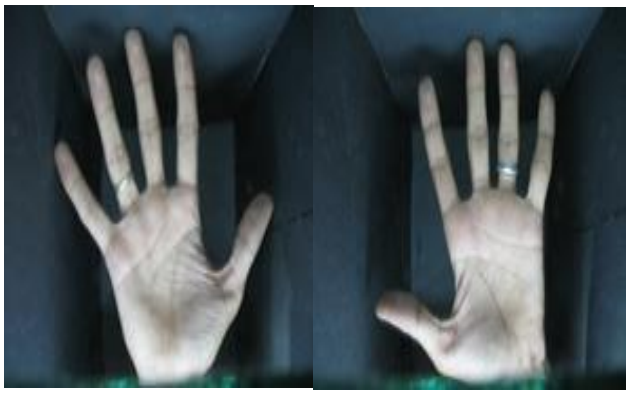


Fig. 9: Palm print images (IIT Delhi)

1) Palmprint Recognition:

In this paper, we have proposed a very simple entropy based method for the recognition based on palm print and also calculated number of edges.

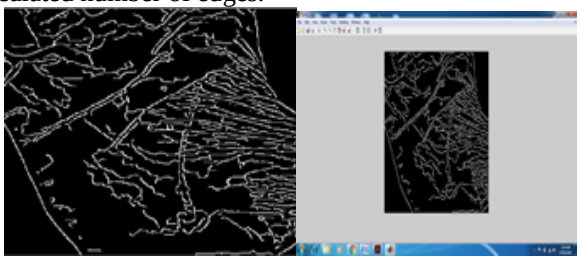


Fig. 10: Number of edges calculated from the templates.

Entropy is the measure of the average uncertainty. Image entropy is a quantity which is used to describe the 'business' of an image, i.e. The amount of information which must be coded for by a compression algorithm. Low entropy images have very little contrast and large runs of pixels with the same or similar values. An image that is perfectly flat will have entropy of zero. On the other hand, high entropy images have a great deal of contrast from one pixel to the next. Formula used to determine entropy is given below: [13].

$$E = -\text{sum}(p.*\log2(p)) \qquad (2.1)$$

Another feature which has been extracted is mean and standard deviation in variance. Variance is the expectation of the squared deviation of a random variable from its mean, and it informally measures how far a set of (random) numbers are spread out from their mean.

The variance of a set of n equally likely values can be written as

$$\mathrm{Var}(X) = \frac{1}{n}\sum_{i=1}^{n}(x_i - \mu)^2. \qquad (2.2)$$

Where is the expected value, i.e.

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i \qquad (2.3)$$

IV. PROPOSED MULTI BIOMETRIC CRYPTOSYSTEM

As we know multibiometric system is a collection of one or more biometrics, which is taken as a reflection in this paper we use fingerprint and palm print. In any system to be made a process flow diagram is must to represent in which manner work is done [14].

The proposed multibiometric cryptosystem is composed of following stages:

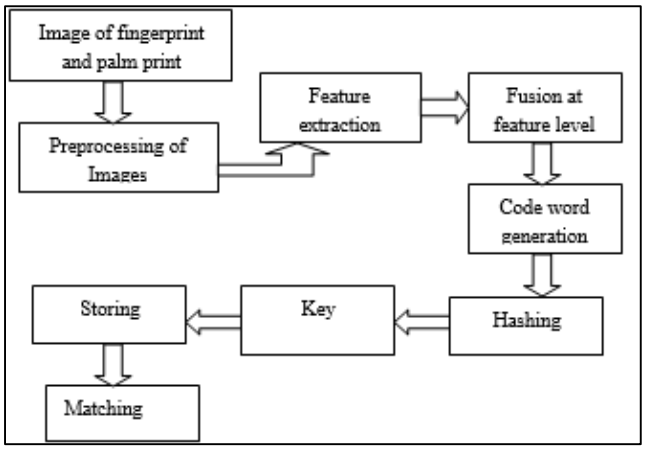


Fig. 11: Process Flow Diagram

A. Preprocessing:

After the images are captured, a Region of Interest (ROI) has to be calculated from the original image before feature extraction. In this part only filter is applied over the samples to remove noise from the images.

B. Feature Extraction:

In this section, after the preprocessing part is done features are extracted from the data. As in our piece of work we have calculated ridges and bifurcation of fingerprint, entropy and number of edges in palm print as features.

C. Fusion based on Feature Level:

Fusion is the process of mixing two or more different entities as a whole new entity. Fusion can be done in following ways i.e. Prior to matching and after matching. We have dealt with feature level fusion which is done prior to matching with the help of fuzzy commitment.

D. Codeword Generation:

Codeword is generated with the use of Hamming Distance algorithm.

E. Hashing:

Key is generated with the help of Message Digest 5 hashing technique.

F. Storing:

The templates are stored during the registration phase, which are later used in the process of matching for authentication purpose.

G. Matching:

When the data is stored during the registration phase, the template is matched with the stored data for the authentication purpose. For matching the identity of an individual this verification process is done to provide authenticity to the user

V. Result and Discussion

To examine the effectiveness of the proposed method, the performance is measured in the following manner such as sensitivity, specificity and accuracy. These are used to evaluate the multibiometric detection. [15]

A. Sensitivity:

Sensitivity is defined as true positive rate or the recall rate to measure the proportion of actual positives.

$$\text{Sensitivity} = TP/(TP+FN) \quad (3.1)$$

Where, TP- True Positive and TN- True Negative

B. Specificity:

Specificity measures the proportion of negatives, which are correctly identified such as the percentage of people who are correctly identified as authorized person.

$$\text{Specificity} = TN/(FP+TN) \quad (3.2)$$

Where, TP- True Positive, FP- False Positive and TN- True Negative

C. Accuracy:

Accuracy is the measurement system, which measure the degree of closeness of measurement between the original value and the retrieved value.

$$\text{Accuracy} = TP+TN/\ TP+FP+TN+FN \quad (3.3)$$

Where, TP- True Positive, TN- True Negative, FP- False positive and FN- False Negative.

Biometric Traits	Finger Print	Palm Print	Fingerprint + Palmprint
Accuracy	0.8521	0.8947	0.9474
Sensitivity	0.8889	0.5000	0.9000
Specificity	0.8000	1.0000	1.0000

Table 1: Performance of the system

The experiment result is measured in terms of matching accuracy. The matching accuracy is measured is rated by the distribution of FRR and FAR of the proposed method [16].

- False Acceptance Rate (FAR) = the false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.
- False Rejection Rate (FAR) = the false rejection rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an unauthorized user.

Rates	Finger Print	Palm Print	Fingerprint+ Palmprint
FAR	15.7%	10.5%	5.2%
FRR	52.6%	78.9%	47.3%

Table 2: Acceptance rejection result

VI. Conclusion and Future Work

A Multibiometric cryptosystem based on the integration of fingerprint and palmprint at feature level extraction using fuzzy commitment has been presented. These two traits are the most widely accepted biometrics in most of the application around. In this system we have used fuzzy commitment for fusion, Hamming distance for code generation and Message Digest 5 for hashing and generation of key or to provide security in terms of cryptography. So, as far as results are concerned we can clearly see from the accuracy, FAR, FRR that using single biometric rather than multibiometric cannot give you higher accuracy and required FAR and FRR. So, it is better to use Multibiometric rather than single biometric to provide proper accuracy and security to the system.

In Future, we would try to implement the system which will provide accuracy more than 95% and would take more different biometric templates as well like face, ear, knuckle etc.

REFERENCES

[1] T.S.Sasikala and Dr.J.Jeya A Celin."Enhancement of Security Using Multimodal Biometrics" International Conference on Circuit, Power and Computing Technologies [ICCPCT] 2014.
[2] Jisha Nair.B.J. and Ranjitha Kumari.S. "A Review On Biometric Cryptosystems" International Journal Of Latest Trends In Engineering And Technology (Ijltet) Vol. 6 Issue 1 September 2015.
[3] Bharti Kashyap and K.J. H 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.
[4] Pranab Garg and 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.
[5] K. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. On Circuits and Systems from Video Technology, Vol. 14, No. 1,pp4-19, Jan. 2004
[6] 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.
[7] A. Cavoukian and A. Stoianov, "Biometric Encryption: a Positivesum Technology That Achieves Strong Authentication, Security and Privacy", Information and Privacy Commissioner, Ontario, Tech. Rep. Mar. 2007.
[8] Madhavi Gudavalli, S.Viswanadha Raju, and K S M V Kumar, A Template Protection Scheme for Multimodal Biometric System with Fingerprint, Palmprint, Iris and Retinal Traits, CUBE, Pune, India 2012
[9] Abhishek Nagar, Karthik Nandakumar and Anil K. Jain "Multibiometric Cryptosystem based on Feature Level Fusion" IEEE 2008.
[10] Roli Bansal, Priti Sehgal and Punam Bedi "Minutiae Extraction from Fingerprint Images – a Review" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011.
[11] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu "Fingerprint Verification System using Minutiae Extraction Technique" International Journal of Computer, Electrical, Automation, Control and Information Engineering
[12] Atul S. Chaudhari, Dr. Girish K. Patnaik and Sandip S. Patil "Implementation of Minutiae Based Fingerprint Identification System using Crossing Number Concept" International Journal of Computer Trends and Technology (IJCTT) – volume 8 number 4– Feb 2014.
[13] Dhanashree Vaidya, Sheetal Pawar, Dr. Madhuri A. Joshi, Dr. A. M. Sapkal and Dr. S. Kar "Feature-level Fusion of Palm Print and Palm Vein for Person Authentication Based on Entropy Technique" IJECT Jan-March 2014
[14] T.S. Sasikala and Dr. J. Jeya A Celin "Enhancement of Security Using Multimodal Biometric" ICCPT 2014.
[15] K. Sasireka and R.S.Rajesh "Dual Biometric Authentication Scheme for Privacy Protection" IEEE 2014.
[16] Chi Chen,Chaogang Wang, Tengfei Yang, Dongdai Lin, Song Wang and Jiankum Hu "Optional Multi – biometric Cryptosystem Based on Fuzzy Extractor" IEEE, 11th International Conference on Fuzzy System and Knowledge Discovery.

