A Novel Palmprint Recognition using Bio-Crypto System

A Dissertation submitted to the University of Hyderabad in partial fulfillment of the degree of

MASTER OF TECHNOLOGY

in

Information Technology

by

ADINARAYANA BAMMIDI

Department of Computer and Information Sciences

School of Mathematics, Computer and Information Sciences

University of Hyderabad
(P.O.) Central University, Gachibowli
Hyderabad – 500 046
Andhra Pradesh
India

CERTIFICATE

This is to certify that the dissertation entitled "**A Novel Palmprint Recognition using Bio-crypto system**" submitted by **Adinarayana B** bearing Reg. No **09MCMB28** in partial fulfillment of the requirements for the award of Master of Technology in Information Technology is a bonafide work carried out by him under my supervision and guidance.

The dissertation has not been submitted previously in part or in full to this or any other University or Institution for the award of any degree or diploma.

Dr. M.V.N.K Prasad
Assistant Professor, IDRBT.

Signature of the Supervisor

Head of the Department

Dean of the School

DECLARATION

I **Adinarayana B** hereby declare that this Dissertation entitled "**A Novel Palmprint Recognition using Bio-crypto system** ", submitted by me under the guidance and supervision of **Dr. M.V.N.K Prasad, Assistant Professor, IDRBT**, is a bonafide work. I also declare that it has not been submitted previously in part or in full to this University or other University or Institution for the award of any degree or diploma.

Date:

Name: **Adinarayana B**

Signature of the Student:

Regd. No. **09MCMB28**

ACKNOWLEDGEMENTS

I wish to express my sincere gratitude to Dr. M.V.N.K Prasad, Assistant Professor, IDRBT, Hyderabad, who generously supported and guided me throughout my project, IDRBT for providing me with the infrastructure and technical support that I needed for this project. The project would not have been possible without his assistance.

I also thank Mr. B. Sambamurthy, Director, IDRBT, Prof. Arun Agarwal, Dean MCIS, School of MCIS, Prof. C.R.Rao, Head of the Department (DCIS), University of Hyderabad for extending their cooperation.

The guidance of all the faculty members of IDRBT and the Department of Computer and Information Sciences, University of Hyderabad has been precious and timely. I wish to thank them for being very patient, understanding and helpful.

I would like to thank Dr.Abdul, Naveen and my classmates for their kind and timely support.

Adinarayana B,

University of Hyderabad & IDRBT,

Hyderabad.

E-mail ID: contact.adinarayana@gmail.com

Abstract

Biometrics plays a vital role in today Networked Security world because of its reliability and uniqueness. Many different recognition methods are proposed to identify an individual based on palmprint. In this study, the main aim is to intramodal palmprint recognition system and along with image and template security for the palmprint.

First, we developed an intramodal palmprint recognition system for effective identification of an individual, basically palmprint has rich set of features like palm lines, texture, ridges etc. we extracted the texture features using Gabor and Log-Gabor filter from the palmprint images. Performance of the two techniques evaluated individually, and then applies a sum rule (i.e. Fusion technique) to combine the features obtained from the two techniques to develop an intramodal palmprint recognition system. Performance of the system is examined on two bench mark databases i.e. PolyU and IIT Delhi. Performance is improved both in FAR as well as in GAR in the developed system compared to the previous intramodal systems.

Further, proposed two approaches 1. Image Security and 2. Template security. Conventional biometric systems store biometric templates and image as it is in the database without any security this may lead to the possibility of tracking personal information stored in database, moreover biometric templates are not revocable and unusable throughout his life time once they lost or stolen. So for image security we used Chaotic mixing with watermarking techniques and for template security random numbers with cryptographic techniques are used.

INDEX

List of Figures

Chapter 1: Introduction to Biometrics

Biometrics-based authentication is a verification approach using the biological features inherent in each individual. Biometrics overcomes the weaknesses of traditional personal identification schemes including token-based approaches and knowledge-based approaches [1, 2]. In this chapter, a brief introduction to biometrics is presented.

1.1 Introduction

Authentication is a fundamental component of human interaction with computers. Traditional means of authentication, primarily passwords and personal identification numbers (PINs), have been utilized but each has its own disadvantages. However, stronger authentication technologies, capable of providing higher degrees of certainty that a user really is who he or she claims to be, are becoming common. Biometrics is one of such strong authentication technologies.

Biometric technologies, as we know them today, have been made possible by explosive advances in computing power and have been made necessary by the near universal interconnection of computers around the world. The increased perception of data and information as near equivalents of money, in conjunction with the opportunities for access provided by the internet, are a paradigm shift with significant repercussions on authentication. If data is money, then server-based or local hard drives are our new vaults, and information-rich companies will be held responsible for their security. Because of this, passwords and PINs are nearing the end of their life cycle for many applications. To overcome the disadvantages with traditional authentication systems (i.e. Knowledge based and Token based) Biometrics came into existence.

Mainly four factors (reduced cost, reduced size, increased accuracy, and increased ease of use) have combined to make biometrics an increasingly feasible solution for securing access to computers, networks and work stations. Problems with traditional authentication systems are overcome with Biometrics so we can say it is simply a replacement of Traditional systems. Below are the some of interesting statics which

show the drawbacks (revenue losses) of using Knowledge or Token based approach.

1. According to Nilson report, in 2005, MasterCard, Visa, American Express and Discover incurred US $ 1.14 billion in fraud losses.[2]
2. Between 20% and 50% of all helpdesk calls for password resets and each password reset costs about US$70[3].
3. In 2005, 9.3 million US citizens suffered from identity theft. The loss is US$54.4 billion.

These figures strongly indicate that we need more effective and reliable solution for human identity system. Millions of people around the world use biometric technology in applications as varied as time and attendance voter registration international travel and benefit distribution. Depending on the application, biometrics can be used for security, for convenience, for fraud reduction, even as an empowering technology. According to "The Feature Biometrics" research report Biometrics revenue to reach $10 billion by 2020 [4].

1.2 Biometric Traits

The selection of biometric traits depends on requirements of applications, and every biometric trait should satisfy minimum constraints (i.e. Universality, Uniqueness, Permanence, Collectability, Performance, Acceptability, and Circumvention) some biometrics traits have high in some requirements some have low, medium. If we say Palmprint in this case Universality is medium, Permanence is High, Collectability is Medium, Performance is High, Acceptability is Medium, and Circumvention is Medium. In this Section, a brief summary of different biometric traits is presented. Every biometric trait has both advantages as well as disadvantages there is no idle biometric trait till now.Fig.1.1 shows different biometric traits.

1. **Deoxyribonucleic Acid** (DNA), DNA is comes under Biological Characteristics, and DNA is a nucleic acid containing all genetic instructions for development of organs, is commonly applied to forensic applications such as criminal investigation and corpse identification. Everyone has unique DNA pattern, except identical twins. DNA can be extracted from blood, hair, and skin etc, which can

always be collected in crime senses. DNA can be collected unintentionally and it contains all genetic disorder so for this trait User Acceptance is low.

2. **Face,** is a widely acceptable biometric trait, It is one of the Behavioral Biometric trait it can change w.r.t to the mood of the person, which can be captured from distance and even without users' cooperation. Nevertheless, face contains limited information for personal identification. Identical twins have very similar facial features. Another inherent difficulty of using face for personal identification is that face images of a person can change a lot due to facial expression, capture environment and aging. As a result, current face recognition systems cannot support high security applications but it is an important component in surveillance systems. Many researchers used PCA (principle component analysis) for the feature extraction in Face.

3. **Fingerprint,** A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points: ridge endings (where a ridge end) and ridge bifurcations (where a ridge splits in two). Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other).the pattern on fingertips, Fingerprints have been used for personal identification for many centuries and current automatic fingerprint systems have achieved high performance. Even identical twins sharing the same DNA also have different fingerprints. The other advantage of fingerprint recognition is that fingerprint scanners are inexpensive and small, which can be embedded in laptops, mobile phones and personal digital assistants. Fingerprints are selected for many large-scale human identity management projects including the US-visit program and the Hong Kong identity card. Although fingerprint recognition has many advantages, it is still not perfect. People with no or few minutia points (surgeons as they often wash their hands with strong detergents, builders, people

with special skin conditions) cannot enroll or use the system.

4. **Iris**, This pattern is unique and stable in whole lifetime. Current iris recognition systems can support real-time large-scale identification up to million records and capture iris images up to 3m. Almost all the commercial iris recognition systems are based on Iris Code developed by Daugman. But the major disadvantages with Iris recognition system is Iris capture devices are costly and User Acceptance is less.

5. **Hand geometry,** Authentication of identity using hand geometry (i.e., length and width of the fingers). Hand geometry is a widely acceptable and robust biometric. It is commonly applied to access control. Nevertheless, the geometric features have only limited information so it is suitable only for verification, 1-to-1 comparisons. The size of the capture device is another problem limiting its applications.
6. **Palmprint,** the inner surface of palms, Palmprint technology is a new branch of biometrics used to identify an individual. Palmprint has rich set of features like palm lines, texture, ridges etc. These features can be used for uniquely identifying a person. Currently, there are two types of palmprint research, high-resolution approach and low-resolution approach. High-resolution approach is suitable for forensic applications while low-resolution approach is suitable for commercial applications. For Higher resolution images minutia points can also be extracted. Chapter 2 gives detailed discussion about palmprint recognition system.

7. **Signature**, Biometric signature recognition systems will measure and analyze the physical activity of signing, such as the stroke order, the pressure applied and the speed. Some systems may also compare visual images of signatures, but the core of a signature biometric system is behavioral, i.e. how it is signed rather than visual, i.e. the image of the signature. It is widely accepted in governmental, legal and commercial transactions like banking applications. Each person can have several signatures for different applications. Nevertheless, a signature cannot uniquely identify a person. Many factors can influence the consistency of signatures such as emotional and physical conditions. Furthermore, professional forgers are capable of reproducing signatures to fool recognition systems. But

well experienced forgers are there to fool the recognition systems by forging the signature of the authenticated user.

8. **Voice** Our voices are unique to each person (including twins), and cannot be exactly replicated. It is regarded as a combination of behavioral and physiological biometrics is based on the size and shape of the appendages that generate sound. Voice recognition is commonly applied to phone-based applications and therefore, no extra input sensor is required. However, voice recognition faces several difficulties. Voice is neither distinctive nor stable. Current voice recognition systems cannot separate identical twins. Voice also changes due to medical condition, emotional state and aging.

9. **Other biometrics** including gaits, lip prints, brain signals, ears, teeth, retinas, odor, keystrokes, heights, weights, Palm vein and genders have been proposed. They have different characteristics and different potential applications.

1.3 Biometric Terms

There are different biometric traits are there, and this biometric refers to broad range of technologies, so it is essential to discuss the terminology, classifications and unique processes that define biometrics. Biometric system is an automated recognition of the person depending on the behavioral or physiological characteristics of the person. An important issue in designing a practical biometric system is to determine how an individual is recognized. Depending on the application context, a biometric system may be called either a verification or identification system.

1. **Genuine user is** a legitimate user of the system (i.e., who registered already in the system).
2. **Imposter user** is a person who is not authorized one but want to access the system.

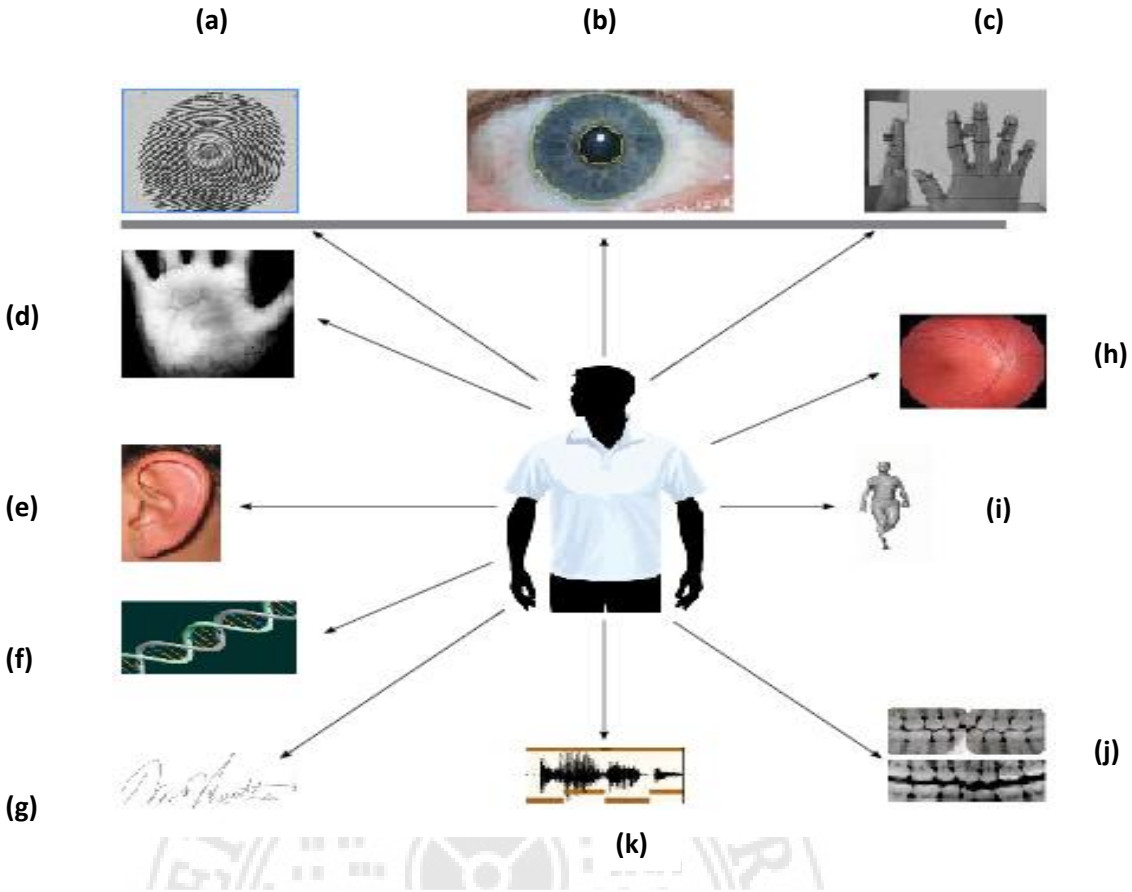


Fig.1.1. Biometric traits (a) Finger print (b) retina (c) hand geometry (d) palmprint (e) ear (f) DNA (g) Signature (h) iris (i) Gait (j) Dental (k) voice

3. **Template** Data which represents the biometric measurement of an enrollee used by a biometric system for comparison against subsequently submitted biometric samples.
4. **Matching score** is a numerical value that represents similarity or dissimilarity between two biometric signals.
5. **Genuine matching score** is a matching score, by matching two biometric signals from the biometric trait of the same person.
6. **Imposter matching score** is a matching score, which is generated by matching two biometric signals from two different biometric traits (i.e., different users).
7. **Genuine distribution** is a distribution of the genuine matching scores.
8. **Imposter distribution** is a distribution of the imposter matching scores.
9. **Verification system** is a biometric system, simply it is a one-to-one matching first user have to provide user identities like smart cards or other tokens to get the template from the database. Then one-to-one matching is done. By using this matching score generated by comparing an input biometric signal and

retrieved biometric template, depending upon this matching score the recognition system take a decision whether to accept or reject.

10. **Genuine acceptance rate (GAR)** is the probability or the percentage of a verification system correctly verifying a genuine user.
11. **False acceptance rate (FAR)** Measures how frequently unauthorized persons are accepted by the system due to erroneous matching. Potentially serious. The FAR of BioCert devices is currently about .001%is the probability or the percentage of a verification system recognizing an imposter user as a genuine user.
12. **False rejection rate (FRR),** the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
13. **Threshold** a numerical value, determines whether to accept two biometric signals from the same trait or not. For dissimilarity measures, if matching score of two biometric signals is greater than a threshold, they are considered to be from two different traits. Otherwise, they are considered to be from the same trait. For similarity measure, if the matching score of two biometric signals is greater than the threshold, they are considered from the same trait. Otherwise, they are considered from different traits.
14. **Receiver operating characteristic (ROC) curve** is a plot of genuine acceptance rate or false rejection rate against false acceptance rate for all possible operating points Fig1.2 shows ROC curve. By seeing this ROC curve we can get the performance of the system.

1.4 Proposed Method

The main aim of our work is extracting the texture features and verifying the individual based on the features extracted from the gray scale pegged palmprint images and builds a intramodal biometric system by fusion of texture features by applying both Gabor and Log-Gabor filters. Performance of the intramodal system is evaluated based on the False Acceptance Rate (FAR) and Genuine Acceptance rate (GAR), and results of every method are shown individually before fusion and after fusion.

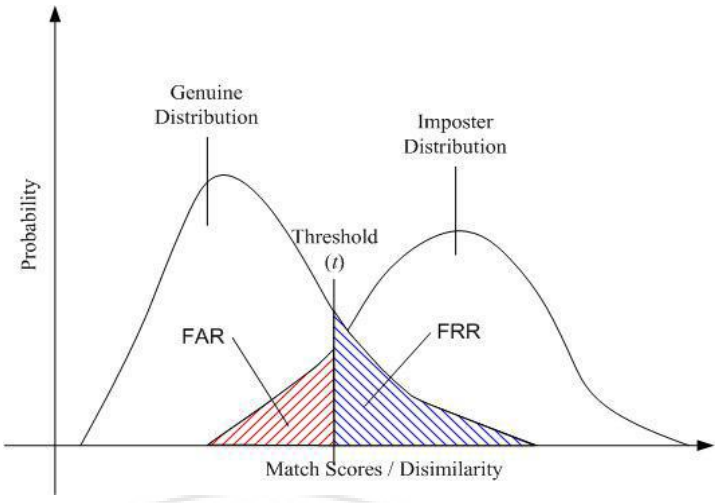


Fig. 1.2 Illustration of common terms used in biometric community

Chapter 2: Palmprint Recognition System

2.1 Overview

A palmprint recognition system generally consists of four parts: palmprint scanners, preprocessing, feature extraction and matcher Fig.2.1 shows palmprint recognition system. Palmprint scanner is to collect palmprint images preprocessing is to setup a coordinate system to align palmprint images and to segment a part of palmprint image for feature extraction. Feature extraction is to obtain effective features from the preprocessed palmprints. Finally, a matcher compares two palmprint features.
In our work we used most popular (i.e. bench mark) databases PolyU [5] and IIT Delhi [6] for our experiments. PolyU Database is acquired by Hong Kong Polytechnic University; they used CCD-palmprint scanners for acquiring the palmprint samples. PolyU Database consists of 7752 grayscale palmprint images from 193 users corresponding to 386 different palms around 17 images per palm are collected. IIT Delhi database consists of 210 users having 12 samples for palm (6 for each right and left) and these images are captured at different intervals.

Next phase in palmprint recognition system is preprocessing. The main aim of Preprocessing is used to align different palmprint images and to segment the central parts for feature extraction. Most of the preprocessing algorithms employ the key points between fingers to set up a coordinate system.

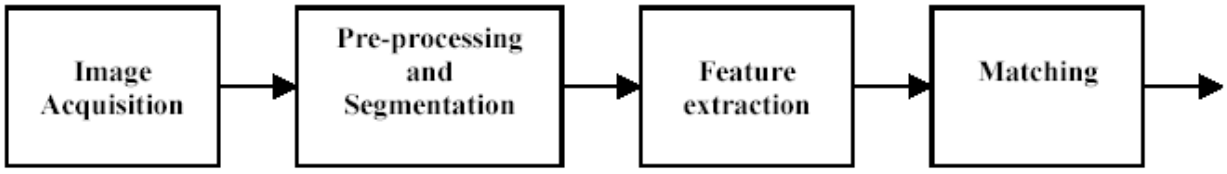


Fig 2.1 Block diagram for palmprint verification system

Preprocessing involves generally five common steps

a. binarizing the palm images,
b. extracting the contour of hand and/or fingers,
c. detecting the key points,
d. establishing a coordination system

e. Extracting the central parts.

For binarizing the palm image we used the Otsu Thresholding algorithm, this is one of the best method, previously many used this for binarizing. For ROI extraction from the palmprint image we used extracted ROI images in our work [5-6]. The resultant ROI image after segmentation is shown in Fig.2.2.

Fig.2.2 ROI of Size 150×150

2.2 Feature Extraction

Comparing with image collection and preprocessing, the research of feature extraction is more diverse. Feature extraction algorithms can be classified into five categories, line-based, subspace- based, local statistical-based, global statistical-based and coding-based approaches. However, some of them cannot be classified.

Many different filters are used to extract the required features from the Biometrics like Ordinal filter, circular Gabor filter to extract the PPOC (Palmprint phase orientation code) in different orientations for his work [7]. In [8] they used Directional Gaussian derivative filters for his work to filter the Palmprint images in different orientations and to extract the phase and orientation information of the Palmprint image obtained high accuracy. 2D Orthogonal Gabor filters in different orientations to extract the texture features efficiently and used phase-coding scheme to represent Palmprint image and they attain high genuine acceptance rate and low false acceptance rate [9]. Two classes of optimal filters in their proposed method, first class filtering is to eliminate the noisy speech frame and in second class filtering obtain noise reduction by filtering not only

current frame but also a number of previous frames and they shown that second class filters gain better noise reduction than the first class filters [10].

In this proposed method, 2D Gabor filter and 2D Log-Gabor filter [11-15] are used for feature extraction and fusion technique also applied to obtain efficient results. In [15] they used 2D hybrid Log-Gabor filter is constructed by combination of 2D Log-Gabor filters to extract the texture mixed-phase features in different directions, they proved that 2D hybrid Log-Gabor filter performance is better than Gabor and 2D Log-Gabor filters.

2.2.1 Gabor Filter

Gabor filters has been used to extract texture features from different biometrics like fingerprint, iris recognition and Palmprint recognition [15-16], in [13] they used Gabor filters for feature extraction in their work, Gabor filters for extracting features from both fingerprint as well as Palmprint [14]. The purpose of the Gabor filters is used to extract the texture information from the Palmprint. This texture information not only includes principal lines but also include wrinkles, ridges. Gabor filters extracts the texture features by capturing the frequency and orientation information from images. The 2D Gabor filter used for Palmprint verification in spatial coordinates has following form.

$$G(x,y,\theta,u,\sigma) = \left(\frac{1}{2\pi\sigma^2}\right) * \exp\left\{-\frac{x^2+y^2}{2\sigma^2}\right\} * \exp\{2 * \pi * i * u(x\cos\theta + y\sin\theta)\} \quad (2.1)$$

Where ‘x’ and ‘y’ represents the coordinates of the filter, ‘u’ denotes the frequency of the sinusoidal wave, here ‘σ’ is the Gaussian envelope, ‘θ’ is the orientation of the function and $i = \sqrt{-1}$.

$$G(x,y) = \frac{1}{2\pi} G(w,v) e^{-jvx} e^{-jvy} dwdv \quad (2.2)$$

$$I_{\theta(i,j)} = \sum_{x=1}^{w} \sum_{y=1}^{w} G_\theta(x,y) I(x-i, y-j) \quad (2.3)$$

(a) (b)

Fig.2.3. (a) Original Palmprint image (b) images after applying 2D Gabor filter

Threshold	FAR	GAR
0.58	0.65	0.1
0.60	0.63	0.99
0.62	0.59	0.98
0.70	0.39	0.97
0.72	0.35	0.96
0.80	0.16	0.95
0.84	0.08	0.92
0.88	0.0303	0.88
0.90	0.0171	0.85

Table 2.1. GAR and FAR rates for different threshold values using 2D Gabor filter technique for PolyU Database.

Threshold	FAR	GAR
0.64	0.9724	0.1
0.74	0.8577	0.99
0.80	0.7064	0.98
0.86	0.442	0.94
0.90	0.200	0.87
0.94	0.023	0.69
0.96	0.0	0.25

Table 2.2. GAR and FAR rates for different threshold values using 2D Gabor filter technique for IIT D Database.

The optimized values for the Gabor filter parameters such as u=0.096 and σ=7.1 have chosen after testing with different values at an orientation of 45^0,where I is the input image, is the image at θ orientation, and w×w is the size of the Gabor filter mask. Gabor filter is applied on 150x150 size ROI to get the texture feature. The texture features using 2D Gabor filters show in Fig.2.3. The results obtained after applying the 2D Log-Gabor filter on two databases is show in Table 2.1 and Table 2.2

2.2.2 Log-Gabor Filter

2D Log-Gabor filter has been used to extract the texture features from iris recognition and face [11]. 2D Log-Gabor filter for extract texture mixed-phase feature [15]. It has the following form

$$G(w,v) = \exp\left\{\frac{-\lg\left(w/w_0\right)^2}{2[\lg(k)]^2}\right\}\exp\frac{-\{\lg\left(v/v_0\right)^2\}}{2[\lg(l)]^2} \tag{2.4}$$

Here, w_0 and v_0 are the 2D filter's center frequencies in vertical and horizontal directions respectively. k and l are a chosen constant to control the filter bandwidth. After inverse Fourier transform of this 2D Log-Gabor function, equation (2) will be obtained.

$$g(x,y) = \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} G(w,v)\, e^{-jwx} e^{-jvy} dwdv \tag{2.5}$$

g(x,y) is rewritten to get real part and imaginary part as:

$$g_{r(x,y)} = Re\big(g(x,y)\big) = \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} G(w,v)\cos(wx+vy)dwdv \tag{2.6}$$

$$g_{t(x,y)} = Im\big(g(x,y)\big) = \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} G(w,v)\sin(wx+vy)dwdv \tag{2.7}$$

The relationship among (2.5) and (2.6) and (2.7) are:

$$g(x,y) = g_r(x,y) + jg_t(x,y). \tag{2.8}$$

$$f_r(x,y) = g_r(x,y) \otimes m(x,y) \quad (2.9)$$

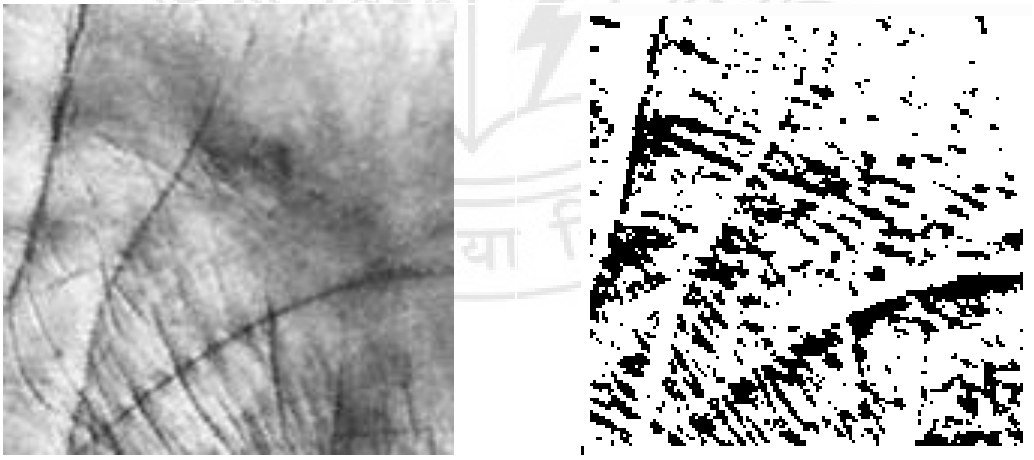
$$f_t(x,y) = g_t(x,y) \times m(x,y) \quad (2.10)$$

The palmprint pattern are then calculated by (equation 2.10)

$$p_r(x,y) = \begin{Bmatrix} 1, & f_r(x,y) > 0, \\ 0, & else \end{Bmatrix} \quad (2.11)$$

$$p_i(x,y) = \begin{Bmatrix} 1, & f_i(x,y) > 0, \\ 0, & else \end{Bmatrix} \quad (2.12)$$

w_0 and v_0 represents the 2D filter's center frequencies in vertical and horizontal directions respectively. *k* and *l* are a chosen constant to control the filter bandwidth. After inverse Fourier transform of this 2D Log-Gabor function the below function will be obtained, g(x,y) is rewritten to get real and imaginary parts. Both the real and imaginary filters are applied on to the segmented image by convolution. We applied result of both real and imaginary on the segmented image. The texture features using 2D Log-Gabor filters show in Fig.2.4. The results obtained after applying the 2D Log-Gabor filter on two databases is show in Table 2.3 and Table 2.4.



(a) **(b)**

Fig. 2.4 (a) Original Palmprint image (b) images after applying 2D Log-Gabor filter

2.3 Template Construction

After extracting the texture features from the Palmprint images by using 2D Gabor filter and 2D Log-Gabor filter then computed the feature vector (FV), in this approach first crop the input Palmprint image into 25 non overlapping sub images (i.e. 30×30) and then calculate standard deviation on each sub image FV=[SD (1), SD (2), …….SD (n)] where FV is the feature vector SD (j) is the standard deviation of the j^{th} block and n is 25,every template consists of 25 values stored in the database. Fig 2.5 represents template image.

Threshold	FAR(100%)	GAR(%)
0.58	0.15	0.1
0.60	0.12	0.99
0.62	0.095	0.98
0.70	0.032	0.98
0.72	0.021	0.97
0.80	0.001	0.95
0.84	0.0009	0.93
0.88	0.0006	0.89
0.90	0.0003	0.87

Table 2.5. GAR and FAR rates for different threshold values using 2D Log-Gabor filter technique for PolyU Database.

Threshold	FAR(100%)	GAR(%)
0.64	0.704	0.1
0.74	0.504	0.98
0.80	0.341	0.98
0.86	0.078	0.94
0.90	0.016	0.88
0.94	0.002	0.71
0.96	0.0	0.43

Table 2.6. GAR and FAR rates for different threshold values using 2D Log-Gabor filter technique for IITD Database.

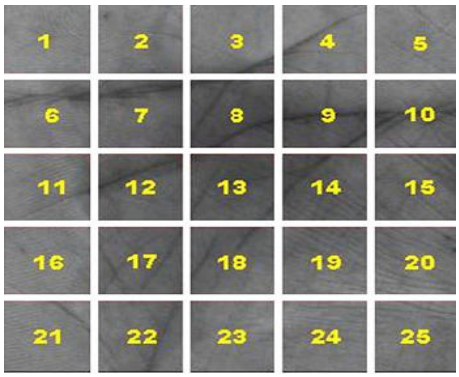


Fig.2.5 Palmprint image portioned into 5×5equal size sub-images.

So in our method the resultant template consists of 25 standard deviation values, these templates are stored in the databases (enrolled templates), and these are matched with the input templates while matching, matching procedure is explained in next section.

2.4 Matching

For matching many algorithms are there like Hamming distance, Euclidean distance and correlation coefficient. Euclidean distance and Hamming distance to compute their matching scores and Pearson correlation coefficient also used to calculate the matching score(association) between two images [16-19]. In this approach used Pearson correlation coefficient to calculate the matching score between two images and this algorithm determines the similarity between two given data sets, Palmprint verification achieved by applying the matching algorithm between the input palm image (template) and the enrolled palm image (template) stored in the database. The linear or Pearson correlation coefficient is the most widely used measurement of association between two vectors.

Let **x** and **y** be *n*-component vectors for which we want to calculate the degree of association. For pairs of quantities (x_i, y_i), $i=1,\ldots,n$ the linear correlation coefficient *r* is given by the formula:

$$r = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i-\bar{y})^2}} \qquad (2.12)$$

here $\bar{x}$ represents mean of the input image template i.e. vector x.

$\bar{y}$ represents mean of the store image template i.e. vector y.

Always r lies between -1 and 1 while 1 meaning that the two series are identical, 0 means they are completely independent, and -1 meaning they are perfect opposite. for matching we used some fixed threshold this should be always between -1 and 1. The results shown for different threshold values.

2.5 Fusion

Fusion is a promising approach to increase accuracy and he concluded that sum rule will give better results. Many biometric traits including finger surface, face and hand shape have been combined with palmprints at score level or at representation level. Combining other hand features such as hand geometry and finger surface with palmprints has an inherent advantage since these features and palmprints can extract from a single hand image. Only one sensor is needed. Researchers have examined various fusion rules including sum, maximum, average, minimum, support vector machines and neural networks. In addition to combining different biometric traits with palmprints, fusion can also be done by fusing different features including line, texture features from palmprints. Although fusion is an effective way to increase accuracy, it generally increases computation cost and template sizes and reduces user acceptance.

They are different possible levels of fusions like (a) fusion at the feature extraction level, (b) fusion at the matching score level, (c) fusion at the decision level. In [20] stated that sum rule performance of a system is better than the decision tree and linear discriminant analysis. In this paper we used the sum rule at feature level by adding the features obtained from images after applying the 2D Gabor filter as well as 2D Log-Gabor filter.Fig.2.6 represents fusion method. We applied fusion on two databases the experimental results shown in Table [2.5-2.6] before and after fusion.

.

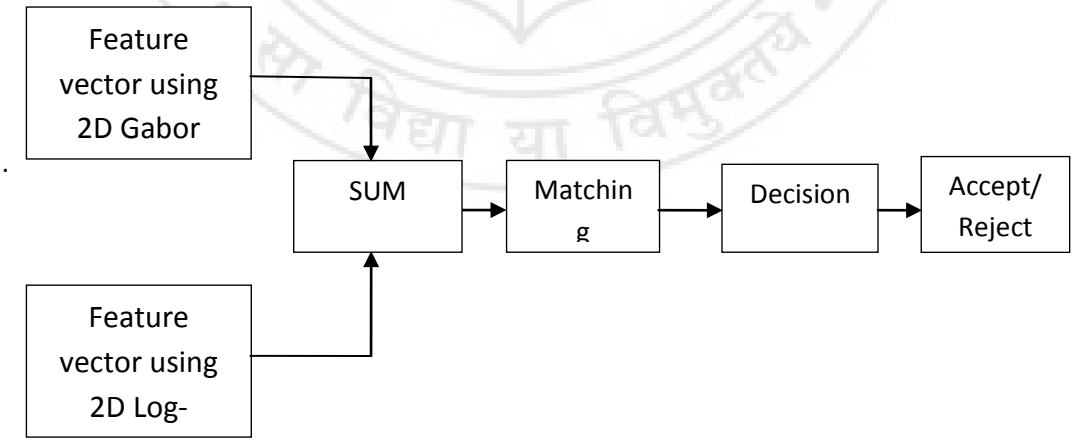


Fig.2.6. Block Diagram for feature level Fusion

2.6 Experimental Results and Conclusion

The results for 2D Gabor and 2D Log-Gabor filter methods on two databases [ref] were shown in Table 2.1 to Table 2.6. At 0.70 threshold value on PolyU database by using 2D Gabor filter gives 0.39(FAR) and 0.97(GAR) for the same threshold value by applying 2D Log-Gabor gives 0.032(FAR) and 0.98(GAR) these results are better compared to the Gabor filter and after applying the feature level fusion on the templates obtained from Gabor and Log-Gabor for the same threshold value gives 0.003(FAR) and 0.981(GAR). On IITD database for 0.90 threshold value by applying 2D Gabor filter gives 0.200(FAR) and 0.871(GAR) for same threshold by applying 2D Log-Gabor gives 0.016(FAR) and 0.88(GAR) these are better compared to the Gabor results, after applying feature level fusion on templates obtained from 2D Gabor and 2D Log-Gabor for the same threshold value gives 0.012(FAR) and 0.878(GAR). For all threshold values fusion gives better results compared to 2D Gabor and 2D Log-Gabor filter methods for two databases.

This work is to evaluate the performance of the intra-model Palmprint system by extracting the reliable features from the Palmprint with 2D Gabor and 2D Log-Gabor filter. Performance of the proposed system is evaluated by calculating FAR and GAR for each technique. It is observed from the empirical results that FAR and GAR rates are better in 2D Log-Gabor filter than that of 2D Gabor filter. It is also observed that by combining the two templates obtained from two techniques using fusion strategy on two databases the performance is improved in FAR as well as in GAR. Hence, it is concluded that proposed multiple features based Palmprint authentication system provides better results compared to previous proposed methods. It is observed from the empirical results that GAR and FAR rates are higher in 2D Log-Gabor filter than that of 2D Gabor filter and fusion method given better results compared to both the 2D Gabor and 2D Log-Gabor filter methods.

Threshold	FAR	GAR
0.58	0.025	0.1
0.60	0.024	0.99
0.62	0.018	0.98
0.70	0.003	0.98
0.80	0.0019	0.97
0.84	0.0006	0.94
0.88	0.0004	0.89
0.90	0.0001	0.88

Table 2.5. GAR and FAR rates for different threshold values using Fusion technique on PolyU Database.

Threshold	FAR	GAR
0.64	0.693	0.1
0.74	0.494	0.99
0.80	0.337	0.98
0.86	0.075	0.94
0.90	0.012	0.87
0.94	0.002	0.71
0.96	0.0	0.41

Table 2.6. GAR and FAR rates for different threshold values using Fusion technique on IIT Delhi Database.

Chapter 3: Image and Template Security

3.1 Overview

With the proliferation of large-scale computer networks (e.g., Internet), the increasing number of applications making use of such networks (e.g., e-commerce, e-learning), and the growing concern for identity theft problems, the design of appropriate personal authentication systems is becoming more and more important. Systems that have the ability to authenticate persons (i) accurately, (ii) rapidly, (iii) reliably, (iv) without invading privacy rights, (v) cost effectively, (vi) in a user-friendly manner, and (vii) without drastic changes to the existing infrastructures are desired. Note that some of these requirements conflict with the others. The traditional personal authentication systems that make use of either a (secret) piece of knowledge (e.g., password) and/or a physical token (e.g., ID card) that are assumed to be utilized only by the legitimate users of the system are not able to meet all of these requirements. But these systems has disadvantages because in Knowledge based forgotten or theft of password is major problem, whereas in Token based systems if we lose the token everything is gone. So to avoid these systems Biometric based authentication system came into existence. But providing security to the biometric samples as well as to template is major concern.

Encryption and watermarking are two widely used techniques to achieve security for biometrics samples and templates, Encryption system do not give complete solution to the problem, because once the password is known everything is gone. With the help of watermarking technique in biometric systems is good way to solve the problems. Watermarking [21-23] simply known as embedding the watermark into cover image in order to protect the copyright and authorization. Watermarking, which can be defined as embedding information such as origin, destination, and access levels of multimedia data into the multimedia data itself, previously it is used as a solution for the protection of intellectual property rights. Cryptography is another technique used to protect the biometric template but the major problem is Biometric variability (i.e. biometric template is variant w.r.t time), for example in the case of palmprint, multiple impressions of a palmprint change because of improper placement of the palm on the sensor, sensor noise, dry or dirty fingers and cuts and bruises on them. So for these type of reasons biometric data cannot be used directly to define a key. Note that, although

these changes in biometric data are “small” the cryptographic system becomes useless if the intra-class variability results in even a 1-bit change in the generated key. Traditional cryptographic systems work only if the key used during encryption is identical to the key used in decryption. Note that, in spite of these intra-class changes, the biometric matcher will normally generate a “higher” similarity score between two impressions of legitimate user’s palmprint.

3.2 Proposed Method

we proposed two methods for image security and template security, for image security we used chaotic mixing with watermarking technique first chaotic mixing is applied to the host image and then this resultant image is embedded in a sample (cover or carrier)image if the intruder get the chaotic mixed image he cannot get the original host image without knowing the ‘n’ value (i.e. no of iterations) for chaotic mixing, and for template security shuffle the palmprint template according to the random number, this shuffling scheme increases the imposter matching distance leaving genuine matching distance. The random number is protected by password which makes the system truly revocable, this random number is store in a secure place it can be accessed by database administrator.

3.2.1 Literature survey for Image Security

In our proposed method for image security we used Chaotic mixing and watermarking, many researchers have been done in watermarking and chaotic mixing for copy right protection. In [15] they used chaotic mixing based watermarking algorithm for embedding of logo, the security of the system lies in the strong parameters of the chaotic mixing system. In [30] they proposed a novel approach for image authentication with chaotic mixing system because it increases the security of the proposed method and watermarking also used for image security [21-23].

3.2.2 Literature survey for Template Security

Many researchers proposed different methods for template security. cancelable iris biometrics by using ECC (error correction code) to minimize the error bits in the iris

code and this iris code is shuffled based on the user specific random generated shuffling key where this shuffling key is protected by a password which makes the system truly revocable [25]. cancelable templates for sequence-based biometrics with application to on-line signature recognition like BioConvolving approach based on the use of a convolution-based noninvertible transformation [26], and these approaches are applied online signature based authentication system in which they used HMM (Hidden Markov Models) for template matching. In [27] they developed a frame work to design and analyze a secure sketch for biometric templates, they also consider the multifactor setting where multiple secrets are used together for authentication and In [28] they proposed a scheme for generating helper data in the fuzzy fingerprint vault framework for securing fingerprint template and they used Iterative Closest Point(ICP) algorithm for align the query fingerprint with respect to the store template and they achieved better results. In [29] they came up with a method it generates irreversible cryptographic key from cancellable fingerprint templates, first the minutiae points are extracted from the fingerprint then these points converted into transformed points in an efficient manner.

3.3 Image Security

3.3.1 Chaotic Mixing

In this our main aim is to secure the palmprint image, for that we simply transform the input palmprint image to another form this was achieved by chaotic mixing and watermarking. Many researchers have been done in watermarking and chaotic mixing for copy right protection. A two dimensional chaotic mixing can be given as spatial transformation of planar regions. It is represented by a map.

$$A: U \to U, U = [0,1) \times [0,1) \subset R^2 \tag{3.1}$$

and is defined by the formula:

$$r` = A\, r (mod\ 1), \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (mod\ 1) \tag{3.2}$$

Where a_{ij}€ Z, detA =1 and $\lambda_{1,2}$ does not in {-1,0,1} are the eigen values of A. iterated actions of A on point r_0 € U form a dynamical system $A^{(n)}$: U→ U, given by the iterative process:

$$r_{n+1} = A^n r_0 (mod\ 1)\ or\ r_{n+1} = A\, r_n\ (mod\ 1) \tag{3.3}$$

Where n=0,1,2…… The set of points $O(r_0)$= {r_0, r_1, …..} is an orbit of the system. Automorphisms belong in a special class of Anosov diffeomophisms which are strongly chaotic systems obeying local instability, periodicity with mixing and decay of correlation [24]. Roughly speaking, if V_0 is a dense subset of U then its image V_n under the map $A^{(n)}$ spreads chaotically over the entire space of U while preserving its area, because detA=1. The Cat map (a_{11}=a_{12}=a_{21}=1,a_{22}=2) is a classical mixing system in dynamics and an example of its performance is shown in Fig.3.1

Although system(3.3) is strongly chaotic it possesses a dense set of periodic orbits. An orbit $O(r_0)$= {r_0, r_1, …..} is periodic, if it is finite, i.e., there exists a number T of iterations such that r_0=r_T. The necessary and sufficient condition for an orbit to be periodic is that the initial position r_0 to have rational coordinates :

$$r_{0=}\left(\frac{p_1}{q_1},\frac{p_2}{q_2}\right) \in U \tag{3.4}$$

Where p_i , q_i are coprime integers. We consider the discrete subset of U:

$$\overline{U} = \{(x,y) | x = k/N\, , y = 1/N\, , k, l\ \circ\in \{0,1 \dots \dots \dots . N-1\}) \tag{3.5}$$

Where N is the least common multiple of q_1 , q_2. If r_0 € U then $O(r_0)$ is periodic, all its elements belong to $\overline{U}$. We consider the following map:

$$A_N = L_N \to L_N, r^1 = A\, r\ (mod\ N) \tag{3.6}$$

Where

$$L_N = \{(k.l) |\ 0 \le k < N, 0 \le l < N\} \tag{3.7}$$

Is an integer (a mesh) of size N. In a similar manner we can have iterated actions of map A_N according to (3.2), thus forming a dynamical evolution. We can easily derive the following equivalence relation between the orbits of A in $\overline{U}$ and the orbits of A_N is L_N:

If $O(r_0)$= {r_0, r_1, …..} belongs $\overline{U}$ is a periodic orbit of A, then the orbit $O(Nr_0)$= {Nr_0,N r_1, …..} is a periodic orbit of A_N and vice versa.

All the orbits of the map A_N are unstable periodic orbits since the eigenvalues $\lambda_1 = 1/\lambda_2$ of the matrix A are positive. Their periods depend on the parameters a_{ij} of A and the size N of the lattice L_N. They follow the same rules as the periods of the periodic orbits of Automorphisms in a real space which are studied in detail in. Based on the properties of periodic orbits, we can state the following corollary:

For any integer lattice L_N of size N, there is an integer P=P (a_{ij}, N) such that:

$$A_N^P r = r(mod\ N), \forall_r \in L_N \tag{3.8}$$

We call the integer P recurrence time. The element r_i of a periodic orbit are distributed quite randomly in L_N. If N is not prime, ideal (Symmetric in some sense) sublattices exit and some classes of orbits lay on them.

The evolution of the orbits depends exclusively on the eigenvalue λ_1 (or λ_2). Subsequently, automophisms are one parameter systems. The parameters a_{ij} in (1) are not independent but are restricted by the relations det A=1 and trace A = a_{11} + a_{22}=$f(\lambda_1)$. We propose a pure one parameter family of maps $A_N(k)$ given by the formula:

$$A_N(k): L_N \to L_N, \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ K & K+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (mod\ N) \tag{3.9}$$

Where $(\boldsymbol{x_n}, \boldsymbol{y_n}) \in \boldsymbol{L_N}$ and k $\in$ [1,N) belongs Z. The greatest eigen value of the matrix is λ_1=1+0.5(K+($\boldsymbol{K^2}$+4K)) and is real and positive for any k>0. Palmprint image after applying the chaotic mixing are shown in Fig.3.1. The images are shown for different 'n' (iteration) values this chaotic mixed image is embedded in the cover image.

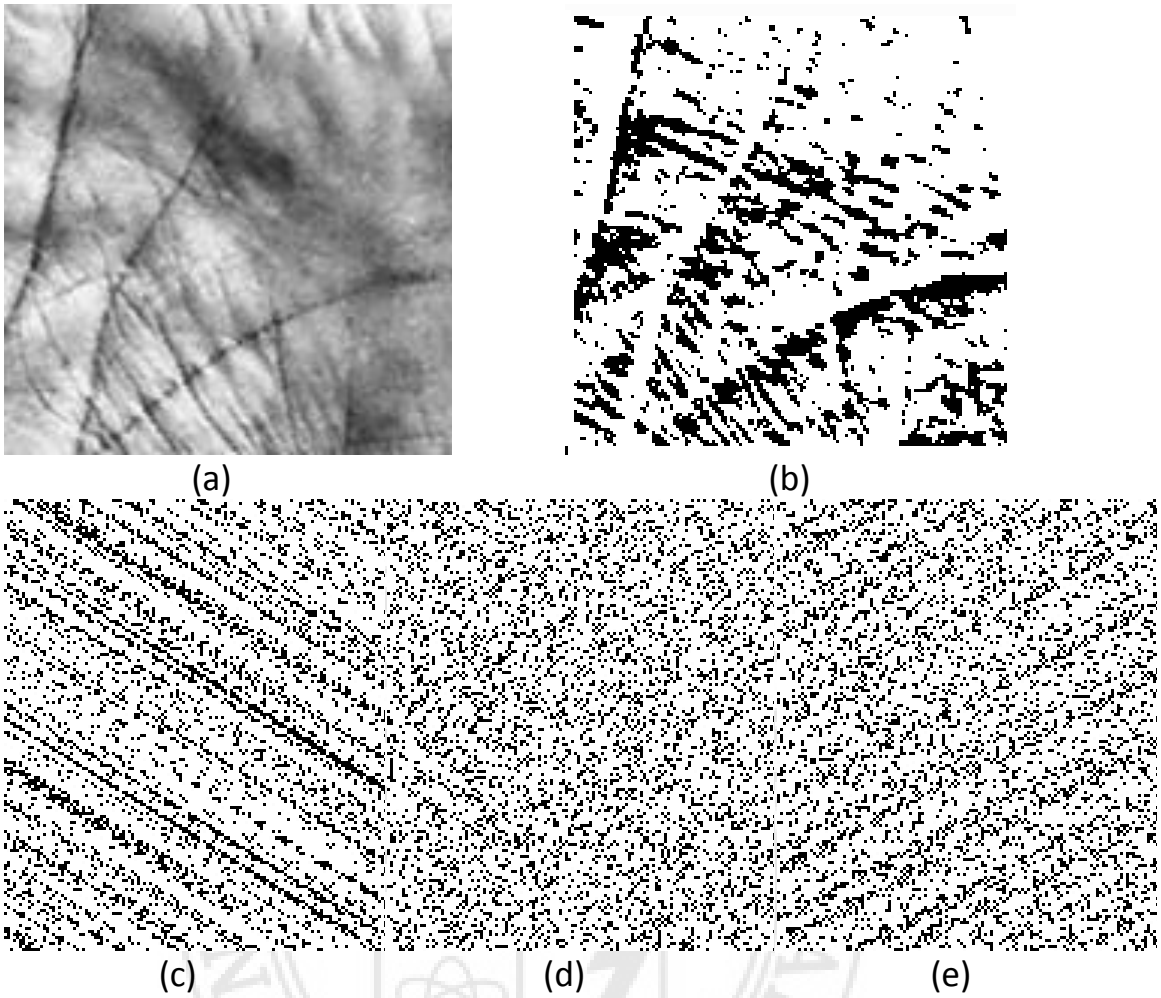


Fig.3.1 (a) original palmprint image (b) Binary image of the (c) Image after n=3 (d) n=5 (e) n=15

3.3.2 Watermark Embedding

The whole process is explained in Fig.3.2. first take binary palmprint image (of size 150 × 150) as a host image because our main intension is to hide this host image into another sample(cover or carrier)image, then apply the chaotic mixing on the host image i.e. palm image after chaotic mixing the images is show in Fig.3.2 here chaotic mixing is dependent on the ‘ n’ value if ‘n’ value changes the resulting image is varied so here ‘n’ value is confidential this can be clearly observed from the Fig.3.2, after take a sample gray scale image as a cover or carrier image(of size 150 × 150) here we taken person as a cover image now embedded the host image in the cover image for this we used the well known LSB technique, take each pixel value from the host image (i.e. here host image is binary image so ‘0’ and ‘1’ will be the possible values) and replace

the least significant bit pixel value in the cover image with the appropriate value in the host image pixel value, so the resultant image is the watermarked image(of size 150 × 150) these images are stored in the database, even intruder cannot observe the palmprint image with naked eye, if he came to known that the watermarking is applied he cannot get the original palmprint image instead he will get the chaotic mixed palmprint image with this he cannot get back the original palmprint image without knowing the 'n' value. For recovery of original image we used the reverse process and then used the reverse chaotic mixing to recover the original image.

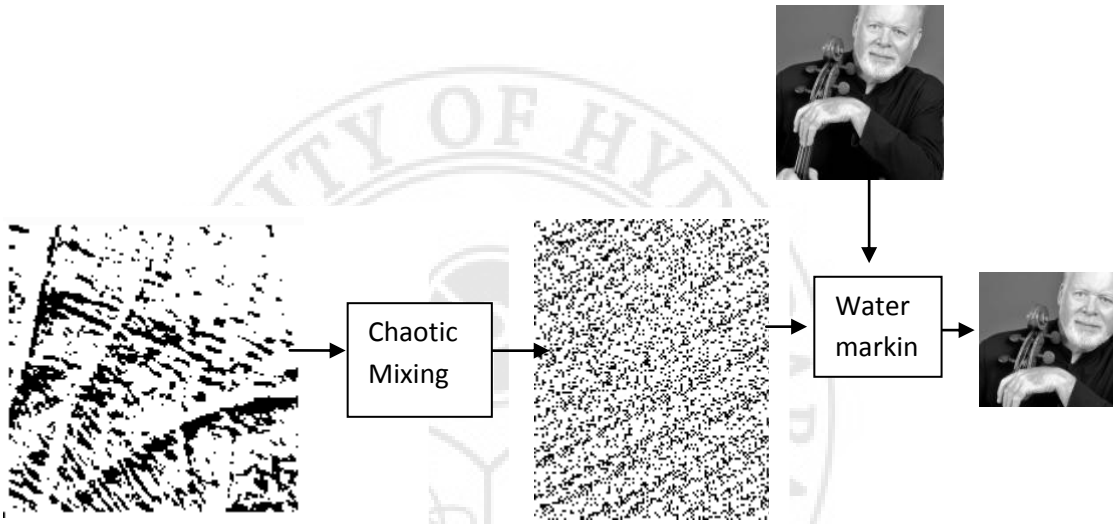


Fig.3.2 Water Marking Procedure.

3.4 Template Security

Biometrics Authentication systems is to authenticate a person depend upon his physical and behavioral characteristics but unfortunately these biometric based authentication systems facing new challenges related to personal data protection, because of these security and privacy issues**,** many researchers came up with new techniques towards protecting the biometric templates against possible attacks. In today biometric systems, biometrics data are not protected and if it is compromised or lost or stolen at any phase in the authentication process cannot be used again (difficult to revoke or replace) as an identity, because of its permanence nature since they should remain stable over the life time of an individual. To address these types of problems several methods have been

proposed in the literature and these methods can be classified into Bio-crypto systems and cancellable systems. Bio-crypto systems means integration of biometrics with cryptography and numerous advantages can be obtained by this combination. Cancellable biometric have been introduced in [25], where the template protection has been achieved by transforming the template into other domain, where data cannot be revert back to its original form, for recognition the input template is also transformed and then matched. If the data is lost then biometric template can be reissued with cancellable systems.

The whole process for template protection is explained in Fig.3.3. First get the template for the input palmprint image, section 2.3 explains procedure for construction the template. After getting the template, then generate random number range in 1 to 25 then arrange the generated template according to the input random number if our first random number is 10 then get 10^{th} standard deviation value from original template and store it in the first position in the new template and so on, but in this approach the constraint is duplicate random numbers are not allowed if it is allowed there is possibility of losing some features, then for every template store both shuffled template and as well as random numbers in the database, but an intruder can access the random numbers and he can reshuffle the transformed template to the original form with this random number so avoid such problems here we encrypted the random numbers and store encrypted form(cipher text) of random numbers in the database instead of storing them as it is in the database, the password for encryption of random numbers is with administrator of the database so that nobody else cannot access the template, here it is very difficult to the attacker to find the original template from the shuffled template because the number of possibilities are around 25! it is computational infeasible. Fig.3.4. shows the procedure for matching input template to the enrolled template here first decrypt the random numbers then reshuffle the enrolled template according to the random numbers then matching is done with the input template in our experiment for matching we used Pearson correlation coefficient, this will give the matching score between two templates or a value means how they are correlated, previously many people used same method in their work [16-19] this is explained in section 2.4, we got the satisfactory results using this method. Fig.3.4 shows the template matching procedure.

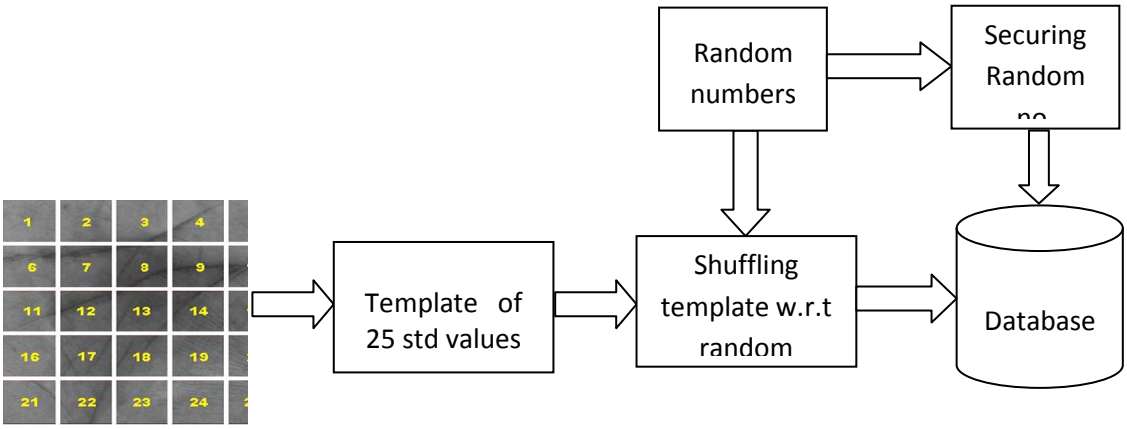


Fig.3.3 Template Protection Procedure

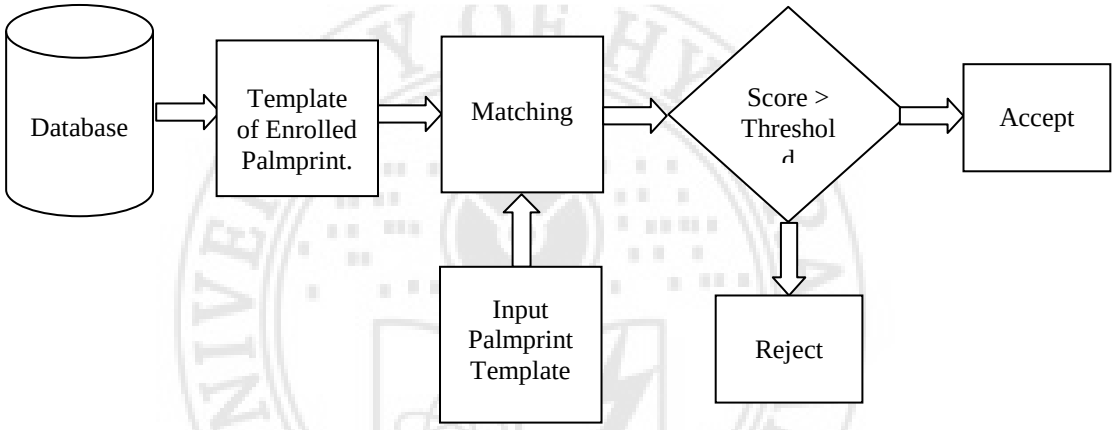


Fig. 3.4 Template Matching Procedure

3.5 Conclusion

In this work, Image security and Template security has been discussed, and this image security technique can be applied for any image, and for template security random number encryption and shuffling are used, this two methods are simple methods for providing security, this approach can be applied to some of the biometric traits so these techniques can be used for enhancing security to image database and as well as for template database.

Chapter 4: Future work

Our future work is to generate a palmprint recognition system with enhanced fusion approach (i.e. means instead of summing the sub blocks directly with our any priority or preference, find the discrimination ability of each sub-block and give weight to each block) so to improve the overall performance of the recognition system and second one is to design a palmprint recognition system robust to occlusion and develop a Cancellable palmprint recognition system.

References

1. Jain, R. Bolle, and S. Pankanti (eds), "Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, Boston, 1999.
2. A.K. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1,2004, pp. 4-20.
3. http://www.credit.com/blog/2006/07/the_real_cost_o/, "The real cost of credit card frauds". 2006.
4. http://www.researchandmarkets.com/reports/236457/advanced_biometric_technology_market_outlook.pdf , 2010.
5. PolyU Palmprint database available: http://www4.comp.polyu.edu.hk/~biometrics/
6. IITD Touchless Palmprint Database: http://web.iitd.ac.in/~ajaykr/DatabasePalm.html
7. Xiangqian Wu, Kuanquan Wang, Fengmiao Zhang and Zhang, D, "Fusion of phase and orientation information for Palmprint authentication", IEEE International Conference on Image Processing (ICIP), 2005, pp.29-32.
8. Xiukun Li, Xiangqian Wu and Kuanquan Wang, "Directional Gaussian Derivative Filter Based Palmprint Authentication", International Conference on Computational Intelligence and Security, Vol. 2, 2008, pp.467-471.
9. Zhao Song, Xu Yan, Liu Yuan Peng and Zheng Zhou, "Palmprint Verification Based on Orthogonal Code", Third International conference on Information and Computing (ICIC), Vol.3, 2010, pp.221-224.
10. J.Chen, B. Jacob and Y.Huang, "Study of the Noise-Reduction Problem in the Karhunen Loeve Expansion Domain", IEEE transactions on audio, speech, and language processing (ISSN), Vol.17, 2009, pp.787-802.
11. Ling Fan, Hong Duan and Fei Long, "Face recognition by subspace analysis of 2D Log-Gabor wavelets features", Third International Conference on Intelligent system and Knowledge Engineering (ISKE), Vol.1, November 2008, pp. 1167-1172.
12. Munaga. V.N.K. Prasad, P. Manoj, D. Sudhir Kumar and Atul Negi,"Intramodal Palmprint Authentication", Signal Processing for Image Enhancement and Multimedia Processing, Vol.31, 2008, pp.201-212.

13. Wanfeng Huang, Xirong Lin,Xiaoqing Dai, “A Novel Approach for Palmprint Ridges Features Extraction”, 2nd International Congress on Image and Signal Processing (CISP), 2009, pp.1-5.
14. Yong Jian Chin, Thian Song Ong, Michael K.O. Goh and Bee Yan Hiew, “Integrating Palmprint and Fingerprint for Identity Verification”, Third International Conference on Network and System Security, 2009, pp.437-442.
15. Ping Zheng and Nong Sang, “Using Phase and Directional Line Features for Efficient Palmprint Authentication”, 2nd International Congress on Image and Signal Processing (CISP), 2009, pp 1-5.
16. Yiteng Huang, Jacob Benesty and Jingdong Chen, “Using the Pearson correlation coefficient to develop an optimally weighted cross relation based blind SIMO identification algorithm”, IEEE International Conference on Acoustics, Speech and Signal Processing, pp.3153-3156.
17. Chang, D. J., Desoky, A. H., Ouyang, M. and Rouchka, E. C, “Compute Pairwise Manhattan Distance and Pearson Correlation Coefficient of Data Points with GPU”, Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing. SNPD '09. 10th ACIS International Conference on, 2009, pp.501-506.
18. Fei xue Huang,Xin Zhao and Cheng Li, “Clustering Effect of Style Based on Pearson Correlation”, International Conference on Internet Technology and Applications, 2010, pp 1-4.
19. Wen-Jie Wu and Yan Xu, “Correlation analysis of visual verb’s sub categorization based on Pearson's correlation coefficient”, International Conference on Machine Learning and Cybernetics (ICMLC), 2010, pp.2042-2046.
20. Arun Ross and Anil Jain, “Information fusion in biometrics”, Third International Conference on Audio and Video Based Biometric Person Authentication, Vol.24, 2003, pp. 2115-2125.
21. Mauro Barni, Franco Bartolini, Vito Cappllini and Alessandro Piva, “Copyright protection of digital images by embedded unperceivable marks” , Image and Vision computing, Vol.16, 1998, pp.897-906.
22. S. Pereira, "Robust Digital Image Watermarking", Doctoral Thesis, University of Geneva, 2000.
23. I. Pitas, “A method for watermark casting on digital image”, IEEE Transactions on Circuits and Systems for Video Technology, Vol.8, August 2002, pp.775-780.

24. G.Voyatzis and I.Pitas, “Digital image watermarking using mixing systems”, Computers and Graphics, Vol-22, 1998, pp.405-416.
25. Kanade S, Petrovska-Delacretaz.D and Dorizzi.B, “Cancelable iris biometrics and using Error Correcting Codes to reduce variability in biometric data”, IEEE Conference on Computer Vision and Pattern Recognition (CVPR), June 2009, pp.120-127.
26. Maiorana.E, Campisi P,Fierrez J and Ortega-Garcia.J, “Cancelable Templates for Sequence-Based Biometrics with Application to On-line signature Recognition”, IEEE Transactions on Systems, Man and cybernetics, Part-A: Systems and Humans, Vol.40, May 2010, pp.525-538.
27. Yagiz Sutcu, Qiming Li and Memon N, “Protecting Biometric Template with Sketch: Theory and Practice”, IEEE Transactions on Information Forensics and Security, Vol.2, Sept.2007, pp.503-512.
28. Uludag U and Anil K Jain, “Securing Fingerprint Template: Fuzzy Vault with Helper Data”, CVPRW’06.Conference on Computer Vision and Pattern Recognition Workshop, June.2006, pp.163-163.
29. N.Lalithamani and K.P.Soman, “Towards generating irrevocable key for cryptography from cancelable fingerprint”, 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2009, pp.563-568.
30. Tefas A and Pitas, “Image authentication using chaotic mixing systems”, IEEE International Symposium on Circuits and Systems (ISCAS), Vol.1, May 2000, pp.216-219.