RESEARCH ARTICLE OPEN ACCESS

# Personal Identification And Verification Using Multimodal Biometrics

Vishwas. Ramesh. Wadekar [1], Rajesh. Namdeo. Patil [2]
[1] (Department of Electronics & Communication, Dr. BAMU University, India)
[2] (Department of Electronics & Communication, Dr. BAMU University, India)

**ABSTRACT**
In this paper we present an overview of the fundamentals of personal authentication based on hand geometry measurements and palm print features. Researchers have used some complex methods or algorithms like quadratic spline function of wavelet transform (QSW), Voronoi diagram, Gaussian Mixture Model (GMM), Radial basis function neural networks (RBF), k-Nearest Neighbor (k- NN), Bayes method etc. It is essential to develop an algorithm, which is less complex, however more accurate. Biometric systems that operate using any single biometric characteristic have some limitations that can be overcome by using multiple biometric modalities. Finally, a description of the design and development of a multimodal personal authentication system based on the fusion of hand geometry and palm print features. Commonly used hand based biometrics are fingerprint, palm print, hand geometry and palm vein patterns. Among these, fingerprint has been used from a long time. But now a days, researchers are developing the systems based on palm print, hand geometry also. This paper includes the basics of palm print, hand geometry and biometric identification method based on these two biometric of human hand.

**Keywords**— Biometrics, wavelet transform, hand geometry and palm print.

## I. INTRODUCTION

As the personal and institutional security requirements increased, a person has to remember lots of passwords, pin numbers, account numbers, voice mail access numbers and other security codes. However passwords have their own weaknesses. The weak passwords can be easily guessed and the strong ones can be broken. It is recommended that people should not use the same password for two different applications and should change them regularly. In the modern world, that would mean memorizing a large number of passwords. Biometric authentication is the ideal solution to all these requirements Biometric is automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics. Behavioral characteristic are traits that are learned or acquired.Dynamic signature verification, speaker verification and keystroke dynamics are examples of behavioral characteristics.

Biometric authentication requires comparing a registered or enrolled biometric sample against a newly captured biometric sample. Biometric recognition can be used in Identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. This is sometimes called “one-to-many” matching. A system can also be used in Verification mode, where the biometric system authenticates a person‘s claimed identity from their previously enrolled pattern. This is also called “one-to-one” matching. In most computer access or network access environments, verification mode would be used.

## II. TYPES OF BIOMETRICS

A number of biometric characteristics exist and are in use in various applications. Figure 2.1 shows different types of biometrics. Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. In other words, no biometric is “optimal.”

The applicability of a specific biometric technique depends heavily on the requirements of the application domain. No single technique can outperform all the others in all operational environments. So rather than using single biometric trait we can combine two biometric traits simultaneously to increase the accuracy and reliability.

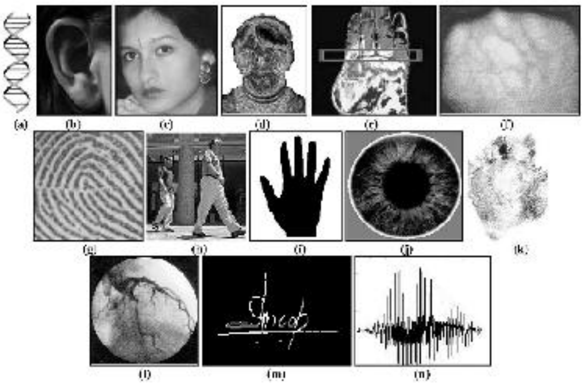

Figure 2.1 Types of biometrics (a) DNA, (b) Ear, (c) Face, (d) Facial Thermogram, (e) Hand Thermogram, (f) Hand vein, (g) Fingerprint, (h) Gait, (i) Hand Geometry, (j) Iris, (k) Palm print, (l) Retina, (m) Signature and (n) Voice .

TABLE 2.1 Comparison of various biometric technologies. High, Medium and Low are denoted by H, M and L respectively.

| Biometric identifier | Universality | Distinctiveness | Permanence | Collectability | Performance | Acceptability | Circumvention |
|---|---|---|---|---|---|---|---|
| DNA | H | H | H | L | H | L | L |
| Ear | M | M | H | M | M | H | M |
| Face | H | L | M | H | L | H | H |
| Facial thermogram | H | H | L | H | M | H | L |
| Fingerprint | M | H | H | M | H | M | M |
| Gait | M | L | L | H | L | H | M |
| Hand geometry | M | M | M | H | M | M | M |
| Hand vein | M | M | M | M | M | M | L |
| Iris | H | H | H | M | H | L | L |
| Keystroke | L | L | L | M | L | M | M |
| Odor | H | H | H | L | L | M | L |
| Palmprint | M | H | H | M | H | M | M |
| Retina | H | H | M | L | H | L | L |
| Signature | L | L | L | H | L | H | H |
| Voice | M | L | L | M | L | H | H |

A brief comparison of the above biometric techniques based on seven factors is provided in Table 2.1.

## 2.1 SELECTION CRITERIA FOR BIOMETRIC

Generally biometrics can be selected by following two criteria.

2.1.1 Personal Biometric Criteria

Any human biological or behavioral characteristics can become a biometric identifier, provided the following properties are met.

(i) Universality
(ii) Distinctiveness
(iii) Permanence
(iv) Collectability

2.1.1.1 Universality

Every person should have the characteristic. There are always exceptions to this rule: mute people, people without fingers, or those with injured eyes. Most biometric devices have a secure override if a physical property is not available, such as a finger, hand, or eye.

2.1.1.2 Distinctiveness

No two people should have identical biometric characteristics. Monozygotic twins, for example, cannot be easily distinguished by face recognition and DNA-analysis systems, although they can be distinguished by fingerprints or iris patterns.

2.1.1.3 Permanence

The characteristics should not vary or change with time. A person's face changes significantly with aging and a person‘s signature and its dynamics may change as well, sometimes requiring periodic re-enrollment. The degree of permanence of the biometric feature has a major impact on system design.

2.1.1.4 Collectability

Obtaining and measuring the biometric features should be easy, non-intrusive, reliable, and robust, as well as cost effective for the application

2.1.2 Biometric System-Level Criteria

The preceding personal biometric criteria may be used for evaluating the general viability of the chosen biometric identifier. Once incorporated into a system design, the following criteria are keys to assessing a given biometric system for a specific application:

(i) Performance
(ii) Circumvention
(iii) Acceptability

2.1.2.1 Performance

Performance refers to the accuracy, resources and environmental conditions required achieving the desired results.

2.1.2.2 Circumvention

Circumvention refers to how difficult it is to fool the system by fraudulent means.

2.1.2.3 Acceptability

Acceptability indicates to what extent people are willing to accept the biometric system.

## 2.2 KEY ELEMENTS OF BIOMETRIC SYSTEMS

There are three universal elements to all biometric systems.

(i) Enrollment
(ii) Biometric Template or Reference
(iii) Comparison

2.2.1 Enrollment

Proper enrollment instruction and training are essential to good biometric system performance. In enrollment, a biometric system is trained to recognize a specific person. Typically, the reader takes multiple samples of the same biometric that is presented by the user and averages them or selects the best quality sample to produce an enrollment reference or The features of the presented biometric are read, calculated, coded, and stored as the enrollment template for future comparisons.

2.2.2 Biometric Reference

The data that is captured during enrollment is stored in the biometric system as a template or reference. The biometric system software will use a proprietary algorithm to extract features that are appropriate to that biometric as presented by the user. Templates are usually not actual images of the fingerprint, iris, or hand, etc.

Typically, templates are relatively small in terms of data-storage size when compared with the original image or source pattern data and, therefore, allow for more efficient storage and quick processing. Each must be stored, whether in a central database or on a smart card or other token, so when the user attempts to access the system, the characteristics derived from the live biometric can be directly compared to the enrolled template.

2.1.3 Comparison

Comparison is the act of comparing one or more acquired biometric sample to one or more stored biometric templates to determine whether they “match”, that is, come from the same source. Upon comparison, a score representing the degree of similarity between the sample and template is calculated, and this score is compared to the threshold to make a match or no-match decision. For algorithms for which the similarity between the two is calculated, a score exceeding the threshold is not considered a match. For algorithms for which the difference between the two is calculated, a score below the threshold is considered a match.

## 2.3 BIOMETRIC PERFORMANCE MEASURES

The performance of a biometric system is measured in certain standard terms. These are main three types of standard terms given below-

(i) False Acceptance Rate (FAR)
(ii) False Rejection Rate (FRR)
(iii) Equal Error Rate (EER)

2.3.1 False Rejection Rate

FRR is the ratio of the number of authorized users rejected by the biometric system to the total number of attempts made. This is known as type 1 error.FRR is calculated by:

$$FAR\ (\lambda) = \frac{Number\ of\ False\ Rejection}{Total\ Number\ of\ Attempts} \qquad (1)$$

2.3.2 False Acceptance Rate

FAR is the ratio of the number of unauthorized users accepted by the biometric system to the total of identification attempts made. This is also known as type 2 error.FAR is calculated by

$$FAR\ (\lambda) = \frac{Number\ of\ False\ Attempts}{Total\ Number\ of\ Attempts} \qquad (2)$$

Where (λ) = Security Level

2.3.3 Equal Error Rate

Equal error rate is a point where FRR and FAR are same as shown in figure 1.2. The ERR is an indicator on how accurate the device is, the lower the ERR is the better the system.

As we can see the curves of FAR and FRR crosses at a point where FAR and FRR are equal, this value is called Equal Error Rate or the Crossover Accuracy Most manufactures often publish the best achieved rates and not all manufactures use the same algorithms for calculating the rates.

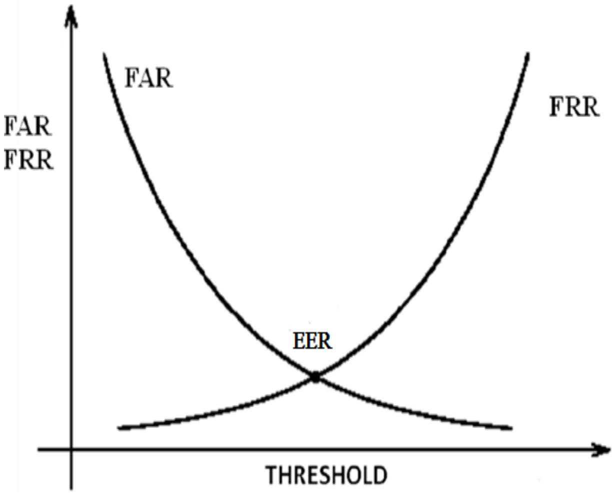

Fig 2.3.3 Equal Error Rate

### 2.4 MATLAB SOFTWARE

Matrix Laboratory is a programming language for technical computing. This software is used for a wide variety of scientific and engineering calculations, especially for automatic control and signal, image processing, it also has extensive graphical capabilities. Matlab allows easy matrix manipulation, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs in other languages.

2.4.1 Image Processing Toolbox

Image Processing Toolbox provides a comprehensive set of reference-standard algorithms and graphical tools for image processing, analysis, visualization, and algorithm development. We can perform image enhancement, image de-blurring, feature detection, noise reduction, image segmentation, spatial transformations, and image registration.

## III. SCHEME OF IMPLEMENTATION

### 3.1 PALMPRINT DETAILS

Palmprint recognition inherently implements many of the same matching characteristics that have allowed fingerprint recognition to be one of the most well known and best publicized biometrics. Both palm and finger biometric are represented by the information presented in a friction ridge impression. This information combines ridge flow, ridge characteristics, and ridge structure of the raised portion of the epidermis. Because fingerprints and palms have both uniqueness and permanence, they have been used for over a century as a trusted form of identification

3.1.1 Definition and Formation of Palmprint
Three types of lines can be found in a palm: flexure lines, tension lines (secondary lines) and papillary ridges.The flexure lines on our palm are the strongest and are in effect skin hinges which open and close during grasping and gripping. These permanent creases are called the principal lines. In palmist terminology, these lines are called as life line, head line and heart line. Secondary lines are also called as wrinkles.

3.1.2 Features from Palmprint
Palmprint authentication is a means of personal authentication that uses unique palmprint features, which may or may not be observable to naked eye. It can be achieved by designing an appropriate algorithm capable of separating two persons by their palmprint features. Palmprints are rich in features: principal lines, wrinkles, ridges, singular points and minutiae points as shown in figure 3.1. Palmprints have a surface area much larger than a finger tips but are covered with the same kind of skin of a finger.

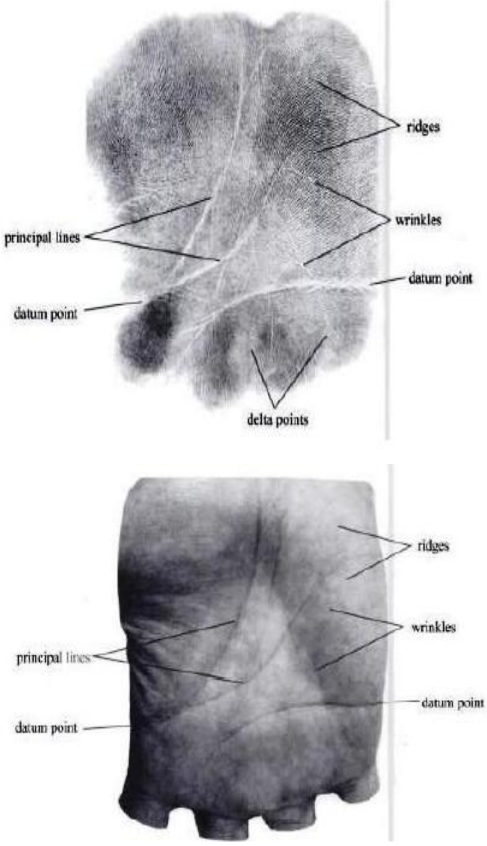

Figure 3.1 Partial information of palmprint: (a) inked palmprint, (b) inkless palmprint**.**

The palmprints have adequate information to uniquely identify a person. Six major types of features can be observed on a palm.

3.1.2.1 Geometry Features
According to the palm's shape, we can easily get the corresponding geometry features, such as width, length and area.

3.1.2.2 Principal Line Features
Both location and form of principal lines in a palmprint are very important physiological characteristics for identifying individuals because they vary little over time.

3.1.2.3 Wrinkle Features
In a palmprint, there are many wrinkles which are different from the principal lines in that they are thinner and more irregular. These are classified as coarse wrinkles and fine wrinkles so that more features in detail can be acquired.

3.1.2.4 Datum Points
Two end points called datum points are obtained by using the principal lines. These intersect on both sides of a palm and provide a stable way to register palmprints as shown in figure. 4.1. The size of a palm can be estimated by using the Euclidean distance between these points.

3.1.2.5 Delta Point Features
The delta point is defined as the centre of a delta-like region in the palmprint. Usually, there are delta points located in the finger-root region. These provide stable and unique measurements for palmprint authentication.

3.1.2.6 Minutiae Features
A palmprint is basically composed of the ridges, allowing the minutiae features to be used as another significant measurement.

### 3.2 HAND GEOMETRY

All biometric techniques differ according to security level, user acceptance, cost, performance, etc. One of the physiological characteristics for recognition is hand geometry, which is based on the fact that each human hand is unique. Finger length, width, thickness, curvatures and relative location of these features distinguish every human being from any other person. Hand geometry is considered to achieve medium security, but with several advantages compared to other techniques:
• Medium cost as it only needs a platform and medium resolution reader or camera.
• It uses low-computational cost algorithm, which leads to fast results.
• Low template size, which reduces the storage needs.
• Very easy and attractive to users – leading to great user acceptance.
• Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems.

### 3.2.1 Hand Geometry Features

As shown in figure 3.2 the lengths of the five fingers (L1 to L5), the widths of the four fingers (except the thumb) at two locations (W1 to W8). Like this, one can choose some more features like, all fingers width (including thumb), finger width at three locations, palm width at some location on palm

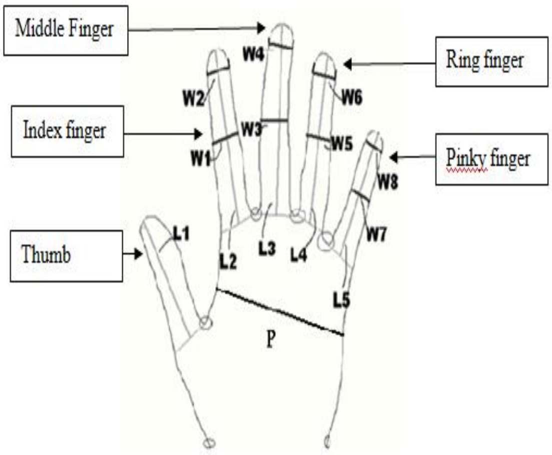

Figure 3.2 Hand geometry features

### 3.2.2 Finger Lengths and Widths

For each finger, the fingertip point and the middle point of its baseline determine its finger length. Similarly, to determine widths at different points one can select the distance with respect the fingertips and middle point of baselines.

### 3.2.3 Palm Width

In figure 3.2, 'P' indicates palm width (from left corner to right corner).

## IV. SYSTEM ARCHITECTURE

The system consists of four major blocks: Image acquisition block, image pre-processing block, feature extraction and verification. The detailed system block diagram is shown in the figure 4.1 First, the palmprint and hand geometry image acquisition module uses a digital camera to capture the hand images, and then the pre-processing module employs image processing algorithms to demarcate the region of interest (R.O.I) from an input image. This module performs three major tasks, including palmprint and hand geometry pre-processing, noise reduction and smoothening of boundary. Next, the feature extraction module extracts the features of hand geometry and palmprint. Finally, recognition module employs a minimum distance classifier according to city block distance metric to recognize the hand pattern by comparing the feature vector with the enrolled data in the database.

### 4.1.1 Image Acquisition

A contact free image acquisition system can be developed. The acquisition system consisted of a black box with a slit at a side and a window in the front. The black box eliminates the effect of the ambient lighting during image capture. Pegs are inserted on the hind wall of the box in order to guide the person while inserting his hand.The size of the images used is 1600 × 1200 pixels.

### 4.1.2 Pre-Processing and Segmentation

Colored pegs with distinct hue values are used for guiding the person inserting the palm. These pegs are first removed from the image by making their corresponding hue values in the image black. The image is then converted to gray scale. Since the variations in the ambient lighting play no role, and the wall of the box is black, a global threshold is sufficient for binarization of the gray scale image.

The next step is to determine the tips of the fingers and the valley points between the fingers. Once the thumb tip point is found out, the tips of other fingers are determined as the highest white points in the image. Once the tips of the fingers are found out, the valley points can be found out as the lowest points on the palm between the tips.

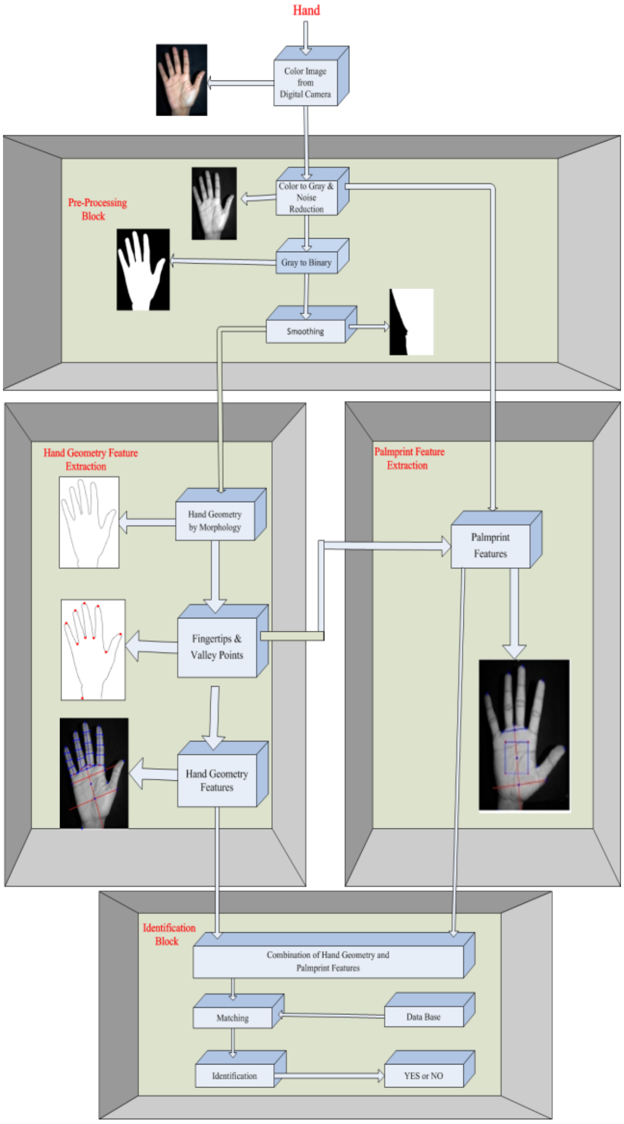
Hand
Color Image from Digital Camera
Pre-Processing Block
Color to Gray & Noise Reduction
Gray to Binary
Smoothing
Hand Geometry Feature Extraction
Hand Geometry by Morphology
Fingertips & Valley Points
Hand Geometry Features
Palmprint Feature Extraction
Palmprint Features
Identification Block
Combination of Hand Geometry and Palmprint Features
Matching
Data Base
Identification
YES or NO

Fig 4.1 System Block Diagram

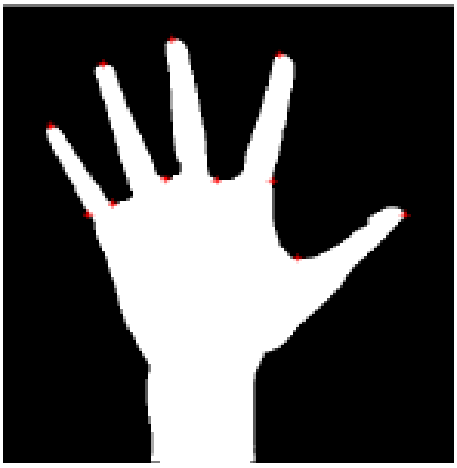

Fig 4.2 Extraction of finger tips and valley points from the segmented palm image

4.1.3 Feature Extraction

The main steps involve in this module is to extract hand geometry features (finger lengths, finger widths, palm width) and palmprint features. All the features of the hand geometry are in the form of the Euclidian distance between two points i.e. between two pixels. Palmprint features are in the form of Standard Deviation.

4.1.3.1 Palmprint Feature Extraction

After finding the tips and valleys, to find the palmprint features, a region of interest (ROI) needs to be found out. The ROI is found out as follows. A line passing through thumb valley point, parallel to the line joining the valley points adjacent to the middle finger is drawn across the palm. A square of size 300 × 300 pixels with a side parallel to the above line and with centre at the midpoint of the above line is drawn on the palm. The region of the palm lying inside this square is the ROI. This is shown in figure 4.3.

As two different biometric are used, the constraints on the individual biometric features are relaxed. A median filter is applied for reduction of noise which also helps the system become more robust, without the loss of accuracy.It is divided into four parts around the centre. The 2D DCT is then applied to each of the four parts of the ROI separately. The DCT coefficients are now grouped into nine different frequency bands (blocks) as shown in figure 4.3 Standard deviation for each of the numbered blocks is calculated. Since there are 9 blocks in each of the four parts of the ROI, there are a total of 36 palmprint features [4.3].

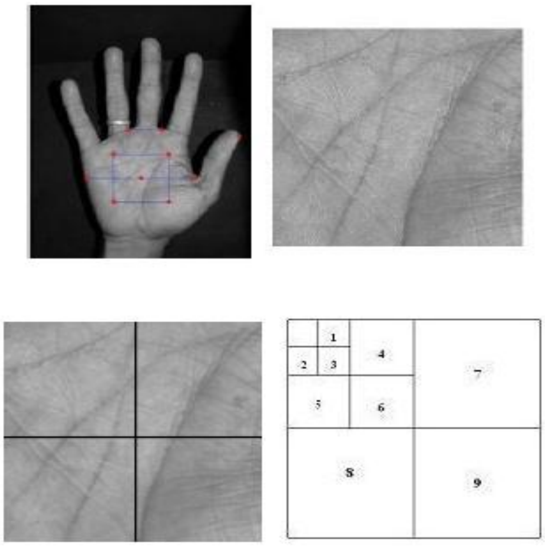

Figure 4.3 Extraction of ROI from the palm image, its sub division into four parts, and the numberedblocks of the DCT.

4.1.3.2 Hand Geometry Feature Extraction

Hand geometry features used in this work are the various Euclidean distance measurements which define the size and the shape of the palm. The various hand geometry features used are the finger lengths (excluding thumb), finger widths taken at locations of 1/6 and 5/6 along the length of each finger, palm width and the height of the upper half of the palm at two points as shown in figure 4.4. The finger lengths are the Euclidean distances between the tips of the fingers and the midpoints of the valley points. Thus, a total of 15 hand geometry features are used.

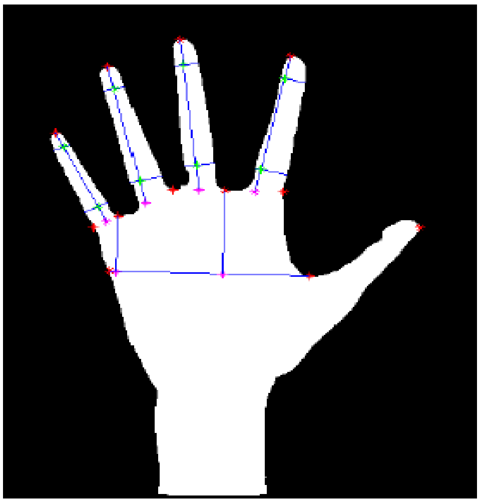

Fig 4.4 Hand geometry features extracted from the palm image

Thus, total 15 geometrical features (4 finger lengths, 8 finger widths and 3 palm widths) are taken in to consideration. Arrange all the features in the form of a vector and store in the data base for verification process.

### 4.3.4 Verification

In the verification mode, the system recognizes an individual by comparing the extracted features with those stored in the database. In a verification application, the biometric device reads a sample, processes it, and compares it against one record or template in the database. This type of comparison is called a "one-to-one" matching as discussed in fundamentals. The system conducts a comparison to verify the claimed identity of the user as shown in figure 4.5. This comparison is made against stored user templates. Here comparison is made by Euclidean distance, DE is the most common technique of all, and performs it measurements with the following equation:

$$D_E = \sqrt{\sum_{i=1}^{n}( Ts_i^2 - Tr_i^2)} \qquad (7)$$

where, $Ts_i$ = $i^{th}$ Testing feature vector
$Tr_i$ = $i^{th}$ Database feature vector
n = total number of features

Figure 4.5 gives the idea about verification process based on hand geometry features.

After extracting feature vector, the comparison is done with data base and the decision is made about the person identity.

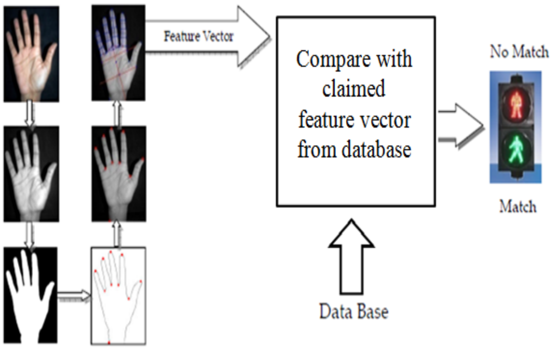

Fig 4.5 Verification Process

## V. RESULTS AND DISCUSSIONS

In this chapter, experimental results are presented which explores the performance of multimodal biometric system over unimodal biometric system used and tested. The comparative analysis has been presented on the basis of distance metric, named, Euclidean distance.

The optimum threshold for a biometric system is determined for a system from the FAR and FRR values. The graphs of FAR and FRR are plotted against the threshold values and the threshold at which FAR and FRR are equal is the optimum threshold.

The graph consists of surfaces of FAR and FRR varying against two thresholds. These two planes intersect in a curve. The lowest point on this curve gives the optimum values for the two thresholds.

These figures for the database for the Euclidean distance is shown. And also for example GUI window is created to show whether claimed identity is matched or not in fig 5.3.

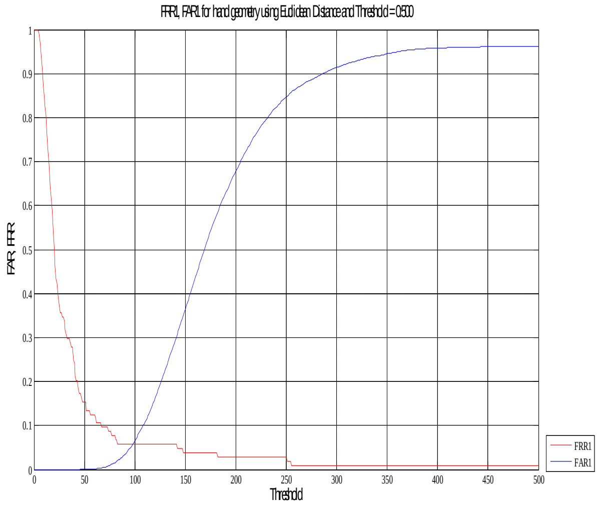

Fig 5.1 FRR and FAR for hand geometry using Euclidean distance.

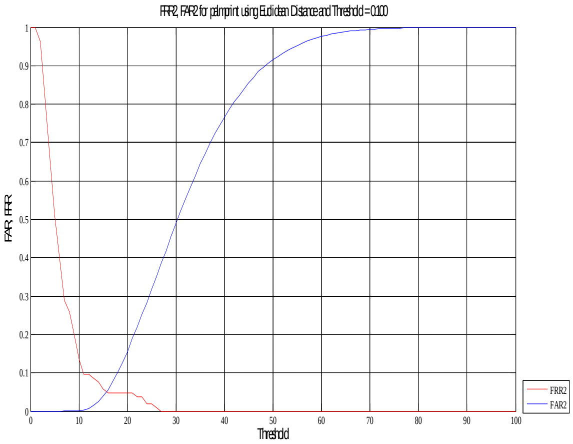

Fig 5.2 FRR and FAR for palmprint using Euclidean distance.

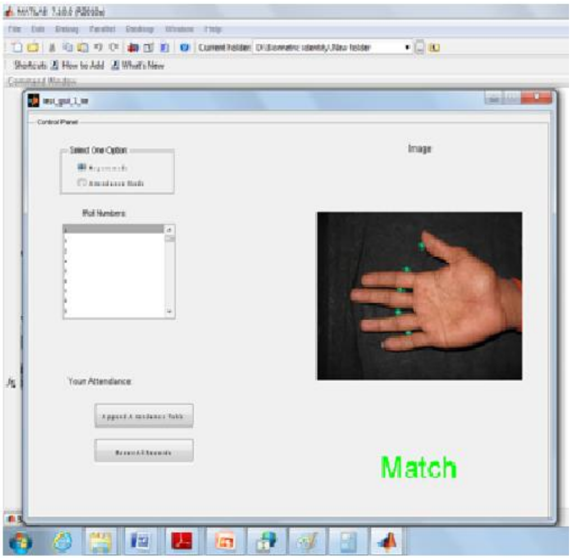

Fig 5.3 Matching attempt

## VI. CONCLUSION

This dissertation work focuses on hand geometry and palmprint features used for the proposed system are shown as enough unique to use them to verify the person's identity. It is concluded that a fusion of two biometrics results in a better performance, rather than using individual biometric.

The comparison of input image features and database stored template features can be done by using Euclidean distance, City block distance and Canberra distance. Out of these three distances, the system is verified by using Euclidean distance.

The multimodal biometric system is verified against two unimodal biometric systems i.e. Hand Geometry Biometric System and Palmprint Biometric System.

This special project would detect a user is a member of a system or not. If he/she is a valid user of the system, then he/she is identified and the output is 'Matched'. If the user could not be identified by the system, it output is 'No Match'.

## REFERENCES

[1] Dewi Yanti Liliana, Eries Tri Utaminingsih, *The combination of palm print and hand geometry for biometrics palm recognition*, International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS *Vol: 12 No: 01*, February 2012

[2] Anil K. Jain, Arun Ross and Salil Prabhakar, An Introduction to Biometric Recognition, *IEEE Transactions on Circuits and Systems for Video Technology*, *Vol. 14, No. 1,* January 2004.

[3] Reddy, P.V.; Kumar, A.; Rahman, S.; Mundra, T.S.; , *A New Antispoofing Approach for Biometric Devices*, IEEE Transactions on Biomedical Circuits and Systems, *vol.2, no.4,* pp.328-337, Dec. 2008

[4] Anil K. Jain, Arun Ross, Salil Prabhakar: *Fingerprint matching using minutiae and texture features*. International Conference on Image Processing *(ICIP)(3) 2001*: 282-285

[5] M. P. Dale, M. A. Joshi, N. Gilda, *Texture Based Palmprint Identification Using DCT Features,* Seventh International Conference on Advances in Pattern Recognition *(ICAPR), 2009*, p.221-224.

[6] Saroj Kumar Panigrahy, Debasish Jena and Sanjay Kumar Jena,"*An Efficient Palmprint Recognition System*, Proceedings of National Conference on Soft Computing, SynSoft-08, 19th-20th Jan 2008, SIET, Dhenkanal, 2008.

[7] Xiang-Qian Wu; Kuan-Quan Wang; Zhang, D.;*Palmprint recognition using valley features,* Proceedings of 2005 International Conference on Machine Learning and Cybernetics, *vol.8, no., pp.4881-4885 Vol. 8,* 18-21 Aug. 2005

[8] P. Varchol and D. Levicky, *Using of Hand Geometry in Biometric Security Systems*, Radio engineering - Special Issue: Advanced Digital Signal Processing, *Volume 16, Number, 2007*.

[9] Lin Hong, Anil Jain, Integrating faces and fingerprints for personal identification, *IEEE Transactions on Pattern Analysis and Machine Intelligence,vol.20, no.12,* pp.1295-1307, Dec 1998