International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 3 Issue 2 ǁ February. 2014 ǁ PP.39-49

Design of Hand Geometry Combined With Signature Recognition System

[1]Swarna N, [2]Lavanya C B, [3]Reshma B
[1]M.Tech in CSE,2nd Sem, Dr.AIT,Bangalore Karnataka, India
[2]M.Tech in CSE,2nd Sem, Dr.AIT,Bangalore Karnataka,India
[3]M.Tech in CSE 2nd Sem, Dr.AIT, Bangalore Karnataka, India

ABSTRACT: *Biometrics which can be used for identification of individuals based on their physical or behavioral characteristics has gained importance in today's society where information security is essential. This paper demonstrates a study about personal verification and identification using hand geometry along with signature recognizer to improve the accuracy rate. Hand geometry used in this research consists of the lengths and widths of fingers and the width of a palm. The system accepts a grayscale handprint from which it extracts the finger lengths, finger widths and perimeter along with dynamic signature. The system produces an accuracy of around 98%.*

KEYWORDS: *Biometric, Hand geometry, Recognition, Identification, dynamic signature.*

I. INTRODUCTION

With the ever increasing technological systems that require authentication, personal identification has become an absolute necessity. With decreasing personal contact among the people, the utilization of technical means for personal identification is increasing. Everything from the bank ATM to the internet requires some form of passwords. Passwords however have their own weaknesses; not only weak passwords can be easily guessed but the strong ones can be broken through too. It is recommended that people should not use the same password for two different applications and should change them regularly.

Biometric is gaining more attention in recent years. In this paper we describe a verification system that uses the geometry of a person's hand to authenticate. There are many biometric systems based on different characteristics and different parts of the human body. Each biometrics has its strengths and weakness depending on its application and use.

The advantages of a hand geometry system are that it is a relatively simple method that can use low resolution images and provides high efficiency with great users' acceptance. [1,2] Other biometrics include iris scan, speech, retinal scan, facial thermo grams and handwriting recognition, facial recognition, Voice recognition.

"Dynamic Signature" is a biometric modality that uses, for recognition purposes, the anatomic and behavioral characteristics that an individual exhibits when signing his or her name (or other phrase). Dynamic Signature devices should not be confused. With electronic signature capture systems that are used to capture a graphic image of the signature and are common in locations where merchants are capturing signatures for transaction authorizations. Data such as the dynamically captured direction, stroke, pressure, and shape of an individual's signature can enable handwriting to be a reliable indicator of an individual's identity (i.e., measurements of the captured data, when compared to those of matching samples, are a reliable biometric for writer identification.)

II. WHY BIOMETRICS

Biometrics which can be used for identification of individuals based on their physical or behavioral characteristics has gained importance in today's society where information security is essential. Biometrics features can be classified as physiological characteristics and behavioral characteristics. The various physiological characteristics that are generally used are face, iris, fingerprints, palm prints, hand geometry and voice. The behavioral characteristics include signature, handwriting analysis, voice, keystroke pattern and gait. Not every physiological or behavioral characteristic can be recognized as a biometric. The qualities of a good biometric are:

Uniqueness: The trait should be as unique as possible, so as to say that the same feature does not appear in any two different individuals.
Universality: The biometric trait should be present in as many different individuals as possible.
Permanence: The trait should have little or no change with age.
Measurability: The trait should be measurable by relatively simple methods.
Collectability: The users of the biometric system should find it easy to present the biometric for measurement.
A biometric system could have either or both of the two features, Identification and Verification.

III. HAND GEOMETRY

Hand Geometry, as the name suggests, refers to the geometric structure of the hand. This structure includes width of the fingers at various locations, width of the palm, thickness of the palm, length of the fingers, etc. Although these metrics do not vary significantly across the population, they can however be used to verify the identity of an individual. Hand geometry measurement is non-intrusive and the verification involves a simple processing of the resulting features. Unlike palm print verification methods [5], this method does not involve extraction of detailed features of the hand (for example, wrinkles on the skin). Hand geometry-based verification systems are not new and have been available since the early 1970s. However, there is not much open literature addressing the research issues underlying hand geometry-based identity authentication; much of the literature is in the form of patents [2, 3, 4]

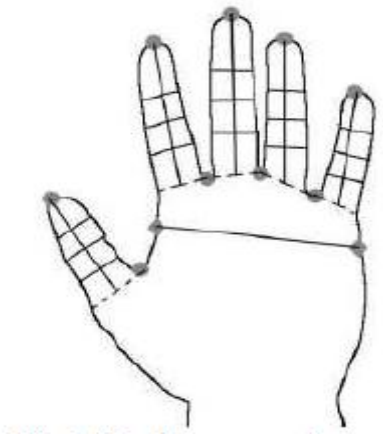

Fig.1: Hand geometry features

application-oriented description. Sidlauskas [4] discusses a 3D hand profile identification apparatus that h been used for hand geometry recognition.

IV. SIGNATURE RECOGNITION

The use of the signature has a long history, which goes back to the appearance of the writing itself. Utilization of the signature as an authentication method has already become a tradition in the western civilization and is respected among the others. The signature is an accepted proof of identity of the person in a transaction taken on his or her behalf. Thus, the users are more likely to approve this kind of computerized authentication method. Another advantage of the use of signature recognition as an authentication method is that most of the modern portable computers and personal digital assistants (PDAs) use handwritten inputs, thus there is no need in invention of principally new devices for biometric information collection. At the same time there are very few signature recognition solutions that can provide sufficiently high recognition rates at a reasonable level of efficiency. However, this area of research is vastly growing and has a promising future. Signature verification systems c n generally be divided into two vast areas: static methods (or sometimes called off-line) that assume no time-relayed information, and dynamic (sometimes called on-line) with time-related information available in the form of p-dimensional function of time, where p represents the number of features of the signature.

V. METHODOLOGY

Hand geometry features are extracted from an image by 4 steps as follows: image acquisition, image pre-processing, feature extraction and verification
As shown in fig 2.

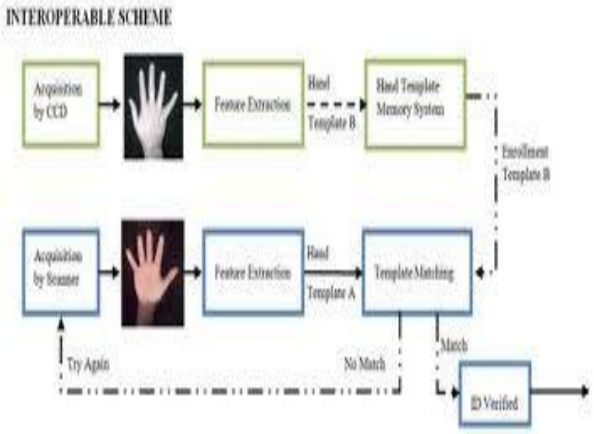

Fig 2: steps followed for hand geometry processing

I. Enrollment Phase

This process involves one of the following two tasks:

1) add a new user to the database;
2) update a current user's feature vector.

During the enrollment phase, five images of the same hand are taken in succession; and the unique signature given to individual user is acquired; the user removes his hand completely from the device before every acquisition. These five images are then used to compute the feature vector of the given hand. Recomputing a feature vector simply involves averaging the individual feature values.

II. Image Acquisition

The image acquisition system comprises of a light source, a CCD digital camera, and a black flat surface used as a background. A user places one hand, pointing up, on the flat surface with the back of the hand touching the flat surface. The user can place a hand freely since there is no peg to fix the position of the hand. Then an image is acquired by using a CCD digital camera.

Fig.3: Example images from Image Acquisition.

Users are only requested to make sure that their fingers do not touch one another and that the back of the hand lies flat and stays on the flat surface. In our experiments, only the left hand images of the users are acquired.

III. Image Preprocessing

Since the acquired image is a color image, it is converted to a grayscale image. Median filter

Eg: In case you want to apply a median filter on a image A using aNxN window, you can have your own filtering facility via

my_median = @(x) median(x(:))

A_filtered = nlfilter(A,[N N], my_median);

is applied to remove noise in the image. Because of the black background, there is a clear distinct in intensity between the hand and the background. Therefore, the histogram of the image is bimodal. The image can be easily converted to binary image by thersholding. The threshold value is automatically computed using Otsu method [7][8].

In Otsu's method we exhaustively search for the threshold that minimizes the intra-class variance (the variance within the class), defined as a weighted sum of variances of the two classes:

$\sigma_\omega^2(t) = \omega_1(t)\,\sigma_1^2(t) + \omega_2(t)\sigma_2^2(t)$ ---------- (a)

Weights ω_i are the probabilities of the two classes separated by a threshold t and variances σ_i^2 of these classes.

Otsu shows that minimizing the intra-class variance is the same as maximizing inter-class variance:[2]

$\sigma_b^2(t) = \sigma^2 - \sigma_\omega^2(t) = \omega_1(t)\,\omega_2(t)[\mu_1(t) - \mu_2(t)]2$ --(B)

Which is expressed in terms of class probabilities ω_i and class means μ_i.

The class probability $\omega_1(t)$ is computed from the histogram as t:

$\omega_1(t) = \sum_0^t p(i)$ ----------(c)

while the class mean $\mu_1(t)$ is:

$\mu_1(t) = [\sum_0^t p(i)\ x(i)]/\ \omega_1$ ----------(d)

where x(i) is the value at the center of the ith histogram bin. Similarly, you can compute $\omega_2(t)$ and μ_t on the right-hand side of the histogram for bins greater than t.

Then the border of the hand silhouette is smoothed by using morphological opening and closing. The result is shown in fig. 3.

Fig.3: Example images from image preprocessing process.

IV. Feature extraction

By scanning the pixels at the bottom of the image from left to right, the left-most pixel of the hand image, S1, and the right-most pixel, E1 are located.

The reference point is simply the middle point between S1 and E1. The next step is to find all the fingertips and valley points of the hand. The distances between the reference point and each contour point of the hand , from S1 to E1, are measured by Euclidean distance as defined in equation (A).

$D = \sqrt{(x - xr)^2 + (y - yr)^2}$ ---------- (A)

Where (x, y) is a point in the contour and (xr, yr) is the reference point.
Comparing the distances with those of other neighbor points' on the hand contour in some distances, the fingertips are the points that have the most distances, and the valley points, the least. The result positions of fingertips and valley points are marked as circles and shown in Fig. 4. The extracted features used in our research are the lengths of each finger, the widths of each finger at 3 locations and the width of the palm. This results in 21 features all together. These features can be found as follows.

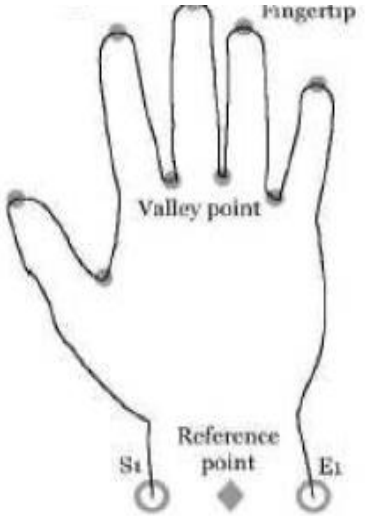

Fig.4: Fingertips and valley points of a hand.

D. 1 ***Finger Baselines***

The finger baselines of a middle finger and a ring finger are obtained by connecting the valley points which are on both sides of that particular finger. However, for a thumb, an index and a little finger; each has only one adjacent valley point. Thus, in our research, the other valley points are assumed to be on the opposite side fig 4 of the finger with the same distance from the fingertip to the existing valley point.For example, the located valley point of an index is on the right of the index contour with a distance D1 from the index fingertip as shown in Fig 6. Therefore, the assumed other valley point of the index must be D1 distance on the left of the index contour as well. All valley points are located and shown in Fig. 6. Baselines are the lines connected between two valley points, also shown in Fig. 6 as dashed lines.

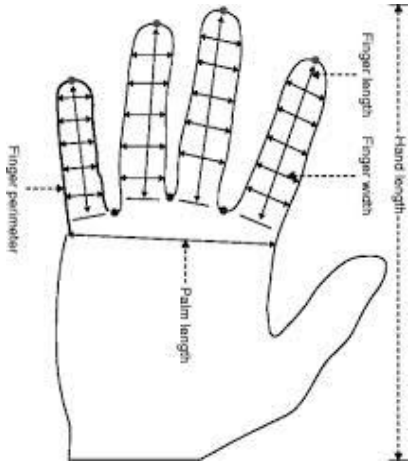

Fig.5: Definitions of finger lengths and widths

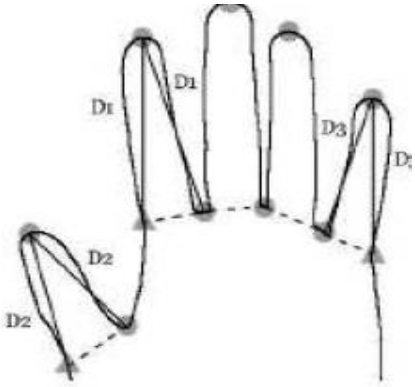

Fig.6: Definitions of finger baselines.

D.2 ***Finger Lengths***

The "finger lengths" are obtained by measuring the distances from the fingertips to the middle points of the finger baselines. These finger lengths are shown in Fig. 6.

D.3 ***Finger Widths***

In this research, the "finger widths" are the widths of a finger measured at 3 locations as shown in Fig.6. The first one is measured at the middle of the finger length, the second one, at the one-third, and the last one, at the two third of the finger length. All the finger widths are shown in Fig. 6.

D.4 ***Palm Width***

The "palm width" is the distance from b1 to b2 in database. The matching process can be divided into two types based on the application. They are verification and identification. Distance functions are utilized in the matching process to help differentiate the authorized and unauthorized persons fig 7.

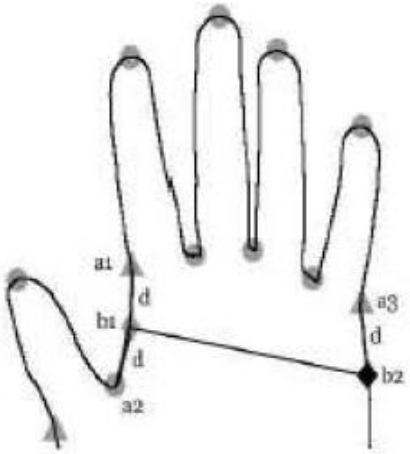

Fig.7: Definitions of a palm width.

Distance **Functions**

As mentioned earlier, a personal verification system and an identification system compare the claimer's bio data with the templates in the database. Distance functions are used to decide whether the claimer is the claimed person or as whom the claimer is recognized.

1. **Distance Function-1**

$$DI=\frac{1}{n}\sum_{k=0}^{n}\frac{\min(uk,dk)}{\max(uk,dk)} \qquad \text{----------(1)}$$

where $U=\{u1,u2,u3,.....,un\}$ is the feature vector of an unknown individual or a claimer, and $D=\{d1,d2,d3,\ldots, dn\}$is the database vector.

Including the variances of the database vectors, two additional functions are also examined as follows:

2. Distance Function-2

DII= $\sum_{k=1}^{n} \frac{|uk-dk|}{uk+dk}$ ----------(2)

3. Distance Function-3

DIII= $\sqrt{\sum \frac{(uk-dk)^2}{vk^2}}$ ----------(3)

Where V={v1,v2,v3,……..vn}is the variance vector having the entries of the variances of each features in the database vector. To measure the similarity and find the best match, a statistical method correlation is also used. Correlation is an effective technique for image recognition. This method measures the correlation coefficient between a number of known vectors with the same size unknown vectors with the highest correlation coefficient between the vectors producing the best match. There are two forms of correlations: autocorrelation and cross correlation. Autocorrelation function (ACF) involves only one vector and provides information about the structure of the vector or the data. Cross correlation function (CCF) is a measure of the similarities or shared properties between two vectors. Since there are two vectors as unknown input feature vector and known database vector in this study, cross-correlation is used. In the simplest form, the correlation between f (x, y) and w(x, y) is as the following:

c(x,y) =$\sum_s \sum_t f\ (s,t) w(x\ +s, y+\ t)$ -------(4)

V. Verification

In verification, the process involves matching a given hand to a person previously enrolled in the database. The claimer feature vector is then compared with the feature vector stored in the database associated with the claimed identity and the system decides that the claimer is right or not. Verification performance is measured from the two types

VI. SIGNATURE RECOGNITION

Dynamic signature verification methods can generally be divided into two broad groups: functional and parametric. In the first case the feature set, upon which the decision process is built, is constructed of functions, meaning that complete signals (e.g. pressure, velocity, acceleration etc.) are represented by time-dependent functions, whose values constitute the feature set. On the other hand, parameters of the measured signal can be considered as the feature sets [16]. The dynamic or also called on-line methods of human signature verification exhibit a variety of methods applied. Let us look at some of the techniques used in the area.

Most HSV (Handwritten signature verification) techniques use the following six-step procedure for performance evaluation:

a) Registration: This involves capturing of a few signatures for each individual at enrolment or registration time (these signatures are called sample signatures).
b) Pre-processing and building reference signature(s): This involves the deletion of virtual pen-up strokes from the raw signatures. The main reason of virtual pen-up is not keeping enough pressure of the pen all through the signing process. When the pressure of the pen point is less than minimum pressure which the tablet can detect, it causes virtual pen-up. Usually the pressure is high when there is straight virtual pen up or turning virtual pen up. The required features are computed and one or more reference signatures are produced. Then the parameters are decided on which the threshold is calculated.
c) Test signature: When a user wishes to be authenticated, he/she presents a signature (we call this signature the test signature). The features of this test signature are computed as usual.
d) Comparison processing: The test signature is then compared with the reference signature(s) based on feature or feature set values and the difference between the two is then computed using one of the distance or time measurements.
e) Performance evaluation: For each signature that claims to be a genuine one, we compare the distance or time computed with the threshold decided in Step 2 above. If the difference between the two is smaller, accept the signature otherwise reject it.
f) Steps 3–5 are then repeated for the given set of genuine signatures and forged ones; false rejection and false acceptance rates are then computed.

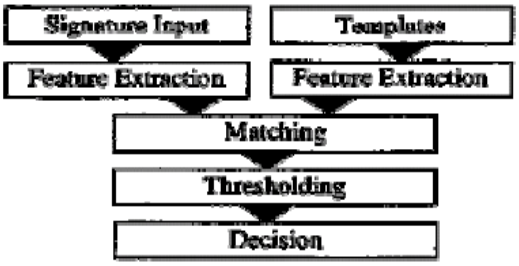

Fig 8: steps for signature verification

Online systems use the dynamic features of a handwritten signature considering the time and frequency factors which involves signal processing techniques like the normalization, Fourier transforms and correlation functions for the proper analysis of the handwritten signatures.

1. **Online methods of verification are divided into four approaches.**

a) Global parametric feature based approach - All the available values are not used. Instead, a number of global values, called statistical features or parameters like time, distance, pen up and pen down times, are computed and compared.

b) Function based approach - all the collected position (or velocity or acceleration) values of the test and reference signatures are compared point-to-point, perhaps by computing a set of correlation coefficients between the two signatures. Such comparison may require signature segmentation and comparison of corresponding segments may require alignment.

c) Hybrid method for both feature based and function based approaches and

d) Trajectory Construction methods.

2. **Feature Extraction**:

The feature extraction is the key step in the recognizing of the on-line hand-written signatures. According to the coordinates, curvatures and the recorded time information, a series of biological features of the signatures are usually obtained for such systems. The systems extract the features like time, length of strokes and speed and then obtain a resultant function using the Gauss function to calculate the probability density through other density functions also. During the estimation, the system obtains the corresponding averages, variances and standard deviations which will be the unique features for the signatures.

Simple features selected are

a. **D : Total distance of the pen travelled on the hand-written signature the Euclid distance of all the points:**

$$D= \sum \sqrt{(x_i - x_{i+1})^2 + (y_i - y_{i+1})^2} \text{ -------(5)}$$

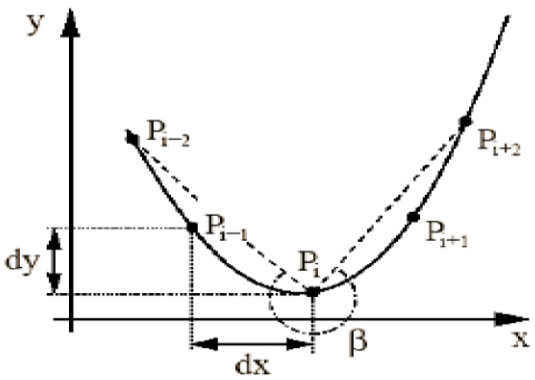

Fig 9: graph of feature extraction of signature

xi is the coordinate in direction x and yi is the coordinate in direction y;
Speed vx and vy express the functions of time, which can be calculated with the following formulae

$$\begin{cases} v_{x_m} = (x_{m+1} - x_m)/(t_{m+1} - t_m) \\ v_{y_m} = (y_{m+1} - y_m)/(t_{m+1} - t_m) \end{cases}$$

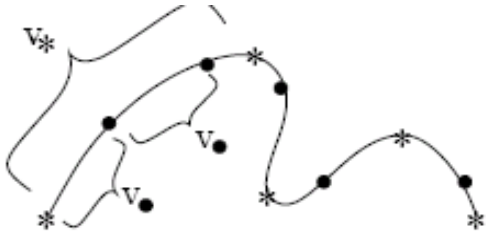

Fig 10: stroke of a signature

where m is the serial number, m=0, 1, …, N−1; xm is the coordinate in direction x; ym is the coordinate in direction y; tm is the time of movement; vx is the speed at point tm in direction x; vy is the speed at point tm in direction y. Acceleration ax and ay can be calculated with different speeds, the acceleration at point tm in directions x and y can be expressed in the following formulae:

$$\begin{cases} a_{x_m} = (v_{x_{m+1}} - v_{x_m})/(t_{m+1} - t_m) \\ a_{y_m} = (v_{y_{m+1}} - v_{y_m})/(t_{m+1} - t_m) \end{cases}$$

Most signatures take between 2 and 10 seconds with an average time of 5 seconds (slightly longer times for forgeries). Previous studies say that the average amount of time for a genuine signature is usually 3 to 6 seconds and for a forged was 10 to 11 seconds.

b. Tk , total time of the hand-written signature;

The total time, the length of the strokes, the time for lifting the pen can be different for the same user's different signatures. These features oscillate about the average and variance which can symbolize one person's biometric features. There are two time-related features: the first is the total signature time T. The second is the time down ratio Tdr, which is the ratio of pen-down time to total time.

- Total Signature time T = tK − t1
- Pen-down time ratio Tdr = td / T
  k = 1,2..., K data points for a given signature.
- Length-to-width ratio Lw = Vm Td / Xw Vm, Xm, Ym, are the means of v; x; and y respectively

Xw = max(x) − min(x)

The other features that can be implemented are:

- Nvx and Nvy , amount of zero speed in direction x and y directions.
- Nax and Nay amount of zero acceleration in direction x and y directions.

VII. EXPERIMENTS AND RESULTS

We divide the tests into 2 operation modes, a verification mode and an identification mode. four different distance functions, as shown in section C, are used in the feature matching process.

I. Data Used in Our Experiments

There are 96 test users in our experiments. Ten left-hand images and signatures are acquired from each user. These images are divided into 2 groups. The first group consists of the images of all 96 users, 5 images and a signature from each user. They are used for the enrolment process to define the user's templates, or feature vectors. The features are extracted as mentioned earlier in section 2a. Five hand images and a signature from each user are used for forming the database feature vectors. The signature and average values of each feature are kept as the database vectors, and also the variances of each extracted features are registered for recognition purposes. The other hand images are used for testing the performance of the proposed algorithm. The algorithm has been tested on both identification and verification tasks. In identification, an unknown individual signature and feature vector is matched with all the vectors registered in the database and the algorithm determines or makes a decision that the claimer is one of the registered users or not and the system identifies the claimer. The performance of the algorithm is evaluated by the system's percent error or by the correct identification rate. Only if both signature and feature vector matches only then the correct match is declared. The algorithm used three distance functions and correlation function defined on the recognition section for hand geometry matching and different approaches for signature recognition the claimer vector with the vectors on the database. The results for identification task are given in Table-1.

TABLE-I
Identification Performance Test Results

Matching Algorithm	Identification Rate
Distance 1	% 96.04
Distance 2	% 94.02
Distance 3	% 57.15
Correlation	% 93.71

TABLE-II
Verification Performance Test Results

Matching Algorithm	Verification Error
Distance 1	% 98.07
Distance 2	% 97.88
Distance 3	% 75.18
Correlation	% 97.85
Sum of weighted Distance-3 and weighted-correlation	% 99.72

Table-I shows that the matching algorithm using the Distance-IV function and the algorithm using the correlation have better correct identification rates. If these two functions can be combined with their weights, this new function can give better result. The performance of this matching algorithm is %97.44.

II. Experiments and Results from Verification Mode

In verification, the process involves matching a given hand and a signature to a person previously enrolled in the database. The claimer feature vector is then compared with the signature and feature vector stored in the database associated with the claimed identity and the system decides that the claimer is right or not. Verification performance is measured from the two types of errors; False Rejection Rate (FRR) and False Acceptance Rate (FAR). Even after using a threshold value to filter out the false acceptance of unregistered individuals the system can give incorrect results.

FAR is the ratio of the number of unauthorized (unregistered) users accepted by the biometric system to the total of identification attempts made. FRR is the ratio of the number of number of authorized users rejected by the biometric system to the total number of attempts made. Equal error rate is a point where FRR and FAR are same.. The results are summarized in Table-2. The performance of a biometric system is measured in certain standard terms. These are false acceptance rate (FAR), false rejection rate (FRR) and equal error rate (EER) also called crossover error rate (CER).

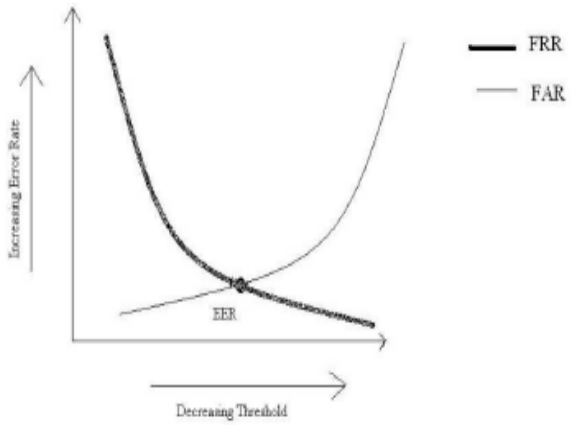

Fig 10: equal error rate

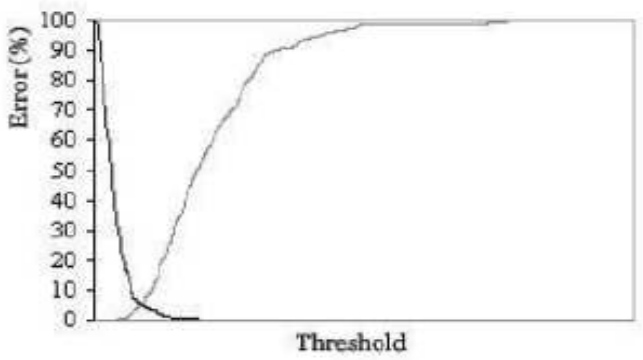

Fig 11: Graph FAR and FRR with vary threshold.

VIII. CONCLUSIONS

Hand geometry has proved to be a reliable biometric. The proposed work shows how to utilize the shape of the palm to extract features using very simple algorithms. Dynamic signature verification in a biometric can be easily integrated into existing systems because of the availability and prevalence of signature digitizers and the public's acceptance of the characteristic collection. By combining hand geometry we can obtain accuracy around 98%. The FRR is found to be close to 0.1 and the FAR to be around 0.05.

REFERENCES

[1] K. Jain, A. Ross, and S.Prabhakar,"An Introduction to Biometric Recognition," IEEE Transactions on circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, pp. 4-20, Jan. 2004.

[2] John Chirillo, and Scott Blaul,Implementing Biometric Security, John Wiley & Sons, Apr. 2003.

[3] R. Sanchez-Reillo, C. Sanchez-Avila, and A.Gonzalez- Marcos,"Biometric Identification Through Hand Geometry Measurements," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 22, No. 10, pp. 1168-1171, 2000

[4] Sezgin, M., Sankur, B., "Survey over image thresholding techniques and quantitative performance evaluation", Journal of Electronic Imaging, 13 (1), 2004, pp.146–156.

[5] K. Jain and N. Duta,"Deformable Matching of Hand Shapes for Verfication," IEEE International Conference on Image Processing, pp. 857- 861, Oct.1999.

[6] R.Sanchez-Reillo,"Hand Geometry Pattern Recognition Through Gaussian Mixture Modeling," 15th, International Conference on Pattern Recognition, Vol. 2, pp. 937-940, Sep. 2000

[7] N. Otsu,"A Threshold Selection Method From Gray-scale Histogram," IEEE Transaction Syst., Man, Cybern., Vol. 8, pp. 62- 66, 1978.

[8] Otsu, N., "A threshold selection method from gray-level histograms", IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-9 (1), 1979, pp. 62–66.

[9] Using position extrema points to capture shape in on-line handwritten signature verification G.K. Guptaa,∗, R.C. Joyceb, aFaculty of Information Technology, Monash University, Clayton, Victoria 3800, Australia, bOutsource Laboratories, Eatontown, NJ 07724-1878, USA.

[10] Hand written signature verification methods K R Radhika, M K Venkatesha and G N Sekhar

[11] HAND GEOMETRY: A New Method for Biometric Recognition Nidhi Saxena, Vipul Saxena, Neelesh Dubey, Pragya Mishra

[12] Prototype Hand Geometry-based Verification System Anil K. Jain & Arun Ross Sharath Pankanti