Authentication Using Hand geometry And Finger geometry biometric Techniques

[1]AmandeepKaur Bhatia, [2]SupreetKaurGujral

[1]M.E (CSE)Student, Punjabi University Regional Centre for IT &Management, Punjab, India,

[2] Assistant Professor (CS), Punjabi University Regional Centre for IT &Management, Punjab, India,

***Abstract*—Biometric authentication systems are gaining importance in the today's world where information security is essential. Hand geometry verification systems use geometric measurements of hand for authentication of individuals. It is believed that the combination of different features of the hand is unique for a particular person. Different hand geometry authentication systems use reference pegs for capturing the image of the hand. We propose peg free hand geometry and finger geometry system**

***Keywords*- Biometrics, Recognition, Verification, Identification, Hand Geometry**

I. INTRODUCTION

As increase of security requirements, a person has to remember lots of pin numbers, passwords and other security codes. The passwords can be easily guessed and stolen electronically. Once an intruder acquires the user ID and password, the intruder has total access to the user's resources. It is suggested that people should not use same password for different applications. In the modern world that would mean memorizing a large number of Security codes. Biometric is most suitable solution to all these requirements. In the future,the biometric system will be more convenient and reliable[1].

In the era of Information Technology, openness of the information is a major concern. As the confidentiality and integrity of the information is critically important, it has to be secured from unauthorized access. Security refers toprohibit some unauthorized persons from some important data or from some precious assets. So we need accurateautomatic personal identification in various applications such as ATM, driving license, passports, citizen's card,cellular telephones, voter's ID card. Hand geometry is most widely used for person identification in the recentyears. Hand geometry based biometric system are gaining acceptance in low to medium security applications [2]. Hand geometry recognitions terms are based on a number of measurements taken from the humanhand, including its shape, size of palm, and length and widths of the fingers.The technique is very simple, relatively easy to use, and inexpensive. 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-basedsystems. The hands images can be obtained by using a simple setup including a web cam, digital camera.However other biometric traits require a specialized, high cost scanner to acquire the data. The useracceptability for hand geometry based biometrics is very high as it does not extract detail features of theindividual. An individual's hand does not significantly change after a certain age. The strengths of hand geometry Biometrics are as follows [3].

- Ease of use: Hand is placed on the unit's surface but the system also works fairly well with dirty hand.
- Resistant to fraud: model of an enrolled person's hand and fingers, it would be difficult to submit a fake sample.
- Template size: template size of hand geometry is extremely small if it is compared with other biometrics systems.

Traditional hand geometry systems are always used thepegs to fix the placement of the hand [4].Two main weaknesses of using pegs are that pegs will definitely deform the shape of the hand silhouette and users might place their hands incorrectly as shown in Figure 1. These problems can certainly reduce the Performance of the biometric system.

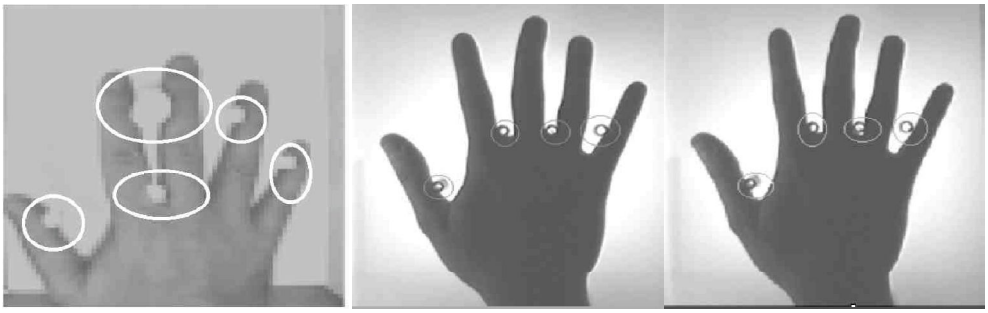

Figure 1: Three peg-fixed hand photos: deformed hand shape

II. MODULES OF BIOMETRIC SYSTEM

As shown in the Figure 2, a biometric system comprises of fivemajor steps involved in Hand Geometry Based identification. These steps are Image acquisition, Imagepre processing, Feature extraction,Matching and Decision as follows:

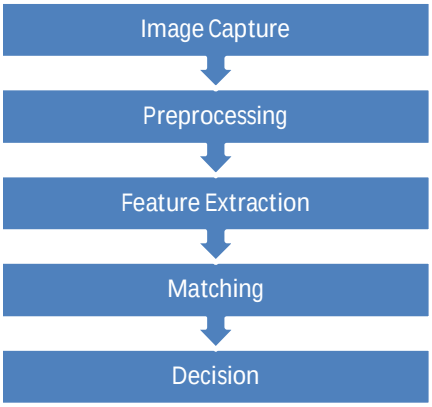

Figure 2: Components of a Biometric System

A. *Image Acquisition*

Image acquisition is the first step in a hand geometric system. This process involves the capturing and storage of digital image from vision sensors like colour digital cameras, monochrome and colour CCD camera, video cameras, scanners etc. The proposed image acquisition system consists of digital camera and black flat surface used as a background. User can placed one hand pointing up, on flat surface with the back of hand touching the flat surface or the user can place hand freely as there are no pegs to fix position of hand, then image is acquired using digital camera. Users are only requested to make sure that their fingers do not touch one another. In this experiment right hand images of users are acquired. There are various format stored for the images such as .jpeg, .tiff, .png,.gif and .bmp. The captured images are stored in one of these formats on the computer for possible image processing.

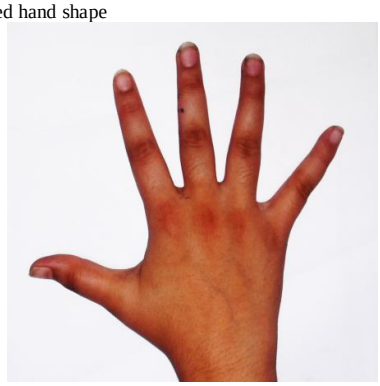

Figure3:Image Acquisition

B. *Pre-processing*

The next stage is image pre-processing module. Image pre-processing relates to the preparation of an image for later analysis and use. The role of the pre-processing module is to prepare the image for feature extraction. The images are captured using a digital camera. The input image is a coloured image of the right hand without any deformation. The input image, shown in Figure 3 is stored in jpeg format. In cases of standard deformity such as a missing finger the system expresses its inability to process the image. It is also critical that the fingers are separated from each other. However it is not required to stretch the fingers to far apart as possible. The hand should be placed in a relaxed state with fingers separated from each other. Since features such as length and width which are dependent on the image size and resolution are being used, it is critical that to have uniform size of images. Image pre-processing module is consisting of operations such as Gray scale image, Noise Removal, Binarized Image and Edge detection [5].

1) *Gray scale image*

In this proposed system hand image is captured through digital camera so the original image is colour image. For digital image processing it is necessary to convert the coloured hand image into the gray scale image as shown in Figure 4.

Figure 4: Gray scale image

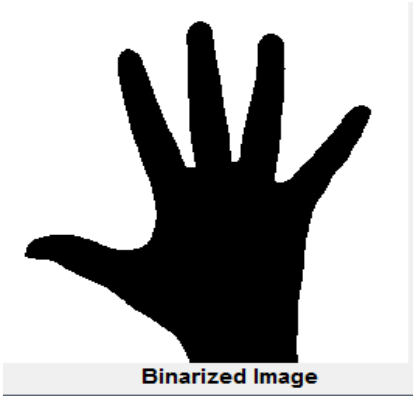

Figure 5: Binarized image

Figure 6: Filtered Image

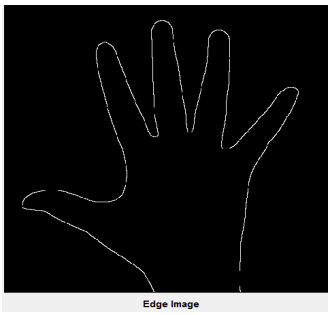

Figure 7: Image contains only edges

2) Binarized Image

In this step gray level image is converted into an image with two levels 0 or 1.Where 1indicates the white colour and 0 indicates the blackcolor.Red, green and blue (RGB) values of each pixel are extracted. Since a monochromaticimage is required for the proposed system a threshold is determined. All pixels withRGB values above the threshold are considered white pixels and all pixels below the thresholdare considered as black pixels [8].

3) Filtered image

It is necessary to remove the noise from the image because it may produce difference between the actual image and captured image. Basically noise produced in the image is due to device using for capturing image, atmosphere condition or surrounding condition. There are many methods to remove the noise in MATLAB simulation tool. So, before extracting features from the image, it is very important to remove the noise from the image (Figure 6).

4) Edge detection

In order to extract geometric features of the hand it is required that image contains only edges(Figure 7). The image obtained after elimination of noise contains regions of black andwhite pixels. In order to extract geometric features of the hand it is require that the image contains only edges. Consequently it is required to convert regions of black space to an image containing only the boundary of the white pixels. Thisis achieved by using an edge detection algorithm. The algorithm converts all pixelsexcluding those at the boundary of black and white regions to white pixels. Thealgorithm also has to ensure that the thickness of this boundary is as low as possible. This is because a thick boundary will adversely affect the accuracy of the feature detection algorithm[8].

C. *Feature Extraction*

Since there is no peg to fix the placement of hand, users can place their hands in various positions as shown in Figure 8. Before extracting the hand features, the “landmark points” have to be located [6]. These landmark points include the fingertips and valley points that can be seen in (Figure 9).

Figure 8: Various poses of hand placement

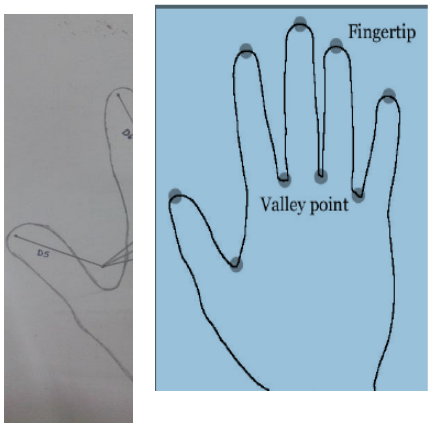

Figure 9:fingertip and valley points of a hand

After pre-processing, 19 features have been extracted(9 fingertip and valley point, 4 widths, 5 heights) where width is the distance from thumb valley point to all fingers valley point and Height is the height of the all the finger is measured as shown in Figure 10.

D. Matching

The feature matching determines the degree of similarity between stored feature vector and claimed feature vector. TheAs shown in figure 10 feature vector obtained from the input image which is matched against the features vector of images in the database. It is not necessary that under the best of condition the obtained features match exactly with the features of the same individual. The extracted features are in the form of positive integer. These are referred to as magnitude of the features. Absolute distance function is defined as [7].

$$D_a = \sum_{i=1}^{n} (Yi - Fi) \qquad (1)$$

Where, Fi=h(F1,F2,F3……Fd) is the feature vector with d dimension of a registered user in the database,
Y_i=h(Y_1,Y_2,Y_3…….Yd) is the features vector of an unknown or a claimer and

Figure 10: Features Extraction of hand

$F_i$is the mean of the 50 feature vector of 50registered person. Therefore distance between claimer features vector $Y_i$and database feature vector $F_i$is shown in following equation:

$$\text{Match Value} = \frac{Absolutedistance}{No.offeatures} \qquad (2)$$

After calculating the match, the system has compared the result with the predefined threshold and classifies the claimer. The system accepts the claimer if and only if the calculated match value is lower than the threshold and it rejects the claimer if and only if the calculated distance is higher than the threshold [7].

III. Simulation Results

The system has been tested on 500 images. Database of this system consist of 10 different acquisitions of 50 people. These images have contained some images of the same individuals taken at different time intervals. Since no pegs are used to align the position of the palm it is obvious that the alignment may vary for the images of the same individual. Although a slight rotation is acceptable the system is not completely rotation invariant [6]. One image of each users hand was selected to compute the feature vector which is stored in the database along with the user's name. The authentication refers

to the problem of confirming or denying a claim of individuals and considered as one to one matching.

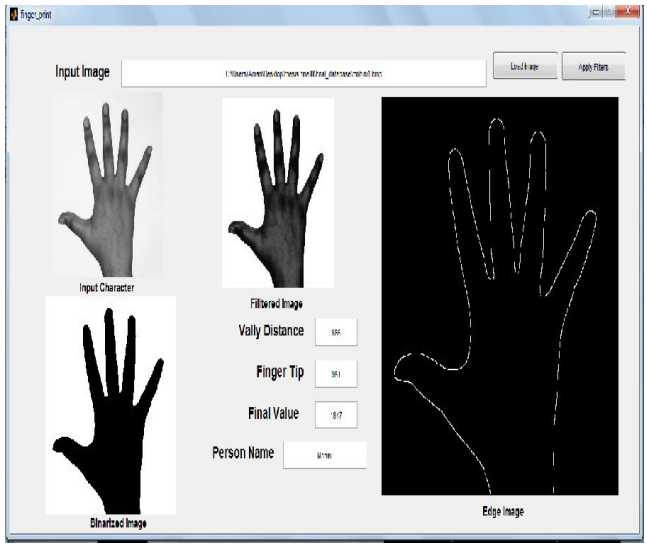

Figure 11:Results of Hand Geometry Measurement

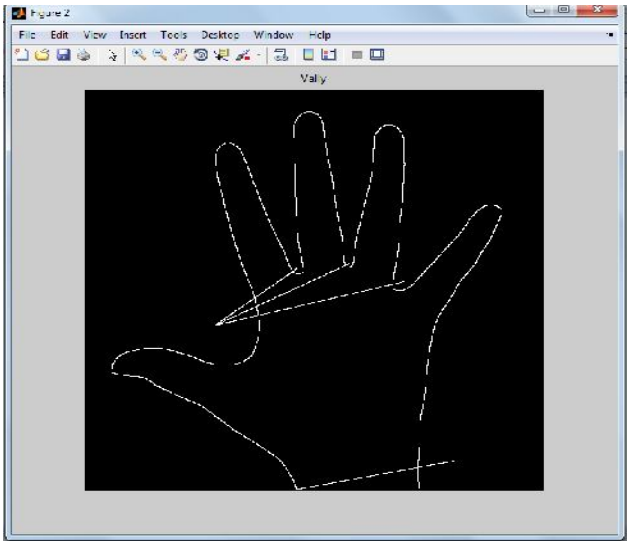

Figure 13:Distance from thumb to all fingers valley point

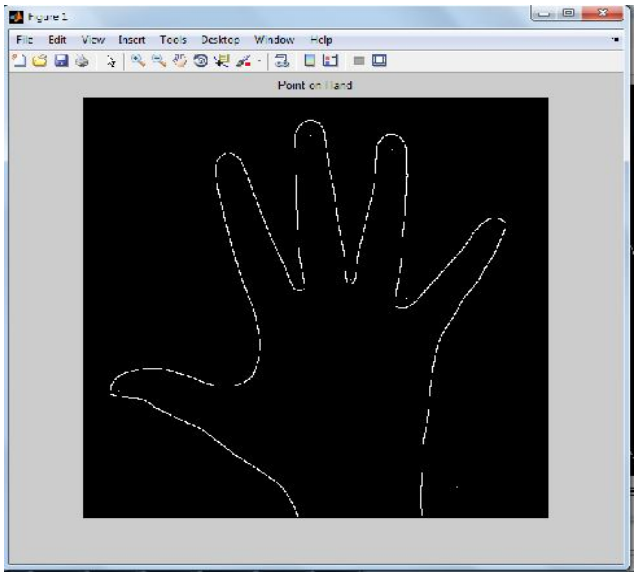

Figure 12:Fingertipand valley point of hand

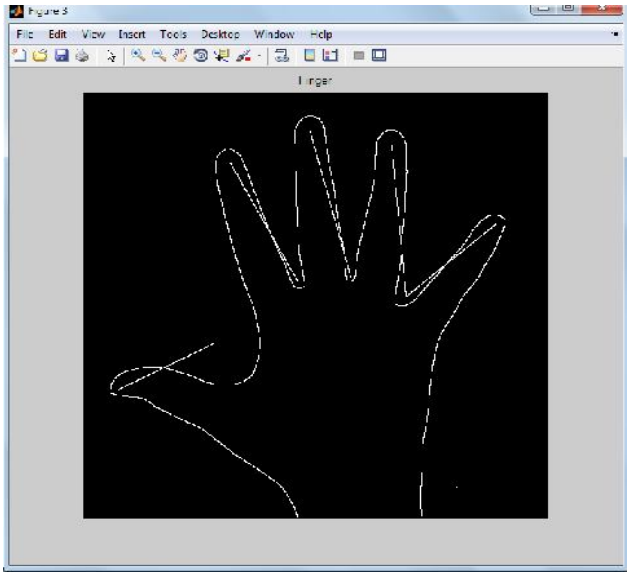

Figure 14: Distance from tip point to valley point

There are various performance measurement parameters of this proposed work, these are explained below:

1) **False Acceptance rate (FAR):**In access control systems, a false acceptance occurs when a sample is incorrectly matched to a different user's template in a database (in the case of an access control system, an impostor is allowed in the building)[2].

$$\text{FAR} = \frac{Total\ False\ Acceptance}{Total\ False\ Rejection} \quad (3)$$

2) **False Rejection rate (FRR):** A false rejection occurs when a sample is incorrectly not matched to an otherwise correct matching template in the database (in the case of an access control system, a legitimate enrolee is falsely rejected)[2].

$$\text{FRR} = \frac{Total\ False\ Rejection}{Total\ true\ attemts} \quad (4)$$

3) **Equal Error Rate (EER):** Error rate is a point where FRR and FAR are same. The ERR is an indicator on how accurate the device is lower the ERR is the better the system. The results of this experiment shows that EER=3%. The graph between error and threshold is shown in Figure 12[2].

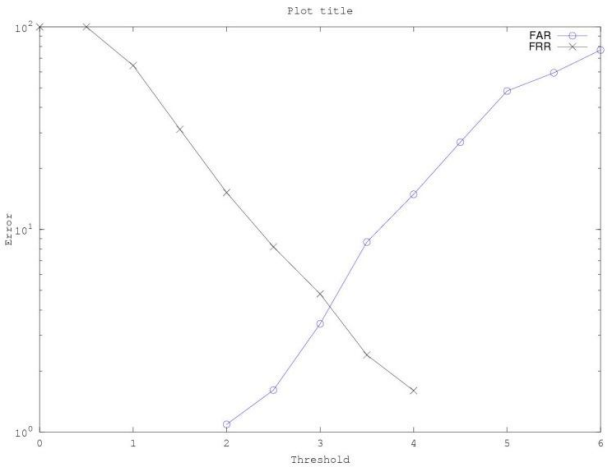

Figure 12: FAR-FRR CURVE(graph between error and threshold) shows that EER=3%.

IV. CONCLUSION AND FUTURE WORK

A peg free hand geometry authentication system has been developed in this work which is independent of orientation and placement of the hand. The system is experimented with a database consisting of 500 images collected over time from 50 users. Ten sample images from each user were used for authentication purpose. The authentication system extracts feature vector from the image and stores the template for later authentication. FRR is obtained by comparing the features vector of two different hands. The system shows effectiveness of results with accuracy around 97%. The ERR is found to be 3%.

The proposed work utilizes primarily the geometry of the hand. The palm creases and even the fingerprints can be extracted from the input image. Combining all these features in biometrics would result in a multimodal system with very high accuracy. The image extracted is in grayscale format. If a colour image is utilized for the system additional features such as the colour of the palm can also be used. For huge databases the search takes a long time and colour is so distinct. A feature that it can be used as an initial classifier so as to narrow the search space in the database considerably. The use of neural network based classifier trained on a larger database may result in further improvement of the system accuracy.

REFERENCES

[1] Rashmi Singhal and Payal Jain, "Biometrics:Enhancing Security," Asian Journal of computer science and information technology, pp. 89-92, 2011.

[2] Biometric Technology Application Manual Volume One:Biometric Basics Compiled and Published By National Biometrics Security Project Updated Summer 2008.

[3] R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos, "Biometric Identification Through Hand Geometry Measurements", IEEETrans. on PAMI, vol. 22, no. 10, pp. 1168-1171, October 2000.

[4] K. Jain, N. Duta, "Deformable Matching of Hand Shapes for Verification", Proc. of IEEE International Conference on ImageProcessing, Kobe, October1999.

[5] K. Jain, A. Ross, S. Pankanti, "A Prototype Hand Geometry-based Verification System", 2nd Int. Conference on Audio- and VideobasedPersonal Authentication (AVBPA), Washington, pp. 166-171March 1999.

[6] Y. Bulatov, S. Jambawalikar, P. Kumar, and S. Sethia, Hand recognition usinggeometric classifiers. 1999.

[7] N Covavisaruch,P Prateepamornkul, P Ruchikachorn and P Taksaphan,"Personal Verification and Identification Using Hand Geometry ," ECTI TRANSACTIONS ON COMPUTER AND INFORMATION TECHNOLOGY, vol.1, no.2, November 2005.

[8] Sampda A Dhole and V.H. Patil, "Person identification using pegfree hand geometry measurement," International journal of engineering science and technology, vol. 4, no. 6, 2012.