Biometric Feature based Person Unique Identification System

Trupti S. Indi
M.E. (CSE) - II
Walchand Institute of Technology
Solapur University
India

Suhas D. Raut
Phd, Professor Dept. CSE
Orchid College of Engineering & Technology
Solapur University
India

ABSTRACT
A wide variety of systems require reliable and accurate personal identification system. Major goal of such systems is to provide access of an application to legitimate users only. Such a set of applications include, but not limited to, banking applications, military applications, hospital applications, digital library. Majority of systems have started shifting towards biometric features of human beings for personal unique identification. Most popular biometric feature used is Thumbprint or thumb impression. Various researchers have come out with different solutions, albeit partially best, for personal identification based on thumb impression. However there exists no single solution that encompasses best of all & provides collectively a better solution. An effort is made in this paper to perform exactly the same based on experimental setup, findings, & analysis. Features of biometric characteristics of thumb print are extracted and stored into the database in text format. The matching algorithm uses these text formatted features for matching purpose & identification.

KEY WORDS
Biometrics, Minutiae, Thumbprint, Person, Identification

1. INTRODUCTION
In huge databases, distinguishing people from each other by using some number or code identification is a conventional method of user authentication. In applications where secure access is needed, e.g. banking applications, military applications, hospital applications, digital library access etc. identification of a person is done with the help of some password or PIN numbers or some personal information that is confidential. In such cases, remembering passwords or PIN numbers is difficult and or possibility of hacking passwords and personal information is more. In some systems instead of password entry, a card is given to each person for his/her identification. There is a possibility of card being stolen by some other person and used for illegal operations. Such kind of risks is unacceptable in secure systems.

To avoid such risks, evolving methods use BIOMETRIC features. These methods are used to uniquely identify a person based on one or more intrinsic physical or behavioural traits. Physiological information is the information related to the human's shape of body. E.g. fingerprint recognition, face recognition, iris recognition (retina recognition), hand geometry, DNA, palm print etc. Behavioural information includes information related to personal behaviour like style of walking, typing etc.

2. RELATED WORK
In biometrics system, fingerprint based identification is one of the successful method used for person identification. Each person has unique fingerprint. Local ridge characteristics and the relationship between them describe uniqueness of a fingerprint. These local ridge characteristics at ridge ending or a ridge bifurcation are minutiae points.

Minutiae-based matching grey scale fingerprint image analysis without binarization & thinning has been presented by WIECLAW [2]. He claims that the method is time efficient & avoids false minutiae introduced by skeletonization.

RAVI J et al. [3] presented fingerprint recognition using minutiae score matching in which block filter is used for fingerprint thinning and minutiae extracted from the thinned image. Here, block filter is used to preserve image quality. In this method, minutiae location and minutiae angles are derived as feature of minutiae after minutiae extraction.

Shahi Kumar et al. [4] presented a method for fingerprint verification based on fusion of Minutiae and Ridges using strength factors. In this method, fingerprint image is binarized & thinned during pre-processing step. The Minutiae Matching Score is determined using Block Filter and Ridge matching score is estimated using Hough Transform. The strength factors Alpha (a) and Beta (ß) are used to generate Hybrid matching score for matching of fingerprints.

In Fingerprint images, presence of noise leads to spurious minutiae. To void this problem, Kulwinder Singh et al. [5] proposed new feature extraction method in the paper titled "Fingerprint feature extraction". In this paper, new smoothing algorithm is proposed for detection of features of fingerprints. A method has been introduced for finding ridges in the fingerprint image with the help of eight different masks

Roja M. Mani [6] proposed a method which uses minimum resources to recognize fingerprint for online applications using minutiae extraction in time domain method and using Discrete Cosine Transform (DCT) in frequency domain method. In time domain method, four different features-namely ending, bifurcation, isolation and crossing points are considered. In frequency domain method, the locations of four minutiae features in a particular fingerprint image are combined and represented by an image on which DCT is performed. Three levels of fusion

schemes suggested: Fusion at feature level, Fusion at score level and Fusion at decision level.

Ipsha Panda et al. explained a method for fingerprint recognition which includes three steps: image pre-processing, minutiae extraction and minutiae matching. Here, based on the concept of neighbouring pixels some heuristic rules developed for minutiae extraction [7]. To remove spurious minutiae points, the method explained in this paper is different that a method presented by Kulwinder Singh et al. [5].

.

3. BIOMETRIC SYSTEM

Biometric is the automated recognition of individuals based on their behavioural and biological characteristics. Identification of any specific user can be determined by measuring an individual's suitable behavioural and biological characteristics in recognition process and compare these characteristics with the biometric reference data which had been stored during a registration process.
Anil Jain et al. [1] defined biometrics as pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database.

3.1 Biometric Features:

A biometric characteristic is a biological or behavioural property of an individual that can be measured and which will guide to distinguish individual from other. A biometric input is a representation of biometric characteristics which is required for biometric feature extraction. This can be obtained from biometric capture device like fingerprint sensor or camera. Biometric features are information extracted from biometric input. These features are used to compare with other biometric input features or biometric template. Biometric template stores biometric features.
To qualify biometric characteristic as biometric, it must satisfy following properties [1]:

i. **Universality:** This characteristic should be present in each person.

ii. **Distinctiveness:** Feature of this characteristic should be unique in each person. It should not be repetitive.

iii. **Permanence:** This feature should not change over time.

iv. **Measurability:** This characteristic should be measurable with technical devices.

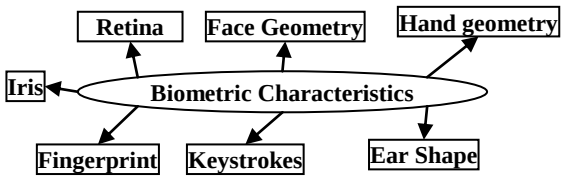
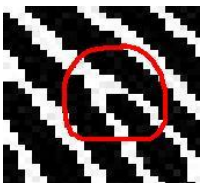


Figure1: Different Biometric Characteristics

Some of characteristics which can be used as biometric are fingerprint, iris pattern, retina pattern, face geometry, ear form etc. as shown in figure1.

3.2 Fingerprints as Biometric Characteristic:

A fingerprint is an impression generated by the friction of human finger. A fingerprint appears as a series of dark lines which represents the high, peaking portion of the friction ridge skin, while the valleys between these ridges appears as white space and are the low, shallow portion of the friction ridge skin. Fingerprint is collection of ridges and valleys on finger tip.
Ridges are dark areas of fingerprint and valleys are white areas that exist between the ridges. Thus, a fingerprint is defined by the uniqueness of the local ridge characteristics and their relationships.
Minutiae points are these local ridge characteristics. Minutiae points occurs at ridge ending called as termination point or at ridge split point called as bifurcation point as show in below figure2.



(a) Termination Point

(b) Bifurcation Point

Figure2: Minutiae Points (a) Termination Point and (b) Bifurcation Point

Fingerprint identification is based primarily on the minutiae, or the location and direction of the ridge endings and bifurcations (splits) along a ridge path.

4. SYSTEM ARCHITECTURE:

We are proposing multi-biometric system to identify person uniquely. In this system, person's left thumb impression and/or ear image is used for unique recognition. This system runs in two modes:

(1) Registration mode

(2) Identification mode

Along with biometric information, demographic information of a person is stored during registration mode. During identification mode, only biometric information will be used to identify person. This multi-biometric system's main advantage is that it can work as single-biometric system and/or as multi-biometric system. In this paper we have presented strategy for thumb impression only. An effort is made in this paper for unique

identification of a person by extracting thumb features and comparing with database thumb features.

As shown in System Architecture (figure 3), thumbprint, scanned using Hamster fingerprint scanner device, is stored in BMP file that becomes input to our system. The thumb processing system is divided into following stages:

1. Pre-processing
2. Binarization & Thinning
3. Minutiae Detection
4. Minutiae Extraction
5. Minutiae Insertion into Database

First four stages are common for registration mode and identification mode. Final stage is needed in registration mode to store data into database for comparison with data collected during identification mode.

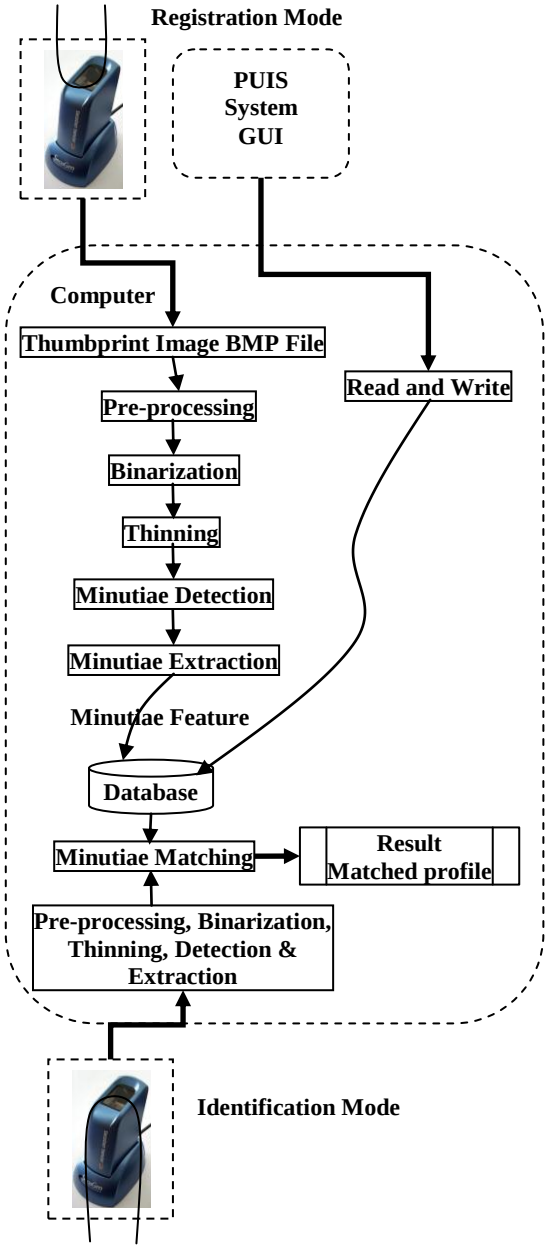


Figure3: System Architecture

In identification mode, fifth stage is needed to compare minutiae feature collected with minutiae features stored into database and display possible matching records.

The working of these stages is explained in detail below.

4.1 Pre-processing:

This stage includes processes related to image enhancement to acquire quality image for further processing. Pre-processing is necessary since input image may include noise or scanned image is not clear or some ridge's impression is unclear. Gaussian smoothing function is applied to enhance quality of an image before further processing. The function adjusts pixel intensity values using upper & below pixel percentages. This determines the desired intensity range. As images are grey-scale images, the input image is normalized by adjusting the range of grey-level values to make intensity values within the desired range. This allows scaling of in between pixel intensity values. Effect of such a pre-processing is shown in the figure4.

(a) Input image

(b) After pre-processing

Figure4: Effect of pre-processing

4.2 Binarization & Thinning:

Binarization process converts gray-scale image into binary image. Each pixel in binary image is converted into one bit value of either '1' or '0'. Thresholds are decided using Otsu's Thresholding Technique [9]. To decide threshold, histogram of image's pixel intensities is created. Valley point can also be used to decide threshold [8]. Spread of pixels is then measured on each side of threshold. This allows identification of each pixel as a foreground or background [9].

Thinning is an operation in which selected foreground pixels are removed from binary images. In thinning operation the topology or connectivity of the original image is preserved while removing selected original foreground pixels. T. Y. ZHANG and C. Y. SUEN presented fast parallel thinning algorithm. Presently it is called as Zhang-Suen thinning algorithm. It consists of two sub-iterations: (1) deleting the south-east boundary points and the north-west corner points (2) deleting the north-west boundary points and the south-east corner points. End points and pixel connectivity are preserved. Each pattern is

thinned down to a "skeleton" of unitary thickness [10]. We applied Zhang-Suen thinning algorithm on the output of binarization step and result is binary thinned image as shown in figure5.

(a) Binary Image

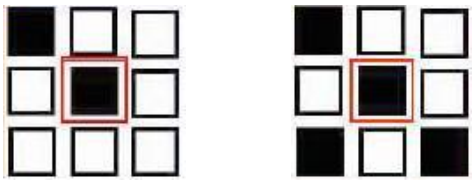
(b) Binary Thinned Image
Figure5: Binarization & Thinned

4.3 Minutiae Detection:

In this stage, Crossing Number is used to locate the minutiae points in fingerprint image as explained by Ravi J. et al. in FRMSM method. Crossing Number is defined as half of the sum of differences between intensity values of two adjacent pixels [3].

To calculate this crossing number for each pixel, 3X3 window is considered as shown in figure6. We considered termination and bifurcation minutiae points only in our implementation. If crossing Number is 1 then minutiae point is termination point and if minutiae point is 3 then minutiae point is bifurcation point as shown in figure6. In this way, minutiae points are detected in original image.

.



(a) Crossing Number 1 **(b) Crossing Number 3**

Figure6: Representation of Crossing Number on 3X3 window

After binarization of original image, complement of binary image is created and then thinning is applied to binary complement image to detect minutiae points.

4.4 Minutiae Extraction:

Once all minutiae points are detected in original image, incorrect minutiae points are removed with the help of complement image of original image. The bifurcation point in original image becomes termination point in complement image and vice versa. Incorrect minutiae points are not extracted.

In minutiae extraction stage, minutiae point location in terms of (X, Y) co-ordinate value and angle of minutiae point is decided. Hence minutiae feature is represented as (X, Y, Angle).

X = column index of minutia point in pixel grid

Y = row index of minutiae point in pixel grid

Angle = tan-1(Len_X / Len_Y)

Where,

LenX = Horizontal distance measured and

LenY = Vertical distance measured

These minutiae features from original image are extracted and stored into database along with demographic information collected from PUIS (Person Unique Identification System) GUI.

Following Table1 shows sample data extracted from one of the input thumbprint image file. This table is having four columns in which two columns gives X & Y co-ordinate value of point where minutiae point is detected. The fourth column indicates type of minutiae point. Here, in type column value 3 indicates that this minutia point is bifurcation point in original image. The third column indicates angle formed by the bifurcation point.

Table1: Sample Minutiae extracted from thumbprint image

X	Y	Angle	Type
118	169	45.0	3
197	203	78.69006752597979	3
43	74	80.53767779197439	3
85	205	80.53767779197439	3
165	154	45.0	3
138	190	63.43494882292201	3
89	174	75.96375653207353	3
110	287	80.53767779197439	3
133	40	80.53767779197439	3
201	69	45.0	3
81	184	45.0	3
138	190	63.43494882292201	3
14	190	63.43494882292201	3
67	260	45.0	3

4.5 Minutiae Insertion into Database:

To save these minutiae feature's data into database along with demographic data of person following tables created into the database. The relationship between tables is also shown in figure7:

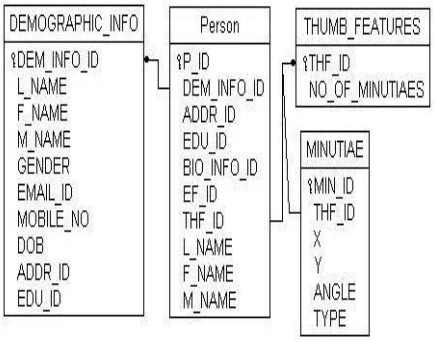


Figure7: Database Tables Used in PUIS System

4.6 Minutiae Feature Matching:

In this stage, minutiae feature points extracted from input fingerprint during identification mode is matched with minutiae feature points from database. Using following formula matching score is generated:

Formula:

$$Minutiae\ Score = \frac{Tn}{Min(Tnd, Tni)}$$

Where,

Tn = Total number of matching minutiae

Tnd = Total number of minutiae from database

Tni = Total number of minutiae from input fingerprint image

Following Table2 shows matching score for thumb of same person taken at different time instance. The original image file which is used during registration is tt.bmp and following image files are taken during identification mode.

Table2: Sample Minutiae extracted from thumbprint image

Day	Image file Name	Matching Score
1	tt1.bmp	0.556
2	tt2.bmp	0.824
3	tt3.bmp	0.236
4	tt4.bmp	0.567
5	tt5.bmp	0.1625

5. RESULT AND ANALYSIS:

We have tested our system for thumb impression processing with some 500 samples. We observed that exact matching ratio 90%+ while nearby thumb prints & their owner information is displayed for around 70% cases where the inputted image for matching in itself contains non-removable noise.

Following figure8 is the snapshot of PUIS system which is displaying thumb image and extracted minutiae features during registration mode. It also shows textboxes used to collect demographic information like name details, city, mobile number, birth date etc.

Figure8: Snapshot of PUIS System in Registration Mode

Following figure9 is the snapshot of PUIS system which displays matching process results along with input thumbprint minutiae list.

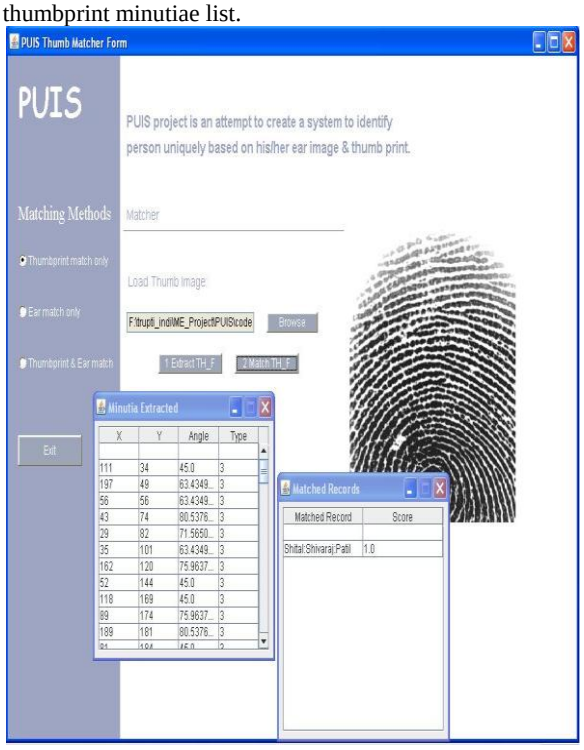


Figure9: Snapshot of PUIS System in Identification Mode

6. CONCLUSION AND FUTURE WORK:

In this paper we have presented a system for unique identification of person based on thumb prints. In thumb processing, we have implemented different image enhancement techniques such as Gaussian smoothing function, adjusting intensity values of each pixels etc. We have studied different binarization methods and selected one which gives us best results for input thumb image. We have studied some thinning algorithms like Hilditch, Rosenfeld and ZS algorithms. Based on results we have used ZS (Zhang-Suen) thinning algorithm. We feel that this is one of the most efficient methods of unique identification of a person based on thumb matching that combines best of all available practices.

We further wish to enhance effectiveness of the system in unique identification by incorporating ear image matching in addition to thumbprint. Together a matching score, based on ear & thumb images, will be generated to more accurate identification.

7. REFERENCES

[1] Jain Anil K., Ross Arun, and Salil Prabhakar: "An Introduction to Biometric Recognition" (IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004)

[2] WIECLAW Lukasz: "A MINUTIAE-BASED MATCHING ALGORITHMS IN FINGERPRINT RECOGNITION SYSTEMS" (JOURNAL OF MEDICAL INFORMATICS & TECHNOLOGIES Vol. 13/2009, ISSN 1642-6037)

[3] RAVI. J., K. B. RAJA, and VENUGOPAL. K. R: "FINGERPRINT RECOGNITION USING MINUTIA SCORE MATCHING" (International Journal of Engineering Science and Technology Vol.1 (2), 2009, 35-42)

[4] Shashi Kumar D. R., R. K. Chhotaray, K.B. Raja., and Sabyasachi Pattanaik: "Fingerprint Verification based on Fusion of Minutiae and Ridges using Strength Factors" (International Journal of Computer Applications (0975 - 8887) Volume 4 - No.1, July 2010)

[5] Kulwinder Singh, Kiranbir Kaur, and Ashok Sardana: "Fingerprint Feature Extraction" (IJCST Vol. 2, Issue 3, September 2011)

[6] M.Mani Roja and Dr.Sudhir Sawarkar: "Fingerprint Verification System - A Fusion Approach" (International Journal of Computer Applications (0975 - 8887)

[7] Ipsha Panda, Saumya Ranjan Giri, Prakash Kumar, and Anjali Mohaptra: "A New Approach To Fingerprint Recognition" (International Journal on Computer Science and Engineering (IJCSE) (0975-3397) Vol. 4 No. 05 May 2012)

[8]http://en.wikipedia.org/wiki/Thresholding_(image_processing)

[9] http://en.wikipedia.org/wiki/Otsu's_method

[10] ZHANG T. Y. and SUEN C. Y.: "A Fast Parallel Algorithm for Thinning Digital Patterns"