Fingerprint Biometric System: A Survey

Monika Sharma
(M.E. Student)
Department of Computer Science
PEC University of Technology
Chandigarh, India
monikasharma2207@gmail.com

Abstract— Fingerprint recognition is one of famous biometric system that is mostly used in various authentication techniques. Human fingerprint exhibit some certain details marked on it, categorized it as minutiae, which can be used as a unique identity of a person if recognize it in a well manner. This survey paper discusses the classification of fingerprints and different matching techniques that used in fingerprint recognition. The main aim of this paper is to discuss a complete system and an indigenous design model for fingerprint verification using minutiae extraction technique. To achieve a good quality minutiae extraction, firstly the fingerprint image is pre-processed by image enhancement which includes histogram equalization, fast fourier transformation and image binerization and then segmentation is done to get the effective area of the fingerprint followed by minutiae extraction which includes ridge thinning and minutiae marking and then a post-processing operation which includes removal of H-breaks, isolated points and false minutiae. Then, go for a final treatment which is minutiae matching, in which post processed fingerprint image is matched with the database and give decision.

Keywords-Fingerprint recognition, Minutiae Matching, Histogram Equalization

I. INTRODUCTION

Biometric is an automated method which is used to recognize an individual's identity by a unique physiological trait or behavioral characteristic, such as a fingerprint, face, retina, palm print, hand geometry, voice or signature. Conventional security systems used either knowledge based methods passwords or pins, and token-based methods driver license, passport, ID card and were prone to threat or fraud because passwords or PIN numbers could be forgotten and the tokens could be stolen, lost or duplicated. So a biometric system is required for robust, reliable, and foolproof personal identification, authentication systems. Biometric data cannot be stolen or guessed in same fashion as of password or token. Each individual has unique biometric traits so they can be used to prevent fraud or theft.

The most commonly used biometric technology is the fingerprint recognition system. Fingerprint recognition system refers to method of authentication by verifying match between two fingerprints. Because of their uniqueness and consistency of fingerprints over time, more recently becoming automated (i.e. a biometric) due to advancement in computing capabilities. Fingerprint recognition can be categorized into identification and verification. In fingerprint recognition, identification is defined as the process of determining identity of a person from biometric database without that person first claimed an identity, it performs one to many comparison and identified who is this person. Fingerprint verification, is defined as the process of accepting or rejecting the identity claim of a person using his fingerprint. It performs one to one comparison and give the decision is this person who claims to be. A fingerprint is the pattern of ridges and valleys on the surface of fingertip. Fingerprint matching is divided into four techniques minutia based matching, correlation based matching, pattern based matching and image base matching. The choice of which technology of matching is used depends on application.

II. FINGERPRINT RECOGNITION SYSTEM

A. Matching: Verification and Identification

Fingerprint recognition is the process of comparing questioned and known fingerprint against another fingerprint to verify that the impressions are from the same finger or not. Fingerprint recognition has two matching techniques: one is fingerprint verification and the other is fingerprint identification as shown in figure 1. In case of verification, a person initially enrolls his or her fingerprint into the verification system and his template is stored into database in some compressed format along with the person's name or by other identity. Each access is confirmed by the person identifying him or himself, then applying the fingerprint to the system such that the identity of that person can be verified [1]. Verification performs one-to-one matching and with the help of verification, biometric system accepts or denies that is claimed. When accessing a network it is a verification event- firstly user enters his ID and then verifies that he or she is a legitimate user by entering password or biometric. Identification, determines identity of any person from biometric database without that person first claiming an identity. Identification performs one-to-many matching*;* it determines who this person is. Fingerprint recognition is mainly used in crime investigations [2].

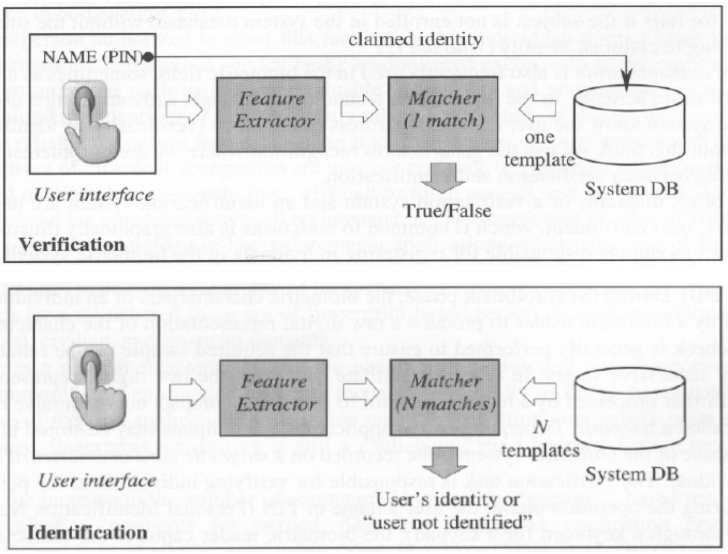

Figure 1 Matching: Verification and Identification

A user enrolls into biomeric system by providing biometric data which is converted into template and saved into biomteric database. In case of verification or identification, firstly user enrolls into biometric system then feature extractor extracts the features. Then matching is performed, in which the features extracted from input fingerprint is compared against one or more existing templates and then decision should be taken.

B. Feature Types

A fingerprint is made up of many ridges and furrows. There are good similarities between these ridges and furrows for a taken small local window, according to their average width and parallelism. but, on the basis of thorough research on fingerprint recognition, come to the conclusion that fingerprint are not recognized using their ridges and furrows, but minutiae plays a vital role in fingerprint recognition, which are differentiated by some abnormal points on the ridges as shown in below figure 2 and in figure 3. There is a variety of minutiae as shown in figure 3 such as termination, bifurcation, lake, independent ridge, dot, spur and crossover. Although there have a variety of minutiae types but two types of minutiae are mainly used and most significant. In which, one is called "termination" which can be characterized as the immediate ending of a ridge and the other one is called "bifurcation" which can be characterized as the point on the ridges where two branches are bifurcated [2] as shown in figure 2.

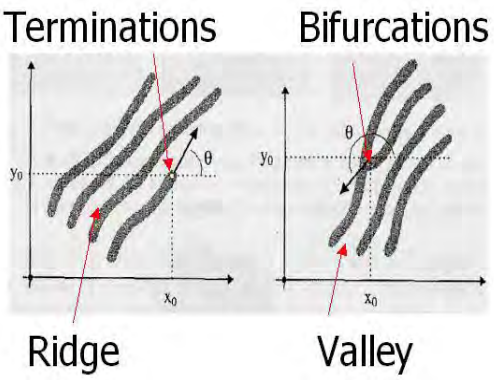

Fig 2: Minutiae (Ridge Termination and Bifurcation)

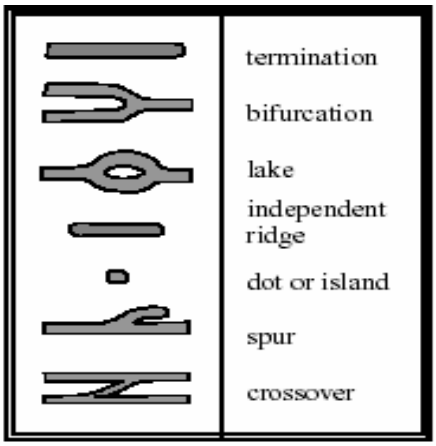

Fig 3: Different types of Minutiae

From more than 30 years, Fingerprint classification techniques have been a research topic. There are many fingerprints classification methods have been designed [5]. The most common fingerprint classes are as given below and also shown in figure 4:

- Arch: A fingerprint pattern in which the ridges pattern begins from one side of the pattern and leaves from other side
- Loop: A fingerprint pattern in which the ridge pattern flows inward and returns in the direction of the origin.

- Whorl: contains at least one ridge that makes a complete 360 degree path around the center of the fingerprint. Two loops (same as one whole) and two deltas can be found.

Two other features that are sometimes used for matching is core and delta shown in figure 4. Fingerprint pattern has a center point which is called core. A singular point from which three patterns are deviated is called delta. The core and delta locations can be employed as landmark locations which are used to orient two fingerprints for subsequent matching [2].

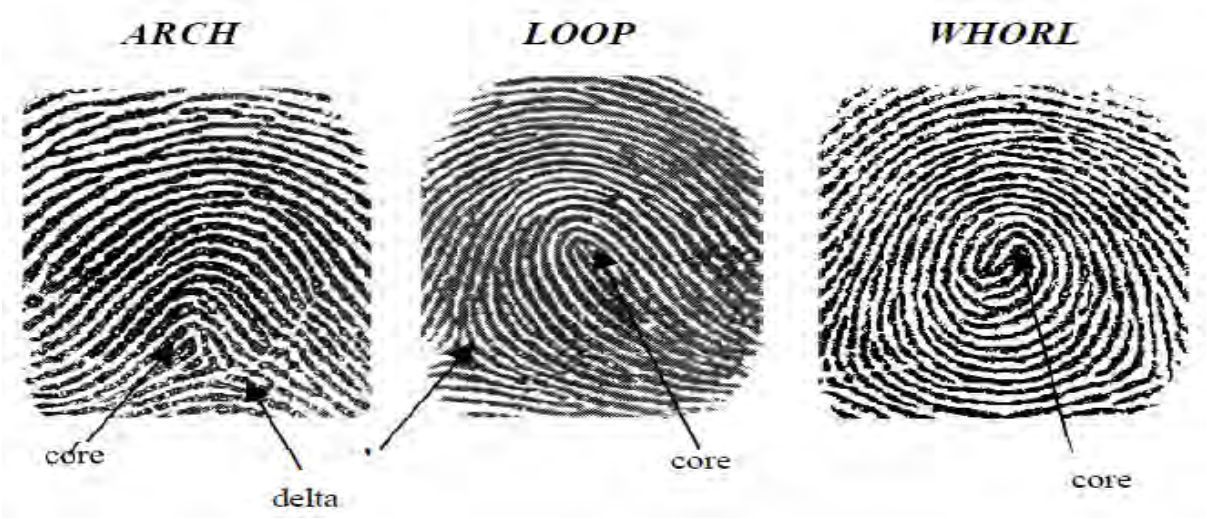

Fig 4: Fingerprint patterns: arch, loop, and whorl; and core and delta fingerprint landmarks

III. FINGERPRINT MATCHING TECHNIQUES

The number of approaches for fingerprint matching can be classified into four families [3]:

A. Minutiae Extraction Technique

Most of the fingerprint technologies are used minutiae extraction techniques. Minutia based techniques characterize the fingerprint by its feature types, ridge terminations and ridge bifurcations. This technique of fingerprint recognition is the most commonly and widely used. Minutiae are extracted from fingerprints and then stored as template into biometric database for further process. Minutiae based matching essentially made of discovering the alignment between the template and candidate fingerprint [4].

B. Pattern Matching or Ridge Feature

Feature extraction and template generation are based on series of ridges as opposed to discrete points which forms the basis of Pattern Matching Techniques [4]. The advantage of Pattern Matching techniques over Minutiae Extraction is that minutiae points may be affected by wear and tear and the disadvantages are that these are sensitive to proper placement of finger and need large storage for templates. In pattern based algorithms comparison of the basic fingerprint patterns such as arch, whorl, and loop is performed between a earlier stored template and a candidate fingerprint. The fingerprint images should be aligned in the same orientation. To get it, the pattern based matching algorithm acquires a innermost central point in the fingerprint image. In a pattern based matching algorithm, the template consists of the size, type and orientation of patterns within the aligned fingerprint image [10]. To find out the degree at which they match the candidate fingerprint image is compared with the stored template graphically.

C. Correlation Based Technique

In correlation based matching techniques initially two fingerprint images are superimposed and then the correlation between consequent pixels is calculated for different alignments. The cross correlation is an excellent measure of determining image similarity and the image maximization.

D. Image Based Techniques

In Image based techniques matching is performed on the basis of global features of a complete fingerprint image. This technique is an advanced and newly emerging method for fingerprint recognition.

IV. FINGERPRINT RECOGNITION SYSTEM USING MINUTIA EXTRACTION TECHNIQUE

The basic method of minutiae extraction is divided in to three part preprocessing of fingerprint image, minutiae extraction, and then post processing [6]. Our method divides three basic steps in to 8 modules which are given below and shown in figure 5.

Step 1: Load image

In this step firstly image is captured and processed through a series of image processing algorithms.

Step 2: Histogram Equalization:

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. the histogram after the histogram equalization occupies the range from 0 to 255 and the visualization effect is enhanced [7].

Step 3: Fast Fourier Transformation:

The image is partitioned into small processing blocks (32 by 32 pixels) and the Fourier transform is performed according to the formula given below:

$G(x,y) = f^{-1} \{ f(u,v) * f(u,v)^{k} \}$

Step 4: Binarization:

Binarization transforms the 8 bit gray fingerprint image into a 1 bit fingerprint image with 0 value used for ridges and 1value used for furrows. Local Adaptive approach is used.

gray value of each pixel g is calculated as

if g > Mean(block gray value) , set g = 1;

Otherwise g = 0

Step 5: Region of Interest:

The fingerprint image area that does not have effective ridges and furrows is firstly discarded because it only holds background information. Then the bound of the remaining useful area is sketched out since the minutia in the bounded region is confusing with that spurious minutia that is produced when the ridges are out of the sensor. To find out the Region of interest, a two step method is used. The first step which is used block direction estimation and direction variety check, while the second step is intrigued from some morphological methods.

Step 6: Thinning:

Ridge thinning is used to remove the redundant pixels of ridges [7]. It uses an iterative, parallel thinning algorithm.

1) To get a thinned image we find the location of middle black pixel at each stage of continuation of the curve.

2) The algorithm used marks down each redundant pixel in each small image window (3x3) in each scan of the full fingerprint image.

3) And after several scans it finally removes all those marked pixels.

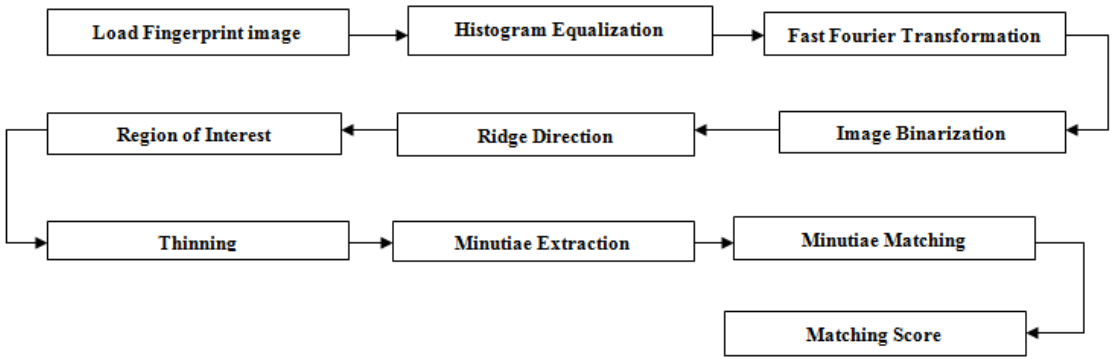

Fig 5: Fingerprint recognition using minutiae extraction technique

Step 7: Minutiae Extraction:

This operation takes thinned image as input and produces refined skeleton image by converting small straight lines to curve to maximum possible extant. For extracting minutiae point we compute the number of one-value of every 3x3 window:

- If the centroid is 1 and has only 1 one valued neighbor, then the central pixel is a termination.
- If the central is 1 and has 3 one-value neighbors, then the central pixel is a bifurcation.
- If the central is 1 and has 2 one-value neighbors, then the central pixel is a usual pixel.

Step 8: False Minutiae Removal

Procedure which is used for removing false minutiae is given below [8]:

- If the two minutiae points are present in the same ridge and the distance between one bifurcation and one termination is fewer than D. Then both of them bifurcations are removed. Where D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.
- If two bifurcations are present in the same ridge and the distance between both of two bifurcations is less than D, then eliminate these two bifurcations.
- If the distance between two terminations is fewer than D and their directions are almost coincident with a small angle variation. And both of terminations satisfied the condition that any other termination is located between the two terminations. Then both of two termination points are marked as false minutia which is derived from a broken ridge and are removed.
- If two terminations are placed in a short ridge with length less than D, then remove the two terminations.
- If a branch point has at least two neighboring branch points, and each of branch points are no further away than maximum distance threshold value and these branch points are closely connected on common line segment than remove the branch points.

And in last minutiae matching is performed. Two fingerprint images to be matched and any one of minutia is chosen from each image, and then the similarity of the two ridges associated with the two referenced minutia points is evaluated. If the similarity is larger than a predefined threshold value, then results come true otherwise false.

V. CONCLUSION

Biometrics is a means of verifying personal identity by measuring and analyzing unique characteristics like fingerprints. Finger print biometrics is one of the efficient, secure, cost effective, ease to use technologies for user authentication .This paper presents the detailed information about fingerprint biometrics. Fingerprint classification and fingerprint matching techniques such as minutiae based matching, correlation based matching, pattern based matching and image based matching techniques are discussed. Fingerprint recognition system using minutiae extraction technique is discussed in detail.

REFERENCES

[1] Anil Jain and Lin Hong, (1996) “On-line Fingerprint Verification”, Proc. 13th ICPR, Vienna, pp. 596-600.
[2] Anil Jain, R. Bolle and S. Pankanti, Biometric Personal identification in network society, Kluwer publishers, 1998.
[3] L.C. Jain, Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press, 1999.
[4] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder Sandhu, “Fingerprint Verification System using Minutiae Extraction Technique”, World Academy of Science, Engineering and Technology 46 2008.
[5] D. Maltoni , D. Maio, A. K.Jain and S. prabhakar , “Handbook of Fingerprint Recognition,” Second Edition, Springer , 2009.
[6] NTSC Subcommittee on Biometrics, "Fingerprint Recognition", 2000.
[7] Lin Hong, Yifei Wang, and Anil Jain, “Fingerprint Image Enhancement: Algorithm and Performance Evaluation”‘ IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(8), August 1998.
[8] Ravi.J.et al , “Fingerprint Recognition Using Minutia Score Matching” IJEST,Vol.1(2),2009,35-42.
[9] Gualberto Aguilar, Gabriel Sanchez & Mariko Nakano, “Fingerprint Recognition”, IEEE, Second International Conference on Internet Monitoring & Protection, 2007.
[10] Gualberto Aguilar, Gabriel Sanchez, “Fingerprint Recognition” IEEE, 2007.
[11] Jun Ma, Xiaojun Jing, Yuanyuan zhang, “Simple effective fingerprint segmentation algorithm for low quality images”, IEEE 2010.