

Fingerprint Recognition Using Minutiae Extractor

¹Manisha Redhu ² Dr.Balkishan

Department of Computer Science, Maharshi Dayanand University, Rohtak, India

ABSTRACT

The popular Biometric used to authenticate a person is fingerprint which is unique and permanent throughout the person life. Fingerprint Recognition or fingerprint authentication refers to the automated methods of verifying a match between two human fingerprints. Fingerprints are widely used in daily life for more than 100 years due to its feasibility, distinctiveness, permanence, accuracy, reliability, and acceptability. A large number of approaches to fingerprint matching and various algorithms and methods are behind their matching procedure. Example of these matching are correlation matching, Minutiae Based matching and pattern based matching. In this paper we projected Fingerprint Recognition using Minutiae Score matching method.

Keywords – Biometric authentication, Fingerprint recognition, Minutiae matching, Correlation Matching, Pattern Matching.

I. INTRODUCTION

Fingerprints have been scientifically studied for a number of years in our society. The characteristics of fingerprints were studied as early as the 1600s. In 1684, the English plant morphologist, Nehemiah Grew, published the first scientific paper reporting his systematic study on the ridge, furrow, and pore structure. In 1788, a detailed description of the anatomical formations of fingerprints was made by Mayer. In 1823, Purkinji proposed the first fingerprint classification, which classified into nine categories. Sir Francis Galton introduced the minutiae features for fingerprint matching in late 19th century.

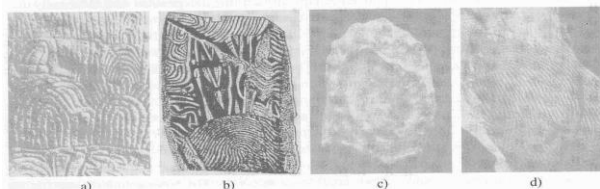


Figure 1.8. Examples of archaeological fingerprint carvings and historic fingerprint impressions a) Neolithic carvings (Gavrinis Island) (Moenssens, 1971); b) standing stone (Goat Island, 2000 B.C.) (Lee and Gaensslen, 2001); c) a Chinese clay seal (300 B.C.) (Lee and Gaensslen 2001); d) an impression on a Palestinian lamp (400 A.D.) (Moenssens, 1971). Although impressions on the Neolithic carvings and the Goat Island standing stones might not be used to indicate identity, there is sufficient evidence to suggest that the Chinese clay seal and impressions on the Palestinian lamp were used to indicate the identity of the providers. Figures courtesy of A. Moenssens, R. Gaensslen, and J. Berry.

Figure 1: Example of historic fingerprint impression

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints.

Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Because of their uniqueness and consistency over time, fingerprints have been used for over a century, more recently becoming automated (i.e. a biometric) due to advancement in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration.

II. FINGERPRINT

Fingerprints are fully formed at about seven months of fetus development. General characteristics of the fingerprint emerge as the skin on the fingertip begins to differentiate flow of amniotic fluids around the fetus and its position in the uterus change during the differentiation process. Thus the cells on the fingertip grow in a microenvironment that is slightly different from hand to hand and finger to finger.

Fingerprint is a pattern of ridges, furrows and minutiae, which are extracted using inked impression on a paper or sensors.

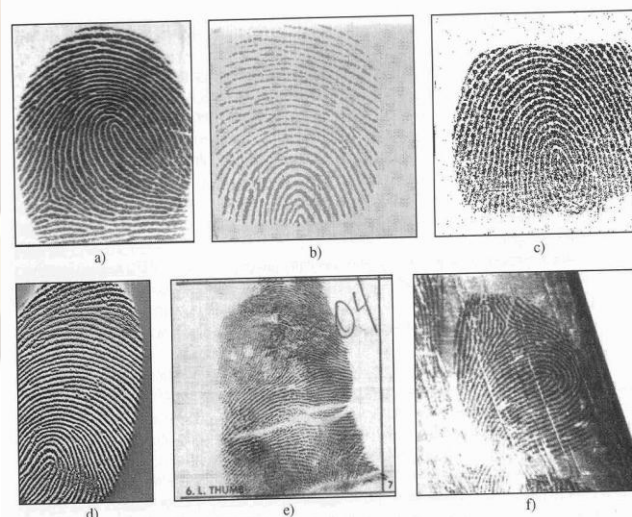


Figure 1.10. Fingerprint images from: a) a live-scan FTIR-based optical scanner; b) a live-scan capacitive scanner; c) a live-scan piezoelectric scanner; d) a live-scan thermal scanner; e) an off-line inked impression; f) a latent fingerprint.

Figure 2: Different fingerprint Images

Fingerprints have a core around which patterns like swirls, loops, or arches are curved to

ensure that each print is unique like arch ,loop ,whorl.

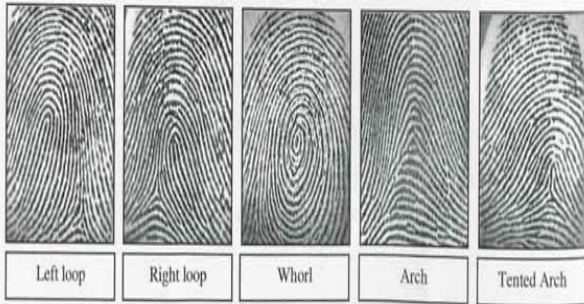


Figure 2.1. Examples of fingerprint classes
 The ridges and furrows are characterized by irregularities known as *minutiae*, the distinctive feature upon which finger scanning technologies are based. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown as identical.

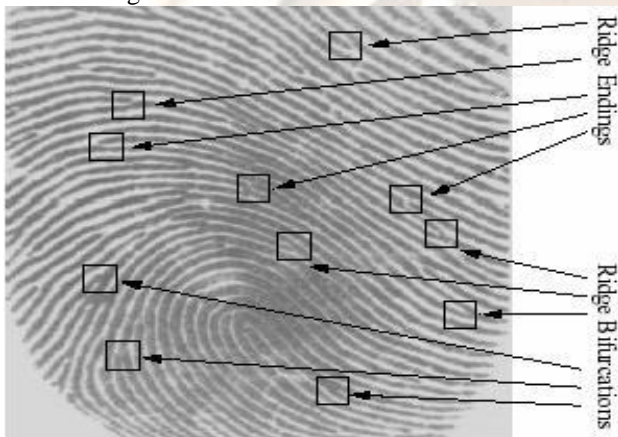


Figure 2.2 Minutiae points on fingerprint

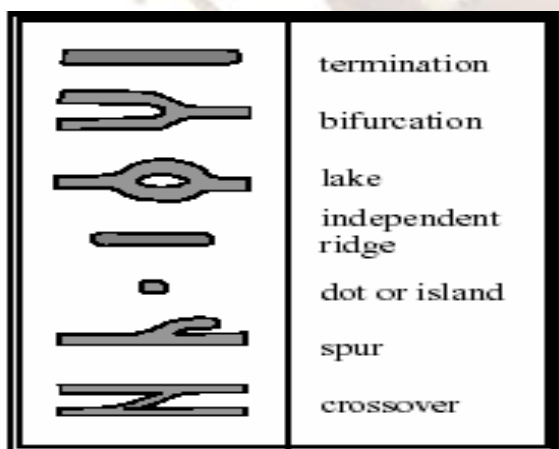


Figure 2.3 Different types of minutiae

III. FINGERPRINT FEATURE EXTRACTION

Fingerprint pattern exhibits different types of fingerprint features:

- Level 1 (Global Level): When the ridges are parallel. They are classified as loop, delta, and whorl are shown in Figure 3.1

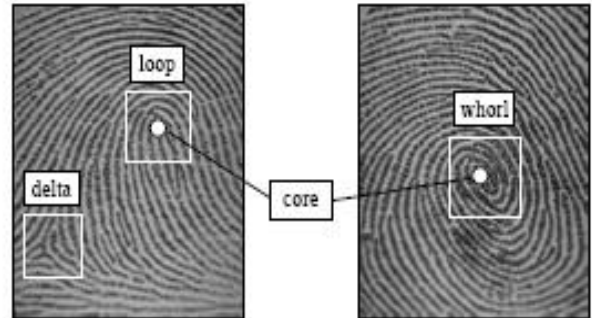


Figure 3.1 Delta, loop, whorl

- Level 2 (Local Level): It is based on minutiae in which the ridges are discontinuous. They are classified as ridge ending, ridge bifurcation, lake, independent ridge, point or island, spur, crossover are shown in Figure 3.2

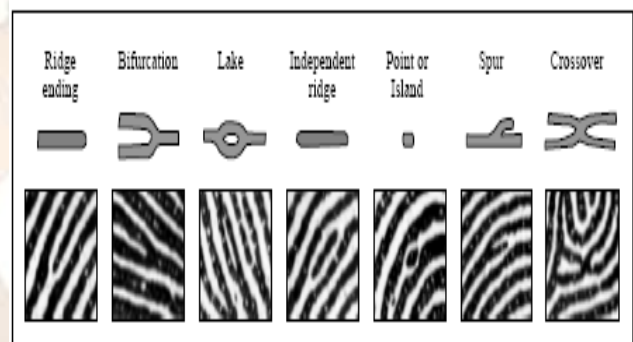


Figure 3.2 Ridge ending, Bifurcation, Lake, Independent ridge, Point or Island, Spur, Crossover

- Level 3 (Very Fine Level): Intra ridge details are detected. Sweat pores are considered at this level is shown in Figure 3.3



Figure 3.3 White pores are Sweat Pores.

IV. FINGERPRINT MATCHING TECHNIQUES

The large number of approaches to fingerprint matching can be coarsely classified into three families.

1. **Correlation-based matching:** Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations).
2. **Minutiae-based matching:** This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two- dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets that results in the maximum number of minutiae pairings
3. **Pattern-based (or image-based) matching:** Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

In Our project we have implemented a minutiae based matching technique. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products.

V. IMPLEMENTATION

We have concentrated our implementation on Minutiae based method. In particular we are interested only in two of the most important minutia features i.e. Ridge Ending and Ridge bifurcation. (Figure 5.1)

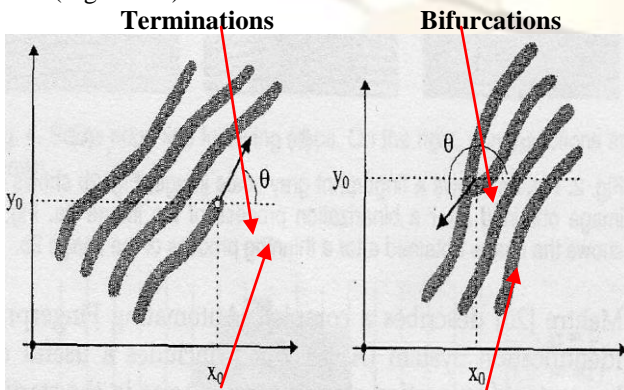


Figure 5.1(a) Ridge Ending, (b) Ridge Bifurcation

The outline of our approach can be broadly classified into 2 stages - Minutiae Extraction and Minutiae matching. Figure 5.2 illustrates the flow diagram of the same.

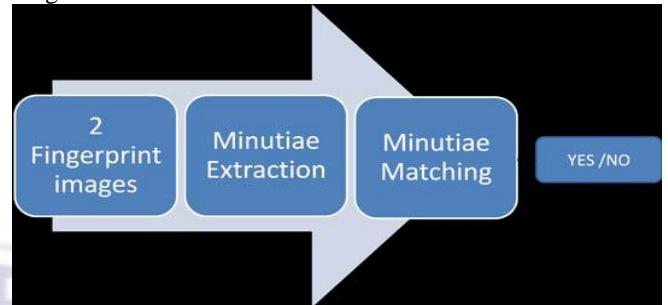


Figure 5.2 System Flow Diagram

The system takes in 2 input fingerprints to be matched and gives a percentage score of the extent of match between the two. Based on the score and threshold match value it can distinguish whether the two fingerprints match or not. The input fingerprints are taken from the database provided by FVC2004 (Fingerprint Verification Competition 2004).as shown in Figure 5.3

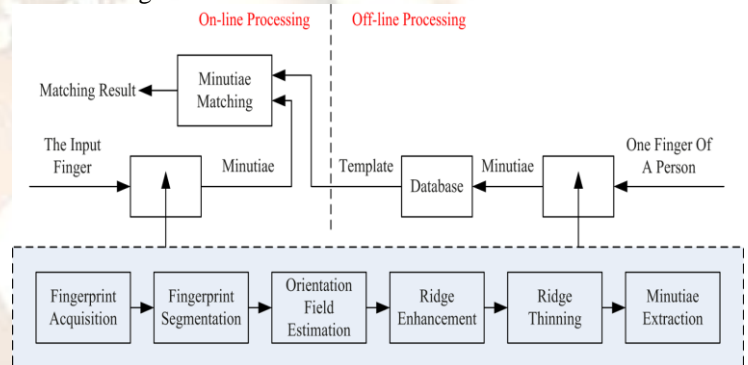


Figure5.3 Implementation Procedure

5.1 Design Description

The above system is further classified into various modules and sub-modules as given in Figure 5.1.1

- System level design
- Algorithm design

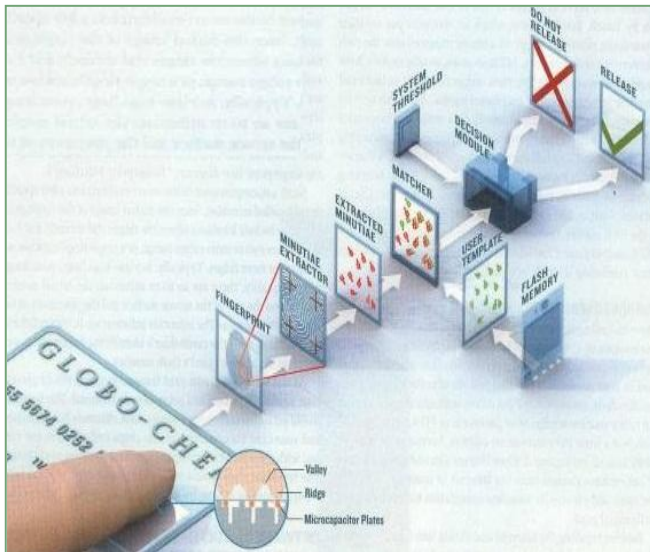


Figure 5.1.1 System Design

Minutia extraction includes Image Enhancement, Image Segmentation and Final Extraction processes while Minutiae matching include Minutiae Alignment and Match processes.

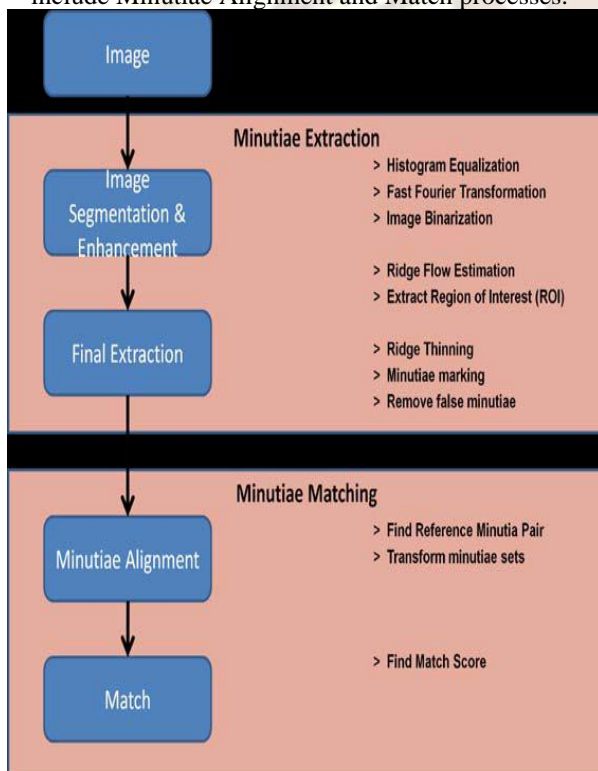


Figure 5.1.2 Detailed Design Description

- Under image enhancement step Histogram Equalization, Fast Fourier Transformation increases the quality of the input image and Image Binarization converts the grey scale image to a binary image.
- Then image segmentation is performed which extracts a Region of Interest using Ridge Flow Estimation and MATLAB's morphological functions.

Thereafter the minutia points are extracted in the Final Extraction step by Ridge Thinning, Minutia Marking and Removal of False Minutiae processes.

Using the above Minutia Extraction process we get the Minutiae sets for the two fingerprints to be matched. Minutiae Matching process iteratively chooses any two minutiae as a reference minutia pair and then matches their associated ridges first. If the ridges match well, two fingerprint images are aligned and matching is conducted for all remaining minutiae to generate a Match Score. As shown in figure 5.1.3

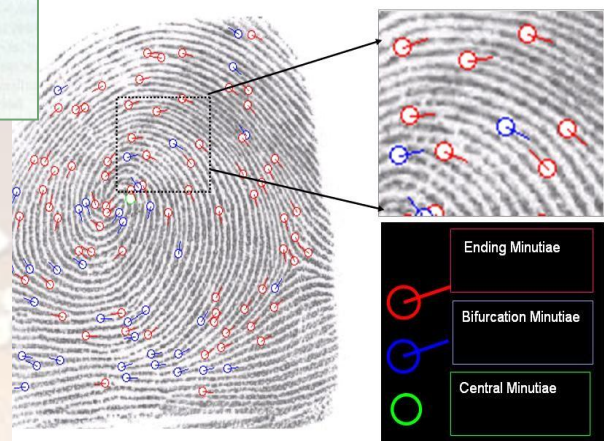
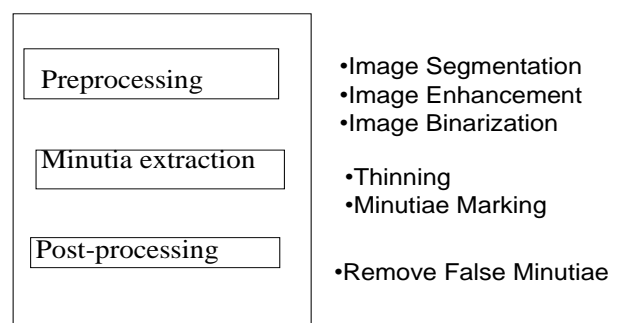


Figure 5.1.3 Minutiae Matching

VI. MINUTIAE EXTRACTAR

As described earlier the Minutiae extraction process includes image enhancement, image segmentation and final Minutiae extraction.as shown in flowchart.



Flowchart in explains the minutiae extraction process from the fingerprint. In the first stage Image maps are generated from the input fingerprint. The quality maps indicate internal quality of the fingerprint. The values 0-4 mark different conditions (low contrast, high contrast, high curvature, low ridge flow) within the fingerprint [15].

These values help in removing the false minutiae from the fingerprint. In the second stage image binarization is performed and the minutiae are detected from the binarized fingerprint image. Removal of false minutiae from the fingerprint is based on the quality factor. After removing false minutiae the minutiae which are left are known as real minutiae.

6.1 Fingerprint Image Enhancement/Pre-Processing

The first step in the minutiae extraction stage is Fingerprint Image enhancement. This is mainly done to improve the image quality and to make it clearer for further operations. Often fingerprint images from various sources lack sufficient contrast and clarity. Hence image enhancement is necessary and a major challenge in all fingerprint techniques to improve the accuracy of matching. It increases the contrast between ridges and furrows and connects the some of the false broken points of ridges due to insufficient amount of ink or poor quality of sensor input.

In our project we have implemented three techniques: Histogram Equalization, Fast Fourier Transformation and Image Binarization.

6.1.1 Histogram Equalization

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptual information. The original histogram of a fingerprint image is shown in [Figure 6.1.1.1], the histogram after the histogram equalization is shown in [Figure 6.1.1.2].

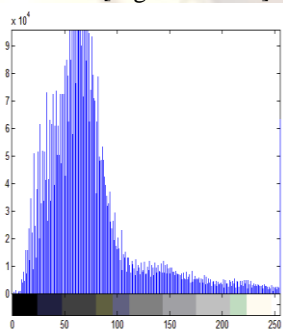


Figure 6.1.1.1

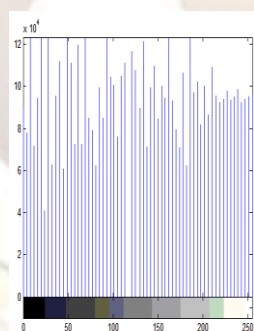


Figure 6.1.1.2

- For a grayscale image $\{x\}$
- let n_i be the number of occurrences of gray level i . Then the probability of an occurrence of a pixel of level i in the image is:

$$p_x(i) = p(x=i) = \frac{n_i}{n}, \quad 0 \leq i < L$$

- 'L' is total number of gray levels in the image
- 'n' is total number of pixels in the image
- 'p_x(i)' is the image's histogram for pixel value i
- Also, the cumulative distribution function corresponding to p_x is:

$$cdf_x(i) = \sum_{j=0}^i p_x(j)$$

- The transform of the image is defined as:

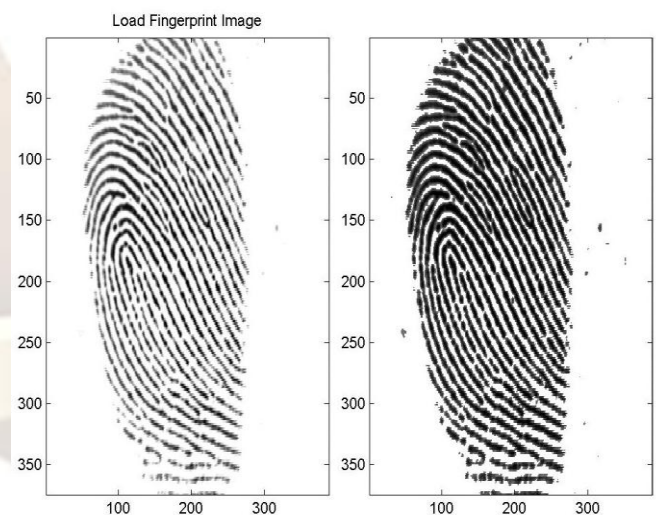
$$y = T(x) = cdf_x(x)$$

- The cdf of a pixel x represents the probability that a random pixel is less than or equal to x.

- After this process, the cdf of each pixel is normalized to [0,255]

$$h(v) = \text{round} \left(\frac{cdf(v) - cdf_{min}}{(M \times N) - cdf_{min}} \times (L - 1) \right)$$

- Cdf_{min} is the minimum value of the cumulative distribution function (in this case 1)
- M × N is the image's number of pixels
- L is the number of grey levels used (most cases L=256)



Fingerprint Verification - 99050056
Figure 6.1.1.3(a) Original Image, (b) Enhanced Image after histogram equalization

6.1.2 Fast Fourier Transform

The Fourier transform is done to find the frequency of the pixel. So the output would be an image in the frequency domain. The image is divided into blocks in order to enhance a specific block by its

dominant frequencies .so, the process is to multiply the FFT of the block by its magnitude a set of times.

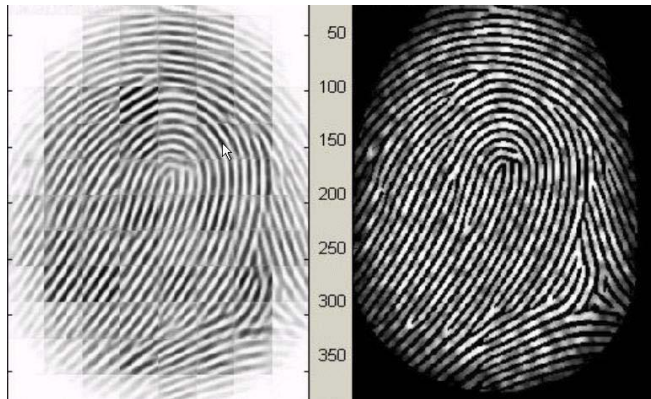


Figure 6.1.2.1(a) Enhanced Image after FFT, (b) Image before FFT

The enhanced image after FFT has the improvements as some falsely broken points on ridges get connected and some spurious connections between ridges get removed.

6.1.3 Image Binarization

This step is done to convert a 256-level image to a 2-level image It's done to differentiate image pixels from background Because of variations in contrast, locally adaptive thresholding is used

- **First, the image is divided into blocks (16x16)**
- **The mean intensity value is calculated for each block**

Assume gray value of each pixel= g ;

if $g > \text{Mean}(\text{block gray value})$, set $g = 1$;

Otherwise $g = 0$

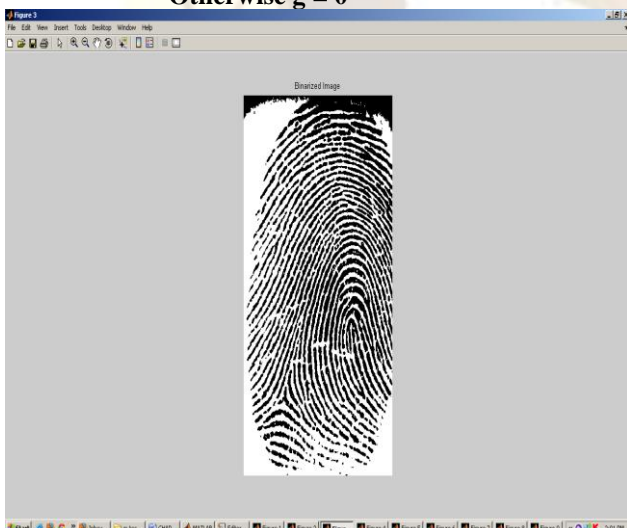


Figure 6.1.3.1 Binarized Image

6.1.4 Image Segmentation

Only a certain Region of Interest (ROI) is useful to be recognized for each fingerprint image To extract the ROI, a two-step method is used; block direction estimation and ROI extraction.

Block direction estimation

- Get gradient $x (g_x)$, gradient $y (g_y)$
- Estimate the θ according to:

$$\theta = \tan^{-1} \left(\frac{G_y}{G_x} \right)$$

ROI extraction (Morphological Method)

- **Close** (shrink images and eliminate small cavities)
- **Open** (expands images and remove peaks introduced by background noise)

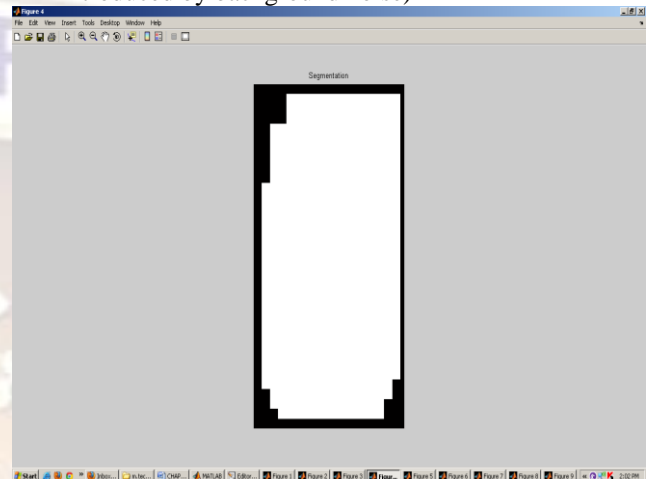


Figure 6.1.3.1 Segmented Image

6.2 Final Minutiae Extraction

Now that we have enhanced the image and segmented the required area, the job of minutiae extraction closes down to four operations: Ridge Thinning, Minutiae Marking, False Minutiae Removal and Minutiae Representation.

6.2.1 Image Thinning

To eliminate the redundant pixels of ridges till the ridges are just one pixel wide.

Morphological approaches:

- $\text{bwmorph}(\text{binaryImage}, 'thin', \text{Inf})$

This process is done by turning pixels off according to these conditions:

- If there is at least 1 switch from on to off among boundary pixels
- Not all 8-neighborhood pixels are on.
- Neither a center nor ending pixel.

P9	P2	P3
P8	P1	P4
P7	P6	P5

Figure 6.2.1.1 Image Thinning image

Filter by other Morphological operations to remove some H breaks and isolated points. In this

step, any single points (single-point ridges or single-point breaks) in a ridge are eliminated and considered processing noise. Done using imerode and imfill.



Figure 6.2.1.2(a) Image before, (b) Image after thinning

6.2.1 Feature extraction/ Minutiae marking

The concept of Crossing Number (CN) is used. CN is calculated by investigating the 8-neighborhood of each central pixel (p) in order to determine the count of crossover occurrences

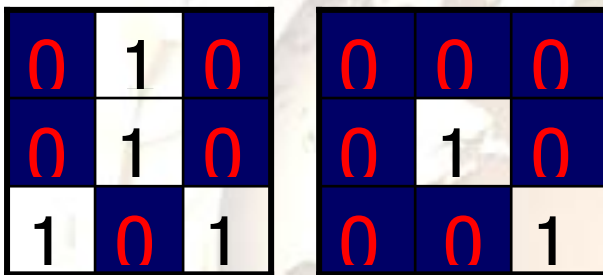


Figure 6.2.1.1 Bifurcations and Termination For a 3x3 window:

- If $p=1$ and has only 1 one-value neighbor, then the central pixel is a ridge ending
- If $p=1$ and has exactly 3 one-value neighbors, then the central pixel is a ridge branch

i.e. for a pixel P, if $C_n(P) = 1$ it's a ridge end and if $C_n(P) = 3$ it's a ridge bifurcation (Cn being the number of 1-valued neighboring pixels)

6.3 False Minutiae Removal/Post Processing

The preprocessing stage does not usually fix the fingerprint image in total. For example, false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. Actually all the earlier stages themselves occasionally introduce some artifacts which later lead to spurious minutia. These false minutiae will significantly affect the accuracy of matching if they are simply regarded as genuine minutiae. So some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective.

Seven types of false minutia are specified in following diagrams:

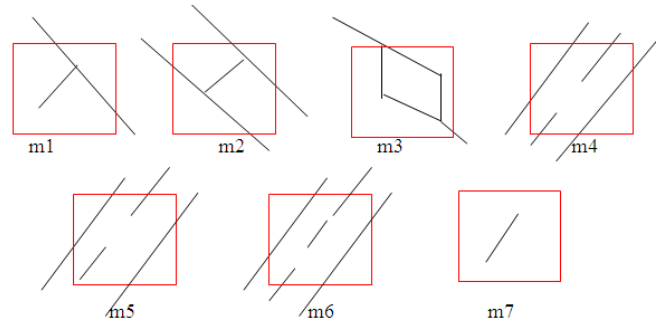


Figure 6.3.1 False Minutia Structures

Procedures to remove false minutia are:

1. . If the distance between one bifurcation and one termination is less than D and the two minutiae are in the same ridge (m1 case). Remove both of them. D is the average interreges width representing the average distance between two parallel neighboring ridges.
2. . If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations (m2, m3, m4, m6, m7 cases).
3. . If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that no any other termination is located between the two terminations. Then the two terminations are regarded as false minutia derived from a broken ridge and are removed (case m4, m5, m6).
4. . If two terminations are located in a short ridge with length less than D, remove the two terminations (m7).
5. . If a branch point has at least two neighboring branch points, which are each no further away than maximum distance threshold value and these branch points are closely connected on common line segment than remove the branch points (m12). Each minutia is completely characterized by the following parameters: 1) x-coordinate, 2) y-coordinate, and 3) orientation.

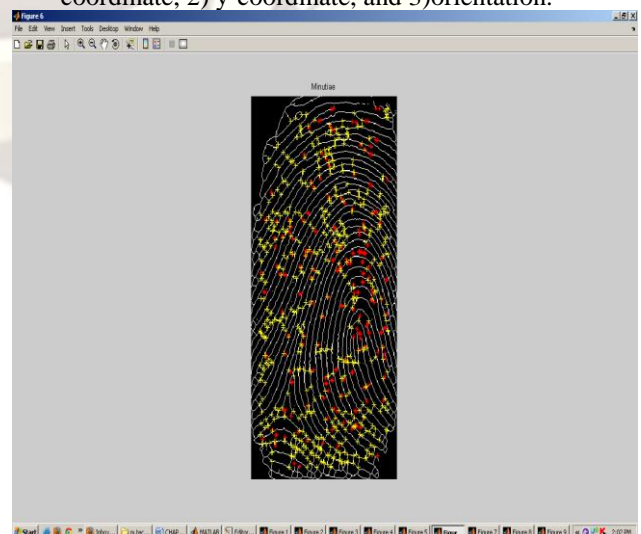


Figure 6.3.2 Minutiae Extracted Image

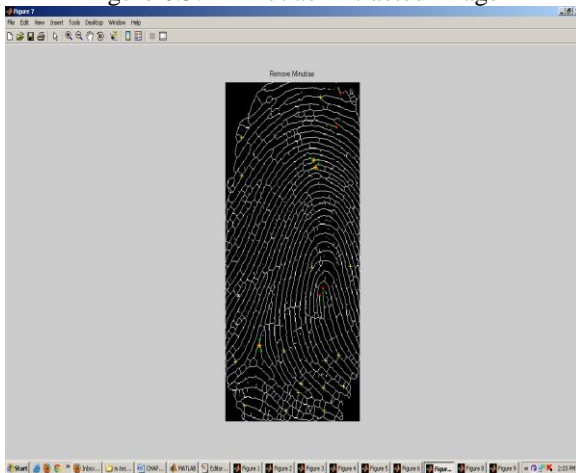


Figure 6.3.3 Removal of Minutiae

VII. MINUTIAE MATCH

After successfully extracting the set of minutia points of 2 fingerprint images to be tested, we perform Minutiae Matching to check whether they belong to the same person or not.

We use an iterative ridge alignment algorithm to first align one set of minutiae w.r.t other set and then carry-out an elastic match algorithm to count the number of matched minutia pairs.

7.1 Minutiae Alignment

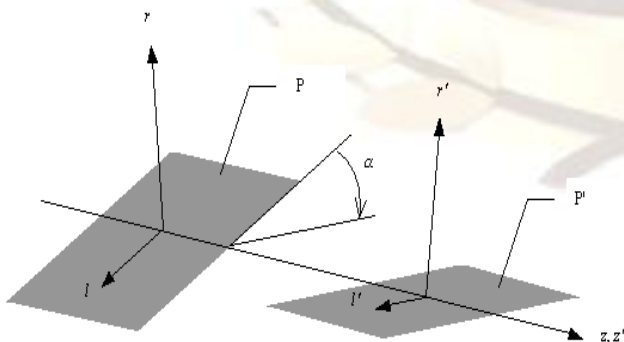
To match 2 prints, determine their reference minutiae (most similar pair/at 0.8 threshold) using similarity equation:

$$S = \sum_{mi=0}^n x_i x_i / [\sum_{mi=0}^n x_i^2 x_i^2]^{0.5}$$

where $(x_i \sim x_n)$ and $(X_i \sim X_N)$ are the set of minutia for each fingerprint image respectively

m is minimal one of the n and N value (n & N are total number of minutiae in each print)

- Now, the reference minutia is the origin point of the coordinate system, and the x & y coordinates are found using its orientation angle.



All other minutiae are then aligned to the new coordinate system, and component of their vectors can be found using the transform matrix:

7.2 Minutiae Match

Adaptive matching is used, not all parameters are exactly same achieved by placing a bounding box around each template minutia .If the minutia to be matched is within the rectangle box and difference between them is very small, then the two minutiae are regarded as a matched minutia pair .

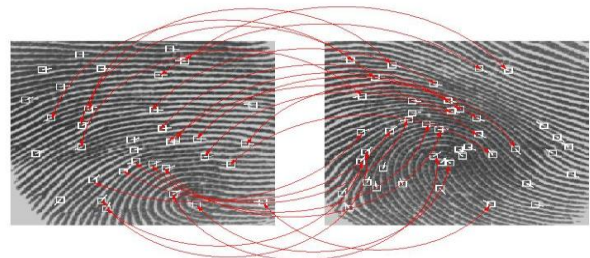


Figure 7.2.1 Minutiae Matching



Figure 7.2.2 Adaptive matching procedure

The final match ratio is:

$$\text{Match Score} = \frac{\text{Num}(\text{Matched Minutia})}{\text{Max}(\text{Num Minutia}(\text{image1}, \text{image2}))} \quad \text{Of}$$

- The score ranges from 0 to 100
- If the score is larger than a pre-specified threshold, the two fingerprints are from the same finger.

7.3 System evaluation (FRR & FAR)

This step is done using the False Reject Rate (FRR) and the False Accept Rate (FAR)

- (%) $FAR = (FA/N) * 100$

Where FA = number of incidents of false acceptance & N =total number of samples

- (%) FRR=(FR/N)*100

Where FR=number of incidents of false rejections
For a database of 10 prints, the results of the evaluation were as follows:

7.4 Experiment Analysis:

A fingerprint database from the FVC2002 (Fingerprint Verification Competition 2002) is used to test the program's performance. A series of correct and incorrect match score is recorded.

Following is the distribution curve obtained after experiments (Figure 7.3..1).

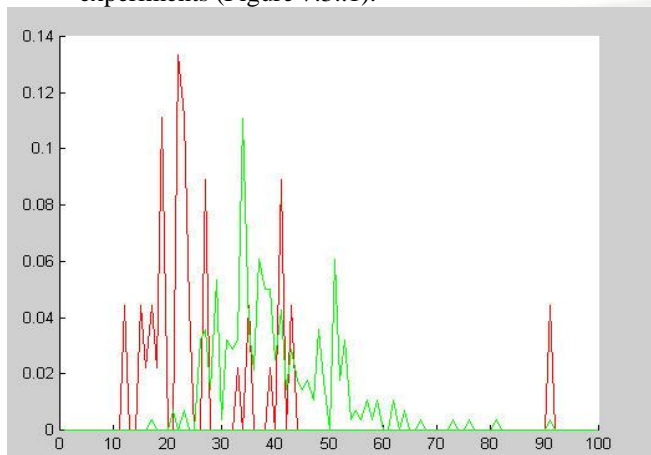


Figure 7.3.1 Distribution of Correct Scores and Incorrect Scores
(Red: Incorrect Scores, Green: Correct Scores)

In our experiments distribution curve gives an average correct match score of about 30 and average incorrect match score of 25 on the database chosen.

The FAR and FRR curve as claimed by the algorithm is shown under (Figure 7.3.2)

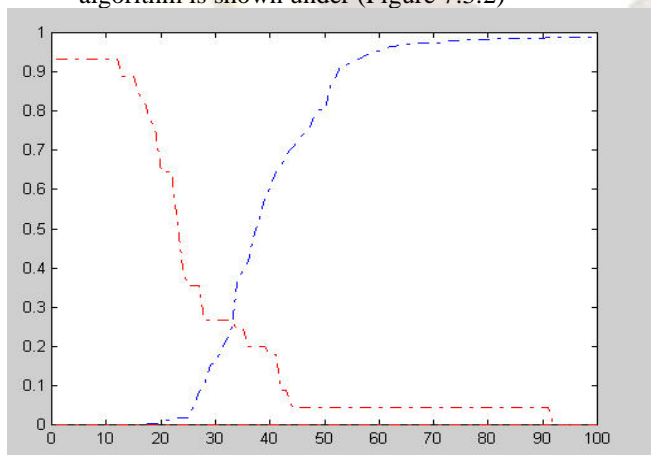


Figure 7.3.2 FRR and FAR curve (Red: FAR, Blue: FRR)

In our experiments FAR and FRR values were 30-35% approximately. Thus at a threshold match score of about 28 the verification rate of the algorithm is about 65-70%.

The relatively low percentage of verification rate is due to poor quality of images in the database and the inefficient matching algorithm which lead to incorrect matches.

VIII. CONCLUSION AND FUTURE WORK

The above implementation was an effort to understand how Fingerprint Recognition is used as a form of biometric to recognize identities of human beings. It includes all the stages from minutiae extraction from fingerprints to minutiae matching which generates a match score. Various standard techniques are used in the intermediate stages of processing.

The relatively low percentage of verification rate as compared to other forms of biometrics indicates that the algorithm used is not very robust and is vulnerable to effects like scaling and elastic deformations. Various new techniques and algorithm have been found out which give better results. Also a major challenge in Fingerprint recognition lies in the pre processing of the bad quality of fingerprint images which also add to the low verification rate..

REFERENCES

- [1] Handbook of Fingerprint Recognition by Davide Maltoni, Dario Maio, Anil K. Jain & Salil Prabhakar
- [2] Fingerprint Recognition, Paper by WUZHILI (Department of Computer Science & Engineering, Hong Kong Baptist University) 2002
- [3] Fingerprint Classification and Matching by Anil Jain (Department of Computer Science & Engineering, Michigan State University) & Sharath Pankanti (Exploratory Computer Vision Group IBM T. J. Watson Research Centre) 2000
- [4] Fingerprint database - FVC2002 (Fingerprint Verification Competition 2002)
- [5] Wikipedia link - http://en.wikipedia.org/wiki/Fingerprint_recognition.
- [6] Journal of Electronic Imaging/Mehmet Sezgin and Bulent Sankur; Survey over image thresholding techniques and quantitative performance evaluation/Jan.2004
- [7] Computer science/International Journal of Image Processing (IJIP)/Dec.2010 (CSCjournals.org) .
- [8] Interpol's public records/History of fingerprints <http://www.interpol.int/Public/Forensic/fingerprints/History/BriefHistoricOutline.pdf>
- [9] Fingerprint Recognition using MATLAB Graduation project by Zain S. Barham Supervised by: Dr. Allam Mousa(pdf)

- [10] Raju Rajkumar , K Hemachandran, A Rohtak Haryana,India.. Her subject of interests includes Image Processing.,
Secondary Fingerprint Enhancement and Minutiae Extraction, Signal & Image Processing : An International Journal (SIPIJ) Vol.3, No.2, April 2012.
- [11] Khalid Saeed, Marek Tabe,Dzki, Mariusz Rybnik, Macin Adamski, *K3M: A Universal Algorithm for Image Skeltonization and Review of Thinning Technique*, Int. J. Appl. Math. Computer. Sci., 2010, Vol. 20, No. 2, 317–335.
- [12] Tatsat Naik, Om Sri Satyasai, *Study of Fingerprint Recognition System*”, B.Tech. (Project), National Institute of Technology, Rourkela
- [13] Lin Hong, Student Member, IEEE, Yifei Wan, and Anil Jain, Fellow, IEEE, *Fingerprint Image Enhancement: Algorithm and Performance Evaluation*, IEEE Transactions on Pattern Analysis and Machine Intelligence, VOL. 20, NO. 8, AUGUST 1998.
- [14] Hui Xu, Yifan Qu, Yan Zhang, Feng Zhao, *FPGA Based Parallel Thinning for Binary Fingerprint Image*, IEEE, 2009.
- [15] raig T. Diefenderfer, *Fingerprint Recognition*, M. Sc. Thesis, Ensign, United States Navy, B.S., United States Naval Academy, 2005.
- [16] Neeta Murmu, Abha Otti, *Fingerprint Recognition*, National Institute of Technology, Rourkela.
- [17] Shahram Mohammadi, Ali Frajzadeh, *A Matching Algorithm of Minutiae for Real Time Fingerprint Identification System*, World Academy of Science, Engineering and Technology, 2009.
- [18] Roli Bansal, Priti Sehgal and Punam Bedi, “Minutiae Extraction from Fingerprint Images - A Review” IJCSI, 2011.
- [19] Pravesh Kumar, “Use of Fuzzy Set and Neural Network to Extract Fingerprint Minutiae Points and Location”, M.E. Thesis, Computer Science and Engineering Department, Thapar University, June 2009.
- [20] Nasim MirArmandehi, “Fuzzy Image Restoration”, Final Project, Sharif University of Technology, 2007

Bio Data



Manisha Redhu received B.Tech. Degree in Computer Science and Engineering from Jind Institute of Engineering and Technology, Jind, Haryana in 2010. Currently she is pursuing her M.Tech Degree in Computer Science and Engineering from Maharshi Dayanand University,