Dissertation on
FINGERPRINT RECOGNITION

Thesis submitted towards partial fulfilment
of the requirements for the degree of

Master of Technology in IT (Courseware Engineering)

Submitted by
Papiya Dey

EXAMINATION ROLL NO.: M4CWE22023
UNIVERSITY REGISTRATION NO.: 154505 of 2020-21

Under the guidance of
Prof. Dr. Matangini Chattopadhyay

School of Education Technology
Jadavpur University

Course affiliated to
Faculty of Engineering and Technology
Jadavpur University
Kolkata-700032
India

2022

M.Tech. IT (Courseware Engineering)
Course affiliated to
Faculty of Engineering and Technology
Jadavpur University
Kolkata, India

CERTIFICATE OF RECOMMENDATION

This is to certify that the thesis entitled **"FINGERPRINT RECOGNITION"** is a bonafide work carried out by Papiya Dey under our supervision and guidance for partial fulfillment of the requirements for the degree of Master of Technology in IT (Courseware Engineering) in School of Education Technology, during the academic session 2021-2022.

SUPERVISOR
School of Education Technology
Jadavpur University,
Kolkata-700 032

DIRECTOR
School of Education Technology
Jadavpur University,
Kolkata-700 032

DEAN - FISLM
Jadavpur University,
Kolkata-700 032

M.Tech. IT (Courseware Engineering)
Course affiliated to
Faculty of Engineering and Technology
Jadavpur University
Kolkata, India

CERTIFICATE OF APPROVAL **

This foregoing thesis is hereby approved as a credible study of an engineering subject carried out and presented in a manner satisfactory to warranty its acceptance as a prerequisite to the degree for which it has been submitted. It is understood that by this approval the undersigned do not endorse or approve any statement made or opinion expressed or conclusion drawn therein but approve the thesis only for purpose for which it has been submitted.

Committee of final examination for evaluation of Thesis **----------**

** Only in case the thesis is approved.

DECLARATION OF ORIGINALITY AND COMPLIANCE OF ACADEMIC ETHICS

I hereby declare that this thesis contains literature survey and original research work by the undersigned candidate, as part of her **Master of Technology in IT (Courseware Engineering)** studies.

All information in this document has been obtained and presented in accordance with academic rules and ethical conduct.

I also declare that, as required by this rule and conduct, I have fully cited and referenced all materials and results that are not original to this work.

NAME: PAPIYA DEY

EXAMINATION ROLL NUMBER: M4CWE22023

THESIS TITLE: FINGERPRINT RECOGNITION

SIGNATURE: DATE:

Acknowledgement

I feel extremely glad while presenting this dissertation at school of Education Technology, Jadavpur University, Kolkata, in the partial fulfilment of the requirement for the degree of Master of Technology in IT (Courseware Engineering).

I hereby take this opportunity to express my gratitude from the core of my heart to my guide Prof. Dr. Matangini Chattopadhyay for being so kind and supportive throughout the time of thesis completion. She has encouraged me and has guided me with all possible suggestions and best information with which this thesis was brought to fruition.

I am also grateful for the constant support provided to me by Prof. Dr. Ranjan Parekh, Dr. Saswati Mukherjee and Mr. Joydeep Mukherjee.

I also thank my classmates and other staffs of this department for their help.

Last but not the least I would like to thank my mother and acknowledge her constant endless support and care throughout the journey.

Contents

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

Acronym	Full-Name
FAR	False Acceptance Rate
FRR	False Rejection Rate
C2CL	Contact to Contactless Fingerprint
FFT	Fast Fourier Transform
IFFT	Inverse Fast Fourier Transform

Executive Summary

There are various types of applications for fingerprint recognition which is used for different purposes. Fingerprint is one of the challenging pattern recognition problem. The fingerprint recognition system is divided into four stages. First is Acquisition stage to capture the fingerprint image. The second is Pre-processing stage that includes enhancement, binarization and thinning. The third stage is Feature Extraction Stage to extract the feature from the thinning image. The minutiae extraction method is used to extract ridge ending and ridge bifurcation from thinning. The fourth stage is matching (Identification, Verification) to match two minutiae points by using minutiae matcher method in which similarity and distance measurement are used. The algorithm is tested accurately and reliably by using fingerprint images from different databases. The fingerprint databases used are FVC2000 and FVC2002. It has been seen that the FVC2002 database performs better results compare with FVC2000 database.

CHAPTER 1
Introduction

1.0 Introduction

Due to enhancement of technology Fingerprint is being used for identification of citizens. Fingerprint technology has become more popular and connected to human being life. This technology is now replacing traditional identification and recognition process for human being. The fingerprint will continue to substitute the ID of citizens as soon as possible in the future. Fingerprint refers to a complex combination between gap of ridges and valleys on all the fingertips. Clearer ridges quality is more convenient to analyse who you are and system can recognize your unique identity.

1.1 Fingerprint

Fingerprints are the most important part of human finger. It is experienced from the research that human beings have different finger prints and these finger prints are permanent for whole life. So, fingerprints have been used for the forensic application and identification for a long time.

Figure 1.1: Fingerprint image

A fingerprint is the composition of many ridges and furrows. Finger prints can't be distinguished by their ridges. It can be distinguished by Minutia, which are some abnormal points on the ridges. Minutia is divided in to two parts such as: termination and bifurcation. Termination is also called ending and bifurcation is also called branch.

1.2 Types of Fingerprint Patterns

There are eight types of Fingerprint patterns. They are:

(i) **Plain Arch** is a pattern that has ridges at one side, makes a rise at the centre, and flows or tend to flow towards opposite side.

(ii) **Tented Arch** has resemblance to plain arch but, ridges create an angle or a steep thrust. It possesses some basic characteristics of the loop.

(iii) **Ulnar Loop** patterns loops flow in the direction of little finger.

(iv) **Radial Loop** patterns loops flow in the direction of thumb.

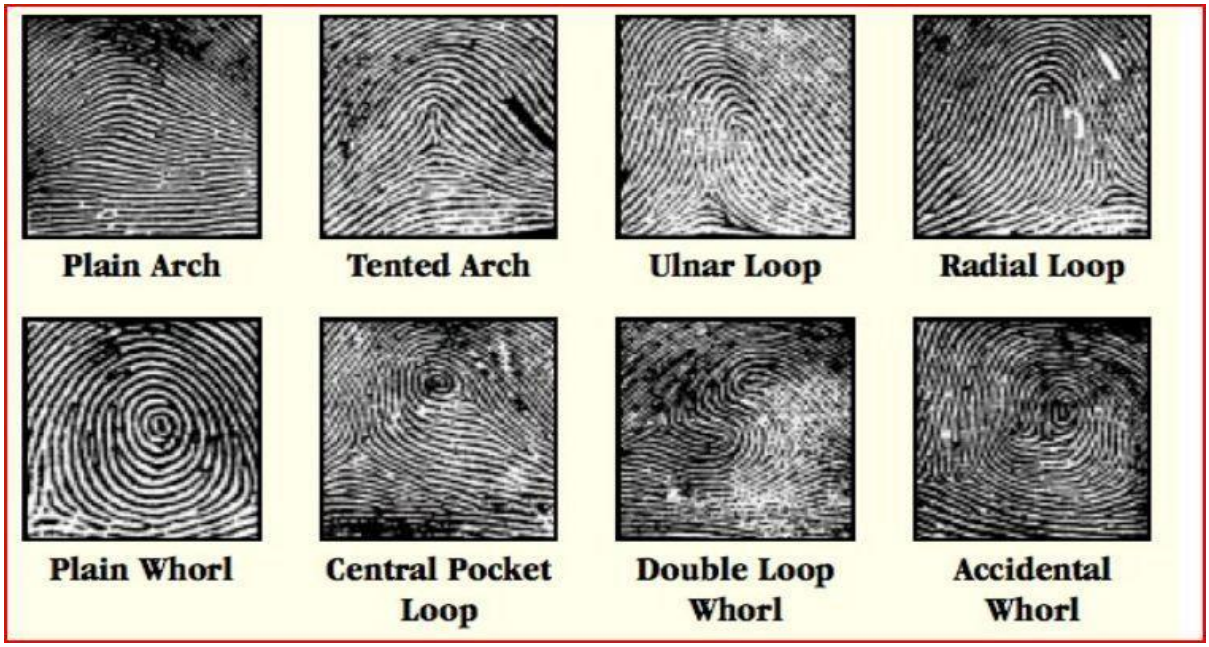


Figure 1.2: Types of Fingerprint patterns

(v) **Plain Whorl** consists of pattern with two deltas and minimum one ridge will make a complete circuit of spiral, oval or any form of circle. The imaginary line drawn between two deltas will touch or cross, at least one recurving ridge within the inner pattern area.

(vi) **Central Pocket Loop** has a pattern with minimum one recurving ridge or an obstruction at right angles to the line of flow. The

imaginary line drawn between two deltas will not cut or touch the inner recurving ridge in the inner pattern.

(vii) **Double Loop Whorl** is distinguished with two separate loop formations. It is composed of two separate and distinct set of shoulders and two deltas.

(viii) **Accidental Whorl** is the only pattern which is connected with minimum two deltas. It unites two or more distinctive type of patterns excluding the plain arch.

1.3 Fingerprint Biometrics

An image capturing module acquires the raw biometric data of a person using a sensor. Utilizing suitable algorithms feature extraction module improves the quality of the captured image. Database stores the biometric template information of enrolled persons. Pattern matching module compares the extracted features with the stored templates.

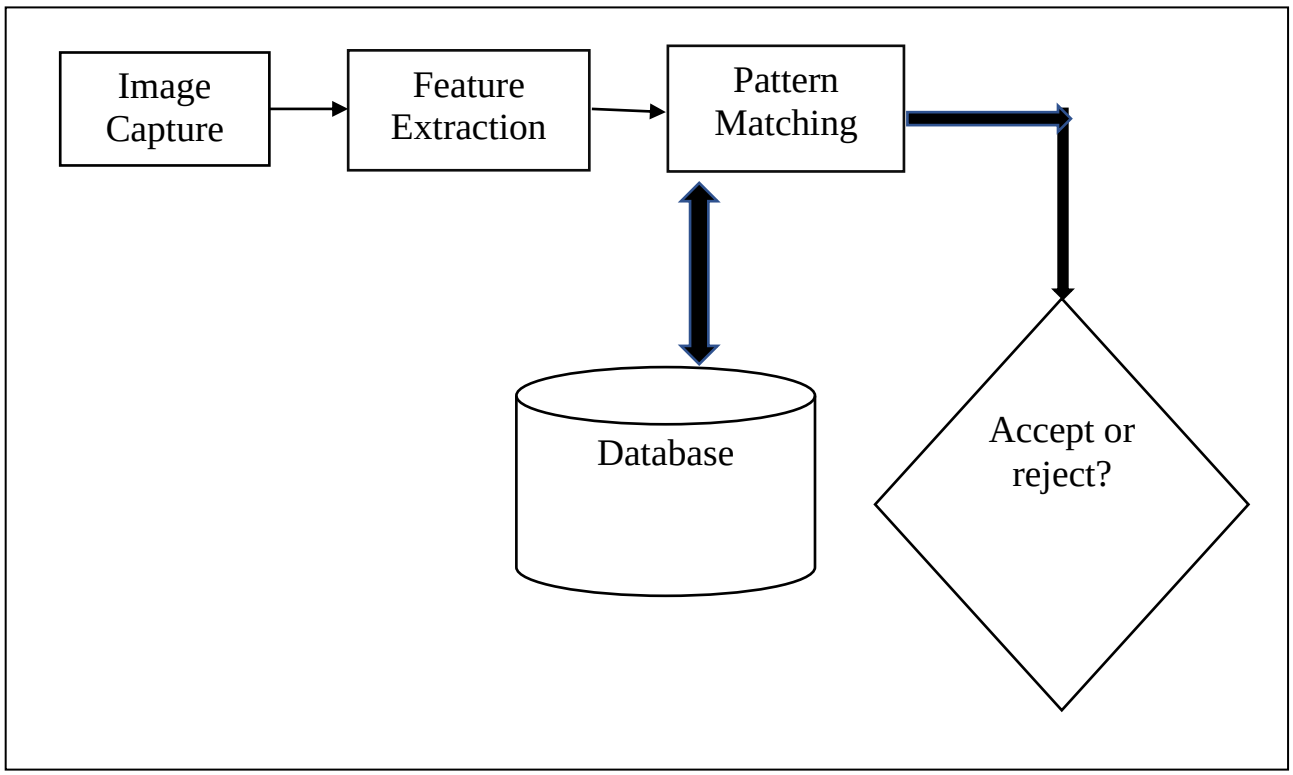


Figure 1.3: Biometric System

Fingerprint Verification

Verification is a searching function that is not dependent on a suggested identification and therefore, the enquiry template interrogates the entire database for a possible match. Verification system is a comparison method to identification individual and has to claim his/her identity by compared to their fingerprint template, which stored in the database.

Fingerprint Identification

Identification is a process to compare the enquiry template with the database template and confirms that either the two templates originate from the same person or that they do not. Biometric technologies collect and usually store unique or distinctive biological and/or behavioural characteristics of a person (biometrics data) for the automated verification of an identity claim or for the identification of that person. All biometric data is first captured by camera or sensor devices as an image and then further processed into a biometric template. Matching algorithms used for verification and de-duplication are based on comparing these biometric templates. A fingerprint identification system is an automatic pattern recognition system that consists of three fundamental stages:

- **Data Acquisition:** The fingerprint to be recognized is sensed.
- **Feature Extraction:** A machine representation (pattern) is extracted from the sensed image.
- **Decision-making:** The representation derived from the sensed image are compared with a representation stored in the system.

Fingerprint is a unique pattern of individual without duplicate data even twins. Ridge and valley on the fingertip surface are used to identify each characteristic. Fingerprint with high quality contains 25 to 80 number minutiae depending on fingerprint capture device and finger’s condition. Different fingerprint sensors produce different quality of fingerprint data.

Biometric Technology and Analysis

Biometric has the potential to make authentication dramatically faster, easier and more secure than traditional passwords, but companies need to be careful about biometric data they collect. Any human biological or behavioural characteristics can become a biometric identifier, provided seven analysis pillars of biometrics as the following properties below:

- **Universality:** refers to any trait of human characteristics to determine their identity. Each individual should have the biometric characteristic.

- **Uniqueness (distinctiveness):** refers to unique of person recognition to determine their identity without duplicate features even from twins such as fingerprint or iris patterns. Each person should have the feature but distinct from others.

- **Permanence:** refers to any identity of human have untransformed of their characteristics, for instance fingerprint and iris are good stability recognized, whereas signature, facial, and voice features have changes them significantly by aging and trait along the time life. The biometric trait should be constant for certain period of time.

- **Collectability (measurability):** refers to obtaining, acquisition, or measurement of the trait feature(s) that non-intrusive, reliable, and robust according to quality and cost devices. For instance, face recognition may need a simple webcam but fingerprint and iris may need very specialized devices and cost is not so expensive, ease of data capturing, measuring and processing.

- **Performance:** refers to the results of analysis by systems to prove accuracy levels, speed, and robustness of technology used. It is used to evaluate the accurate level of false acceptance rate (FAR) of automated systems, security, speed, accuracy and robust.

- **Acceptability:** refers to vital points to obtain end-users support and willingness of people to evaluate the necessities of technology among population to adopt and share their biometric data and assessed or not accepted by the user population without any objection.

- **Circumvention:** refers to evaluation how difficult it is to fool the system with high false acceptance rate (FAR) by easy methodologies to matching

level. This is so important to prevent consideration of any fake fingers hacking to the system.

CHAPTER 2
LITERATURE SURVEY

2.0 Introduction

A typical fingerprint automated biometric system consists of four major components. The components are image capturing, feature extraction, pattern matching and database. In image capturing component, a sensor captures biometric data in digital format for data acquisition. For feature extraction component, an algorithm is required to produce the feature vector which consists of numerical characterizations of the biometrics of interest. The third component, pattern matching, a matcher compares feature vectors to get a score, which shows the degree of similarity between the pair of biometrics data under investigation. Results from this process is controlled by FAR and FRR. False Acceptance Rate (FAR) is the rate where the system falsely accepted an unregistered or another registered user as a registered one compared to the total number of trials. While, False Rejection Rate (FRR) happened when the system falsely rejects a registered user over the total number of trials. A high FRR indicates a low FAR and a high FAR indicates low FRR. The best and ideal system should have moderate values of both. The fingerprint technologies are being applied and used in identity management and access control. Fingerprints consist of series of ridges and furrows on the surface of the finger and patterns such as swirls, loops or aches surrounded the core which make them distinctly different for each person. Ridges are the outer layer segments of the finger while valleys are the lower layer segments. Both are identified by irregularities called as minutiae which become the basis of finger scanning technologies. Minutiae has the form of ridge ending and bifurcations [2].

2.1 Biometric recognition

Biometric recognition is based on uniqueness and permanence. The uniqueness means that there is no similarity of feature between two different biometrics data. For example, there are no two persons having the same fingerprint feature even if they are twins. And when the features of biometrics do not change over the lifetime or aging, it is called permanence. Biometrics can have physiological or behavioural characteristics. The physiological characteristics are included in the physical part of body such as fingerprint, palm print, iris, face, DNA, hand geometry, retina etc. The behavioural characteristics are based on an action taken by a person such as Voice recognition, keystroke-scan, and signature-scan. Any biometrics system includes two phases; first phase is enrolment phase and second is recognition phase. The recognition phase is divided into two things which are verification and identification. During the enrolment phase, the biometrics data are captured and digital image is generated. Then Pre-processing is applied to digital image for removing unwanted data and after the post-processing, this data is stored in database. In

case of identification process, the fingerprint acquired from one person is compared with all the fingerprints which are stored in the database. Also, it is known as (1:N) matching. it is used in the process of seeking the criminals. In the verification process, the person's fingerprint is verified from the database by using matching algorithms. It is known as (1:1) Matching. Matching Algorithm compares a claimant fingerprint against enrolled fingerprint. Initially, the person enrols his/her fingerprint into verification system, and the result shows whether the fingerprint which is taken from the user is matching with the fingerprint stored as a template in database or not [3].

Authentication is the key parameter to speak the truth of an attribute claimed by the real entity. There are several ways to make authentication more robust and biometrics is one among them. From the past decade, biometric technology is widely adopted and accepted everywhere to authenticate an individual's identity. Also, the adopted technology overcomes the limitations faced by the traditional authentication process such as knowledge based issues including password for the authentication of an individual [4].

In paper [5] detection of the fingerprint consists of five main steps - image acquisition, image pre-processing, feature extraction, classification, and decision making. Classification process is the main step to detect fingerprint. The temperature, humidity affects the temperature of the skin, which causes the images of fingerprints to be blurred. Also, the position of the finger when it is placed on a scanner and the way it is pressed also leads to changes in the fingerprints image. Image pre-processing is used to reduce noise, enhance contrast, and so on. It can be used in banking systems, education, and business. This method for authentication can be used to login to devices and application without having to remember passwords. Also, this method is very cheap, reliable, highly secured, and accurate. Besides, this method requires only small size of memory to save the fingerprint image which in turn reduces the memory requirement.

Matching Contactless Fingerprint images with a legacy database of contact-based fingerprint impressions has received increased attention in the wake of COVID-19 due to the superior hygiene of the contactless acquisition and the widespread availability of low-cost mobile phones capable of capturing photos of fingerprints with sufficient resolution for verification purposes. This is an end-to-end automated system, called C2CL, comprises a mobile finger photo capture app, pre-processing, and matching algorithms to handle the challenges inhibiting previous cross-matching methods; namely i) low ridge-valley contrast of contactless fingerprints, ii) varying roll, pitch and distance of the finger to the

camera, iii) non-linear distortion of contact-based fingerprints, and iV) different image qualities of smartphone cameras. The pre-processing algorithm segments, enhances, scales, and unwarps contactless fingerprints, while the matching algorithm extracts both minutiae and texture representations. A sequestered dataset of 9, 888 contactless 2D fingerprints and corresponding contact-based fingerprints from 206 subjects (2 thumbs and 2 index fingers for each subject) acquired using the mobile capture app is used to evaluate the cross-database performance of the proposed algorithm [6].

In paper [7], the experiment of FVC2000 and FingerDos databases has been shown. Table 2.1 is the summary report of False Non-Match Rate on FVC2000 and FingerDos Databases.

Table 2.1: FVC2000 and FingerDos database

	FVC2000				**FingerDOS**					
					LEFT HAND			**RIGHT HAND**		
	DB1_B	**DB2_B**	**DB3_B**	**DB4_B**	**INDEX**	**MIDDLE**	**THUMB**	**INDEX**	**MIDDLE**	**THUMB**
Total Comparisons	280	280	280	280	2700	2700	2700	2700	2700	2700
Matched Impressions	271	271	280	280	2636	2621	2578	2656	2653	2691
Unmatched Impressions	9	9	0	0	64	79	122	44	47	9
FNMR	3	3	0	0	2	2	4	1	1	0
Average FNMR (%)	1.2				1.67					

Table 2.2: Percentage of FMR, FNMR and Accuracy of FVC2000 and FingerDos images

Database	**Recognition Accuracy**		
	FMR	FNMR	Accuracy
FVC2000	2	1.2	98.4
FingerDOS	0	1.67	99.16

Table 2.2 displays the Percentage of FMR, FNMR and Accuracy of FVB2000 and FingerDos Images.

The paper [8] proposes three algorithms to enhance image, extract minutiae and match with fingerprint templates. The first step is used to enhance the image quality using brightness and Gabor filters on the fingerprint surface to make ridge lines darker. The second step is to extract minutia. It used to convert the images to binary (0 and 1) and process thinning image with Zhang Suen algorithms. Then, the pictures moves through the fixing procedure to correct any missed links, error ridges or spurious minutiae that are generated by fingerprint algorithms before they undergo final analysis, calculate location of minutiae and the total of the minutiae on the fingerprint surface. The last step is matching algorithms that can be proof of a person's identity by comparing minutiae result with those in the database. If a person is already enrolled, the result will confirm his/her identity.

Various machine learning and neural network approaches have been proposed for fingerprint acquisition, detection, classification, and analysis. In the paper [9], evaluation of fingerprint classification algorithms and fingerprint application in the area of criminal investigation are proposed. Analysing and comparing machine learning algorithms of fingerprint in terms of classification, matching, feature extraction, fingerprint and finger-vein recognition, and spoof detection are shown.

A new algorithm for increasing fingerprint with large noise is enhanced in paper [10]. The fingerprint image is first pre-improved using Gabor filters, and local adaptive thresholds are used to achieve a binary fingerprint. In order to reconstruct these regions, which are incorrectly improved in the first stage, the classification Deep Boltzmann machines (DBMs) with a range pattern before are used. The proposed technique completely enhances each other by a

traditional technique of improvement relying upon Gabor filtering and deep learning. The FVC 2004, Crossmatch, and Swipe databases are conducted by different techniques. Experiments indicate that in contrast with other techniques, the suggested technique achieves better outcomes and enhances fingerprint performance. Experimental findings indicate that the use of the proposed technique allows the extremely accurate fingerprint image to be reconstructed. The average performance of the proposed method is 91.31%, which is better than the average performance of another method. The proposed technique is superior for removing noise than other techniques, in particular, for improving fingerprints of poor performance.

The paper [11] reviews recent Latent Finger Print (LFP) enhancement techniques including metal oxides, multi-metal deposition (MMD-I/II/SMD/Au-ASP), optical, chemical, physical, and physicochemical. Among numerous LFP enhancement techniques, the application of chemical methods in combination with optical techniques has a greater place to recover Fingerprints with sufficient quality. However, instead of using such a complex and costly enhancing agent, nowadays nanotechnology used specific techniques is used for visualizing, inspecting, gathering, and analyzing trace evidence at the scene of a crime. Use of simple metal oxides such as ZnO that have superior fluorescent properties and also that consider both the surface and cost of the materials, enhancement of the LFP is functioning.

An accurate estimation of fingerprint orientation fields is an essential step in the overall fingerprint recognition process. Conventional gradient-based approaches are popular but very sensitive to noise. In paper [13], a novel implementation is proposed to improve the performance of gradient-based methods. The enhanced algorithm chooses the best orientation estimate from four overlapping neighbourhoods of every image block, where the voting scheme is based on the reliability measures. The algorithm was tested on real fingerprint images. The experimentation results suggest that the enhanced algorithm achieves visibly better noise resistance with modest computation time in comparison with other gradient-based methods.

Image enhancement and thinning are very important pre-processing steps of biometric fingerprint recognition system. This reduction is accomplished by two pre-processing steps. The overall performance of the fingerprint recognition system is highly dependent on image enhancement phase of recognition process. The image enhancement is a very important phase in fingerprint recognition for improving the image quality by removing noise, connecting

broken ridges and making smooth image. The process of obtaining the skeleton of the image using skeletonization is known as thinning. The enhanced image will be thinned and all ridges will be coming 1 pixel breadth. The performance of the fingerprint minutiae extraction is highly dependent on the thinning process of the enhanced image. Thus, the overall performance of the fingerprint recognition system is highly affected by the image enhancement and the image thinning phase of recognition process. It is the precondition of minutiae extraction. In paper [14], image enhancement of fingerprint image is done using Gaussian Mask and Sobel Convolution and then after Zhang - Suen Thinning algorithm is applied on fingerprint image for better performance. This will give efficient results in terms of image quality and thinning speed. The implementation of research work is done in .Net platform using custom fingerprint database of 100 images of 25 users.

A fuzzy rule based system for removing false and spurious minutiae is experimented in paper [16]. Removal of false minutiae begins only after their extraction is complete from the enhanced fingerprint image. Hence, this process is named as post processing activity in the enhancement process. The proposed methodology is simple and proved effective in removing false minutiae from the extracted minutiae of a fingerprint image. It also proves to be effective with respect to its implementation as it needs less computational effort.

Thinning is the pre-processing stage to make easy higher-level analysis and recognition for such applications like OCR, Fingerprint classification, Pattern recognition. In paper [17], thinning and its various algorithm are discussed. It is concluded that there are some loopholes in thinning algorithm. So, there is a need to improve thinning rate. All the thinning algorithms are classified into two broad categories: Iterative thinning algorithm and Non-iterative thinning algorithm. Iterative (Pixel Based) thinning algorithm produces a skeleton by examining and deleting contour pixels through an iterative process in either sequential or parallel way. Sequential thinning algorithms which examine contour pixels of an object in a predetermined order, and this can be accomplished by either raster scanning or following the image by contour pixels. In parallel thinning algorithms, pixels are deleted on the basis of results obtained only from the previous iteration. Hence, parallel thinning algorithms are suitable for implementation in parallel processors.

a) **Sequential thinning:** This algorithm inspects contour points in a predetermined order of an object and this can be accomplished by either raster scanning or following the images by contour pixels.

b) **Parallel Thinning**: In this type of algorithms pixels are inspected for deletions on the basis of some previously available iteration results. Non-iterative (non-pixel based) Thinning is not based on examining individual pixels. Without examining all the individual pixels, these algorithms produce a certain median or centre line of the pattern to be thinned directly in one pass. Some popular non-pixel based methods include medial axis transforms, distance transforms, and determination of centre lines by line following. Medial axis transforms often use gray-level images where pixel intensity represents distance to the boundary of the object. Distance transform based methods compute the distance to the image background for each object pixel and use this information to determine which pixels are part of the skeleton.

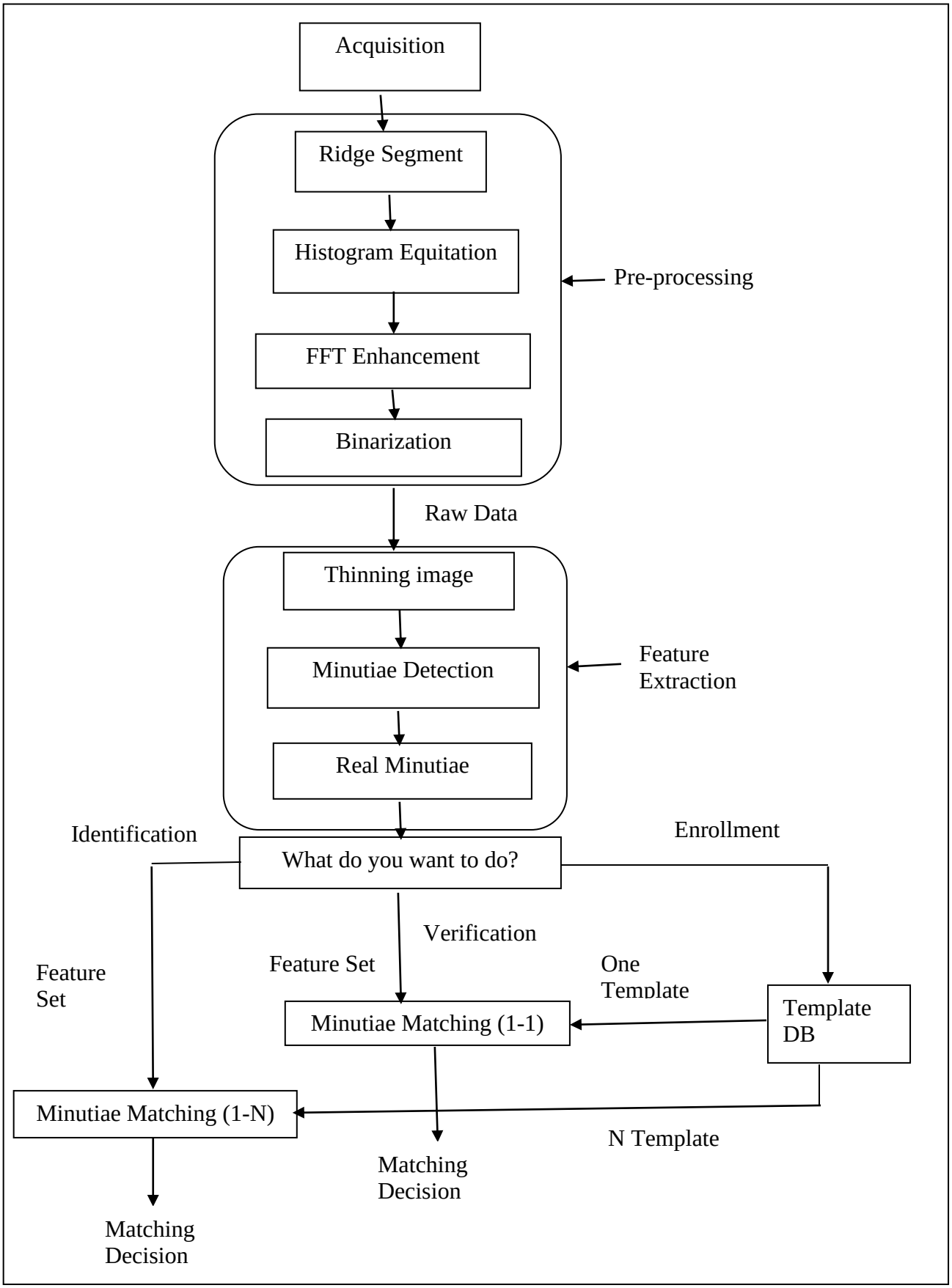
Chapter 3:
Proposed Approach

3.0 Proposed approach

The fingerprint recognition system is divided into three stages: fingerprint image pre-processing, feature extraction and matching. The matching stage is divided into identification and verification process. At the time of capturing fingerprint image, the pre-processing stage is applied to it. The output of this stage will be passed to feature extraction stage which extracts the minutiae point (ridge ending, Bifurcation) from thinning fingerprint image, then the false minutiae removal is applied to extract real minutiae. Finally, the real minutiae are stored in MATLAB file (.mat). Then, if the fingerprint is already enrolled, then it sends to matching stage otherwise do enrolment stage and store it in the database as template. In identification case (one-to-many matching), the input feature set which is matching with N template from database, N matching will be done. The result will be considered as matching score. If matching score is closer to 1 then both fingers are from same user. If matching score is near to zero then both fingers are from deferent user. In verification case (one-to-one matching), the input feature set which is matching with one template from database, one matching will be done and is decided whether the input fingerprint verified or unverified.

Figure 3.1 shows the flow chart of Fingerprint Recognition System.

Figure 3.1: Block Diagram of Fingerprint Recognition System



Chapter 4:
Experimentations and Results

4.0 Experimentation and Results

The experiment is performed by using MATLAB (R2015a) and tested on databases FVC 2000 and FVC 2002. Table 3.1 show the databases used in our work.

Table 4.1: Fingerprint Images Databases

Database	Competitions	Image Size	Resolution	Sensor Type
DB1_B	FVC2000	300x300	500 dpi	Low-cost optical sensor
DB2_B	FVC2000	256x364	500 dpi	Low-cost capacitive sensor
DB1_B	FVC2002	388x374	500 dpi	Optical Sensor
DB2_B	FVC2002	296x560	569 dpi	Optical Sensor
DB3_B	FVC2002	300x300	500 dpi	Capacitive Sensor

To evaluate the fingerprint recognition system FAR and FRR are calculated. We used different databases. The first experiment on FVC2000 (DB1_B) contains 80 images (10 users X 8 impression). The second Experiment on FVC2002 (DB1_B) contains 80 images (10 users X 8 impression). We see that the FVC 2002 gives better result than FVC2000. The formula to calculate Accuracy is given below:

Accuracy = 100 – (FAR + FRR) /2

False Acceptance Rate (FAR) occurs when we accept a user who actually has been rejected. This type of issue is also referred to as false positive or False Match Rate (FMR). FMR is calculated using the formula mentioned below.

FAR = (Number of false acceptance / Number of identification attempts) *100%

False Rejection Rate (FRR) is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. FRR is calculated using the formula mentioned below.

FRR = (Number of false rejection / Number of identification attempts) *100%

Step 1: Acquisition stage

The acquisition stage is the process to obtain image by different ways such as Online and Offline. In online method, the optical fingerprint reader is used to capture the image of fingerprint. In offline method, the fingerprint image is obtained by ink in the area of finger and then put the fingerprint on a sheet of white paper and scan it to get a digital image. The resolution of the fingerprint must be 500dpi while the size is (640x480) pixels. In this experiment, we have used two standard databases which are available online (FVC2000 and FVC2002). They contain 80 fingerprints of 10 different fingers.

We divided the dataset randomly to training and testing dataset. The training dataset contains 60 images and the testing dataset contains 20 images. Figure 4.1 shows the image of testing dataset.

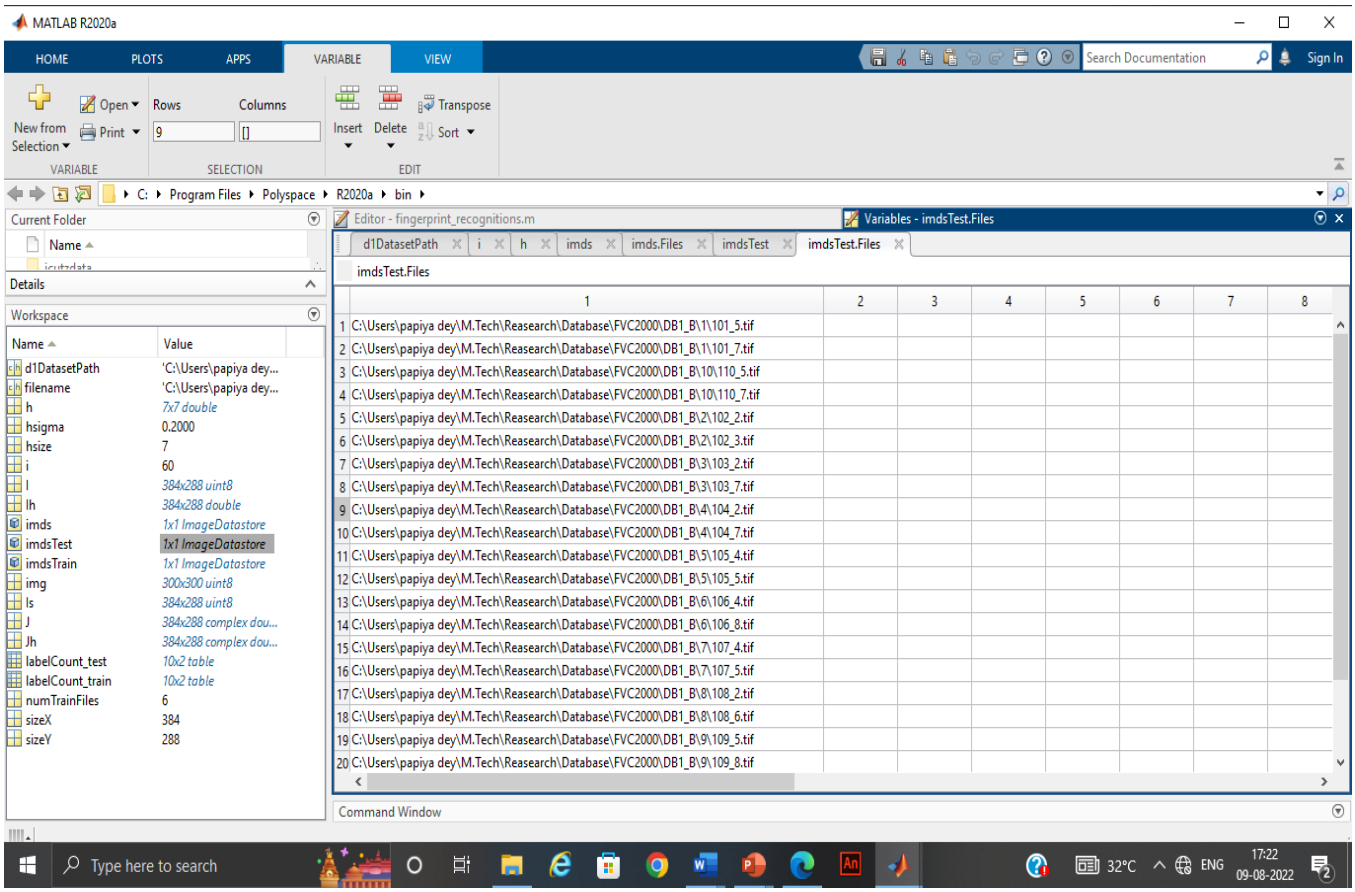


Figure 4.1: Image of testing dataset

Step 2: Pre-processing stage

The Pre-processing stage is the process of removing unwanted data in fingerprint image such as noise, reflection, etc. It is used to increase the clarity of ridge structure. The main steps of pre-processing stage are enhancement fingerprint image by histogram equalization and binarization. Figure 4.2 shows original image.

Figure 4.2: Original image

Histogram Equalization

In order to enhance the quality of fingerprint image, histogram qualization is used. Histogram equalization is mainly used to increase the pixel value of an image. Histogram represents the relative frequency of various types of gray levels in an image. By using this method we can improve the contrast of an image and it is one of the most deserving technique in image enhancement. The original histogram of a fingerprint image is like a bimodal type. After histogram equalization, it occupies the range from 0 to 255 and the visualization effect is also increased.

Figure 4.3 shows the Histogram of original image.

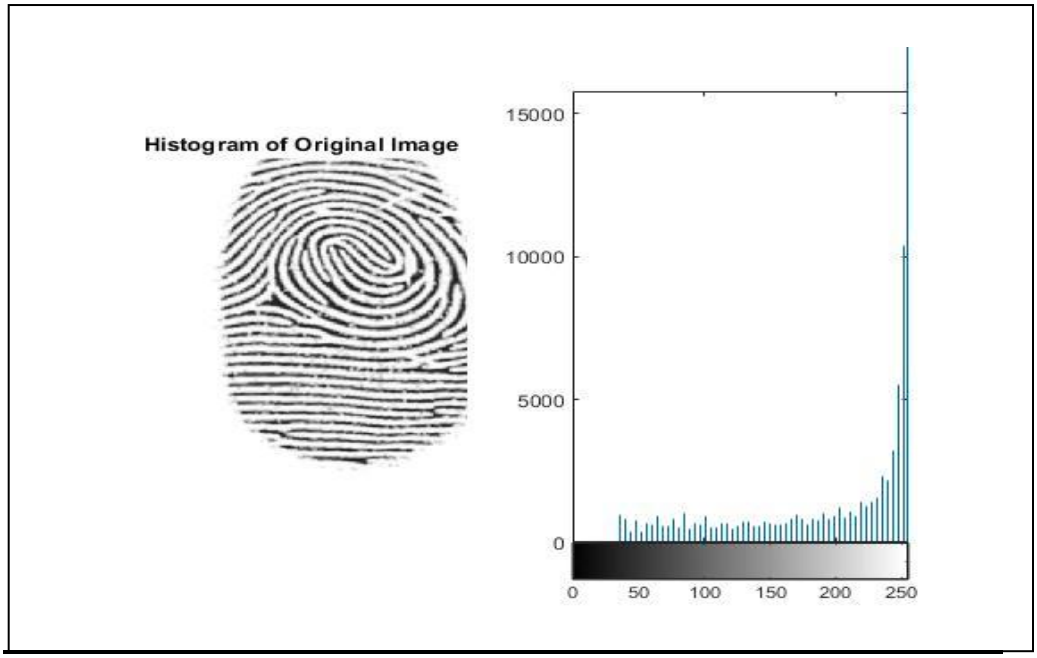


Figure 4.3: Histogram of Original Image

Apply Filters

To largen the image quality, we apply a high-pass filter (Laplacian of Gaussian LoG). First, we transform the image to its frequency domain using a Fast Fourier Transformation (FFT) and a shift. Then, we augment the amplitude of the dominant frequencies over relatively small regions and finally retransform the image back to the spatial domain by the use of an inverse FFT (IFFT).

Step 3: Feature Extraction stage

Bifurcation:

Figure 4.4 shows the Bifurcation of the image. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridges. In biometrics and fingerprint scanning, bifurcation refers to the point in a fingerprint where a ridge divides to form two ridges.

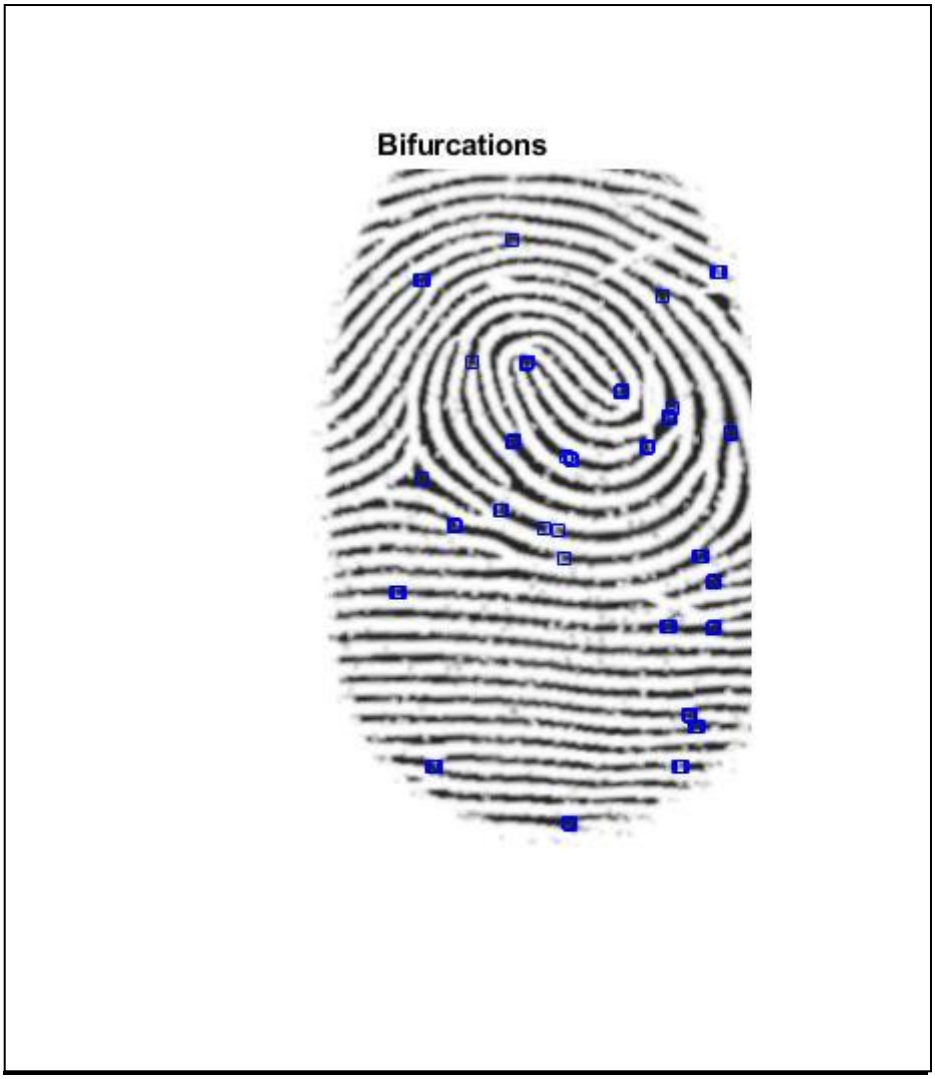


Figure 4.4: Bifurcation of the image

Ridge Endings:

Figure 4.5 shows the Ridge Endings of the Fingerprint Image. A ridge ending is defined as the point where a ridge ends abruptly. A ridge

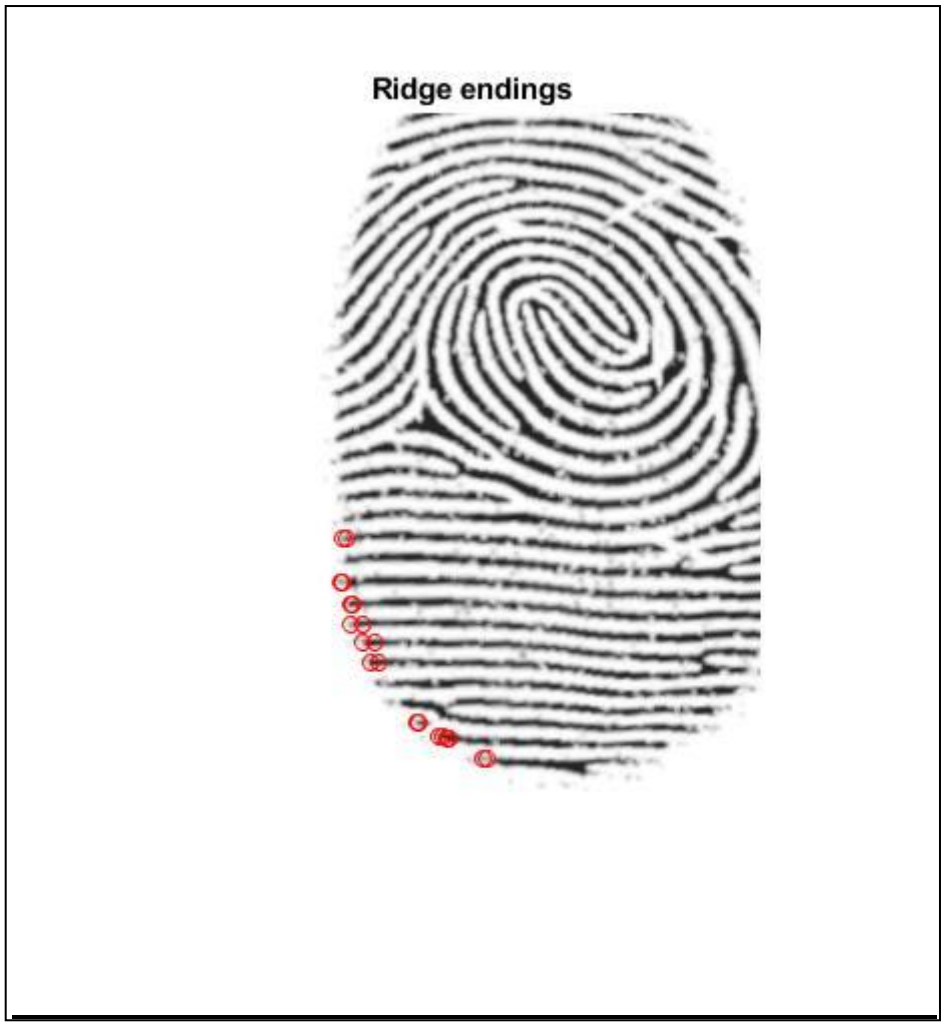


Figure 4.5: Ridge Endings of the fingerprint image

Thinning:

Figure 4.6 shows the thinned image of the fingerprint. To enhance the binary image the thinning algorithm is used to reduce the ridges of fingerprint images. There are number of thinning methods. The most popular thinning algorithms are medial axis method, contour generation method, local thickness based thinning approach, sequential and parallel thinning.

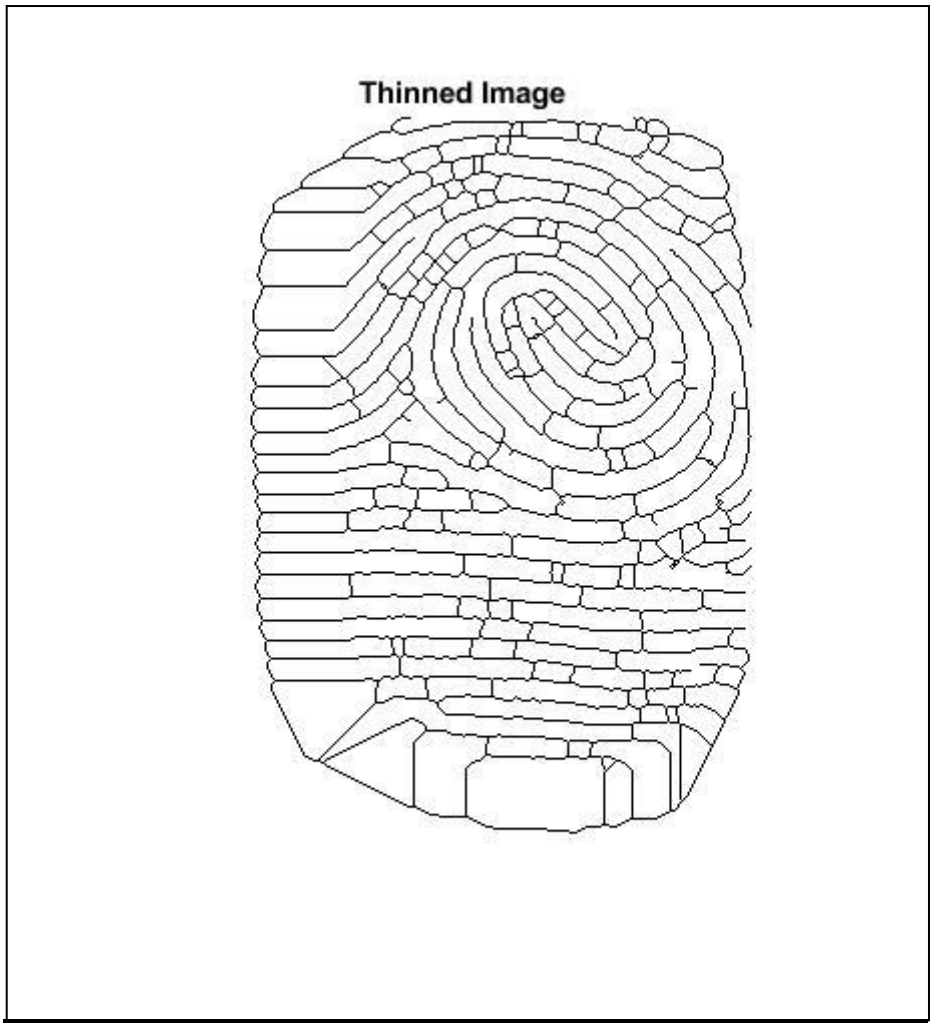


Figure 4.6: Thinned Image of the fingerprint

Minutiae Matching:

Figure 4.7 shows the matching minutiae of the fingerprint images. The summaries of algorithm of finding minutiae of fingerprint are given in the steps as follow:

Input: the thinning of fingerprint image, the orientation image in radians and mask.

Output: Ridge ending, Ridge Bifurcation.

Step1: find the size of thinning image.

Step2: find the label connected components in 2-D binary image which get the total number of ridge and ridge map.

Step3: scan the thinning fingerprint image to detect the minutiae, the 8-neighborhoods pixel are used to determine the ridge endings and ridge Bifurcation for each block have (0 ,1) Zero for thinning and one for determine the minutiae.

Step 4: if there is one neighbour for the pixel minutiae considered as ridge ending whereas it is considered as ridge bifurcation if there are at least 3 neighbours for the pixel.
Step 5: store the ridge endings and ridge Bifurcation in MATLAB file.
Step 6: End.

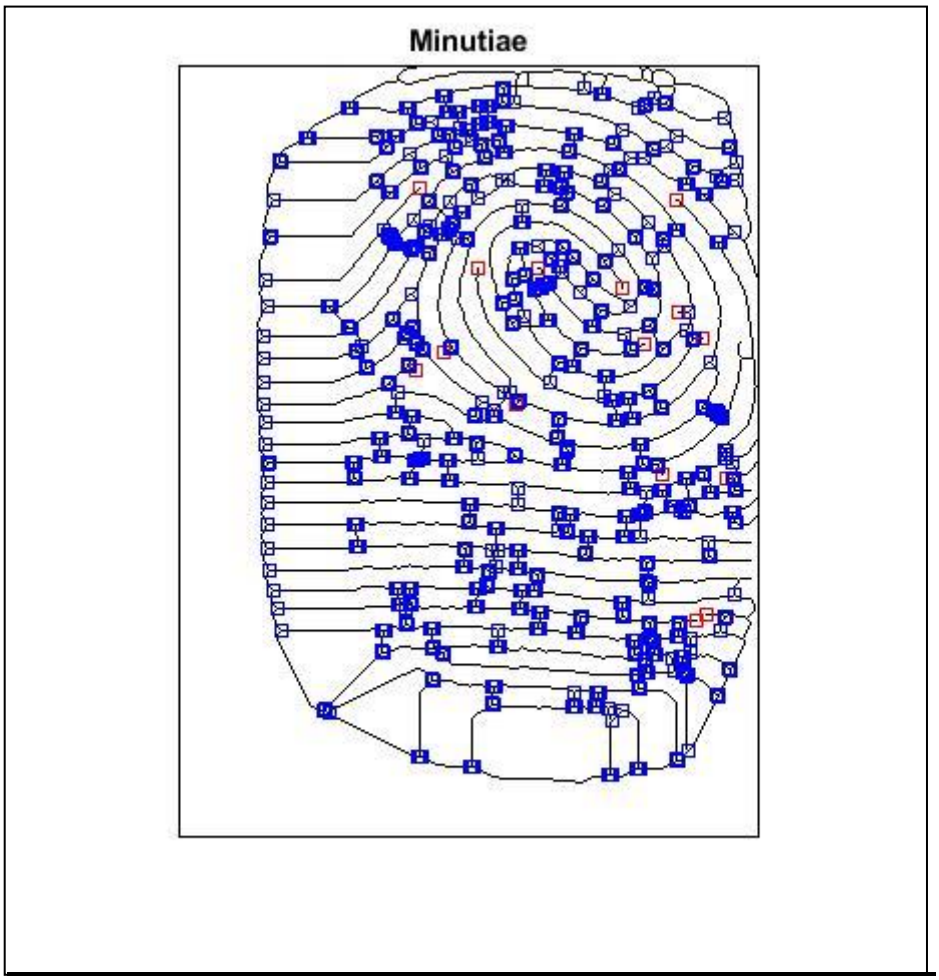


Figure 4.7: Matching Minutiae of the fingerprint image

Chapter 5:
Comparative Analysis

5.0 Comparative Analysis

Due to insufficient time, I was unable to complete my experiment. I have taken the experimental data from [1].
The comparison of Minutiae Extraction without/ with Enhancement is given in Table 5.1.

Table 5.1: Comparison of minutiae extraction

Images	Minutiae					
	Without Enhancement			With Enhancement		
	Ridge End	Bifurcation	Total	Ridge End	Bifurcation	Total
101_1	18	375	393	31	11	42
102_1	10	620	630	70	23	93
103_1	147	343	490	41	30	71
104_1	44	770	814	59	29	88

Chapter 6:
Conclusions and Future Scopes

6.0 Conclusions and future scope

In this work, we have presented fingerprint identification and verification based on minutiae features. The work is done in a sequence starting from the first stage which is pre-processing. Pre-processing stage is used to remove unwanted data and increased the clarity of ridges of fingerprint image. The second step is the feature extraction stage which is used to extract the fingerprint features. In this work, we focus on ridge ending and bifurcation which are done by using minutiae extractor algorithm. The third step of this work is the matching which is divided into two parts: identification process also known as (1:N) matching or verification process also known as(1:1 matching).

The experiments are tested on two fingerprint databases which are FVC2000 and FVC2002. The result of FVC2002 is better compared to FVC2000 in this work.

In future, fingerprint identification and verification can be done by using neural network and fuzzy logic. Using neural network and fuzzy logic, the performance of fingerprint recognition system will be enhanced. FAR & FRR may be reduced and testing can be done with more number of images.

References

1. Mouad.M.H.Ali, Vivek H.Mahale, Pravin Yannawar, A.T. Gaikwad; "Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching", IEEE 6th International Conference on Advanced Computing, 2016.

2. Y. Faridah , A.K. Kushsairy, Haidawati Nasir, Sairul I. Safie, Sheroz Khan, Teddy S. Gunawan; "Fingerprint Biometric Systems: Article in Trends in Bioinformatics", September, DOI: 10.3923/tb.2016.52.58, ISSN 1994-7941, 2016.

3. Mouad. M. H. Ali, Vivek H. Mahale, Pravin Yannawar, A. T. Gaikwad; "Overview of Fingerprint Recognition System", Conference Paper, March 2016, DOI: 10.1109/CEEOT.2016.7754902.

4. Sunil S. Harakannanavar, Raja K. B., Prashanth C. R.; "Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends", Volume 10, Issue: 04, pp. 3958-3968, ISSN: 0975-0290, 2019.

5. Abdullah Saud, Nazar Elfadil; "Biometric Authentication by using Fingerprint Recognition System", International Journal of Scientific Engineering and Science; Volume 4, Issue 5, pp. 22-28, 2020.

6. Steven A. Grosz, Joshua J. Engelsma and Anil K. Jain, "C2CL: Contact to Contactless Fingerprint Matching", 8 Apr 2021.

7. Meghna B. Patel, Satyen M. Parikh, Ashok R. Patel; "An Improved Approach in Fingerprint Recognition Algorithm", DOI: 10.1007/978-981-13-6295-8_12, January 2019.

8. Sek Socheat, Tianjiang Wang; "Fingerprint Enhancement, Minutiae Extraction and Matching Techniques, Journal of Computer and Communications", 8, pp. 55-74, 2020.

9. Khin Nandar Win, Kenli Li, Jianguo Chen, Philippe Fournier Viger, Keqin Li; "Fingerprint classification and identification algorithms for criminal investigation", A survey; 2019.

10. Nouf Saeed Alotaibi; “A New Method to Enhance Fingerprint Image Reconstruction Using Deep Boltzmann Machine”, International Journal of Intelligent Engineering and System, Vol. 13, No.1, 2020.

11. Buzuayehu Abebe, H C Ananda Murthy, Enyew Amare, Yilkal Dessie. “Latent Fingerprint Enhancement Techniques”, A Review. Journal of Chemical Reviews, 2(1), pp. 40-56, 2020.

12. Josef Ström Bartůněk; “Fingerprint Image Enhancement, Segmentation and Minutiae Detection”; Blekinge Institute of Technology 371 79 Karlskrona ISBN: 978-91-7295-321-5, ISSN 1653-2090, 2016.

13. Yi Wang, Jiankun Hu, Fengling Han; ‘’Enhanced gradient-based algorithm for the estimation of fingerprint orientation fields”;Book: Applied Mathematics and Computation, 185 pp. 823–833, 2017.

14. Ronak B Patel, Dilendra Hiran, Jayesh M Patel; “Fingerprint Image Thinning by applying Zhang – Suen Algorithm on Enhanced Fingerprint Image”; International Journal of Computer Sciences and Engineering; Vol. 7, Issue-4, May 2019.

15. Roli Bansal, Priti Sehgal and Punam Bedi; “Minutiae Extraction from Fingerprint Images - a Review”; International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011.

16. Mr. N.Surya, Mr. K.BhavaNarayana, Mr. K.Sathish; “Removal of False Minutiae Using Fuzzy Rules”, International Journal of Engineering And Science, Vol.3, Issue 6, pp. 56-62 ISSN (e): 2278-4721, ISSN (p):2319-6483, 2013.

17. Sonam Soni, Sukhmeet Kaur; “To Propose an Improvement in Zhang-Suen Algorithm for Image Thinning in Image Processing”; International Journal of Science Technology & Engineering , Volume 3, Issue 01 , July 2016.

18. FVC2000 database images http://bias.csr.unibo.it/fvc2000/

19. FVC2002 database images http://bias.csr.unibo.it/fvc2002/

Appendix

```
%% Fingerprint Analysis - Preprocessing and Feature Extraction

clear variables; clear globals; close all; clc;
% Load and Explore Image Data
d1DatasetPath = fullfile('C:\Users\papiya
dey\M.Tech\Reasearch\Database\FVC2000\DB1_B');
imds = imageDatastore(d1DatasetPath, ...
    'IncludeSubfolders',true,'LabelSource','foldernames');
numTrainFiles = 6;
[imdsTrain,imdsTest] =
splitEachLabel(imds,numTrainFiles,'randomize');

labelCount_train = countEachLabel(imdsTrain)
labelCount_test = countEachLabel(imdsTest)

for i = 1 : length(imdsTrain.Files)
    filename = imdsTrain.Files{i};
    img = imread(filename);
    imshow(img);
end



%% 1. Capture
% Our capture is reduced to a read in of a raw fingerprint
image. We assume
% the image is in grayscales (white: 255, black: 0).

I = imread('C:\Users\papiya dey\Downloads\Matlab
fingerprint\fingerprints\14_2.png');
[sizeX, sizeY] = size(I);
figure; imshow(I); axis off; title('Original Image');
figure
subplot(1,2,1)
imshow(I); title ('Histogram of Original Image');
subplot(1,2,2)
imhist(I,64)



%% 2. Preprocessing
hsize = 7;
hsigma = 0.2;
h = fspecial('log', hsize, hsigma); %creates a two dimensional
filter h of the specified type

 Ih = imfilter(Is,h);
 Ih = I - Ih;
```

```
J = fftshift(fft2(double(Is))); %rearranges a fourier
transform
Jh = imfilter(J,h);
Jh = J - Jh;
Ih = abs(ifft2(ifftshift(Jh)));

hsize = 7;
hsigma = 1;
h = fspecial('gaussian', hsize, hsigma);

[hx,hy] = gradient(h);
Gx = filter2(hx, I);%Gradients Gx and Gy
Gy = filter2(hy, I);

% Local ridge orientation D (in radiant)
hsize = 17;
hsigma = 3;
h = fspecial('gaussian', hsize, hsigma);

Gxy = Gx.*Gy; Gxy = 2*filter2(h, Gxy);
Gxx = Gx.^2;  Gxx =   filter2(h, Gxx);
Gyy = Gy.^2;  Gyy =   filter2(h, Gyy);
denom = sqrt((Gxx - Gyy).^2 + Gxy.^2) + eps;
sin2theta =       Gxy./denom;   sin2theta = filter2(h,
sin2theta);
cos2theta = (Gxx-Gyy)./denom;   cos2theta = filter2(h,
cos2theta);
D = pi/2 + atan2(sin2theta,cos2theta)/2;

% Coherence C as reliability of orientation
minima = (Gyy+Gxx)/2 - (Gxx-Gyy).*cos2theta/2 -
Gxy.*sin2theta/2;
Imax = Gyy+Gxx - minima;
z = .001;
C = 1 - minima./(Imax+z);
C = C.*(denom>z);


%% 2.4 Binarisation and skeleton
% Binarisation by threshold. Then we generate a skeleton by
thinning the region.
% We remove pixels from the border and spur pixels 20 times.

thresh = graythresh(I);
binarised = imbinarize(I,thresh);
thinned  = ~bwmorph(~binarised,'thin',Inf); % 'skel'
skeleton =  bwmorph(thinned,'spur',20);

binarisedMask = binarised.*Mask;
skeletonMask = skeleton.*Mask;
```

```
figure; imshow(binarisedMask,[]); axis off;
title('Binarised'); hold off;
figure; imshow(skeletonMask,[]); axis off; title('Skeleton');
hold off;

%% 3. Feature Extraction
[Gx2, Gy2, D2, C2] = ridgeorient(I, 1, 17, 3);
C2Mask = double(C2).*double(Mask);
minima = ~imregionalmin(C2Mask);

candidateFeatures = double(~minima).*double(Mask);
[minimaY, minimaX] = find(candidateFeatures == 1);

%% 3.2 Minutiae

Im = ~xor(skeletonMask, Mask);

% Window
hsize = 3;
window = zeros(hsize);
border = floor(hsize/2);
center = border+1;

% Temporary data to work with
row = sizeX + 2*border;
col = sizeY + 2*border;
double temp(row,col);
temp = zeros(row,col);
temp( (center):(end-border), (center):(end-border) ) =
Im(:,:);

% Minutiae containers
featureRidge       = zeros(row,col);
featureBifurcation = zeros(row,col);

for x = (center+10):(sizeX+border-10)
    for y = (center+10):(sizeY+border-10)
        % fill in window with values from temp
        e = 1;
        for k = x-border:x+border
            f = 1;
            for l = y-border:y+border
                window(e,f) = temp(k,l);
                f = f+1;
            end
            e=e+1;
        end
        if (window(center,center) == 0)
            featureRidge(x,y)       = sum(sum(~window));
            featureBifurcation(x,y) = sum(sum(~window));
```

```
        end
    end
end

% Resize area
featureRidge = featureRidge(1+border:end-border,1+border:end-
border);
featureBifurcation = featureBifurcation(1+border:end-
border,1+border:end-border);

%% 3.2.1 Ridge endings

[ridgeY, ridgeX] = find(featureRidge == 2);
figure; imshow(skeletonMask); axis off; title('Ridge
endings'); hold on; plot(ridgeX, ridgeY, 'ro'); hold off;
figure; imshow(I); axis off; title('Ridge endings'); hold on;
plot(ridgeX, ridgeY, 'ro'); hold off;

%% 3.2.2 Bifurcations

[bifurcationY, bifurcationX] = find(featureBifurcation == 4);
figure; imshow(skeletonMask); axis off; title('Bifurcations');
hold on; plot(bifurcationX, bifurcationY, 'bs'); hold off;
figure; imshow(I); axis off; title('Bifurcations'); hold on;
plot(bifurcationX, bifurcationY, 'bs'); hold off;

%% 3. Feature Extraction
%Program for Fingerprint Minutiae Extraction

%I = imread('C:\Users\USER\Downloads\DB1_B\102_1.tif');
%figure; imshow (I); title('Original Image');

%This program extracts the ridges and bifurcation from a
fingerprint image
%Read Input Image
binary_image=im2bw(imread('C:\Users\papiya
dey\Downloads\Matlab fingerprint\fingerprints\14_2.png'));
%Small region is taken to show output clear
% binary_image = binary_image(120:400,20:250);
figure;imshow(binary_image);title('Input image');

%Thinning
thin_image=~bwmorph(binary_image,'thin',Inf);
figure;imshow(thin_image);title('Thinned Image');

%Minutiae extraction
s=size(thin_image);
N=3;%window size
n=(N-1)/2;
r=s(1)+2*n;
c=s(2)+2*n;
```

```
double temp(r,c);
temp=zeros(r,c);bifurcation=zeros(r,c);ridge=zeros(r,c);
temp((n+1):(end-n),(n+1):(end-n))=thin_image(:,:);
outImg=zeros(r,c,3);%For Display
outImg(:,:,1) = temp .* 255;
outImg(:,:,2) = temp .* 255;
outImg(:,:,3) = temp .* 255;
for x=(n+1+10):(s(1)+n-10)
    for y=(n+1+10):(s(2)+n-10)
        e=1;
        for k=x-n:x+n
            f=1;
            for l=y-n:y+n
                mat(e,f)=temp(k,l);
                f=f+1;
            end
            e=e+1;
        end;
         if(mat(2,2)==0)
            ridge(x,y)=sum(sum(~mat));
            bifurcation(x,y)=sum(sum(~mat));
         end
    end;
end;
```