FINGER PRINT IMAGE RECOGNITION

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE
REQUIREMENTS FOR THE AWARD OF THE DEGREE OF

MASTER OF ENGINEERING

IN

CONTROL & INSTRUMENTATION

SUBMITTED BY

ADITYA GUPTA
(Roll NO. 8662)

UNDER THE ESTEEMED GUIDANCE
OF

Dr. PARMOD KUMAR
(PROFESSOR & HEAD)

DEPARTMENT OF ELECTRICAL ENGINEERING
DELHI COLLEGE OF ENGINEERING
UNIVERSITY OF DELHI
2004-2006

CERTIFICATE

It is certified that Mr. Aditya Gupta, Roll No.8662, student of M.E, Control and Instrumentation, Department of Electrical Engineering, Delhi College of Engineering, has submitted the dissertation entitled **“Finger Print Image Recognition”**, under my guidance towards partial fulfillment of the requirements for the award of the degree of Master of Engineering (Control & Instrumentation Engineering).

This dissertation is a bonafide record of project work carried out by him under my guidance and supervision. His work is found to be good and his discipline impeccable during the course of the project.

I wish him success in all his endeavors.

Date : **(Dr. Parmod Kumar)**

Professor & Head

Dept. of Electrical Engineering

Delhi College of Engineering

ACKNOWLEDGEMENT

I would like to avail this opportunity to humbly thank and appreciate the contribution and support, which various individuals have provided for the successful completion of this dissertation.

My heartfelt thanks to my project guide **Dr. Parmod Kumar**, Professor & Head, Department of Electrical Engineering, DCE, who provided me an opportunity to work under his guidance. His guidance and suggestions helped me to complete the project in this advanced field.

My humble thanks to **Ms. Deepa, Ms. Meenakshi** and **Mr. Sudhir,** Computer Centre, DCE for providing the necessary resources needed for my project. I would thank **Mr. Karan Singh**, Laboratory Assistant, Department of Electrical Engineering, DCE for his kind cooperation during the development of project.

I would like to extend my sincere appreciation to **Mr. Rohan Koudniya** for reviewing this report and providing valuable comments and thoughtful criticism.

I am indebted to my **parents and family** for their love and prayers.

Lastly, I thank Almighty GOD for his countless blessings.

DATE: **ADITYA GUPTA**

College Roll No. 02/C&I/04
Delhi Univ. Roll No. 8662

CONTENTS

ABSTRACT

Fingerprints are imprints formed by the friction ridges of the skin and thumbs. Fingerprints are the oldest and most widely used form of biometric identification. However manual fingerprint recognition is so tedious, time consuming and expensive that is incapable of meeting today's increasing performance requirement. An automatic fingerprint image recognition system is widely accepted in many applications such as building or area security. Contrary to popular belief and despite decades of research, reliable fingerprint image recognition is still an open problem.

The aim of this project is to develop the fingerprint image recognition system. The aim is divided into 3 major steps of image enhancement, feature extraction and feature matching. A comparison of the enhancement techniques available in various literature lead to the five sub-stages in the enhancement i.e. histogram-equalization, normalization, fft-enhancement, binarization and noise filtering.

Minutiae-based matching is employed in this project. This technique is based on the extraction of minutiae using crossing number approach from the thinned, binarized and segmented version of a fingerprint image. Then real minutiae set of the two images are matched to take the decision in Identification and Verification.

Also a program coding with MATLAB going through all the stages of the fingerprint recognition is built. It is helpful to understand the procedures of fingerprint recognition. And demonstrate the key issues of fingerprint recognition.

The aim of the experimental results section is to illustrate the results of each stage in the enhancement algorithm and to assess how well each stage performs.

LIST OF FIGURES

LIST OF TABLES

CHAPTER I

INTRODUCTION

1.1 INTRODUCTION

Security is a major issue in the modern world and valuable information ending up in the wrong hands can result in a lot of inconvenience and damage. Traditional methods used to secure valuables and restricted information include passwords, access cards, PIN codes, credit cards, keys, tokens etc. These methods however are not very secure as they are easily transferable and quite easily obtained by any third parties who want unauthorized access to valuables and information. Biometric methods of identification use physical, behavioral and physiological attributes that are unique to each individual such as fingerprints, patterns of the iris, patterns of the retina, geometry of the hand, speech pattern, signature or gait to authenticate and identify individuals. Biometric identifiers such as these are not as easy to obtain or forge like traditional methods of identification and therefore provide better means of security.

Fingerprints are one of the most reliable biometric features and are extensively used in various areas. Fingerprints are imprints formed by friction ridges of the skin and thumbs. They have long been used for identification because of their immutability and individuality. Immutability refers to the permanent and unchanging character of the pattern on each finger. Individuality refers to the uniqueness of ridge details across individuals; the probability that two fingerprints are alike is about 1 in 1.9x1015.

Latest data suggest more than half the biometric market attributed to fingerprint as the biometric identifier for authentication. Fingerprint biometric systems are widely used in forensics and prison security, criminal investigation, and a multitude of different civilian and government applications. They also have great potential in identification of criminals and terrorists and maintaining security in sensitive places such as airports, railway terminals and government establishments. They are also being increasingly used in internet based authentication so the applications are increasing daily.

1.2 PROBLEM IDENTIFICATION

Existing security measures rely on knowledge-based approaches like passwords or token based approaches such as swipe cards and passports to control access to physical and virtual spaces. Though ubiquitous, such methods are not very secure. Tokens such as badges and access cards may be shared or stolen. Furthermore, they cannot differentiate between authorized user and a person having access to the tokens or passwords

Biometrics such as fingerprint, face and voice print offers means of reliable personal authentication that can address these problems and is gaining citizen and government acceptance. Fingerprints were one of the first forms of biometric authentication to be used for law enforcement and civilian applications. Contrary to popular belief and despite decades of research in fingerprints, reliable fingerprint recognition is still an open problem.

1.3 OBJECTIVE OF STUDY

In the context of fingerprint image recognition, fingerprint images or simply fingerprints are generally used to refer to the impressions of human fingers.
There are two objectives of study**:**

1) To investigate the current techniques for fingerprint image recognition. This target can be mainly decomposed into image preprocessing, feature extraction and feature match. For each sub-task, some classical and up-to-date methods in literatures are analyzed.

2) To develop an integrated solution for fingerprint recognition based on the above analysis. That incorporates both identification and verification. Then the program is implemented in MATLAB in order to demonstrate the various stages of the solution.

1.4 PROPOSED SOLUTION

The project has combined many methods to build the complete solution. The combination of multiple methods comes from a wide investigation into research paper. Also some changes like filtering of isolated pixels, ridges marking using matlab inbuilt function not reported in other referred literatures. The complete solution for fingerprint image recognition problem consists of various stages. The stage-wise solution is as follows:

1) Image enhancement: The image is enhanced in five steps. These are Histogram Equalization, Normalization, FFT-Enhance, Binarization and Noise filtering. First histogram equalization is used for evenly distribution of the pixel values so as to increase the perceptional information [19]. Then normalization is done to make the image have a prespecified mean and variance [1]. FFT-Enhancement is used to increase the discrimination between ridges and valleys and to separate parallel ridges [2]. After the Binarization operation, ridges in the fingerprint are highlighted with black color while furrows are white [19]. Noise filtering removes those single isolated white pixels which are surrounded by black pixels.

2) Feature Extraction: Extraction of appropriate features is one of the important tasks for a recognition system. First the Segmentation is performed to separate the actual fingerprint (Region of Interest) from the background. Direction for every block of image is find out and block without having significant direction is removed out [7]. Thinning operation reduces the ridges thickness to one pixel wide [4]. So that they can be further process easily. Marking of minutiae involves the scanning of the binary image to detect the pixels corresponding to minutiae [5]. Together with the minutia marking, all thinned ridges in the fingerprint image are labeled with a unique ID for further operation. Unfortunately earlier processing stages i.e. thinning introduces some spurious minutiae. These must be removed to improve the accuracy of the system [6].

3) Matching

In verification system, one minutia from both of the input image is taken as a reference minutia and if their ridges matches well then the images are aligned for further matching of other minutiae [7]. Depending on the ratio of number of minutiae matched to the total number of minutiae the percentage of matching is calculated. And if it is above a threshold, the images are declared as successfully matched. In case of identification, the input image is compared with all the images from database. The case in which the matching ratio is above the threshold is identified as of input image.

1.5 DISSECTION OF DISSERTATION

The thesis is organized into 9 chapters. The introduction of each chapter is as follows**:**

Chapter 1: Chapter 1 has identified the problem and the objective of the study. And also the solution which is used in this project.

Chapter 2: This chapter reviews the previous research relevant to the fingerprint enhancement and recognition. The research involves various methods for each stage of the solution; some of them are utilized in this thesis.

Chapter 3: An introduction of the biometrics is provided in this chapter. The advantages causing the adaptability of fingerprints as a biometric are discussed along with the new trends in biometric.

Chapter 4: This chapter starts with the introduction of fingerprint image and its features. Then the methods required for the completion of the recognition system are outlined. The design and implementation of the entire program is then discussed in detail in next chapters.

Chapter 5: The detailed analysis of the set of methods required for the fingerprint enhancement and their implementation is provided in this chapter.

Chapter 6: This chapter includes the analysis and implementation of the methods used in the minutiae extraction stage. And how the efficiency of the recognition is improved is discussed in this chapter.

Chapter 7: The matching algorithm for the minutiae corresponding to the two fingerprint images is discussed along with how the verification and identification task is done

Chapter 8: The results from the enhancement and comparison of fingerprint pairs are provided using the MATLAB, detailing the dependency of the procedure on previous steps. Then achievement of goal is discussed.

Chapter 9: Conclusions about the viability of the automated fingerprint recognition systems are drawn from the results. Scope of the project and further developments are also discussed.

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

In 1893, the Home Ministry Office, UK, accepted that no two individuals have the same fingerprints. Soon after this discovery, many major law enforcement departments embraced the idea of first "booking" the fingerprints of criminals, so that their records are readily available and later using leftover fingerprint smudges (latents), they could determine the identity of criminals. These agencies sponsored a rigorous study of fingerprints, developed scientific methods for visual matching of fingerprints and strong programs/cultures for training fingerprint experts, and applied the art of fingerprint recognition for nailing down the perpetrators.

Despite the ingenious methods improvised to increase the efficiency of the manual approach to fingerprint indexing and search, the ever growing demands on manual fingerprint recognition quickly became overwhelming. The manual method of fingerprint indexing resulted in a highly skewed distribution of fingerprints into bins (types): most fingerprints fell into a few bins and this did not improve search efficiency. Fingerprint training procedures were time-intensive and slow. Furthermore, demands imposed by the painstaking attention needed to visually match the fingerprints of varied qualities, tedium of the monotonous nature of the work, and increasing workloads due to a higher demand on fingerprint recognition services, all prompted the law enforcement agencies to initiate research into acquiring fingerprints through electronic media and automate fingerprint recognition based on the digital representation of fingerprints. These efforts led to development of *Automatic Fingerprint Identification Systems* (AFIS) over the past few decades.

There is a popular misconception that automatic fingerprint recognition is a fully solved problem inasmuch as it was one of the first applications of machine pattern recognition almost fifty years ago. On the contrary, fingerprint recognition is still a challenging and important pattern recognition problem. The following text reflects the progress made in automatic techniques for fingerprint recognition over the past four decades. The existing techniques are divided into various stages so as to present them in a systematic way.

2.2 FINGERPRINT IMAGE ENHANCEMENT

The general purpose image enhancement techniques do not produce satisfying and definitive results for fingerprint image enhancements. However, contrast stretching, histogram equalization, normalization and wiener filtering have been shown to be effective as initial processing steps in a more sophisticated fingerprint enhancement algorithm.

The normalization approach used by Wan and Jain (1998) determines the new intensity value of each pixel in an image based on the global mean and variance and the desired mean and variance [1]. Histogram equalization produces an output image having values evenly distributed throughout the range so as to enhance the contrast [19]. In the case of fingerprint image, it increases the contrast between the ridges and the valleys. The most widely used technique for fingerprint enhancement is based on contextual filters. In conventional image filtering, only a single filter is used for convolution throughout the image. In contextual filtering, the filter characteristic change according to the local context. The filter purposed by O'Gorman and Nickerson (1988, 1989) was one of the first to use contextual filtering for fingerprint enhancement [7]. The filter is bell-shaped elongated along the ridge direction and cosine tapered in the direction normal to the ridges. The image enhancement is performed by convolving each point of the image with the filter. Hong, Wan, and Jain (1998) proposed an effective method based on Gabor filters [9]. Gabor filters have both frequency-selective and orientation-selective properties and have optimal joint resolution in both spatial and frequency domains. For sufficient reliability in poor quality fingerprint images, Jain, Prabhakar, Hong and Pankanti (2000) proposed to apply the bank of gabor filters of a given set at each point in the image [10]. A "selector" then chooses the best response from all the filter responses. Another interesting technique FFT-Enhancement that is able to perform a sort of contextual filtering without requiring explicitly computing local ridge orientation and frequency was purposed by Wills and Myers (2001) [2]. Each block in the image is enhanced separately by multiplying the Fourier transform of the image with its power spectrum. The general problem of image binarization has been widely studied in the fields of image processing and pattern recognition (Trier and Jain, 1995) [12]. The easiest approach uses a global threshold t and works by setting the pixels using whose gray-level is lower than t to 0 and remaining pixels to 1. In local threshold technique the threshold is calculated for each block of the image [19]. Moayer and Fu (1986) purposed a binarization technique based on an iterative application of a Laplacian operator and a pair of dynamic thresholds [11]. At each iteration, the image is convolved through a Laplacian operator and the pixels whose intensity lies outsides the range bounded by the two thresholds are set to 0 and 1.

2.3 MINUTIAE EXTRACTION

Grasseli (1969) first introduces fingerprint orientation image (also called directional image) as a matrix D whose elements encode the local orientation (ϴij) of the fingerprint ridges [7]. Each element of this matrix corresponds to the center pixel of a square-meshed grid located over the center pixel, denotes the average orientation of the fingerprint ridges in a neighborhood of this center pixel. Prewitt and Sobel convolution masks (Gonzales and Woods, 1992) is used to determine the derivatives along x and y direction [13]. Their ratio determines the local orientation. This method presents problem due to the noise present in the image. Kass and Witkin (1987) proposed a simple but elegant solution to the above problem, which allows local gradient estimates to be averaged [14]. Their basic idea is to double the angles so that each element of D is encoded by a vector. Based on the above idea, an effective method is given by Ratha, Chen, and Jain (1995) to compute the local orientation [15]. Their method calculates the dominant ridge orientation by combining multiple gradient estimates with in a 17×17 window centered at [x_i, y_i]. The local ridge frequency at point [x,y] is the inverse of the number of ridges per unit length along a hypothetical segment centered at [x,y] and orthogonal to the local ridge orientation. The local ridge frequency varies across different fingers and may also noticeably vary across different regions in the same fingerprint. Hong, Wan and Jain (1998) estimate the local frequency by counting the average number of pixels between two consecutive peaks of gray-levels along the direction normal to the local ridge orientation [1]. Segmentation is used for the separation of finger print area (foreground) from the image background. Ratha, Chen, and Jain (1995) assigned each 16×16 block to the foreground or the background according to the variance of gray-levels in the orthogonal direction to the ridge orientation [15]. They also derive a quality index from the block variance. The underlying assumption is that the noisy regions have no directional dependence, whereas regions of interest exhibit a very high variance in a direction orthogonal to the orientation of ridges and very low variance along ridges. Maio and Maltoni (1997) discriminated foreground and background by using the average magnitude of the gradient in each image block [16]; in fact, because the fingerprint area is rich in edges due to the ridge/valley alteration, the gradient response is high in the fingerprint area and small in the background. Thinning operation reduces the ridges thickness to one pixel wide [4]. So that they can be further process easily. Arceli and Baja (1984) proposed the minutiae extraction approach using the crossing number [21]. The crossing number of a pixel p is defined as half the sum of the differences between pairs of adjacent pixels in the 8-neighborhood of p. The rules for removing false minutiae are given in number of literatures [6].

2.4 MATCHING

Asker M.Bazen ,Gerben T.B. Verwaaijen, Sabih H.Gerez (2000) suggest the method of Correlation-based matching in which two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations) [20]. Minutiae-based matching is the most popular and widely used technique being the basis of the fingerprint comparison made by fingerprint examiners [7],[8]. The minutiae are first aligned to compensate for the unavoidable errors made by feature extraction algorithms and to account for the small plastic distortion that causes the minutiae position to change. Then aligned minutiae are matched to take the decision of matching. Another approach of minutiae matching using Hough transform is given by Ratha Et Al.(1996) [5]. In this approach the minutiae sets are first registered using a derivative of the Hough transform. A variant of the above method was proposed by Luo, Tian and Wu (2000) where ridge matching was performed in a slightly manner [8]. Instead of correlating the y-coordinates of the sampled points along the two ridges, the authors matched distances and relative angles of the sampled points.

2.5 CONCLUSION

Robust feature extraction remains a challenging problem, especially in poor quality fingerprints. Development of fingerprint-specific image processing techniques is necessary in order to solve some of the outstanding problems. For example, explicitly measuring (restoring or masking) noise such as creases, cuts, dryness and the like will be helpful in reducing feature extraction errors.

Different applications desire different properties in the fingerprint matching algorithms (e.g. template size, matching speed etc.). Most of the fingerprint matching approaches introduced in the last four decades are minutiae-based, but recently correlation-based techniques are receiving renewed interest.

After the extensive study of various literatures it is found that all fingerprint recognition problems, either verification or identification, are ultimately based on a well-defined representation of a fingerprint. As long as the representation of fingerprints remains the uniqueness and keeps simple, the fingerprint matching is straightforward and easy. A number of techniques are proposed in the literature for some operations in the complete recognition, however those techniques which give the accurate result and in minimum time should be taken.

CHAPTER III

BIOMETRICS SYSTEMS OVERVIEW

3.1 INTRODUCTION

A biometric system is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological (e.g. fingerprints, face, retina, iris) and/or behavior (e.g. gait, signature) characteristic possessed by that person. The area of biometrics can therefore be defined as the task of automatically recognizing a person using his/her distinguishing traits.

The idea of biometric identification is not new, it have been around for centuries. We know that the Babylon kings used imprints of their hands to verify documents and handwritten signatures has been a popular way of verifying documents and handwritten signatures has been a popular way of verifying documents ever since man started writing. Another example of a biometric is the photo on identification cards and passports, which still is the most important way of verifying the identity of a person. The difference today is that we now have access to technologies enabling us to do these verifications automatically and almost in real time.

An important issue in designing a practical biometric system is to determine how an individual is recognized. Depending on the application context, a biometric may be called either a *verification* system or an *identification* system.

• **A verification system** authenticates a person's identity by comparing the captured biometric characteristic with her own biometric templates pre stored in the system. It conducts one-to-one comparison that determines whether the identity claimed by the individual is true. A verification system either rejects or accepts the submitted claim of identity (*Am I whom I claim I am*?).

• **An identification system** recognizes an individual by searching the entire template database for a match. It conducts one-to-many comparisons to establish the identity of the individual. In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system database) without the subject having claim an identity (*Who am I*?).

3.2 WORKING OF AN ARBITRARY BIOMETRICS SYSTEM

Most biometrics systems use a similar procedure to verify a biometric. The procedure can be divided into the following steps:

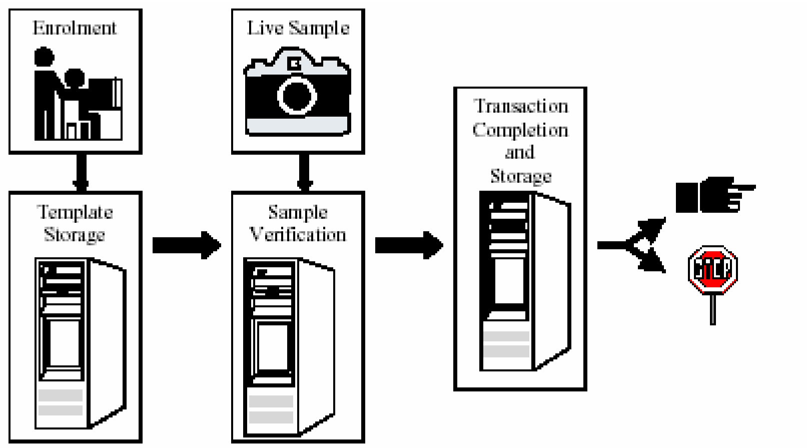


Figure 3.1 General Biometric System

3.2.1 THE ENROLMENT

Before a biometric can be used to identify a person, a trusted sample of the biometric must be captured and saved in some kind of user database. The enrolment is a very important step of the whole identification process. Without having a high quality sample of the user's biometric data, it is not possible to compare live sample with later in the verification procedure. This sample is usually refereed to as the user's biometric template.

3.2.2 TEMPLATE STORAGE

There are some interesting issues concerning the template storage. First of all, one must decide on *what form* to store the actual data on. Let's take the example of the credit card system; one realizes that for a system like that to work some kind of international standard for the storage format has to be achieved. Secondly one would have to decide *where* the template is to be stored. In case of the credit card example, one possibility would be to save the template on some sort of smart card. This alternative has one big advantage, namely user acceptance. People are in general afraid that if personal information and identification data are saved in big databases, it might be misused. Another alternative to template storage is a central user database. If the biometrics system have a large number of users it is not practical to save the templates within the scanning devices.

3.2.3 THE VERIFICATION

When a user tries to be accepted by a biometrics system, a live sample of the users biometric is compared to the stored templates. This is the most complex part of the system and it is called the Verification. The verification process can be subdivided into following stages:

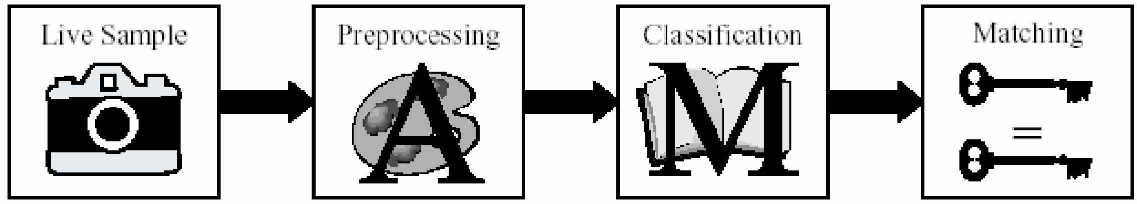


Figure 3.2 Verification Stages

• PREPROCESSING

First, all the system needs to filter the live sample in some way to find the relevant parts. For example, this could be done by removing the background from a face image or by transforming a fingerprint scan from grayscale to black and white. In the fingerprint case one might also want to transform the lines to a width of just one pixel during the preprocessing phase to ease the later phases of the verification process.

• CLASSIFICATION

If the system has a large number of users, it might be a good idea to make some sort of classification of the sample before starting to compare it to the actual templates in the database. That way the number of necessary templates to be tested can be greatly reduced and therefore also the processing time.

Figure 3.3 shows the classical fingerprint classification system that has been used by law enforcement agencies for decades. When a fingerprint was printed on card to be put into an archive, an expert first examined it to classify it. That way it was a lot easier to find a matching template when a new fingerprint arrived. Today the classification is done automatically and the method depends on the type of biometrics system used.

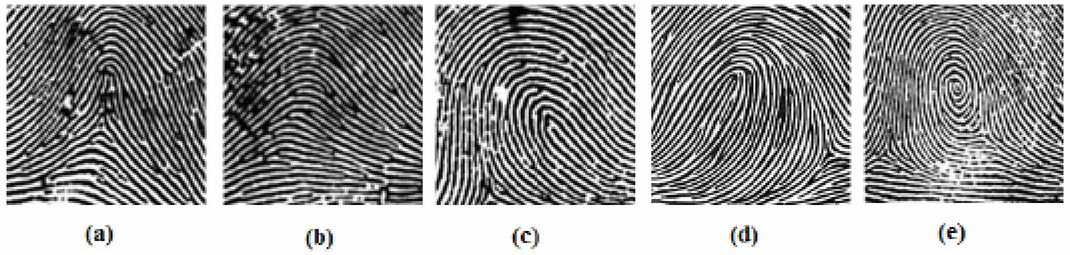


Figure 3.3 Fingerprint Classes: (a) Tended Arch (b) Arch (c) Right Loop (d) Left Loop (e) Whorl

• MATCHING

The matching procedure is the part of the verification process where the system tries to find a template in its database that is "sufficiently" alike the sample provided by the user. Due to the analog nature of the user sample, the system will probably not find a perfect match in its database, but rather a list of possible matches. If the system accepts the user or not, depends on some sort of security threshold set by the system administrator. How the matching procedure actually is performed depend much on the type of biometrics system. Generally, the system would try to find some key features in the user sample to match against the templates. In fingerprint image recognition these features are generally bifurcation and ridge ending.

3.2.4 TRANSACTION COMPLETION AND STORAGE

Depending on if the system is designed for verification or identification the result of the transaction can be to accept, to reject or to list possible matches. In the case of a verification system, it might be a good idea to keep a log of attempted verifications for security reasons and statistical reasons. Some systems might also update the template upon a successful transaction, this way the template quality will constantly improve and the system will be able to handle small natural changes to the biometric. For example scars in fingerprints, aging etc.

3.3 SYSTEM PERFORMANCE

System performance is a vague term and what it means depends much on what type of system it refers to. When talking about biometrics system performance, it is the probability that the system will accept authorized users and reject unauthorized users. Biometrics system usually has some security threshold setting that enables the system administrator to adjust the system to optimal performance.

The ***False Reject Rate*** **(FRR)** and the ***False Accept Rate*** **(FAR)** are often mentioned when describing biometrics systems. The FRR is, the percentage of times the system refuses to accept an authorized user, and the FAR is the percentage of times that the system will accept an unauthorized user.

The FAR and the FRR are closely connected. If the system administrator rises the security threshold, the false accepts will drop. Unfortunately, at the same time the FAR will increase since it also will be harder for the live samples of authorized users to match the higher demands. The reverse is also true, if the threshold is lowered the FRR will drop but the FAR will rise.

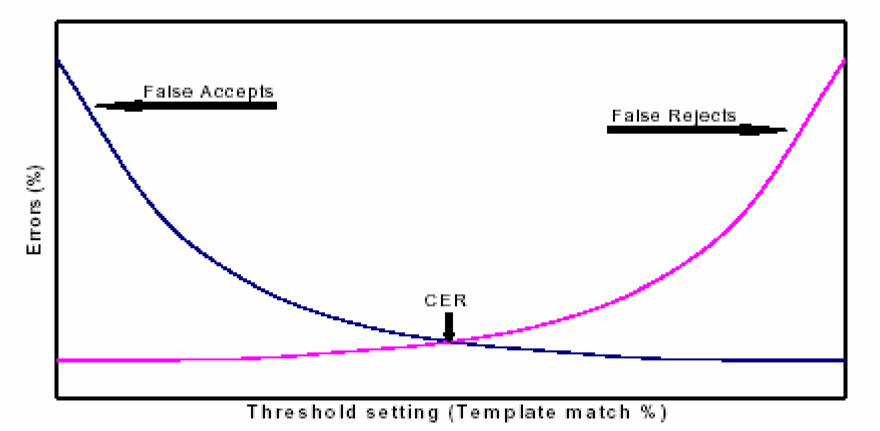


Figure 3.4 Graph showing the relationship between FRR and FAR

The ***Crossover Error Rate*** **(CER)**, or as it is sometimes referred to, the *Equal Error Rate* (EER) is the point where the FRR and the FAR curves meet. Figure 3.4 shows an example how these terms are linked together. CER point is usually the best choice while trying to set the security threshold to get optimal performance out of a biometrics system. Of course this is not always the case; it depends on the type of security levels that are needed. If the system is intended to verify the identity of authorized personnel at very prime location, a few false rejects are probably to prefer compared to the risk of giving unauthorized personnel access to the facilities. On the other hand, if the biometrics system is used in an ATM the risk of a few false accepts are probably to prefer compared to the annoyance of the customers waiting in line if the system keep rejecting authorized users.

Another important term when talking about system performance, though often not mentioned, is ***Failure To Acquire biometric*** **(FTA).** There are also several other issues to consider when evaluating a biometrics system's performance, such as speed, user acceptance etc. For example, one will not use a biometrics system in an ATM if it takes the system a couple of minutes to verify a user. And also, if the users do not trust the biometrics system to be accurate they will not be using the system to start with. Discussions over issues like these are usually collected together with the FAR, FRR, CER etc. into something called the ***Total System Performance*** **(TSP).**

3.4 MOST COMMON BIOMETRICS

- **DNA:** Deoxyribo Nucleic Acid (DNA) is the one-dimensional ultimate unique code for one's individuality, except for the fact that identical twins have identical DNA patterns. It is, however, currently used mostly in the context of forensic applications for person recognition. Several issues limit the utility of this biometric for other applications:

i) Contamination and sensitivity: it is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose.

ii) Automatic real-time recognition issues: the present technology for DNA matching requires cumbersome chemical methods (wet processes) involving an expert's skills and is not geared for on-line non-invasive recognition;

iii) Privacy issues: information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination, for example, in hiring practices.

- **Odor:** It is known that each object exudes an odor that is characteristic of its chemical composition and could be used for distinguishing various objects. A whiff of air surrounding an object is blown over an array of chemical sensors, each sensitive to a certain group of (aromatic) compounds. A component of the odor emitted by a human (or any animal) body is distinctive to a particular individual.

- **Face:** The face is one of the most acceptable biometrics because it is one of the most common methods of recognition that humans use in their visual interactions. In addition, the method of acquiring face images is nonintrusive. Facial disguise is of concern in unattended recognition applications. It is very challenging to develop face recognition techniques that can tolerate the effects of aging, facial expressions, slight variations in the imaging environment, and variations in the pose of the face with respect to the camera (2D and 3D rotations).

- **Facial, hand, and hand vein infrared thermograms:** The pattern of heat radiated by the human body is a characteristic of each individual body and can be captured by an infrared camera in an unobtrusive way much like a regular (visible spectrum) photograph. The technology could be used for covert recognition and could distinguish between identical twins.

A thermogram-based system is non-contact and non-invasive but sensing challenges in uncontrolled environments, where heat-emanating surfaces in the vicinity of the body, such as, room heaters and vehicle exhaust pipes, may drastically affect the image acquisition phase. A related technology using near infrared imaging is used to scan the back of a clenched fist to determine hand vein structure.

- **Iris:** Visual texture of the human iris is determined by the chaotic morphogenetic processes during embryonic development and is posited to be distinctive for each person and each eye. An iris image is typically captured using a non-contact imaging process. Capturing an iris image involves cooperation from the user, both to register the image of iris in the central imaging area and to ensure that the iris is at a predetermined distance from the focal plane of the camera. The iris recognition technology is believed to be extremely accurate and fast.

- **Keystroke dynamics:** It is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometric is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe large variations from typical typing patterns. The keystrokes of a person using a system could be monitored unobtrusively as that person is keying in information.

- **Retinal scan:** The retinal vasculature is rich in the structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature. The image capture requires a person to peep into an eyepiece and focus on a specific spot. However it may not be generally accepted since the user must come into close contact with the scanning device

- **Signature:** The way a person signs his name is known to be a characteristic of that individual. Although signatures require contact and effort with the writing instrument, they seem to be acceptable in many government, legal, and commercial transactions as a method of verification. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories.

- **Voice:** Voice capture is unobtrusive and voice print is an acceptable biometric in almost all societies. Voice may be the only feasible biometric in applications requiring person recognition over a telephone. Voice is not expected to be sufficiently distinctive to permit identification of an individual from a large database of identities.

Moreover, a voice signal available for recognition is typically degraded in quality by the microphone, communication channel, and digitizer characteristics. Voice is also affected by a person’s health (e.g., cold), stress, emotions, and so on. Besides, some people seem to be extraordinarily skilled in mimicking others.

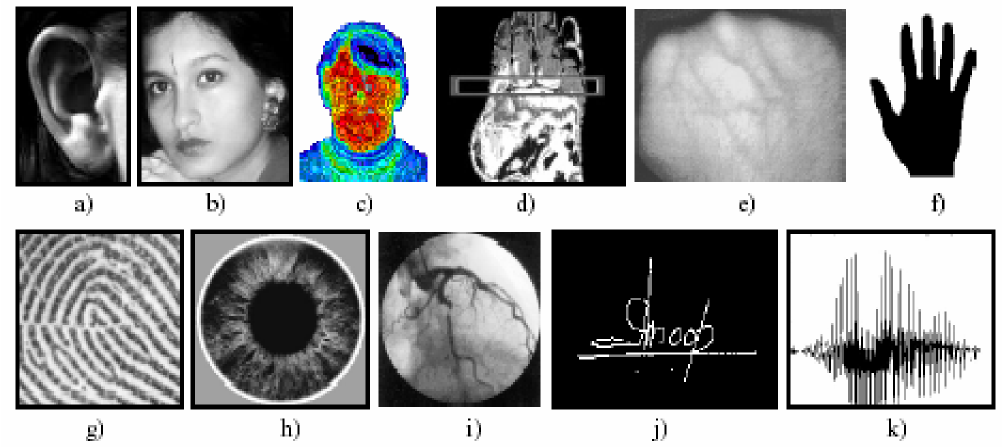


Figure 3.5 Some of the biometrics are shown: a) ear, b) face, c) facial thermogram, d) hand thermogram, e) hand vein, f) hand geometry, g) fingerprint, h) iris, i) retina, j) signature, and k)voice.

3.5 ADVNTAGES AND DISADVANTAGES OF BIOMETRIC TECHNIQUE

Technology	Advantages	Disadvantages
Fingerprint scanning	- Inexpensive - Very secure	-Physical contact to a general scanning device may spread germs.
Hand geometry scanning	- May lead to a better technology (measurements of a vein structure in a hand)	- Not unique as fingerprints
Retina-based scanning	- Accuracy is assured since the retina relatively stable throughout a lifetime	- May not be generally accepted since the user must come into close contact with the scanning device
Iris-based scanning	- Very difficult to fool	-Expensive
Facial recognition	- Process can be invisible	- Expensive - Accuracy
Voice authentication	- Widely known to work well over the telephone -Low cost -May be able to measure stress	- Background noise or sickness may cause interference - Voice can be easily changed
Signature verification	- Widely accepted	- Accuracy is difficult to ensure

3.6 FINGERPRINTS AS A BIOMETRIC

Fingerprints were accepted formally as valid personal identifier in the early twentieth century and have since then become a de-facto authentication technique in law-enforcement agencies world wide. Fingerprints have several advantages over other biometrics, such as the following**:**

1. High universality: A large majority of the human population has legible fingerprints and can therefore be easily authenticated. This exceeds the extent of the population who possess passports, ID cards or any other form of tokens.

2. High distinctiveness: Even identical twins who share the same DNA have been shown to have different fingerprints, since the ridge structure on the finger is not encoded in the genes of an individual. Thus, fingerprints represent a stronger authentication mechanism than DNA. Furthermore, there has been no evidence of identical fingerprints in more than a century of forensic practice.

3. High permanence: The ridge patterns on the surface of the finger are formed in the womb and remain invariant until death except in the case of severe burns or deep physical injuries.

4. Easy collectability: The process of collecting fingerprints has become very easy with the advent of online sensors. These sensors are capable of capturing high resolution images of the finger surface within a matter of seconds. This process requires minimal or no user training and can be collected easily from co-operative or non co-operative users. In contrast, other accurate modalities like iris recognition require very co-operative users and have considerable learning curve in using the identification system.

5. Wide acceptability: While a minority of the user population is reluctant to give their fingerprints due to the association with criminal and forensic fingerprint databases, it is by far the most widely used modality for biometric authentication.

3.7 FINGERPRINT SENSORS

Traditionally fingerprints were acquired by transferring the inked impression onto the paper. This process is termed as *off-line* acquisition. Existing authentication systems are based on *live-scan* devices that capture the fingerprint image in real time. The live-scan devices may be based on one of the following sensing schemes

1. Optical Sensors: These are the oldest and most widely used technology. In most devices, a charged coupled device (CCD) converts the image of the fingerprint, with dark ridges and light valleys, into a digital signal. They are fairly inexpensive and can provide resolutions up to 500 dpi. Most sensors are based on FTIR (Frustrated Total Internal Reflection) technique to acquire the image. In this scheme, a source illuminates the fingerprint through one side of the prism. Due to internal reflection phenomenon, most of the light is reflected back to the other side where it is recorded by a CCD camera. However, in regions where the fingerprint surface comes in contact with the prism, the light is diffused in all directions and therefore does not reach the sensor resulting in dark regions. The quality of the image depends on whether the fingerprint is dry or wet. Another problem faced by optical sensors is the residual patterns left by the previous fingers. Furthermore it has been shown that fake fingers are able to fool most commercial sensors. Optical sensors are also among the bulkiest sensor due to the optics involved.

2. Capacitive Sensors: The silicon sensor acts as one plate of a capacitor, and the finger as another other. The capacitance between the sensing plate and the finger depends inversely as the distance between them. Since the ridges are closer, they correspond to increased capacitance and the valley corresponds to smaller capacitance. This variation is converted into an 8-bit gray scale digital image. Most of the electronic devices featuring fingerprint authentication uses this form of solid state sensors due to its compactness.

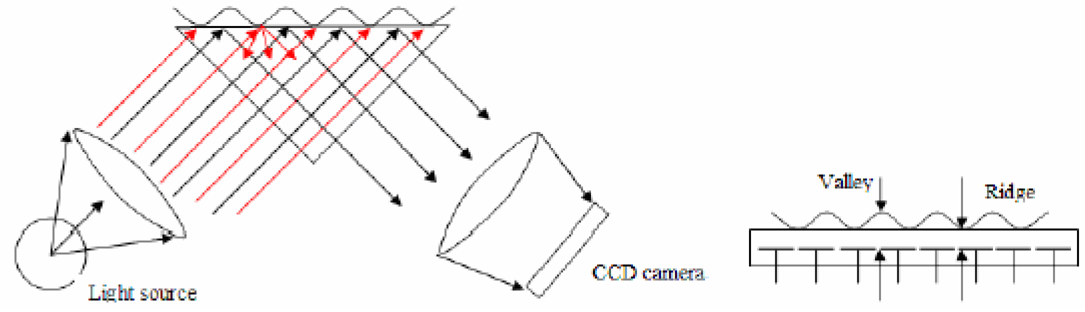


Figure 3.6 (a) General schematic for an FITR based optical (b) Schematic of a capacitive sensor

3. Ultra-sound Sensors: Ultrasound technology is perhaps the most accurate of the fingerprint sensing technologies. It uses ultrasound waves and measures the distance based on the impedance of the finger, the plate, and air. These sensors are capable of very high resolution. Sensors with 1000dpi or more are already available. However, these sensors tend to be very bulky and contain moving parts making them suitable only for law enforcement and access control applications.

4. Thermal Sensors: These sensors are made up of pyro-electric materials whose properties change with temperature. These are usually manufactured in the form of strips. As the fingerprint is swiped across the sensor, there is differential conduction of heat between the ridges and valleys (since skin conducts heat better than the air in the valleys) that is measured by the sensor. Full size thermal sensors are not practical since skin reaches thermal equilibrium very quickly once placed on the sensor leading to loss of signal. This would require us to constantly keep the sensor at a higher or lower temperature making it very energy inefficient. The sweeping action prevents the finger from reaching thermal equilibrium leading to good contrast images. However, since the sensor can acquire only small strips at a time, a sophisticated image registration and reconstruction scheme is required to construct the whole image from the strips.

3.8 NEW TRENDS IN BIOMETRICS

Biometric systems have to contend with noisy data, restricted degrees of freedom, and failure to enroll problems, spoof attacks, and unacceptable error rates. In some situations, it may be feasible to deploy a biometric system that takes advantage of more than one method of identification or authentication to overcome these problems. A biometric device can either be integrated with non-biometric forms of authentication or with other forms of biometric authentication devices. When a biometric device is integrated with other forms of biometric authentication devices, it can be described as a ***"multi-biometric system".*** Multi-biometric systems may be more reliable and provide higher verification rates due to the presence of multiple, independent pieces of evidence.

Multi-biometric systems address the problem of non-universality, since multiple traits ensure sufficient population coverage, and provide anti-spoofing measures by making it difficult for an intruder to steal multiple biometric traits of a genuine user. If there is a weakness in one method of biometrics, then combining it with a biometric method that is stronger with respect to that weakness will alleviate that problem. For instance, it may be feasible to deploy a biometric system in the flight deck that consists of both fingerprint scanning and voice recognition devices. In addition, a multi-biometric system may reduce the false reject rate and the failure to enroll problem.

One must determine the logic used by a multi-biometrics system. Each individual biometric method must be incorporated to logically work with the other biometric method that it is being combined with. The logic of the multi-biometric system may be implemented in an **AND** configuration or in an **OR** configuration. If these two devices must work together to provide continuous authentication using the AND configuration, then they both must output a matching score. This type of configuration will reduce the false acceptances achieved by using either device by itself, but it will increase the number of false rejections.

It is possible that these systems may be combined in an OR configuration. In the OR configuration, either device will be able to provide the continuous authentication needed in the flight deck. If the OR configuration is used then this type of configuration will reduce the number of false rejections, but increase the number of false acceptances. The number of false rejections and false acceptances are based on the matching threshold that the administrators set the device at initially. The matching threshold is used to decide between a genuine user and an impostor.

Usually vendors of biometric devices have suggestions for setting threshold values according to the security level you are trying to achieve. The security level may be labeled as low, medium, and high. Each security level has a threshold value associated with it as well.

A multi-biometric system may increase the certainty that the person is who he claims to be and increases the flexibility and circumstances under which someone can be verified. The accuracy and performance of an authentication system may be increased by employing a multi-biometric system if the most compatible methods are combined together to produce a stronger biometric system (i.e. where weaknesses in one method are complemented by the strengths in the other method). If the results of combining different biometric methods are not fully researched, then it is possible that a layered biometric system may be weaker than using only one method.

3.9 CONCLUSION

Biometrics systems are going to get more and more common in everyday applications due to the fact that new technologies are rapidly developing and the price and size of the hardware is constantly dropping. When it comes to mobile applications, one could expect to find systems for fingerprint verification and voice recognition in mobile phones in the very near future. Also signature verification is a strong candidate for future mobile applications.

The various biometric identifiers are described in this chapter and also compared using a table. However fingerprint recognition has a very good balance of all the desirable properties. Every human being possesses fingerprints with the exception of any hand-related disabilities. Fingerprints are very distinctive. Fingerprint details are permanent, even if they may temporarily change slightly due to cuts and bruises on the skin or weather conditions. Live-scan fingerprint sensors can easily capture high-quality images and they do not suffer from the problem of segmentation of the fingerprint from the background (e.g., unlike face recognition).

CHAPTER IV

FINGER PRINT IMAGE MODELLING

4.1 INTRODUCTION

A fingerprint is the reproduction of a fingertip epidermis, produced when a finger is pressed against a smooth surface. They have long been used for identification because of their immutability and individuality. Immutability refers to the permanent and unchanging character of the pattern on each finger. Individuality refers to the uniqueness of ridge details across individuals; the probability that two fingerprints are alike is about 1 in 1.9×10^{15}

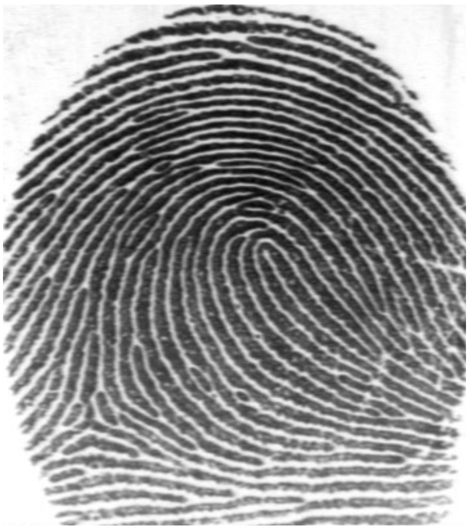


Figure 4.1 Finger print images from a live-scan FTIR-based optical scanner

The most evident structural characteristic of a fingerprint is a pattern of interleaved ridges and valleys; in a fingerprint image, ridges are dark whereas valleys are bright. Ridges vary in width from 100μm, for very thin ridges, to 300μm or thick ridges. Generally the period of a ridge/valley cycle is about 500μm. Injuries such as superficial burns, abrasions, or cuts do not affect the underlying ridge structure, and the original pattern is duplicated in any new skin that grows. Ridges and valleys often run in parallel; sometimes they bifurcate and sometimes they terminate.

A fingerprint image is often represented as a function I(x,y), where I(x,y) is the intensity of the pixel at coordinates x and y. For binary image it has only two values 0 (complete black) and 1(complete white) and for grey images the value at any pixel can vary from 0 to 1.

4.2 FEATURES OF FINERPRINT PATTERN

The fingerprint pattern, when analyzed at different scales, exhibits different types of features.

- **Global level:** When analyzed at the global level, the fingerprint pattern exhibits one or more regions where the ridge lines assume distinctive shapes (characterized by high curvature, frequent terminations, etc.). These regions (called singularities or singular regions) may be classified into three typologies: loop, delta and whorl. Singular regions belonging to loop, delta and whorl types characterized by ∩, Δ and O shapes, respectively. External fingerprint shape, orientation shape and frequency image also belong to the set of features that can be detected at the global level.

Singular regions are commonly used for fingerprint classification that is assigning a fingerprint to a class among a set of distinct classes. This is done with the aim of simplifying the search and retrieval of a fingerprint image from the large database of the images.

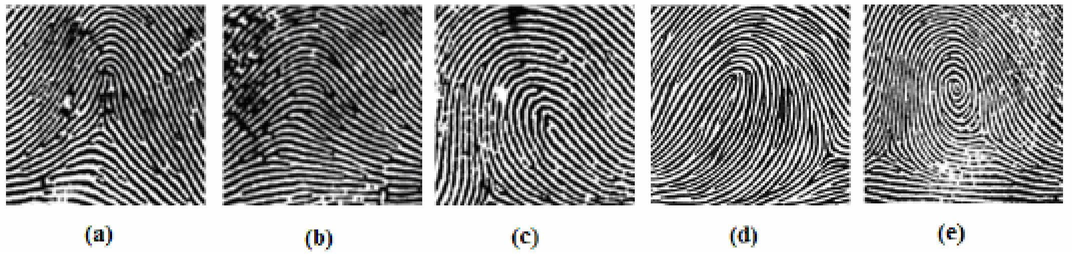


Figure 4.2 Fingerprint Classes: (a) Tended Arch (b) Arch (c) Right Loop (d) Left Loop (e) Whorl

- **Local level:** At the local level, other important features, called minutiae can be found in the fingerprint patterns. Minutia means small details; in the context of fingerprints, it refers to various ways that the ridges can be discontinuous. For example, a ridge can suddenly come to an end (termination) or can divide into two ridges (bifurcation).Although several types of minutiae can be considered, the most common types are Ridge island, Ridge ending, Ridge dot, Ridge enclosure and Ridge bifurcation. These types are shown in the figure below

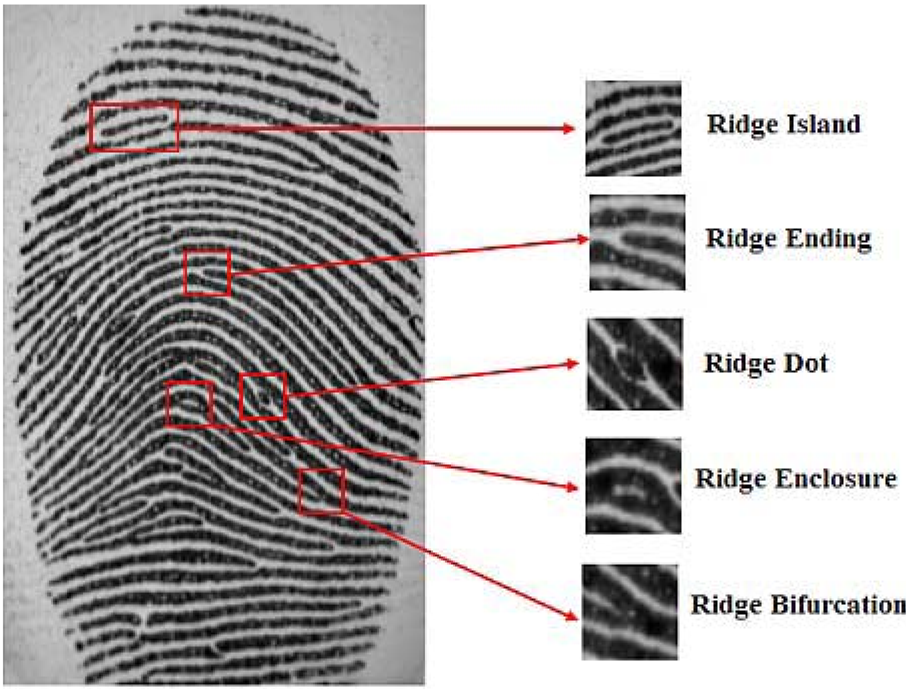


Figure 4.3 Common types of minutiae

Among the variety of minutia types two mostly significant and in heavy usage are Termination and Bifurcation. Termination is also called Ending, and Bifurcation is also called Branch. Each minutia is denoted by its class, the x- and y- coordinates and the angle between the tangent to the ridge line at the minutia position and the horizontal axis.

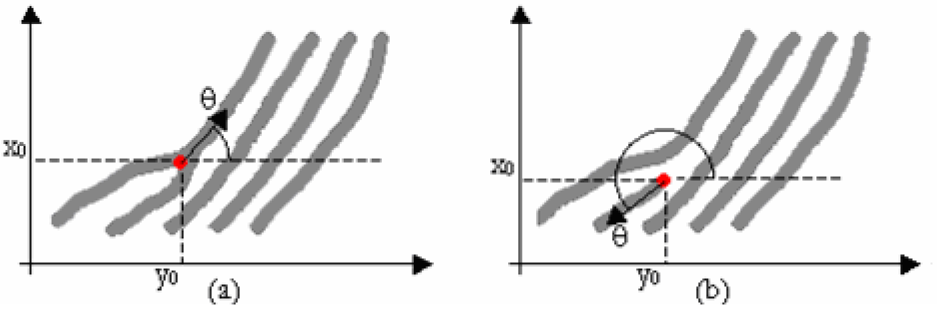


Figure 4.4 The basic properties of (a) ridge bifurcations (b) ridge endings

• **Very Fine Level:** At this level, intra-ridge details can be detected. In fact, each ridge is dotted with *sweat pores* along the entire length and anchored to the dermis (inner skin) by a double row of peglike protuberance or papillae. Although pore information (number, position, shape etc.) is highly distinctive, but very few automatic matching techniques use pores since their reliable detection requires very high resolution (i.e. 1000dpi) and good quality fingerprint images.

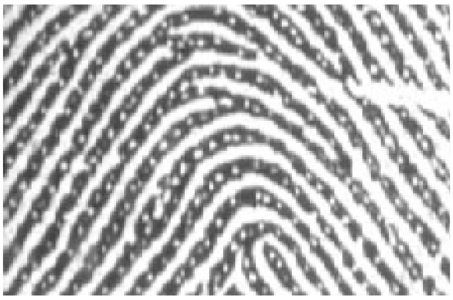


Figure 4.5 Image showing pores

4.3 CLASSIFICATION OF FINGERPRINT MATCHING

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

- **Correlation-based matching:** Two fingerprint images are superimposed and the correlation between the corresponding pixels is computed for different alignments (e.g. various displacements and rotations).
- **Minutiae-based matching:** This is the most popular and widely used technique. 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 result in the maximum number of minutiae pairings.
- **Ridge feature-based matching:** Minutiae extraction is difficult in very low-quality fingerprint images. The approaches belonging to this family compare fingerprints in term of features extracted from the ridge pattern (e.g. local orientation and frequency, ridge shape, texture information).

In principle, correlation- and minutiae-based matching could be conceived of as subfamilies of ridge feature-based matching, inasmuch as the pixel intensity and the minutiae positions are themselves features of the finger ridge pattern.

The advantage with correlation-based matching is that it is capable of dealing with fingerprints of bad image quality from which no minutiae can be extracted reliably. However it has a disadvantage of high computational power required by it.

4.4 INTEGRATED SOLUTION FOR FINGER PRINT IMAGE RECOGNITION

The various stages of a typical fingerprint recognition system are shown in the figure below.

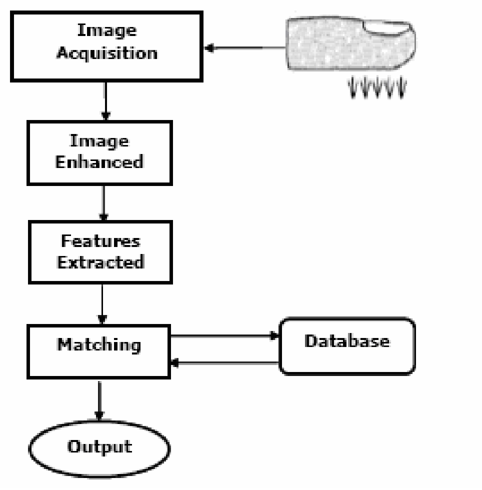


Figure 4.6 Simplified Fingerprint Recognition System

a) Image Acquisition

For fingerprint acquisition, optical or semi-conduct sensors are widely used. They have high efficiency and acceptable accuracy except for some cases that the user's finger is too dirty or dry.

b) Image Enhancement

In this project the image is enhanced in five stages. These are Histogram Equalization, Normalization, FFT-Enhance, Binarization and Noise filtering.

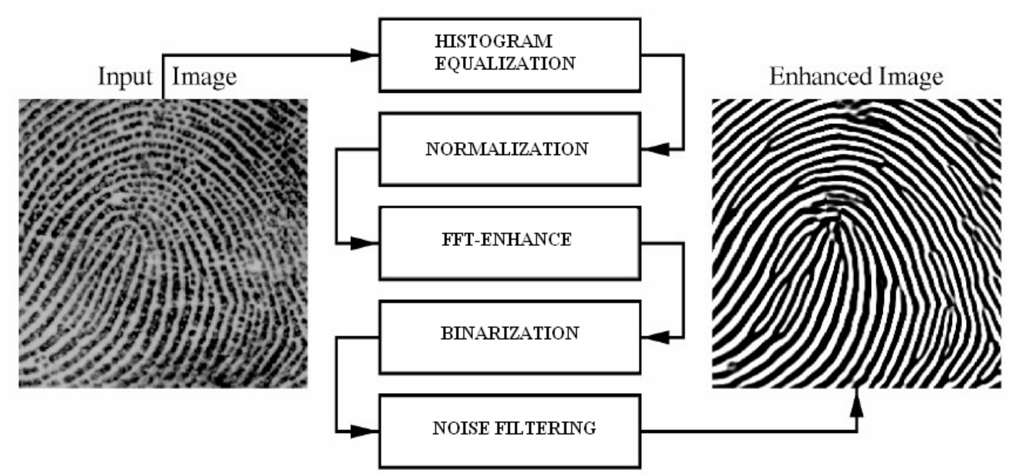


Figure 4.7 Stages of image enhancement

First Histogram equalization is used for evenly distribution of the pixel values so as to increase the perceptional information. Then normalization is done to make the image have a prespecified mean and variance. FFT-Enhancement is used to increase the discrimination between ridges and valleys and to separate parallel ridges. After the Binarization operation, ridges in the fingerprint are highlighted with black color while furrows are white. Noise filtering removes those single white pixels which are surrounded by black pixels.

c) Features (Minutiae) Extraction

Extraction of appropriate features is one of the important tasks for a recognition system. This is done as follows:

- **Segmentation** is performed to separate the actual fingerprint (Region of Interest) from the background. Direction for every block of image is find out and block without having significant direction is removed out.
- **Thinning** reduces the ridges thickness to one pixel wide. So that they can be further process easily.
- **Marking of minutiae**: Thinned binary image is scanned to detect the pixels corresponding to minutiae. Together with the minutia marking, all thinned ridges in the fingerprint image are labeled with a unique ID for further operation.
- **Removal of spurious minutiae:** Unfortunately earlier processing stages i.e. thinning introduces some spurious minutiae. These must be removed to improve the accuracy of the system.

d) Matching

One minutia from each image is taken as a reference minutia and if their ridges matches well then they are taken as reference pair. Now the rest of minutiae in the both images are aligned with respect to their reference minutiae and then are matched. Depending on the ratio of number of minutiae matched to the total number of minutiae the percentage of matching is calculated for every reference pair. The maximum value among them is taken and if it is above a threshold, the images are declared as successfully matched.

4.5 Applications of Fingerprint Recognition Systems

Fingerprint recognition is a rapidly evolving technology that has been widely used in forensics such as criminal recognition and prison security, and has a very strong potential to be widely adopted in a broad range of civilian applications.

Forensic	**Government**	**Commercial**
Corpse Identification,	National ID card,	Computer Network Logon,
Criminal Investigation,	Correctional Facility,	Electronic Data Security,
Terrorist Identification,	Driver’s License,	E-Commerce,
Parenthood Determination,	Social Security,	Internet Access,
Missing Children, etc.	Welfare Disbursement,	ATM, Credit Card,
	Border Control,	Physical Access Control,
	Passport Control, etc.	Cellular Phones,
		Distance Learning, etc.

4.6 CONCLUSION

Different applications desire different properties in the fingerprint matching algorithms (e.g. template size, matching speed, memory requirement, etc.). Embedded applications such as cell phones, PDA and smartcards will benefit from an algorithm with low computational complexity and eventually small template size. Similarly, mission-critical applications that may allow arbitrary resources but no matching errors will require extremely accurate response irrespective of computation and storage requirements.

The disadvantage with minutiae-based matching is that it is not capable of dealing with fingerprints of bad image quality from which no minutiae can be extracted reliably. However it has an advantage of low computational power required by it, which makes the method more applicable for real time applications and especially for identification purpose.

CHAPTER V

FINGER PRINT IMAGE ENHANCEMENT

5.1 INTRODUCTION

The performance of minutiae extraction algorithms and other fingerprint recognition techniques relies heavily on the quality of the input fingerprint images. In an ideal fingerprint image, ridges and valley alternate and flow in a locally constant direction. In such situations, the ridges can be easily detected and minutiae can be precisely located in the image. However, in practice, due to skin conditions (e.g. wet or dry), sensor noise, incorrect finger pressure and inherent low-quality fingers (e.g. elderly people, manual workers), a significant percentage of fingerprint images is of poor quality. The goal of an enhancement algorithm is to improve the clarity of the ridge structures and to improve the contrast between and ridges and valleys.

5.2 HISTOGRAM- EQUALIZATION

The histogram of an image records the frequency distribution of grey levels in that image. The histogram of an 8-bit image, for example can be thought of as a table with 256 entries, or ‘bins’, indexed from 0 to 255, In bin 0 we record the number of times a grey level of 0 occurs; and so on, up to 255.

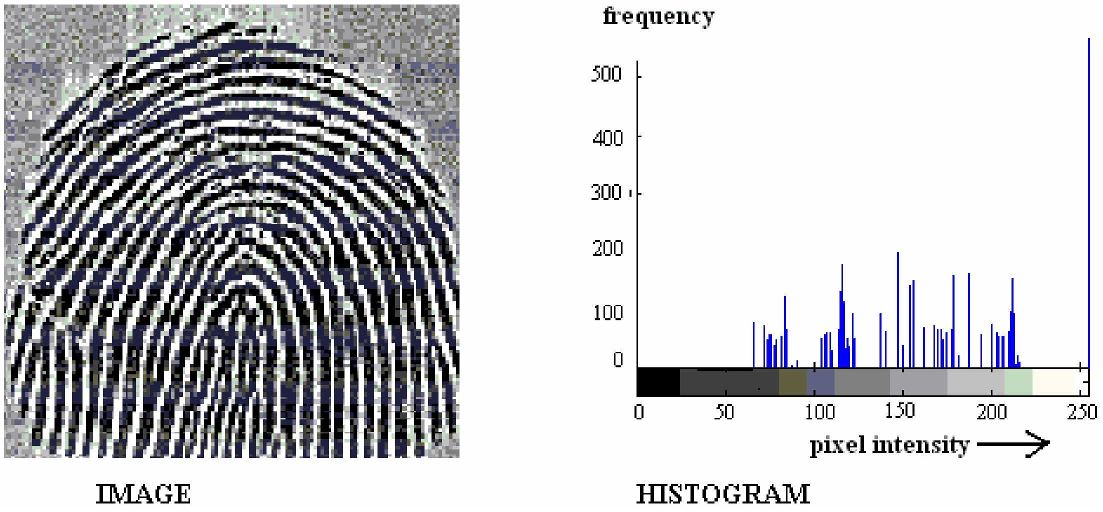
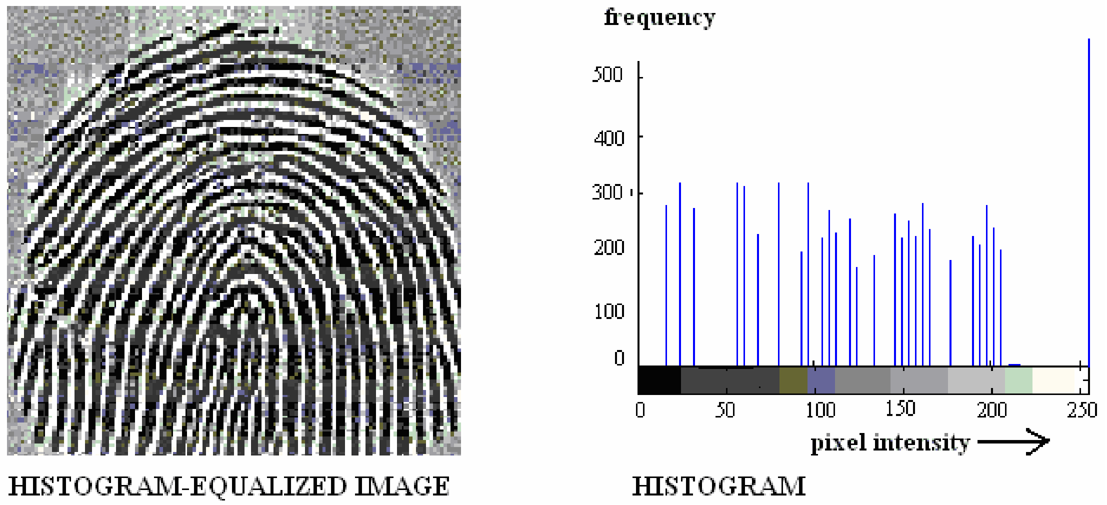


Figure 5.1

This image has low contrast, with most values in the middle of the intensity range.

Histogram equalization produces an output image having values evenly distributed throughout the range so as to enhance the contrast.



HISTOGRAM-EQUALIZED IMAGE

HISTOGRAM

Figure 5.2

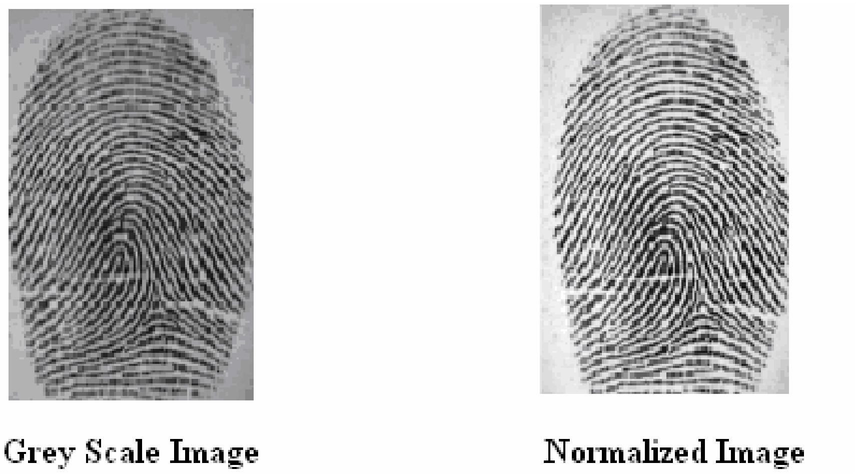
Histogram equalization is done by the calculating the cumulative histogram of the image. Then rescale the values in it so as to obtain a linearised or straighten cumulative frequency distribution.

5.3 NORMALIZATION

Normalization is done to make the image have a prespecified mean and variance. Normalization is a pixel-wise operation (the value of each pixel only depends on its previous value and some global parameters) and does not enhance the image or change the ridge and valley structure, i.e. any breaks in the ridges remain in the normalized image. Normalization increases the contrast between the ridges and the valleys. It is a pixel wise operation and moves the grey scale value of each pixel to a desired mean M_0. The following expression is used to calculate the normalized image.

$$G(i,j)=\begin{cases} M_0+\sqrt{VAR_0(I(i,j)-M)^2/VAR}, & if\ I(i,j)>M \\ M_0-\sqrt{VAR_0(I(i,j)-M)^2/VAR}, & otherwise \end{cases}$$

In the expression, G is the normalized image, M_0 is the desired mean and VAR_0 is the desired variance while M and VAR are the real mean and variance of pixels in the raw image. As can be seen from the image, the contrast between the ridges and the valleys has increased while the cuts present in the original image persist in the normalized image.



Grey Scale Image

Normalized Image

Figure 5.3

5.4 FFT-ENHANCEMENT

This stage enhances the image at the local level (contextual) with the objective to

1) To provide an averaging effect along the ridge direction with the aim of linking small gaps.

2) To increase the discrimination between ridges and valleys and to separate parallel ridges.

The most widely used technique found in the literature at this stage is the use of Gabor-filters. Unfortunately, this approach requires convolution of an image with a large number of Gabor filters which is very computationally expensive; so they do not find application in practical on-line system.

FFT-Enhancement technique is an alternative to the gabor filters which is also able to perform a sort of contextual filtering. Here each 32×32 pixels block in the image is enhanced separately. For each block we compute the Fourier transform according to:

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times \exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\}$$

for u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31.

The power spectrum of the block contains information about the underlying dominant ridge orientation and frequency and the multiplication with the Fourier transform has the effect of enhancing the block accordingly.

$$\mathbf{I_{enh}(x, y) = F^{-1}\left\{F(u, v)\times\left|F(u, v)\right|^{k}\right\}}$$

where the inverse Fourier transform of F(u,v) i.e. F^{-1}(F(u,v)) is calculated as

$$f(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v)\times \exp\left\{j2\pi\times\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\}$$

for x = 0, 1, 2, ..., 31 and y = 0, 1, 2, ..., 31.

The k is an experimentally determined constant, which is chosen as k=0.7.

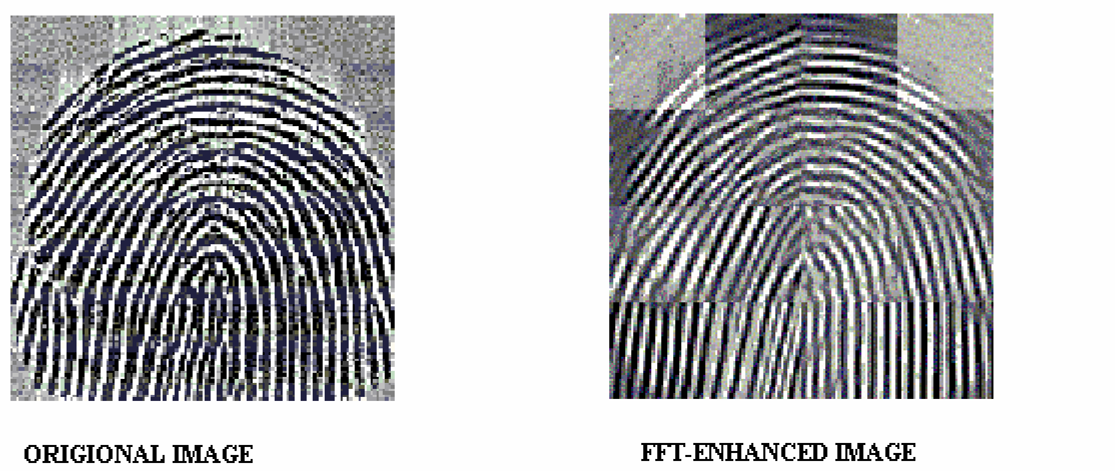


Figure 5.4

Unfortunately, to avoid discontinuities at the edges between adjacent blocks, a large amount of overlap between the neighboring blocks (e.g. 24pixels) is necessary and this significantly increases the enhanced time.

5.5 BINARIZATION

Most minutiae extraction algorithms operate on binary images where there are only two levels of interest: the black pixels that represent ridges, and the white pixels that represent valleys. Binarization is the process that converts a grey level image into a binary image by selecting a threshold. This improves the contrast between the ridges and valleys in a fingerprint image, and consequently facilitates the extraction of minutiae.

Histogram is used to find the threshold. The two major peaks will be found, assumed to be the most commonly used dark pixel and the most common light pixel. The middle rage pixel will then be used to discriminate between black and white pixels for binarization. The figure given below shows the main dark pixel, main white pixel and the middle value of the grey level.

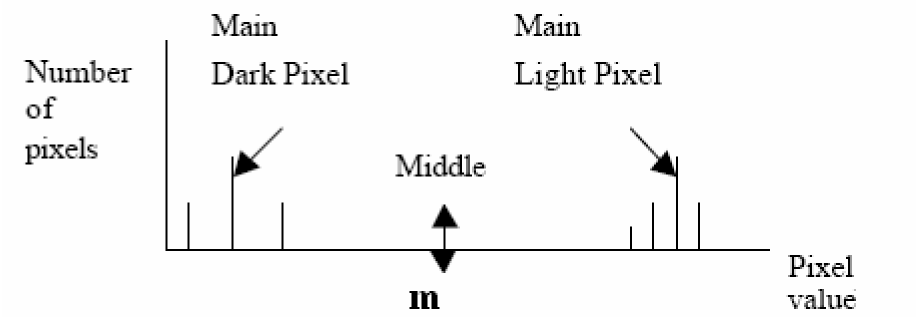
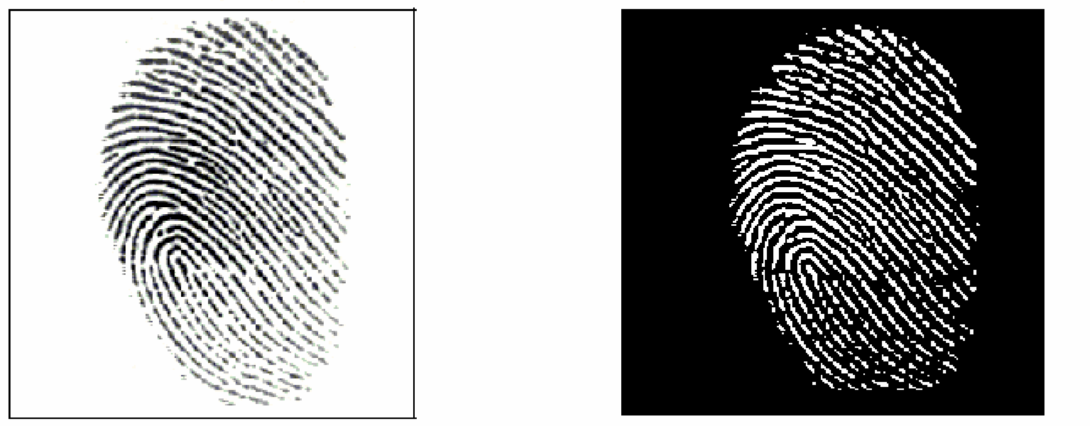


Figure 5.5

Now the binarized image (B(x,y)) is obtained by thresholding each pixel of input image (I(x,y)) as :

$$B(x,y)=\begin{cases} 1 & \text{if } I(x,y)>=m \\ 0 & \text{if } I(x,y)<m \end{cases}$$



ORIGIONAL IMAGE

BINARIZED IMAGE

Figure 5.6

5.6 NOISE FILTERING

Noise filtering removes those isolated single white pixels which are surrounded by black pixels. These pixels are of no use and hence taken as noise. This type of noise is also called ‘salt and pepper’ noise.

This is done by sequentially scanning the binarized image for white pixels and then searching for white pixels around that pixel in a 3×3 window, i.e. for every white pixel B(x,y).

0	0	0
0	**B(x,y)**	0
0	0	0

If all the pixels around are zero then also assign B(x,y) to zero.

5.7 CONCLUSION

This chapter explained various methods needed and used in the project for fingerprint image enhancement. However development of fingerprint specific image processing is still necessary in order to solve some of the outstanding problems. For example, explicitly measuring (and restoring or masking) noise such as creases, cuts, dryness and the like will be helpful in reducing feature extraction errors.

CHAPTER VI

FEATURE (MINUTIAE) EXTRACTION

6.1 INTRODUCTION

Automatic and reliable extraction of minutiae from fingerprint images is a critical step in fingerprint matching. It plays an important role in the performance of automatic identification and verification algorithms. First the Segmentation is performed to separate the actual fingerprint (Region of Interest) from the background. It is a two step process of calculating the direction of each block and classifies each block to foreground or background then obtain the ROI using the morphological close operation. Thinning operation reduces the ridges thickness to one pixel wide. So that they can be further process easily. The ridge width i.e. the distance between the adjacent ridges is calculated. The pixels corresponding to ridge ending and bifurcation are marked in the region of interest. Their position is stored in terms of their type, x-y location and the orientation of the associated ridge. Then spurious minutiae are removed according to some rules. Finally the true minutia set is obtained which will be used to match two fingerprint images**.**

6.2 SEGMENTATION

Segmentation is performed to separate the actual fingerprint area (foreground) from the image background. Separating the actual fingerprint area is useful to avoid extraction of features in noisy areas of the fingerprint and background. The actual fingerprint area is also called Region of Interest (ROI). The technique implemented in this project is based on the direction estimation of each block and block without having significant direction is taken as background.

To obtain the ROI, a two step process is as follows:

1. **Block Direction Estimation:** Direction of each block is dominant ridge orientation in that block. The ridge orientation at [x,y] is angle Θ_{xy} that fingerprint ridges, crossing through. An arbitrary small neighborhood centered at [x,y], form with the horizontal axis.

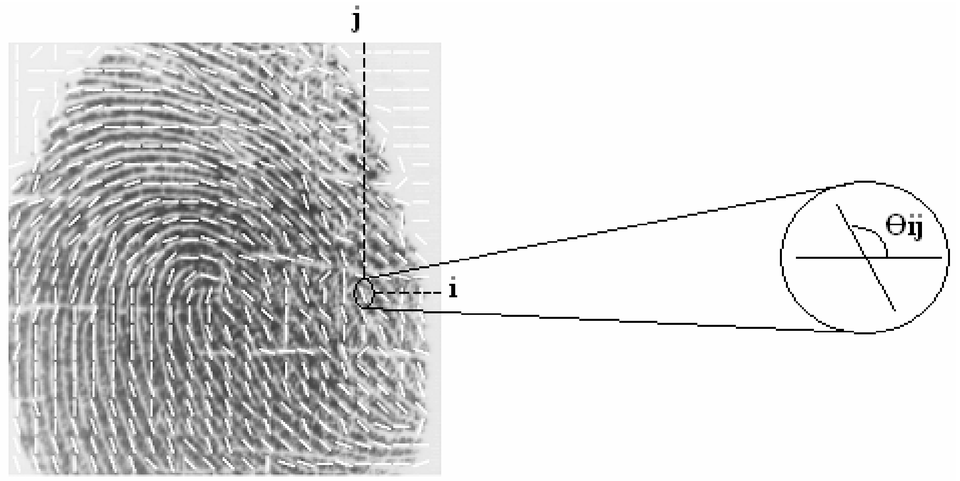


Figure 6.1

The least mean square orientation estimation algorithm has the following steps:

1. Divide the image I, into non overlapping blocks of size 16×16pixels.
2. Compute the gradients $\delta_x(i,j)$ and $\delta_y(i,j)$ at each pixel (i,j) using the 3×3 Sobel convolution mask. Where gradients δ_x and δ_y are the derivatives of I in x and y direction.
3. Estimate the local orientation of each block centered at pixel (i,j) using the following equation:

$$\upsilon x(i,j) = \sum_{u=i-w/2}^{i+w/2} \sum_{v=j-w/2}^{j+w/2} 2\, \delta_x(u,v)\delta_y(u,v)$$

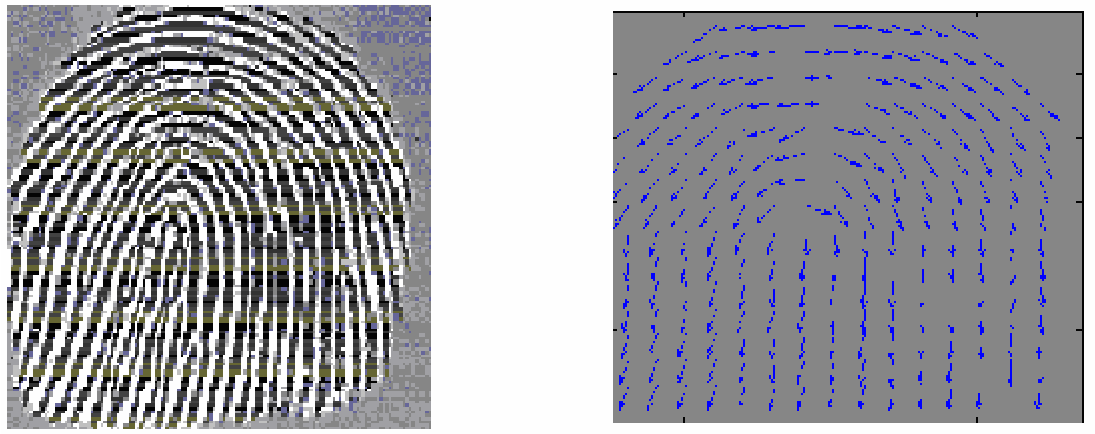
$$\upsilon y(i,j) = \sum_{i-w/2}^{i+w/2} \sum_{j-w/2}^{j+w/2} (\delta^2{}_x(u,v) - \delta^2{}_y(u,v))$$

$$\Theta(i,j) = 90^o + \tfrac{1}{2} \tan^{-1}(\upsilon_x(i,j)/\upsilon_y(i,j))$$

Now the blocks without having significant direction are discarded based on the following formula:

$$L = \{2\sum\sum (\upsilon_x * \upsilon_y) + \sum \sum (\upsilon_x^2 - \upsilon_y^2)\} / 16\times 16 \sum \sum (\upsilon_x^2 + \upsilon_y^2)$$

For each block, if its certainty level is below a threshold (0.1), then the block is regarded as a background. However there will be some cases where a background region may be surrounded by the foreground. Hence morphological closing operation is used in next step to get ROI.

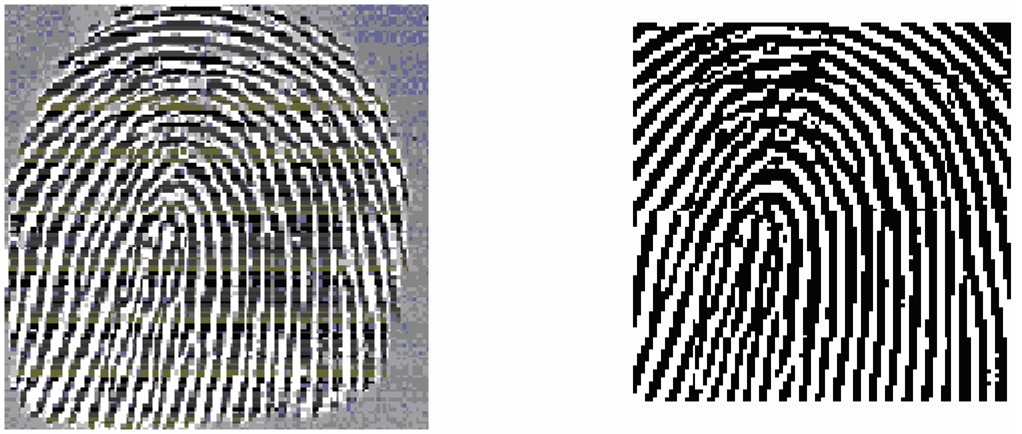


Origional Image Direction Image

Figure 6.2

2. ROI extraction by Morphological close function

Closing does two operations; dilation followed by erosion. The dilation fills any hole enclosed by any region and the erosion restores the region to its original size. This function is directly available in MATLAB.

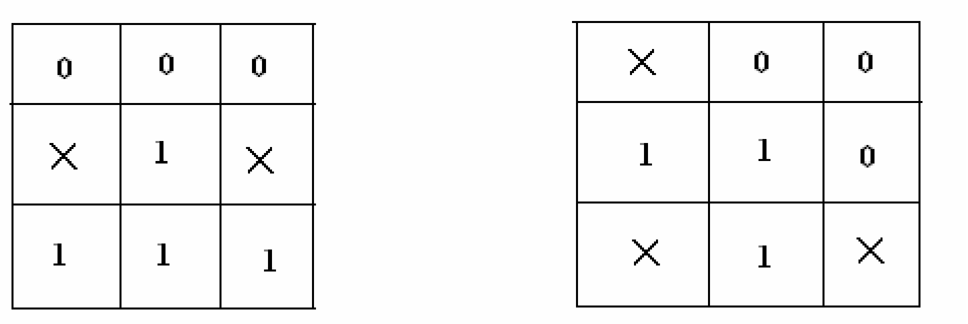


Origional Image ROI

Figure 6.3

6.3 THINNING OPERATION

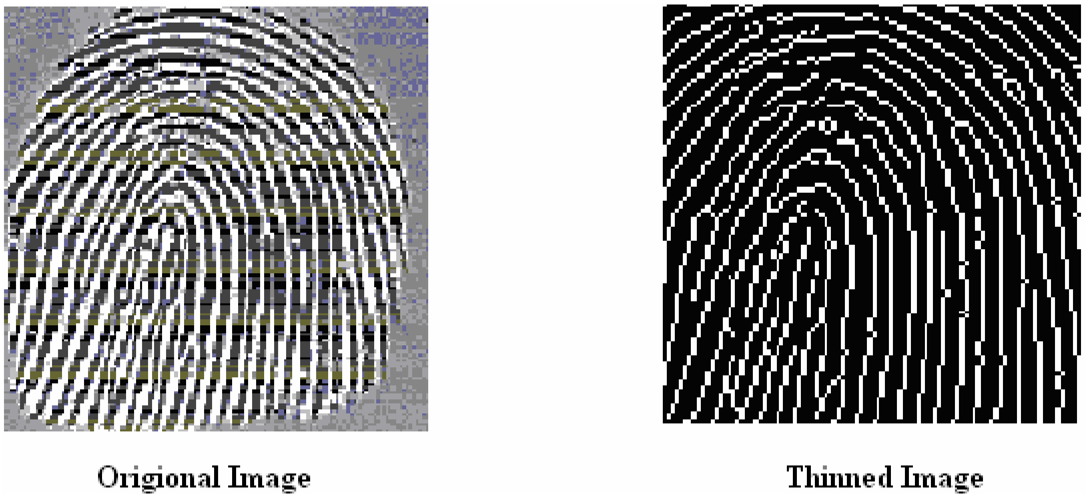
The final image enhancement step typically performed prior to minutiae extraction is thinning. Thinning is a morphological operation that successively erodes away the foreground pixels (ridges) until they are one pixel wide. This is done in order to facilitate the further operation on the image. The first two structuring elements are**:**



0	0	0
×	1	×
1	1	1

×	0	0
1	1	0
×	1	×

Remaining six are 90^0 rotations of these two structuring elements. The thinning operation is performed by translating the origin of structuring element to each possible position in the image and at each such position comparing it with the underlying image pixels. If the foreground and background in the structuring element exactly matches foreground and background pixels in the image, then the image pixel underneath the origin of structuring element is set to background (zero). Otherwise it is left unchanged. The process is repeated in cyclic fashion until none of the thinning produces any further change (i.e. until convergence). This algorithm is accessible in MATLAB via the `thin' operation under the bwmorph function.



Origional Image

Thinned Image

Figure 6.4

6.4 MINUTIAE EXTRACTION

The Crossing Number (CN) method is used to perform minutiae extraction. First the ridges of the thinned images are marked by using bwlabel function available in matlab. After marking each ridge got a separate ID. Then extraction of ridge ending and bifurcation is done by examining the local neighborhood of each ridge pixel using a 3×3 window. Crossing Number of a ridge pixel ‘p’ is defined as half the sum of the differences between pairs of adjacent pixels defining the 8-neighborhood of ‘*p*’.

Mathematically,

$$CN = 0.5\sum_{i=1}^{8}|P_i - P_{i+1}|, \qquad P_9 = P_1$$

where P_1 to P_9 are the pixels belonging to the 8-neighborhood of ‘P’. These eight neighboring pixels are scanned in an anti-clockwise direction as follows:

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

CN=1 represents ridge ending and CN=3 represents bifurcation. Now each minutiae is represented by

- x and y coordinates,
- Orientation of the associated ridge segment, and
- Type of minutiae (ridge ending or bifurcation).

For ridge ending, the direction of ridge flowing from the end point is defined as the minutiae direction. For bifurcation, the direction is defined as the average value of the direction of the two ridges that flow from this bifurcation toward the same side.

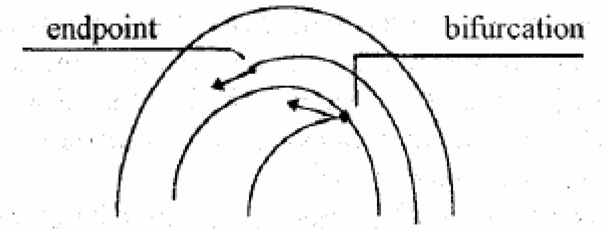


Figure 6.5 Direction of endpoint and bifurcation

To obtain the orientation of the associated ridge the following procedure is adopted: Let the termination is at (x,y) then sum up all the x-coordinates of the associated ridge, take the length of ridge up to ridge width and divide it by ridge width to get x′. Similarly obtain y′; now the orientation is given by

$$\Theta_R = \tan^{-1}\{ (y'-y)/(x'-x) \}$$

6.5 REMOVE SPURIOUS MINUTIAE

False minutiae may be introduced into the image due to factors such as noisy images, and also the earlier processing stages like thinning introduces some false minutiae. These false minutiae will lead to the inaccurate results in the matching stage. Hence, after the minutiae are extracted, it is necessary to employ a post processing stage in order to validate the minutiae. The different types of false minutiae include spike, spur, bridge, ladder, hole, break etc. These are shown in the figure below

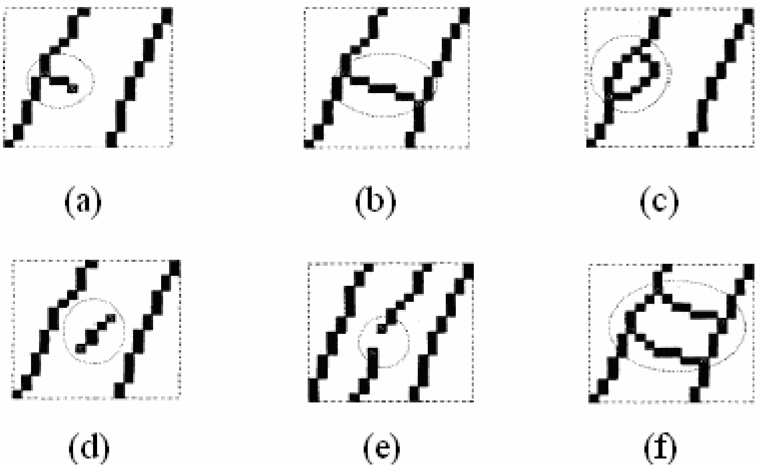


Figure 6.6 (a) Spike (b) Bridge (c) Hole (d) Spur (e) Break (f) Ladder

The total number of initial minutia is divided into two sets. One contains the set of ridge endings (S_e) and other the bifurcations (S_b). Then following procedure is used to detect and remove spurious minutiae

1. Two end points, if closer than ridge width (D) and having nearly similar angle of orientation are removed, i.e. if P_1 and P_2 are two endpoints and $\alpha(P_1)$ and $\alpha(P_2)$ are their directions. Now if P_1 and P_2 are satisfying the conditions:
   $\mathrm{Dist}(P1,P2) < D$
   $\mathrm{Min}(|\alpha(P_1)-\alpha(P_2)|, 2\pi-(|\alpha(P_1)-\alpha(P_2)|)) < \pi/2$
   then delete P_1 and P_2 from Se.

2. If the distance between an endpoint and a bifurcation is less than ridge width, and both sharing the same ridge then delete these bifurcation and endpoint from their respective sets.

3. If there exists two bifurcations closure than ridge width, sharing common ridge then remove both.

At last, the remained minutiae in set Se and Sb are combined to form a true minutiae set which will be used to match two fingerprint images.

6.6 CONCLUSION

This chapter includes the analysis and implementation of the methods used in the minutiae extraction stage. Visual inspection of the image indicates that the majority of the marked minutiae points from the thinned image correspond to the valid minutiae points in the original image. However, there are a few cases where the extracted minutiae do not correspond to true minutiae points in the original image. So the removing of spurious minutiae is a critical step in the fingerprint matching.

CHAPTER VII

MINUTIAE MATCHING

7.1 INTRODUCTION

A fingerprint matching algorithm compares two given fingerprints and returns degree of similarity, on the basis of which the decision of matched/non-matched is taken. There are a few issues to consider when trying to match two sets of minutiae. Since the skin is elastic, two corresponding minutia point might not be in exactly the same place in two sets. The fingerprints might have been rotated in different angles in two images. And hence the alignment stage before the matching stage is mandatory.

- Alignment Stage: If the two minutia from the two given fingerprint images are matched then take them as the reference minutia and other minutiae in the corresponding images are aligned with respect to them.
- Matching stage: Comparing the locations and orientations of each aligned minutiae in the input fingerprint with those of each minutia in other, and hence a similarity measure is calculated. If it is bigger than a predefined reasonable threshold, then it can be said that the two images originate from the same fingerprint.

7.2 ALIGNMENT

Let $\mathbf{T = \{ m_1, m_2, m_3,\ldots,m_M\}^T \quad m_i = \{x_i, y_i, \Theta_i\},\ \ i = 1,2,\ldots,M}$

denote the set of M minutiae in the template image and

$\mathbf{I = \{ m_1, m_2, m_3,\ldots,m_N\}^T \quad m_j = \{x_j, y_j, \Theta_j\},\ \ j=1,2,\ldots,N}$

denote the set of N minutiae in the input image.

A minutiae m_j' in I and a minutia m_i' in T are considered to be matched if their spatial distance (SD) and orientation difference (OD) are within specified thresholds r_o and Θ^o.Let R and r represent the associated ridge of minutia mj′ and m_i'. Match R against r to get the difference of these two ridges according to the following formula:

$$SD(m_j', m_i') = \frac{1}{L}\sum_{i=0}^{L}\left|R(di) - r(di)\right|$$

OD(m$_j$′, m$_i$′) $= \frac{1}{L}\sum_{i=0}^{L}\left|R(\alpha i - r(\alpha i)\right|$

Where L(5) is the number of points recorded. R(di) is the distance from point i on ridge R to minutia m$_j$′. R(α_i) is the angle between the line connecting point i on ridge to minutiae m$_j$′ and the orientation of minutia m$_j$′. r(di) and r(α_i) have similar means.

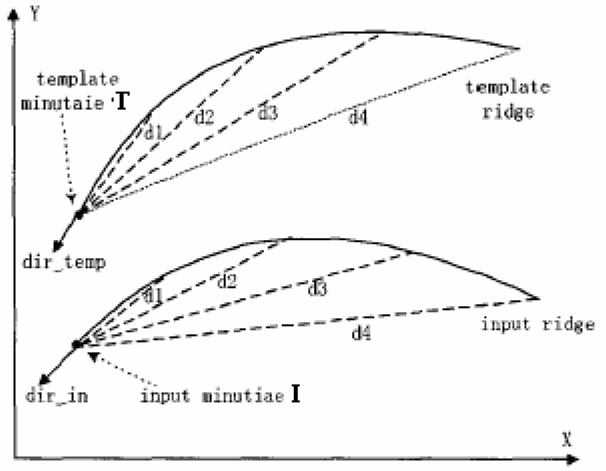


Figure 7.1 Alignment of the input ridge and the template ridge

If SD and OD are larger than threshold then m$_j$′ and m$_i$′ are taken as reference minutiae in their image. Now rests of the minutiae in both images are aligned with respect to their reference minutia.

Alignment is done by setting reference minutia as origin and aligns its orientation to x-axis. Now the geometrical transformation of rest of the minutiae is done by

$$\begin{bmatrix} x^{//} \\ y^{//} \\ \theta^{//} \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x'-x \\ y'-y \\ \theta'-\theta \end{bmatrix}$$

where (x, y, ɵ) is the parameter of the reference minutia and (x′, y′, ɵ′) is the parameter of minutia to be aligned.

7.3 MATCHING

A bounding box defined by ridge-width and small angle (10^o) is placed around template minutia. It is necessary to compensate for the unavoidable errors made by feature extraction algorithms and to account for the small plastic distortions that cause the minutiae position to change. If the input and template minutiae lie inside the same bounding box, with an angle variation less than 10° then they can be considered as a matched pair. However increasing the size of bounding box increases the chance of incorrectly matching two fingerprints from different fingers.

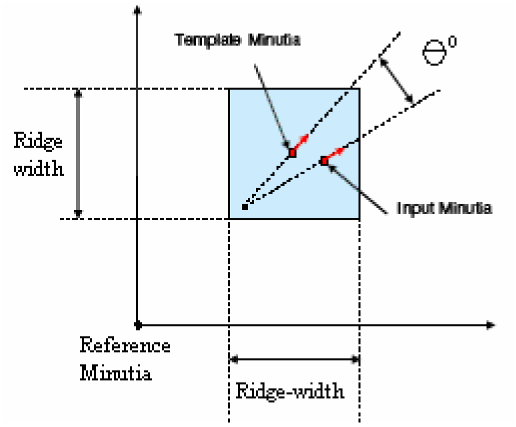


Figure 7.2 Example of minutia matching using a bounding box

Now the matching score match_score[i][j] is calculated, which is equal to the ratio of total numbers of matched minutia pair to the total number of minutiae in the template. If the maximum value of the matching scores calculated for all the reference pairs is higher than a threshold (98%) then it can be said that the two images originate from the same fingerprint.

The steps of complete minutiae matching algorithm are given below:

1) For i $(1 \le i \le M)$ and j $(1 \le j \le N)$, check whether m_j' and m_i' satisfies the criteria to be taken them as reference pair. If all possible minutia pairs have been considered, go to step 4.

2) Take m_j' and m_i' as reference minutia. Now align rests of the minutiae in both images with respect to their reference minutiae.

3) Match the aligned minutiae from both images to calculate the matching score match_score[i][j].

4) Find the maximum value of match_score[i][j] and use it as the matching score of the input and template minutiae set. If the matching score is higher than a threshold, then the input image is considered to come from the same finger as the template image.

The above matching algorithm is common in both Identification and Verification.

7.4 IDENTIFICATION AND VERIFICATION

The fingerprint feature extraction and matching algorithms are usually quite similar for both fingerprint verification and identification problems. This is because the fingerprint identification problem (i.e. searching for an input fingerprint in a database of N fingerprints) can be implemented as a sequential execution of N one-to-one matches (verifications) between pairs of fingerprints.

Identification is implemented through the use of cell array in matlab. This array stores together the minutiae sets and the name of their corresponding image. Minutiae set of the input image is matched sequentially to the stored minutiae set; on matching the name of the corresponding image will be displayed.

7.5 CONCLUSION

How to choose a reliable reference point pair is a very difficult problem in fingerprint image matching. If all possible point pairs are considered and then choose the pair that gives the largest matching score, the computational burden will be too heavy. The introduction of ridge matching, greatly reduces the number of point pairs that can be used as a reference pairs and hence solved the problem of reference point pair choosing with low computational cost. And hence significantly decreases the time required in identification.

Different applications desire different properties in the fingerprint matching algorithms (e.g. template size, matching speed, memory requirement, etc.). Embedded applications such as cell phones, PDA and smartcards will benefit from an algorithm with low computational complexity and eventually small template size. Similarly, mission-critical applications that may allow arbitrary resources but no matching errors will require extremely accurate response irrespective of computation and storage requirements.

Threshold for matching depends on the application. Defence applications require high value of threshold while general applications can have a low threshold.

CHAPTER VIII

EXPERIMENTATION RESULTS & DISCUSSION

INTRODUCTION

All experiments discussed in this chapter are conducted on a set of 40 fingerprints images of varying size. These images are available on the Internet. Although the images of same finger having different alignment are available. They can also be created by “imrotate” function available in the MATLAB. All the programming is done in MATLAB version 7. In the programming phase it was found that some functions used in the whole process of recognition are directly available in the matlab. Like the histogram equalization function and as the available function is showing better results than the program written for the same. Therefore the function is taken from the matlab.

To show the experimentation results, a Graphical User Interface (GUI) is made in the matlab. A figure is made, inside that a frame having push buttons for different functions in the process is created. An axis for showing the images is placed adjacent to the frame. Every pushbutton has some properties that define the size and colour of the pushbutton and a callback function is associated with every pushbutton that calls the corresponding function, when the button is pushed.

For verification purpose two images are needed, the result of percentage of matching of these two images is shown by a textbox that appears on the GUI in bottom part. When the identification pushbutton is pushed it will take an input image, calculate the image real minutiae set and then will try to match it with the sets available in the database. The database is created with the help of cell array. The name of the image and its minutiae set is added in the cell array on clicking the addtodata pushbutton.

For debugging the program the value of some needed variables and other important information is made to shown continuously in the command window. However if the GUI is running on the full screen these will not appear to the user. The following pages show the results of complete fingerprint image recognition process.

• Click on the LOAD INPUT IMAGE

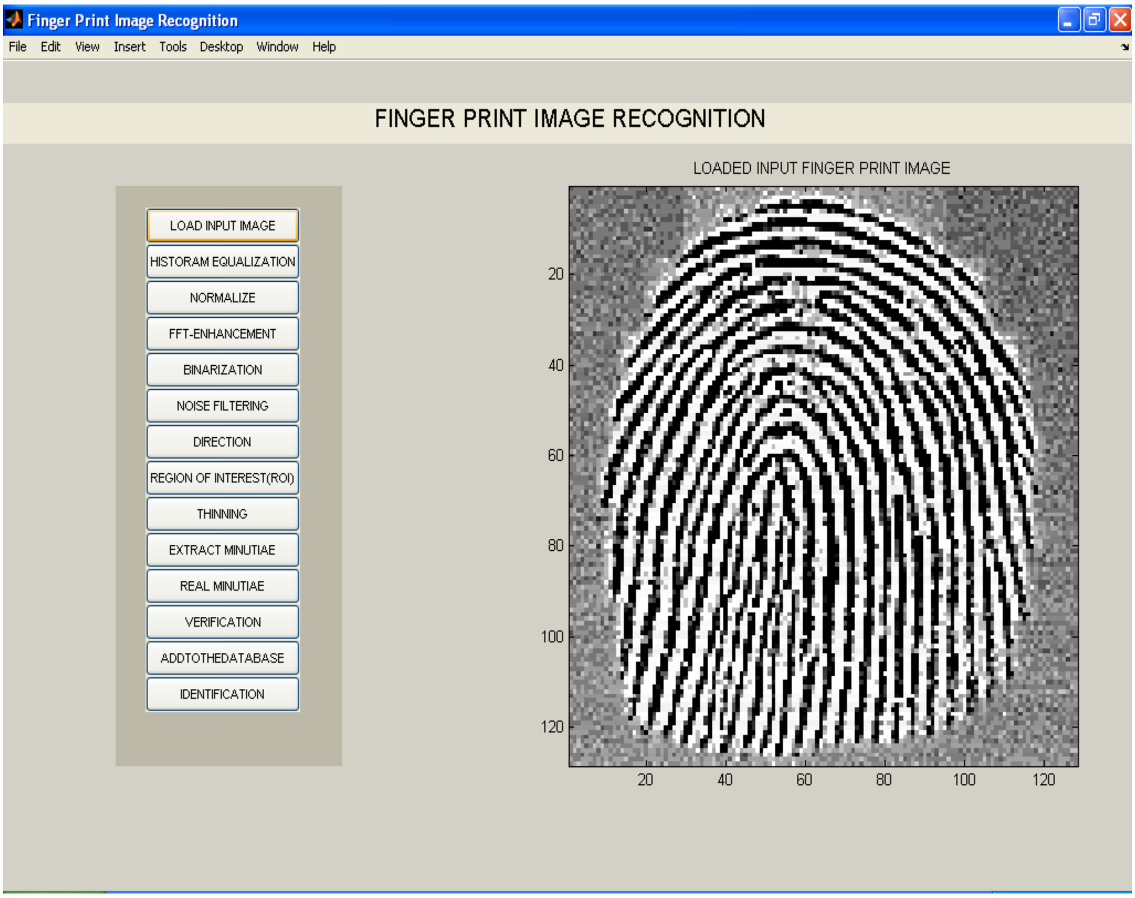


Figure 8.1 Screen shot after click LOADINPUT IMAGE

- ➢ A dialog box for selection of fingerprint image appears. On selection, the input fingerprint image is placed on the axis.
- ➢ The image appears to be noisy. And also the contrast between ridges and valley need to improve. So the enhancement stages are necessary to make it applicable for minutiae extraction.

• Click on the HISTOGRAM-EQUALIZATION

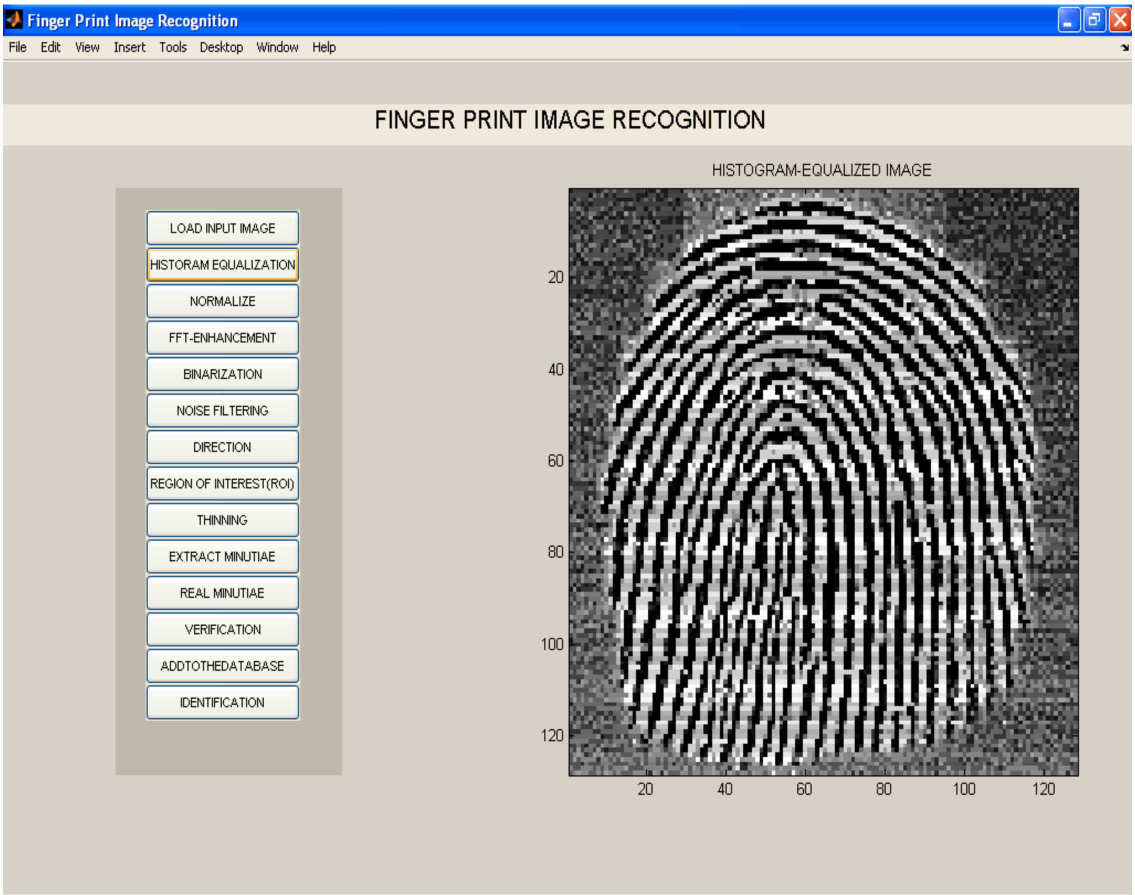


Figure 8.2 Screen shot after click HISTOGRAM EQUALIZATION

- Histogram equalized image appears on the axis.
- In this image the pixel values are evenly distributed throughout the range so as to enhance the contrast.

• Click on the NORMALIZATION

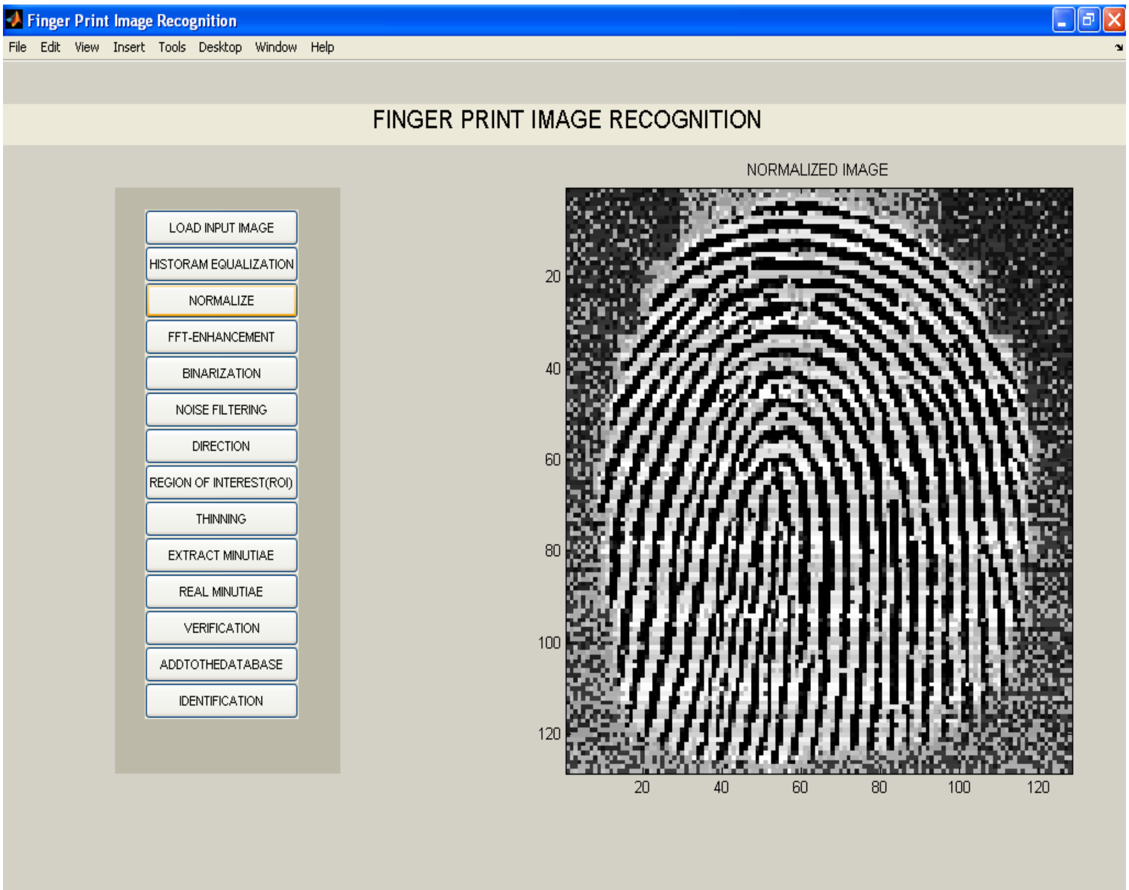


Figure 8.3 Screen shot after click NORMALIZE

- ➢ Normalized image appears on the axis.
- ➢ It can be observed that normalization increases the contrast between the ridges and the valleys.

- Click on the FFT-ENHANCEMENT

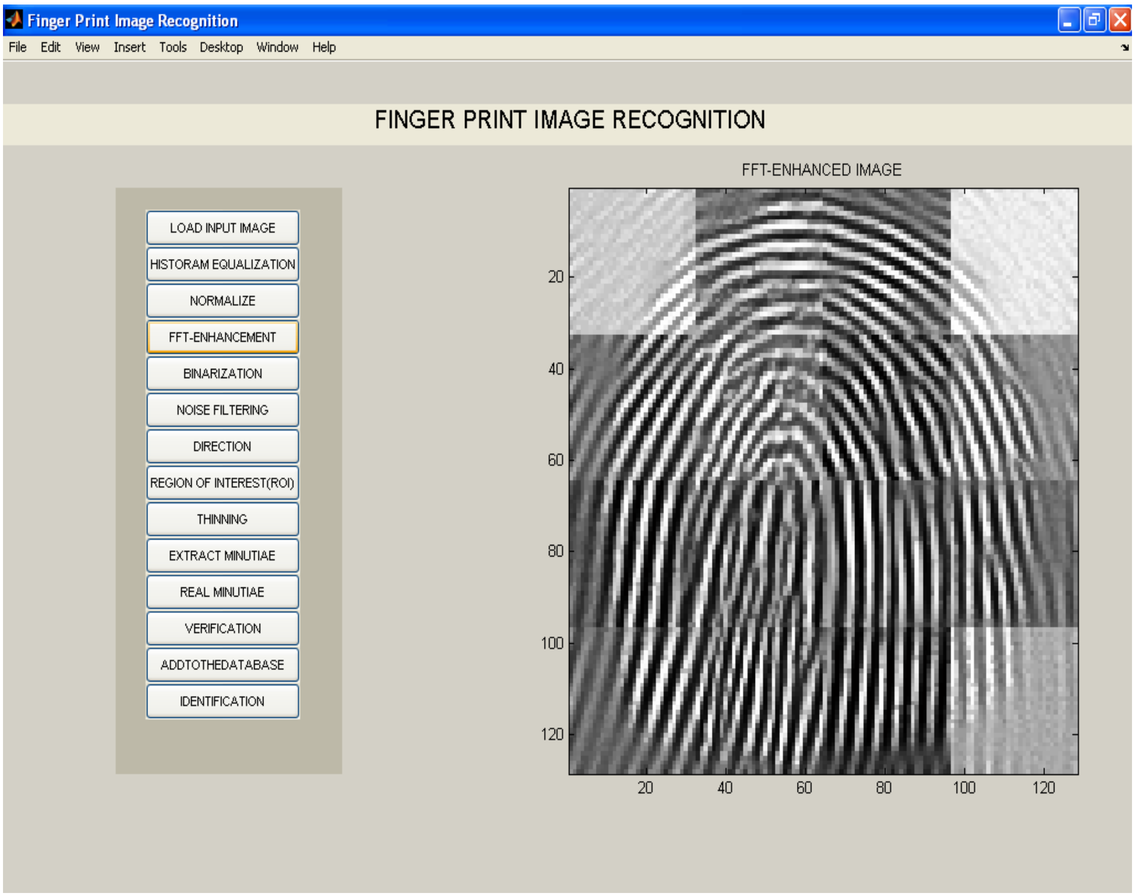


Figure 8.4 Screen shot after click FFT-ENHANCEMENT

- FFT-Enhanced image appears on the axis. The enhanced image after FFT has the improvements to connect some falsely broken points on ridges and to remove some spurious connections between ridges.

- The side effect of each block is obvious but it has no harm to the further operations because it is found that the image after consecutive binarization operation is pretty good as long as the side effect is not too severe.

• Click on the BINARIZATION

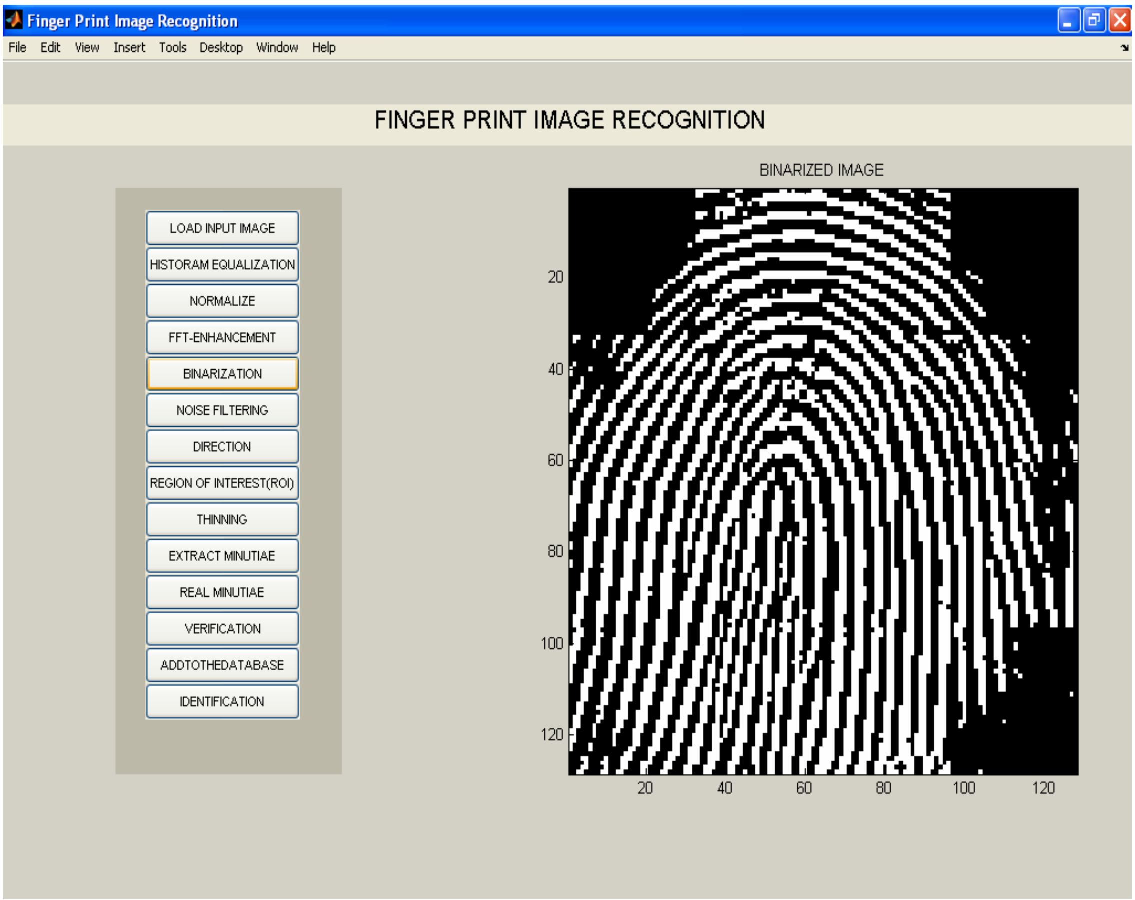


Figure 8.5 Screen shot after click BINARIZATION

- ➢ Binarized image appears on the axis. In this image the pixels can have value either zero or one.

- ➢ The complete white block appears in the three corners of the image. However it will have no effect as the further processing is done only on the region of interest.

• Click on the NOISE FILTERING

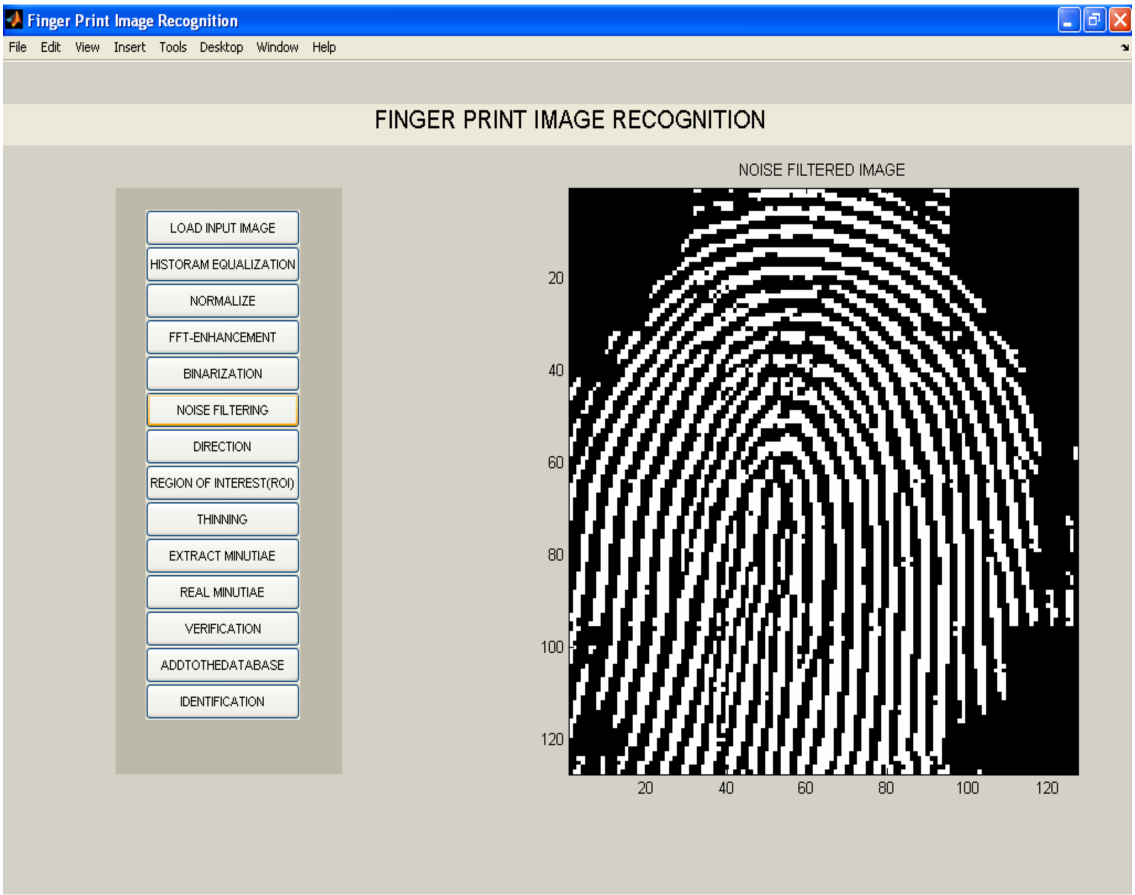


Figure 8.6 Screen shot after click NOISE FILTERING

- ➢ Noise Filtered image appears on the axis.
- ➢ Isolated white pixels which act as noise are no longer present in the image.

- Click on the DIRECTION

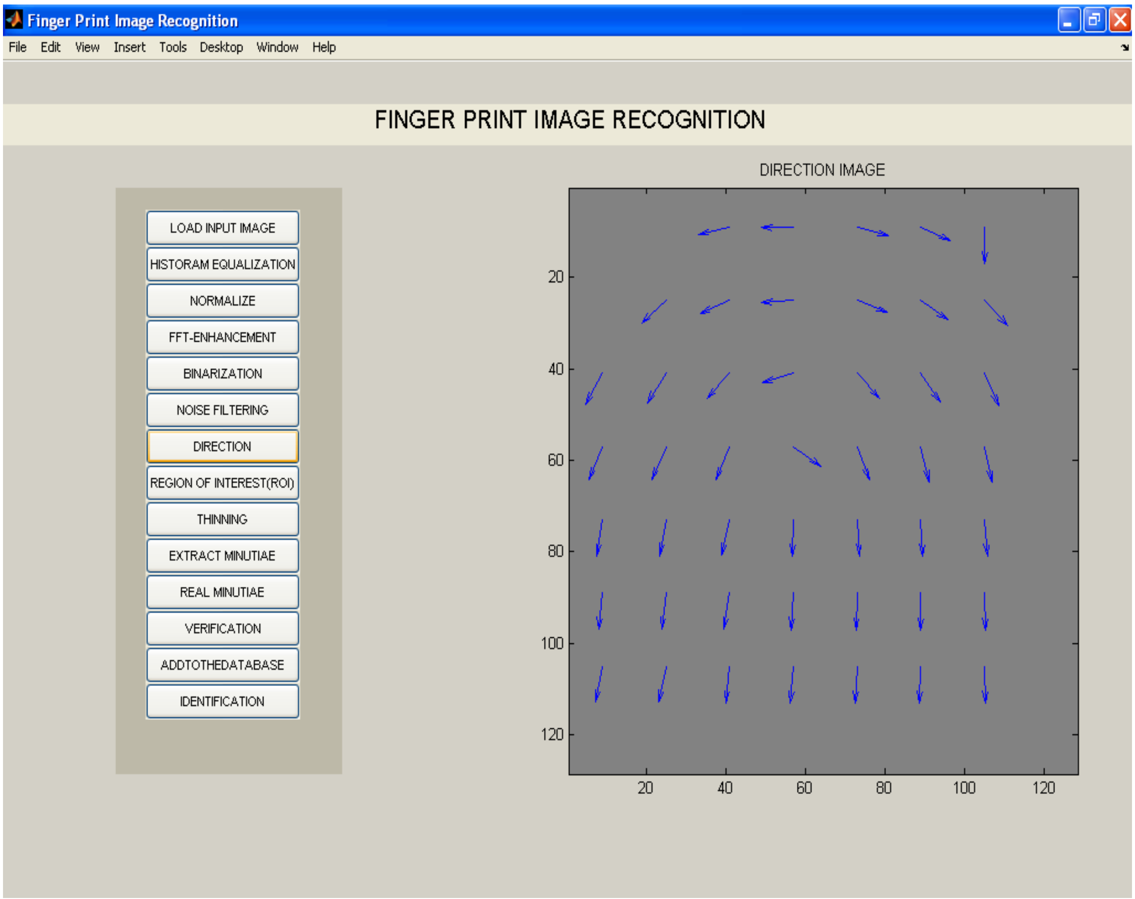


Figure 8.7 Screen shot after click DIRECTION

- Directional image appears on the axis. The arrow indicates the direction of each block. The arrow is made by the ‘quibble’ function available in the matlab. This function also has an option for the colour of the arrow.
- The block size is taken as 16×16 pixels. This is an optimum block size taken in most of the reviewed literatures.

• Click on the REGION OF INTEREST

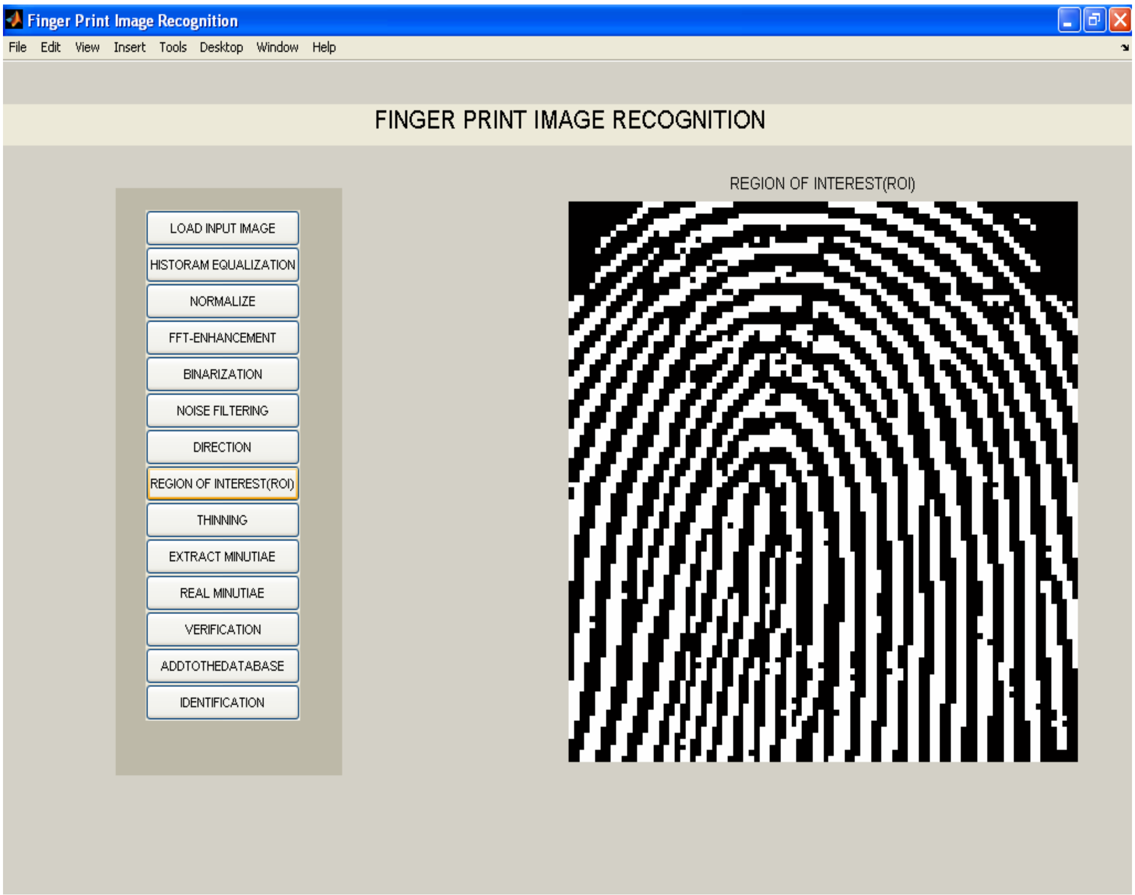


Figure 8.8 Screen shot after click REGION OF INTEREST

- ➢ Region of Interest (ROI) appears on the axis after clicking the pushbutton. Now this is the region which is processed by further techniques.
- ➢ In ROI, the ridges are quite thick. So there is a need of thinning process in next step.

• Click on the THINNING

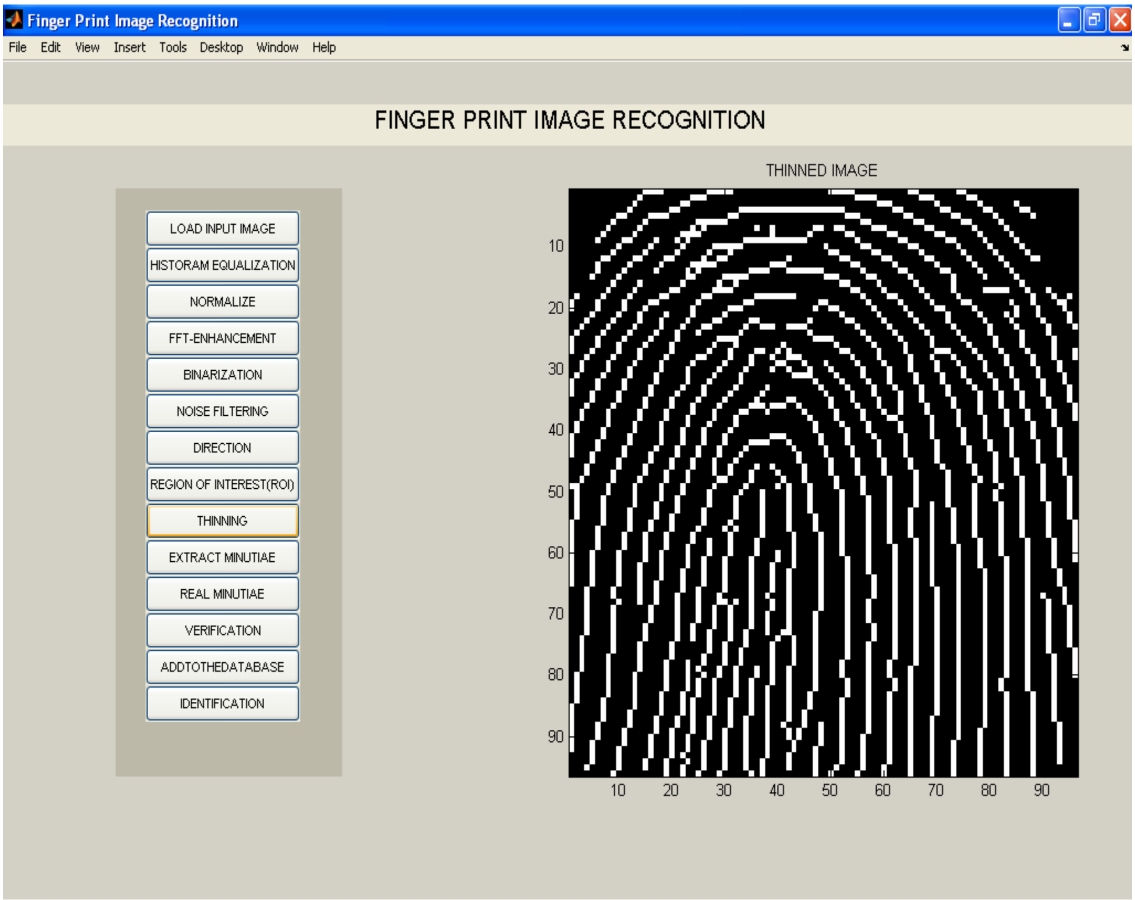


Figure 8.9 Screen shot after click THINNING

- Thinned image appears on the axis. This can be seen that the ridges are now thin i.e. Ridges are one pixel wide.
- Some spurious minutiae appear in the image. So they need to be detected and removed.

• Click on the EXTRACT

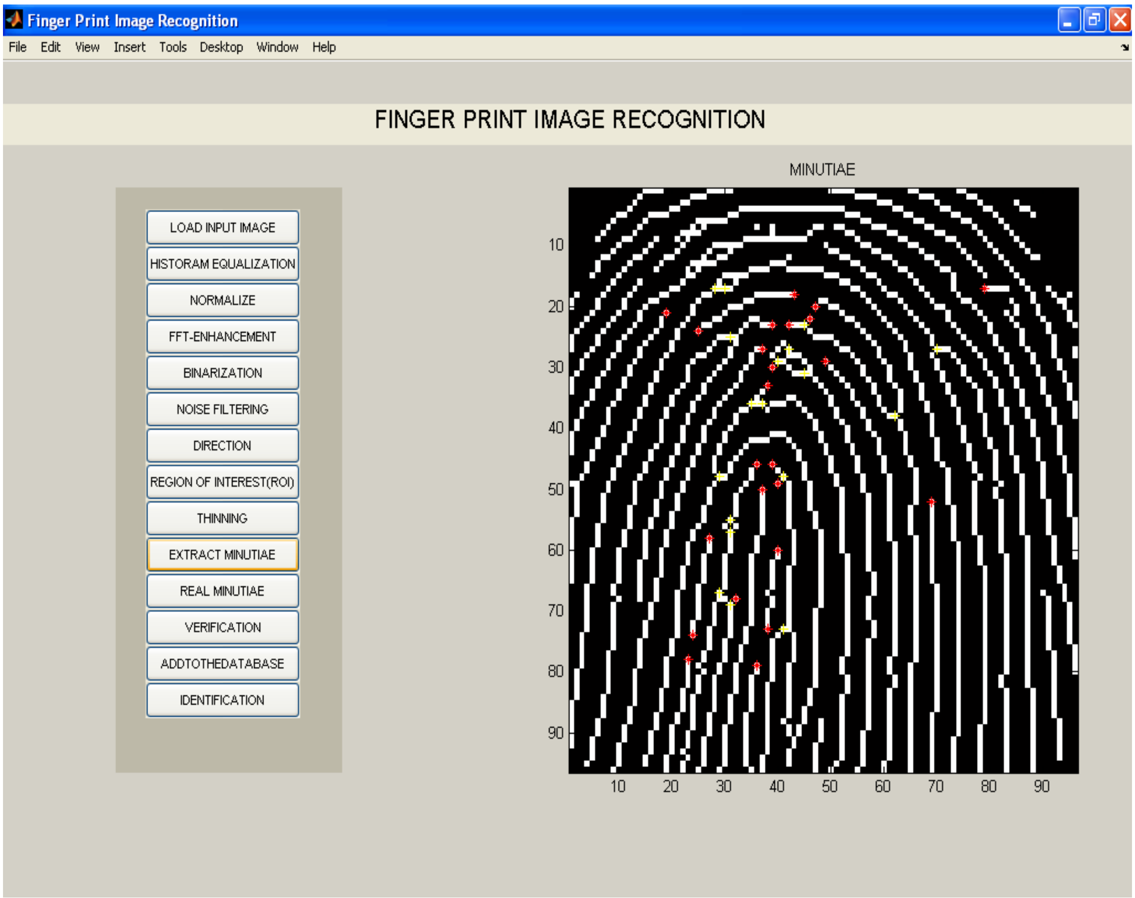


Figure 8.10 Screen shot after click EXTRACT IMAGE

- Minutiae image appears on the axis. Ridge end is shown by the 'red' dot and Bifurcation is shown by the red dot.

- Sufficient numbers of minutiae are extracted from the image.

- Click on the REAL MINUTIAE

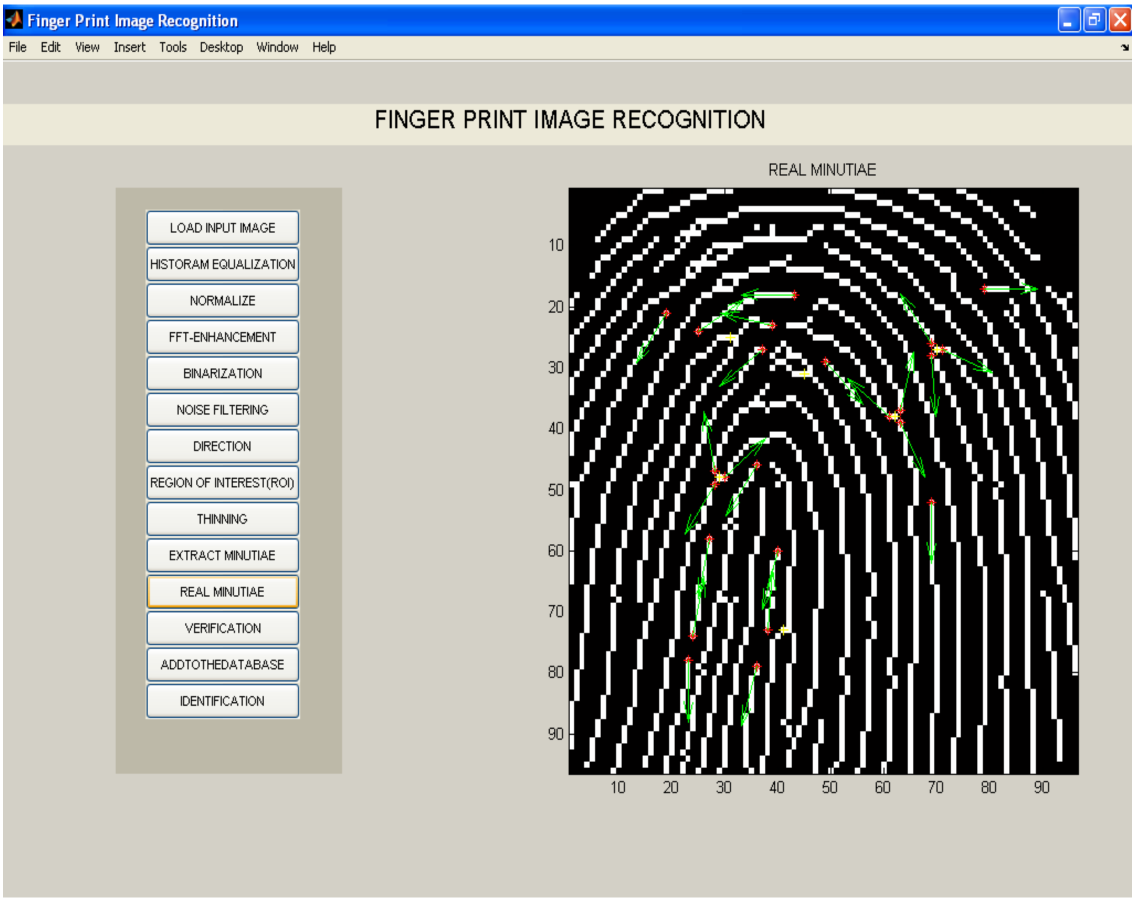
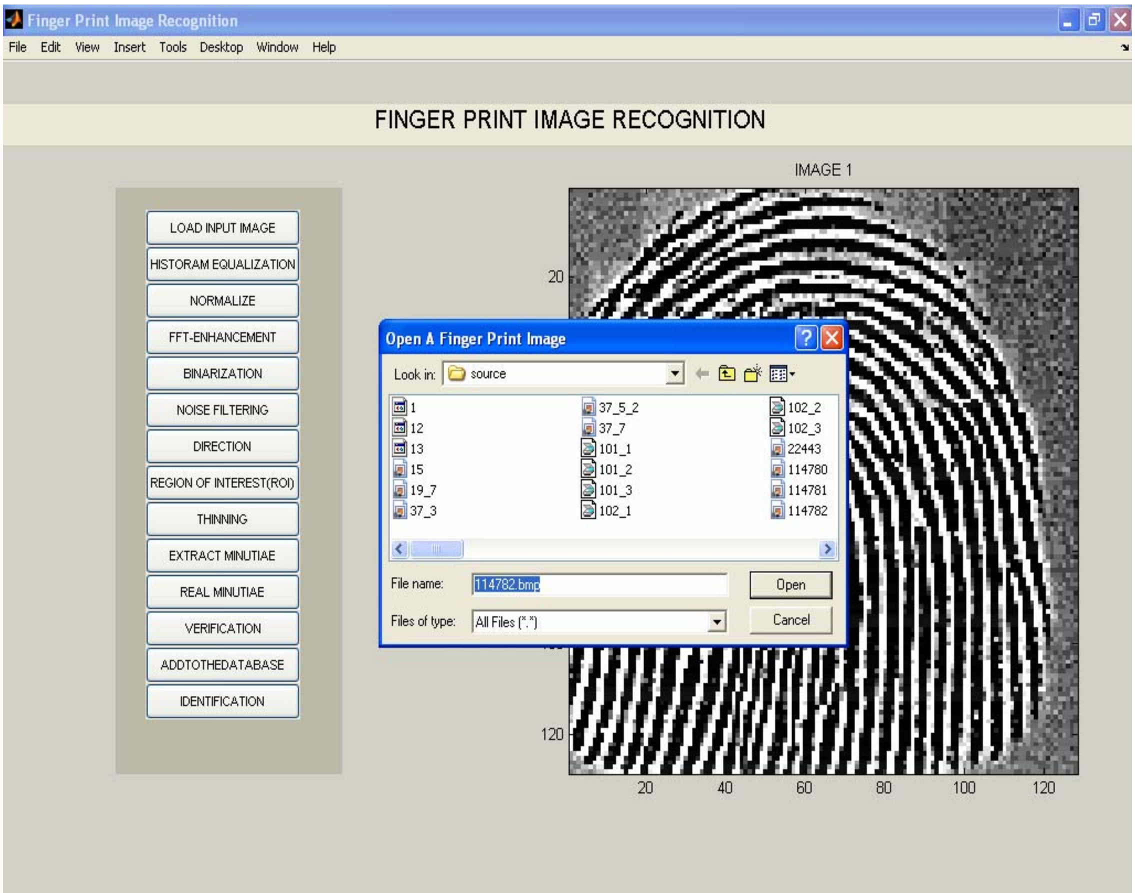


Figure 8.11 Screen shot after click REAL MINUTIAE

- Now the final minutiae set is shown in the image. Ridge end is characterized by a single green arrow. While the bifurcation is characterized by three green arrows.
- As sufficient number of real minutiae is now available from the image, they can be used in the matching.

• Click on the VERIFICATION



Look in: source

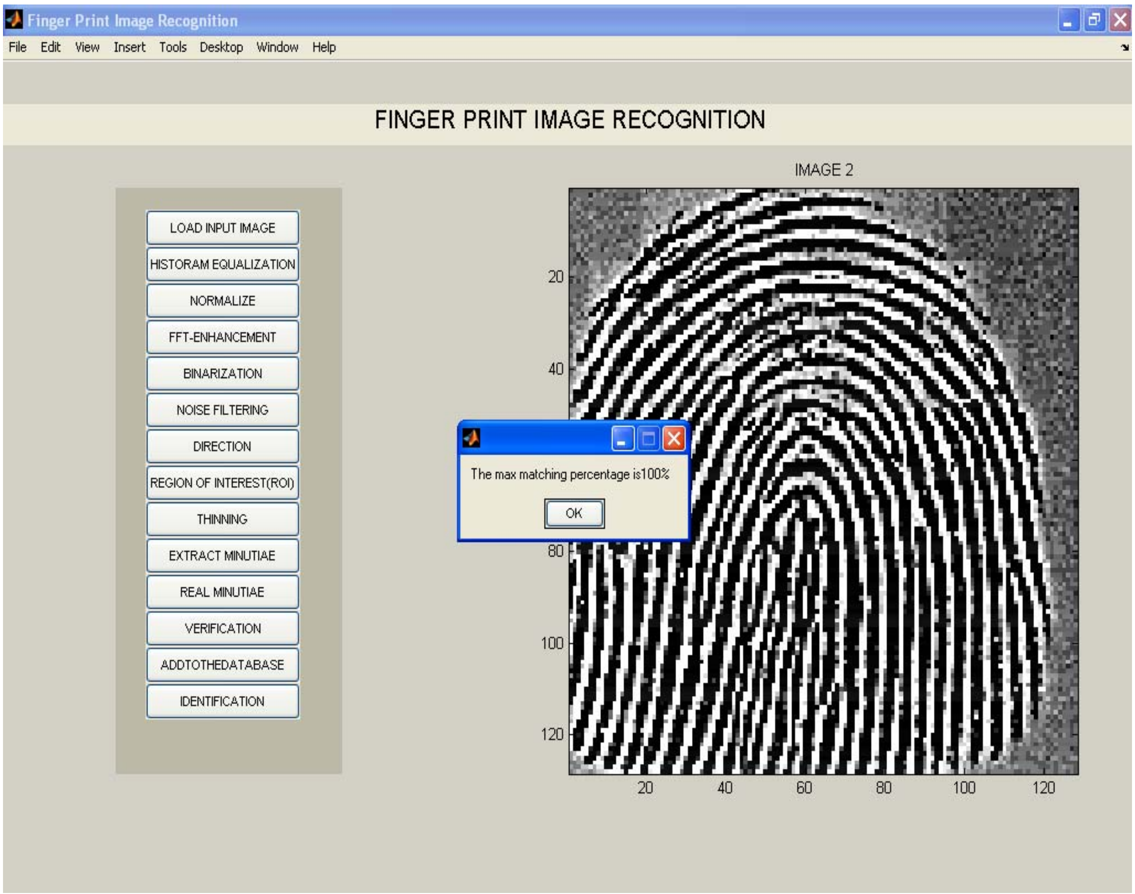
File name: 114782.bmp

Files of type: All Files (*.*)

Figure 8.12 Screen shot after click VERIFICATION

- ➢ A dialog-box appears on the screen, the fingerprint image will be selected from this. After selection the fingerprint image will be appeared on the axis.
- ➢ Now another dialog-box will be appeared, to select another image. This image will again be appeared on the same axis.
- ➢ After selecting the two images, matlab program will calculate the real minutiae set of both the images. And then do the matching of these sets.

• Result of VERIFICATION



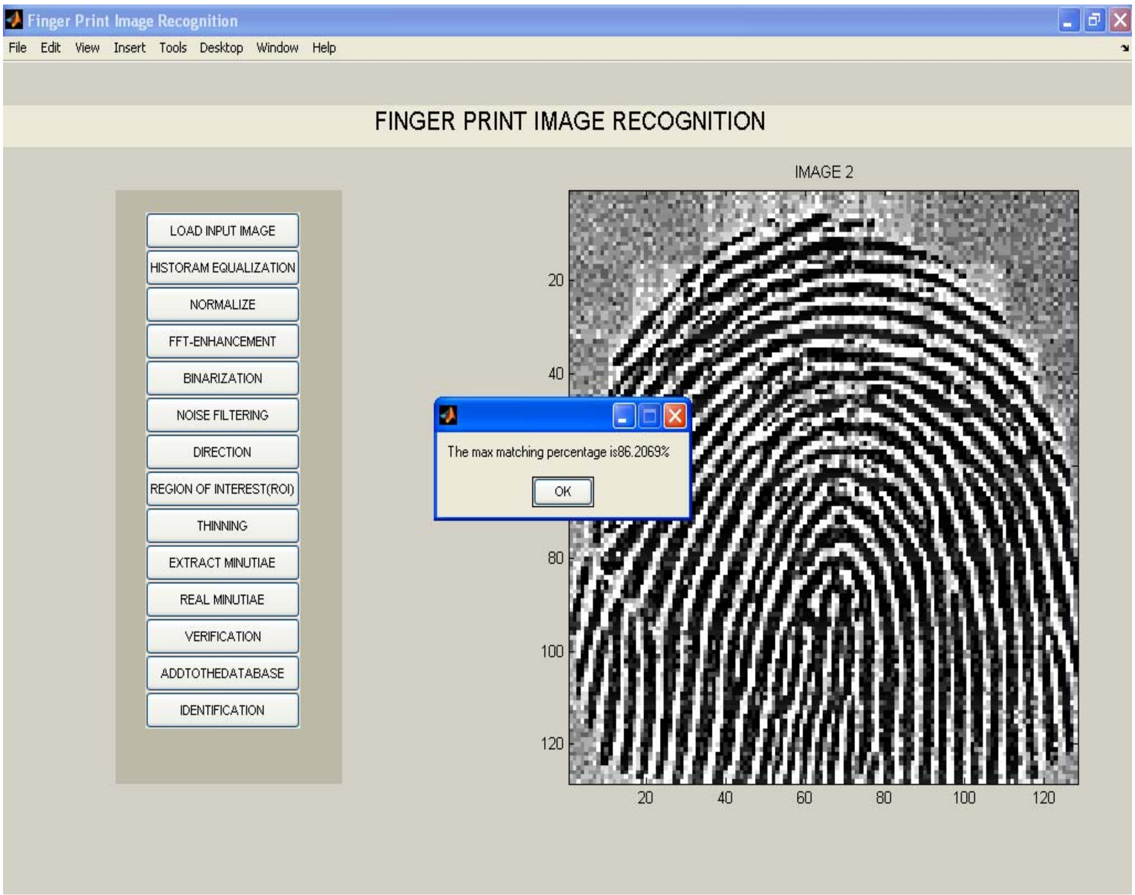
The max matching percentage is100%

Figure 8.13 Screen shot of the result of verification

- When the images of the same finger are selected, the matching percentage calculated is 100%.

- As the threshold for the matching is set to 98%. Hence it is declared that the images are successfully matched.

• Click on the VERIFICATION

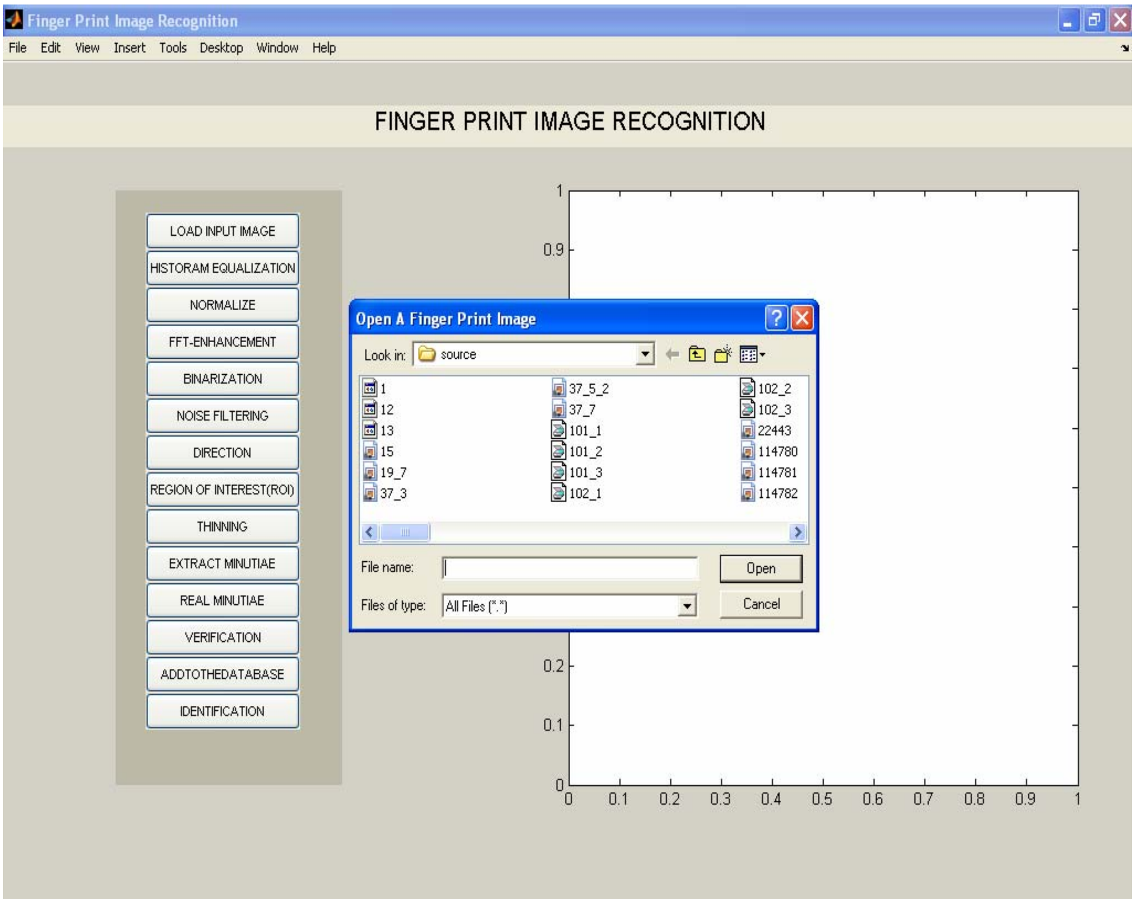


The max matching percentage is86.2069%

Figure 8.14 Screen shot of the result of verification

- In present case, two images of different finger are selected.
- Matching percentage calculated is 86.206%. As this value is less than the threshold, so it is declared that the images are not successfully matched. i.e. they are from different fingers.

• Click on the ADDTOTHEDATABASE



Look in: source

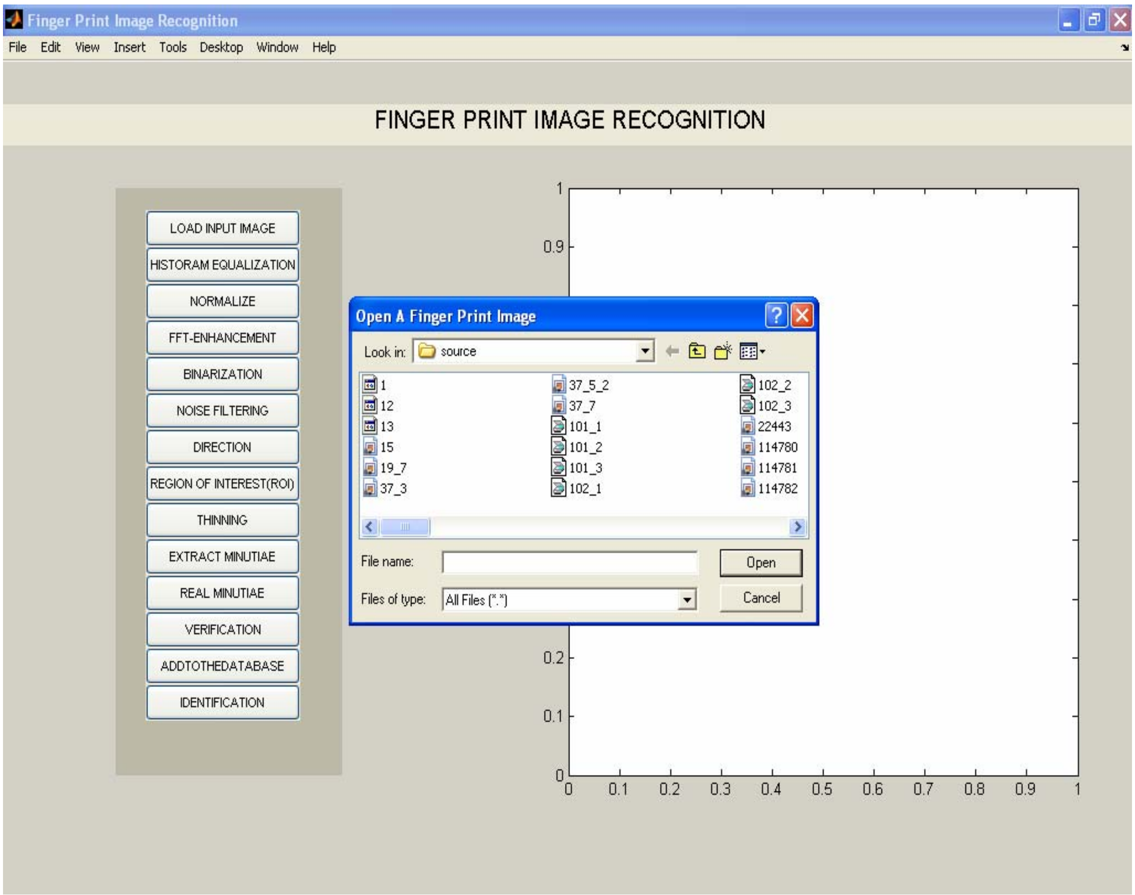
File name:

Files of type: All Files (*.*)

Figure 8.13 Screen shot after click ADDTOTHEDATABASE

- On clicking, a box will appear to input the image which will be added to the database.
- Database has the name of each image and the real minutiae set corresponding to that image.

• Click on the IDENTIFICATION



Look in: source

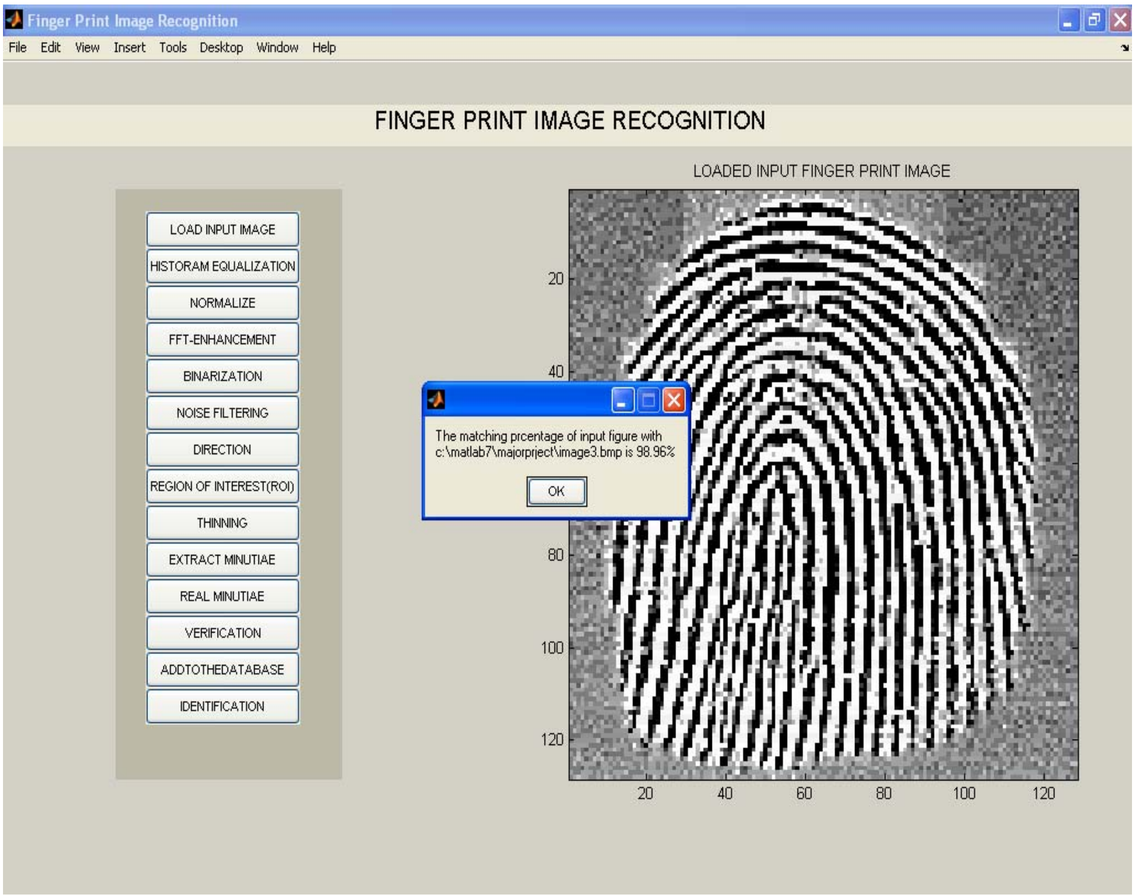
File name:

Files of type: All Files (*.*)

Figure 8.14 Screen shot after click IDENTIFICATION

- ➢ On clicking, a box will appear to input the image which will be taken as template image.
- ➢ Now this image is matched one by one with the images in the database.

• Result of the IDENTIFICATION



The matching prcentage of input figure with c:\matlab7\majorprject\image3.bmp is 98.96%

Figure 8.15 Screen shot of the result of identification

- A box appears after small time showing the result of identification.

- The box shows that the matching percentage of the input image with image at location c:\matlab7\majorproject\image3.bmp is 99.63% and hence the input image is identified as this image.

CHAPTER IX

CONCLUSION & FURTHER WORK

CONCLUSION

The aim of the project was to develop the complete fingerprint recognition system excluding acquisition of the image. And it has achieved successfully as the design methods have been proven to work effectively. It has combined various methods to make the complete system and this is possible by the deep investigation into related literature. There has been no problem in finding materials such as technical articles. However there does not seem to be any good book about fingerprint recognition.

The methods employed satisfactorily enhance the fingerprint image. However some other methods were also tried like use of Gabor filter instead of FFT-Enhancement for context filtering. But the resulting image quality was not good and as it is a middle stage so poor image quality will negatively affect the performance of the subsequent enhancement stages. Also in that case each block of the image is convolved with the bank of Gabor filters, this will significantly increase the enhancement time. Histogram equalization method is directly available in MATLAB, so it is taken from there.

The rules used for removing spurious minutiae although sufficiently remove the spurious minutiae but some spurious minutiae even remained like hole and ladder. The introduction of ridge matching greatly reduced the number of point pairs that can be used as a reference pairs. And hence significantly decreases the time required in identification. The decision of minutiae-based matching is found to be right.

Coding of the whole program in MATLAB is done successfully. Some algorithms which were earlier designed are directly available in the image processing toolbox of the MATLAB. Their accuracy was found to be better then the designed ones. Hence they are taken from the toolbox. Graphical User Interface (GUI) made the procedure easy to understand and analyze. And demonstrate the key issues of fingerprint recognition. The aim of the experimental results section is to illustrate the results of each stage in the enhancement algorithm and to assess how well each stage performs.

FURTHER WORK

A fingerprint authentication and identification system with good accuracy and performance was developed in the project. However there are possible areas of improvement.

• DSP Implementation

The full program is implemented in the MATLAB. But for real-time application it must be implemented in some DSP processor. This could not be implemented due to time constrain

• Hybrid Matching Techniques

Other features such as ridge orientation, ridge count between minutiae can be added to further improve the matching conditions and make the system even more robust and accurate.

• Security

Security is an issue of major concern in any system. In the present system, fingerprint images and information are stored in the database without any encryption so can be easily intercepted. Attacks to manipulate the system however can come at any stage of the system implementation, from the scanner itself to the database and the matcher module, therefore adequate security measures to ensure complete security has to be looked into.

REFERENCES

[1] L. Hong, Y. Wan and A.K. Jain, *"Fingerprint Image Enhancement: Algorithms and Performance Evaluation",* IEEE Tran, Vol. 20, No. 8, pp.777-789, August 1998.

[2] A.J.Willis and L.Mayers, *"A Cost-Effective Fingerprint Recognition System for Use with Low-Quality Prints and Damaged Fingertips",* Pattern Recognition, Vol. 34, No.2, pp.255-270, 2001

[3] A.Ross, J.Shah and A.K.Jain, *"Towards Reconstructing Fingerprints From Minutiae Points",* IEEE Tran, Vol. 557, pp.60-80, March 2005.

[4] Arceli and Baja., *"A Width Independent Fast Thinning Algorithm",* IEEE Transactions On Pattern Analysis And Machine Intelligence, 1984

[5] N. Ratha, S. Chen and A.K. Jain, *"A Real-Time Matching System for Large Fingerprint Databases",* IEEE Trans. Vol 18, No. 8, pp 799-813, 1996

[6] Xiao Sun and Zhuming Ai, *"Automatic Feature Extraction And Recognition of Fingerprint Images",* Proceedings of ICSP, 1996

[7] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, *"Handbook Of Fingerprint Recognition",* Springer, 2003.

[8] Xiping Luo, Jie Tian and Yan Wu, *"A Minutiae Matching Algorithm in Fingerprint Verification",* IEEE 2000.

[9] A.K.Jain, S.Prabhakar, L.Hong, *"FingerCode: A Filterbank for Fingerprint Representation and Matching",* Proc. IEEE Conference on CVPR, Colorado, Vol . 2, pp. 187-193, June 23-25, 1999

[10] A.K.Jain, S.Prabhakar, L.Hong and S.Pankanti, *"A Filterbank-Based Fingerprint Matching"*, IEEE Tran., Vol. 9, No.5, May2000

[11] B.Moayer and K.Fu., *"A Tree System Approach For Fingerprint Pattern Recognition"*, IEEE Trans. Vol. 8, No. 3, 377-388, 1986

[12] L.Coetzee and E.C.Botha, *"Fingerprint Recognition in Low-Quality Images"*, Pattern Recognition, Vol.26 No.10, 1441-1460, 1993

[13] R.C.Gonzales, R.E.Woods, *"Digital Image Processing,"* Addisson Wesley,1992.

[14] M.Kass, A.Witkin, *"Analyzing Oriented Patterns"*, Computer Vision, Graphics and Image Processing, Vol. 37, No. 3, 362-385, 1987

[15] N.K.Ratha, S.Y.Chen, A.K.Jain, *"Adaptive flow Orientation-Based Feature Extraction in Fingerprint Images"*, Pattern Recognition, Vol 28, No.11,1657-1672, November 1995

[16] D.Maio and D. Maltoni., *"Direct gray-scale minutiae detection in fingerprints"*, IEEE Trans. Pattern Anal. And Machine Intell., 19(1):27-40, 1997.

[17] A.K.Jain, L.Hong and R. Bolle, "*On-Line Fingerprint Verification*", IEEE Trans. on Pattern Anal and Machine Intell, 19(4), pp. 302-314.,1997

[18] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, *"An identity Authentication System using Fingerprints"*, IEEE, vol. 85, pp. 1365–1388, Sept. 1997.

[19] Nick Efford , *"Digital Image Processing a practical introduction using JAVA"*,. Pearson Education, 2004.

[20] Asker M.Bazen ,Gerben T.B. Verwaaijen, Sabih H.Gerez, *"A Correlation-Based Fingerprint Verification System"*, ProRISC 2000 Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands, November 2000.

Websites:

www.mathworks.com

www.ieeexplore.ieee.org

www.fmrib.ox.ac.uk/~steve/susan/thinning/node2.html

www.recogsys.com/index.shtml

www.biometric-consulting.com/bio.html