Security Management using Fingerprint Verification

By

MAJOR SYED MUNIR HUSSAIN SABZWARI

NC MUHAMMAD OWAIS UL HAQ

MAJOR BILAL YOUSAF

MAJOR ASIF NAWAZ

Submitted to Faculty of Electrical Engineering

National University of Sciences and Technology, Rawalpindi in partial fulfillments of a B.E. Degree in Telecommunication Engineering.

June 2010

ABSTRACT

In this project a fingerprint based security system has been developed for a department utilizing the Fingerprint verification in order to validate the authorized persons. The image acquisition is done using an optical fingerprint reader. The acquired fingerprint image is visually enhanced, segmented and saved as a template composed of extracted fingerprint features. This template generation is performed as modular programming in software. The template is then compared with the templates present in the database, which were acquired and processed beforehand. This database also contains the requisite information of authorized persons which in turn can be used for multipurpose applications. In the end the information about the authorized person or the intruder will be displayed at the output unit attached to the system.

DEDICATION

We dedicate this effort of us, to our beloved Parents, whose loving, caring, supporting and benevolent personalities have left incredible and indelible impression on our characters as well as this particular piece of project.

ACKNOWLEDGMENT

Praise to Almighty Allah for bestowing upon us strength and knowledge, to conclude this aspiration in time and craft a substantial contribution. We owe a special debt of gratitude to Maj. Dr. Adil Masood who offered his expertise, constructive critic, advice and guidance which made the present work a reality. We thank Dr. Asif Masood, Dr. Imran Tauqeer and Mr. Gulraiz Chaudhry for generously sharing their ideas, enlightening and steering me to achieve this landmark. We are gratified to our colleague Capt. Muhammad Kashif for his valuable encouragement and suggestions.

TABLE OF CONTENTS

Chapter 1 -	**Biometrics**		**1**
1.1	Introduction		1
1.2	Advantages of Biometrics		2
	1.2.1 Non-repudiation		2
	1.2.2 Accuracy and Security		2
	1.2.3 Screening		2
1.3	Biometric Modalities		2
	1.3.1	Physical Biometrics	2
	1.3.2	Behavioral Biometrics	2
	1.3.3	Chemical Biometrics	2
1.4	Fingerprints among Biometric Identifiers		4
1.5	Why Fingerprint is selected		6
Chapter 2 -	**Fingerprint as Biometric Identity**		**9**
2.1	Introduction		9
2.2	Formation of Fingerprints		10
2.3	History of Fingerprints		11
2.4	Fingerprint Sensing and Storage		12
	2.4.1	Optical Sensors	12
	2.4.2	Capacitive Sensors	13
	2.4.3	Ultra Sound Sensors	13

2.4.4 Thermal Sensors 14

2.5 Fingerprint Features 14

Chapter 3 - Project Overview 18

3.1 System Description 18

3.2 Acquisition of Fingerprint Images 19

3.3 Image Pre-processing 19

3.3.1 Enhancement and Histogram Equalization 19

3.3.2 Binarization 20

3.3.3 ROI extraction by Morphological Operation 20

3.4 Minutiae Extraction 21

3.4.1 Fingerprint Ridge Thinning 21

3.5 Minutiae Post-processing 22

3.5.1 False Minutiae Removal 22

3.5.2 Minutiae Matching 22

Chapter 4 - Fingerprint Acquisition 23

4.1 Introduction 23

4.2 Image Capture Devices 23

4.3 Cross Match Verifier 300 LC USB 26

4.3.1 Features of Cross Match Verifier 27

4.3.2 System Requirements 29

4.3.3 Applications 29

Chapter 5 - Image Acquisition 32

5.1 Fingerprint Image Enhancement 32

5.2 Histogram Equalization 33

5.3 Fingerprint Enhancement by Fourier Transform 34

Chapter 6 - Fingerprint Image Preprocessing 36

6.1 Fingerprint Image Binarization 36

6.2 Fingerprint Image Segmentation 36

6.2.1 Block Direction Estimation 37

6.2.2 ROI extraction by Morphological Operation 38

Chapter 7 - Feature Extraction 40

7.1 Fingerprint Ridge Thinning Techniques 40

7.1.1 Parallel Thinning 40

7.1.2 Thinning from Gray Scale 40

7.1.3 Morphological Thinning 40

7.2 Selected Thinning Technique 42

7.3 Minutiae Marking 42

Chapter 8 - Minutiae Purification **44**

8.1 Border Minutiae Purification 45

8.2 Contour Minutiae Purification 45

8.3 Minutiae Purification based on Neighborhood 47

8.3.1 Post-processing of Ridge Bifurcation 48

8.4 False Minutiae Removal 49

8.5 Unify Terminations and Bifurcations 51

Chapter 9 - Minutiae Match 53

9.1 Minutiae Matching 53

9.1.1 Allignment Stage 53

9.2 Local Matching 55

9.2.1 Selection of Secondary Features 55

9.2.2 Indexing of Secondary Features 58

9.2.3 Tolerance Boxes 59

Chapter 10 - Database 60

10.1 Database Management System 60

10.2 Types of Database 61

10.2.1 Operational Database 61

10.2.2 Analytical Database 61

10.2.3 Data ware House 62

10.2.4 Distributed Database 62

10.2.5 End User Database 62

10.2.6 External Database 62

10.2.7 Hypermedia Database on Web 63

10.2.8 Navigational Database 63

10.2.9 Document Oriented Database 63

10.2.10 Real time Database 63

Chapter 11 - Performance Evaluation and Result 64

11.1 Introduction 64

11.2 Classification Error 64

11.3 Experimentation Result 66

11.4 Analysis and Comparison of Results 68

Chapter 12 - Conclusion 70

12.1 Overview 70

12.2 Contribution and Objectives Achieved 70

12.3 Limitations 70

12.4 Future Work 71

Bibliography 72

LIST OF TABLES

Number	Description	Page
TABLE-1.1	Comparison of Different Biometric Techniques	**05**
TABLE-1.2	Features of Different Bio Modulations	**08**
TABLE-4.1	Specifications of Cross Match Input Device	**29**

LIST OF FIGURES

Number	Description	Page
Figure-1.1	Various Biometric Modalities	**3**
Figure-1.2	Different Identification Methods	**4**
Figure-1.3	Biometric Market Report	**6**
Figure-2.1	Fingerprint Image	**9**
Figure-2.2	Optical Sensor Schematic	**13**
Figure-2.3	Fingerprint Patterns	**15**
Figure-2.4	Ridge Ending and BIfurcation	**16**
Figure-2.5	Minutiae marking	**17**
Figure-3.1	System Block Diagram	**18**
Figure-3.2	Simulation Block Diagram	**21**
Figure-4.1	Cross Match Verifier	**27**
Figure-5.1	Original Histogram of Fingerprint	**33**
Figure-5.2	After histogram Equalization	**33**
Figure-5.3	Histogram Enhancement	**34**
Figure-5.4	FFT Enhancement of Fingerprint	**35**
Figure-6.1	Fingerprint Image after Binarization	**36**
Figure-6.2	Direction Map	**38**

Figure-6.3	ROI extraction by Morphological Operation	**39**
Figure-7.1	Bifurcation	**42**
Figure-7.2	Termination	**42**
Figure-7.3	Tripple Counting Branch	**43**
Figure-8.1	False Minutiae	**44**
Figure-8.2	Minutiae Marking	**45**
Figure-8.3	Contour Minutiae Purification	**47**
Figure-8.4	Valid Ridge Ending and Purification	**47**
Figure-8.5	Removal of False Minutiae (example)	**48**
Figure-8.6	Cancelling of false minutiae (example)	**49**
Figure-8.7	Possible False Minutiae structures	**50**
Figure-8.8	A bifurcation to three terminations	**52**
Figure-9.1	Coordinate System at minutiae F	**54**
Figure-9.2	Secondary Features	**56**
Figure-9.3	False Minutiae --- examples	**57**
Figure-9.4	Influence of spurious minutiae	**58**
Figure-9.5	Eight Quadrant	**59**
Figure-9.6	Tolerance Box	**59**
Fig-11.1	Imposter and Genuine Distribution	**65**
Fig-11.2	Receive Operating Curve	**66**
Fig-11.3	Distribution of Correct and Incorrect Scores	**67**

Fig-11.4 FAR and FRR curves **67**

Fig-11.5 Partial Match Images **68**

CHAPTER 1

Biometrics

1.1 Introduction

Biometrics offers a promising solution for reliable and uniform identification and verification of an individual. Biometrics is the science of verifying and establishing the identity of an individual through physiological features or behavioral traits. These traits are unique to an individual and hence cannot be misused, lost or stolen. Biometrics are based on established scientific principles as a basis for authentication. In an increasingly digital world, reliable personal authentication has become an important human computer interface activity. National security, e-commerce, and access to computer networks are some examples where establishing a person's identity is vital. Existing security measures rely on knowledge-based approaches like passwords or token-based approaches such as passports to control access to physical and virtual spaces, but such methods are not very secure. Tokens such as badges and access cards may be shared or stolen. Passwords and PIN numbers may be stolen electronically. Furthermore, they cannot differentiate between authorized user and a person having access to the tokens or knowledge.

Biometrics such as fingerprint, face offers means of reliable personal authentication that can address these problems and is gaining citizen and government acceptance. The manual method of fingerprint indexing resulted in a highly skewed distribution of fingerprints into types, most fingerprints fell into a few types and this did not improve search efficiency. Furthermore, increasing workloads due to a higher demand on fingerprint recognition services 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. Because biometric identifiers cannot be easily misplaced, forged, or shared, they are considered more reliable for person recognition than traditional token- or knowledge-based methods. The tremendous success of fingerprint based recognition technology in law enforcement applications, decreasing cost of fingerprint sensing devices, increasing availability of inexpensive computing power, and growing identity fraud/theft have all ushered in an era of fingerprint-based person recognition applications in commercial, civilian, and financial

domains.

1.2 Advantages of Biometrics

Biometrics is the science of verifying the identity of an individual through physiological measurements or behavioral traits. Since biometric identifiers are associated permanently with the user, are more reliable than token or knowledge based authentication methods. Advantages of Biometrics over traditional security are;

1.2.1 Non-repudiation: With token and password based approaches, the perpetrator can always deny committing the crime pleading that his/her password or ID was stolen or compromised even when confronted with an electronic audit trail. There is no way in which his claim can be verified effectively. This is known as the problem of deniability or of 'repudiation'. However, biometrics is indefinitely associated with a user and hence it cannot be lent or stolen making such repudiation infeasible.

1.2.2 Accuracy and Security: Password based systems are prone to dictionary and brute force attacks. Furthermore, such systems are as vulnerable as their weakest password. On the other hand, biometric authentication requires the physical presence of the user and therefore cannot be circumvented through a dictionary or brute force style attack. Biometrics has also possessed a higher bit strength compared to password based systems and are therefore inherently secure.

1.2.3 Screening: In screening applications, we are interested in preventing the users from assuming multiple identities (e.g. a terrorist using multiple passports to enter a foreign country). This requires that we ensure a person has not already enrolled under another assumed identity before adding his new record into the database. Such screening is not possible using traditional authentication mechanisms and biometrics provides the only available solution.

1.3 Biometric Modalities

The various biometric modalities can be broadly categorized as

1.3.1 Physical Biometrics: These involve some form of physical measurement and include modalities such as face, fingerprints, iris-scans, hand geometry etc.

1.3.2 Behavioral Biometrics: These are usually temporal in nature and involve measuring the way in which a user performs certain tasks. This includes modalities such as speech, signature, gait, keystroke dynamics etc.

1.3.3 Chemical Biometrics: This is still a nascent field and involves measuring chemical cues such as odor and the chemical composition of human perspiration.

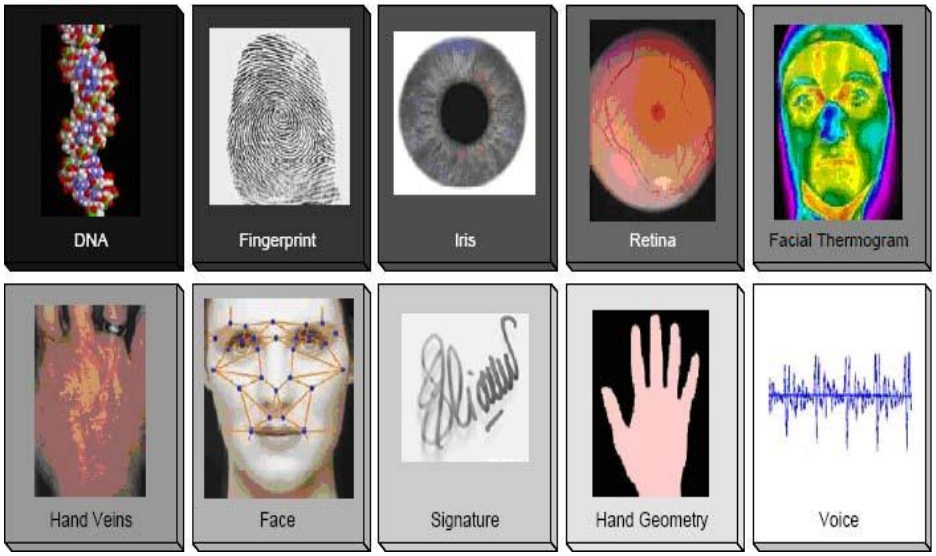


Figure 1.1: Various biometric modalities: Fingerprints, speech, handwriting, face, and geometry and chemical biometrics

Biometrics can be used for identification or for verification. In verification, the biometric is used to validate the claim made by the individual. The biometric of the user is compared with the biometric of the claimed individual in the database. The claim is rejected or accepted based on the match. In identification, the system recognizes an individual by comparing his biometrics with every record in the database.

Biometrics is thus defined as the methods of uniquely identifying humans based on physical, biological and/or behavioral traits. Since the biological characteristics cannot be forgotten and cannot be easily shared, misplaced or stolen, their use is generally considered to be more reliable approach for solving the personal identification problem. Figure 1.2 shows the increase of security and comfort for three different kinds of identification methods.

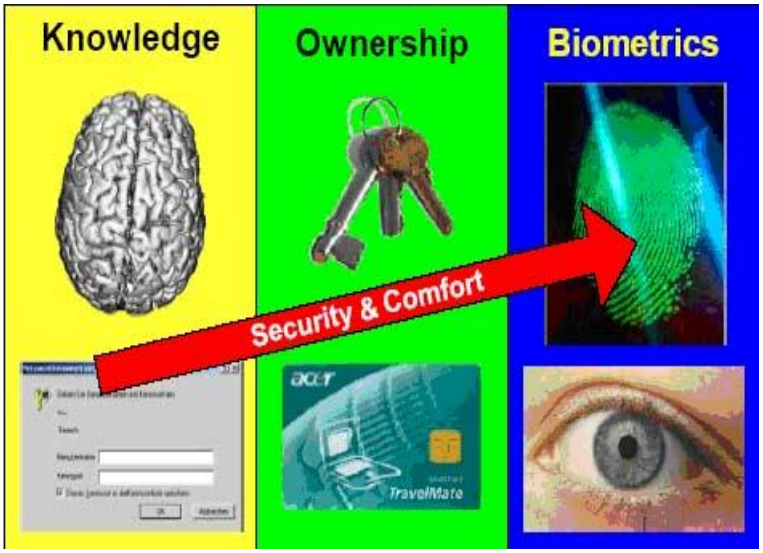


Figure 1.2 Biometrics among three different kinds of identification methods.

A biometric system is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological and/or behavioral characteristic possessed by that person. However, in practical there are a number of other issues which should be considered, these are performance, acceptability and circumvention of a biometric system. A biometric system should have achievable recognition accuracy, speed, robustness, the resource requirements to achieve the desired recognition accuracy and speed, as well as operational or environmental factors that affect the recognition accuracy and speed. Acceptability indicates the extent to which people are willing to accept a particular biometric identifier used in a biometric system in their daily lives. Last but not the least, how easy it is to fool the system by fraudulent methods.

1.4 Fingerprints among Biometric Identifiers

A number of biometric identifiers are in use in various applications. Each identifier has its strengths and weaknesses and the choice typically depends on the application. No single identifier is expected to effectively meet the requirements of all the applications. The match between an identifier and an application is determined depending upon the characteristics of the application and the properties of the biometric identifier. Figure 1.1 shows some of the biometric identifiers currently in use in various applications [2].The identifiers shown are placed in order of their uniqueness (black corresponds to the most unique one and white corresponds to the least

unique one). Uniqueness however is not the only criteria for the selection of a biometric identifier for a particular application. A comparison of different biometric identifiers is shown in Table 1.1

Table 1.1: Comparison of biometric technologies.

Biometric Identifier	Univer-sality	Distinct-iveness	Permanence	Collect-ability	Performance	Accept-ability	Circum-vention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial Thermo Gram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand Geometry	M	M	M	H	M	M	M
Hand Vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 1.1 High, Medium, and Low are denoted by H, M, and L, respectively.

Fingerprint recognition is one of the most mature biometric technologies and is suitable for a large number of recognition applications. This is also reflected in revenues generated by various biometric technologies in the year 2007 (see Figure 1.3).

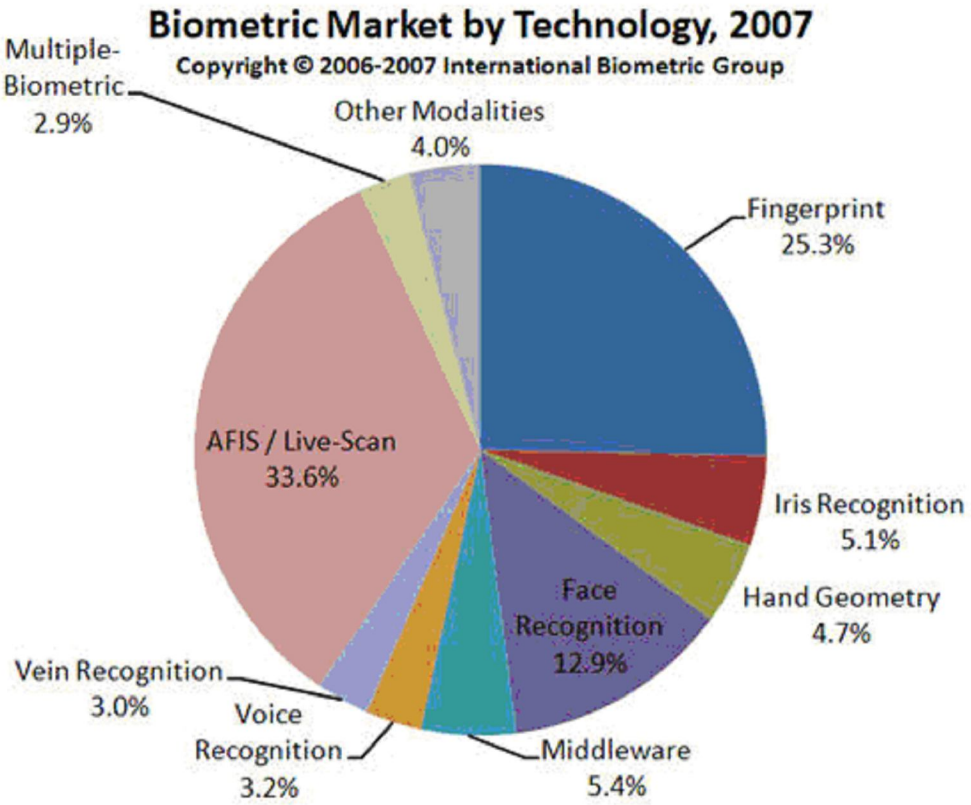


Figure 1.3: Biometric market report (International Biometric Group)

Skin on human fingertips contains ridges and valleys which together forms distinctive patterns. These patterns are fully developed under pregnancy and remain permanent throughout the complete lifetime. Prints of those patterns are called fingerprints. Injuries like cuts, burns and bruises can temporarily damage quality of fingerprints but when fully healed patterns will be restored. Through various studies it has been observed that no two persons have the same fingerprints, hence they are unique for every individual (and each finger). Fingerprints of identical twins are different.

1.5 Why Fingerprint is selected

Note that 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 distinctive and the details are permanent, even if they may temporarily change slightly due to cuts and bruises on the skin or weather conditions. High quality fingerprints can easily be captured using live scan technology and they do not suffer from the problem of segmentation of the fingerprint from the background. At present the fingerprint verification systems deployed are giving excellent performance and their availability is no longer an issue. 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 worldwide. The strong points which form the basis to select fingerprints are:

1.5.1 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.

1.5.2 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.

1.5.3 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.

1.5.4 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 cooperative 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.

1.5.5 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.

Table 1.2 shows selected features of each modality and can be used to determine complementary modalities for multi-modal systems. A few notes on this table:

1. The row for the eye biometric describes features applying to either iris or retinal scanning technologies.
2. In the matching column, whereas all technologies are appropriate for 1-to-1 matching, only fingerprint and eye technologies are proven to have acceptable recognition rates to be practical for 1-to-many matching. This is an indication that these two modalities provide the highest recognition rates for verification as well.
3. Variation of the salient features used for recognition is very different for different modalities. Fingerprint and eye features remain consistent for a lifetime, whereas the others

change with growth. On a day-to-day basis, there is far less variation for all modalities, though voice can change with illness and signature with demeanor.

4. As far as sensor cost, eye systems are currently more costly than the others; voice systems can be zero cost to the user if a telephone is used.

5. Fingerprint and voice systems have the smallest comparative sizes with eye systems currently the largest.

Table 1.2 Features of different biometric modalities

Biometric	**Matching 1-to-1, 1-to many**	**Variation: Lifetime, Day-to-Day**	**Maximum Independent Samples per Person**	**Sensor Cost [$US]**	**Sensor Size**
Fingerprint	yes, yes	none, little	**10**	$10\text{-}10^2$	very small
Eye	yes, yes	none, very little	**2**	$10^2\text{-}10^3$	medium
Hand	yes, no	much, very little	**2**	10^2	medium
Face	yes, no	much, medium	**1**	10^2	small
Voice	yes, no	much, medium	**1**	$0\text{-}10^2$	Very small
Signature	yes, no	much, medium	**1**	10^2	medium

CHAPTER 2

Fingerprint as a Biometric Identity

2.1 Introduction

A fingerprint is the feature pattern of one finger (Fig 2.1). Each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and forensic investigation for a long time.

Figure2.1 A fingerprint image acquired by an Optical Sensor

A fingerprint is composed of many ridges and grooves presenting good similarities in each small local window, like parallelism and average width. Fingerprints are not distinguished by their ridges and grooves, but by Minutia, which are some abnormal points on the ridges.

Compared to other biometrics, fingerprints are relatively inexpensive to capture. Making an identification of a print from a crime scene may not even require the use of a computerized identification system; the examiner may rely instead on the images from a ten print card, the latent print, and the expertise of the examiner.

Fingerprinting does not require a laboratory for analysis, and fingerprints remain relatively constant over time, with the exception of injury. Each person has ten fingers, ten unique tokens tied to his

or her identity. No two fingerprints have ever been found to be identical. The finger images may be scarred or cut, but can still contain enough information to link the image with the owner. The friction ridges on each person's palms also provide unique images.

2.2 Formation of Fingerprints

Fingerprints are fully formed at about seven months of fetus development and finger ridge configurations do not change throughout the life of an individual except due to accidents such as bruises and cuts on the fingertips . This property makes fingerprints a very attractive biometric identifier.

Biological organisms, in general, are the consequence of the interaction of genesand environment. It is assumed that the phenotype is uniquely determined by the interaction of a specific genotype and a specific environment. Fingerprints are, in general , a part of an individual's phenotype. Fingerprint formation is similar to the growth of capillaries and blood vessels in angiogenesis. The general characteristics of the fingerprint emerge as the skin on the fingertip begins to differentiate . The differentiation process is triggered by the growth in size of the volar pads on the palms, fingers, soles, and toes. However, the flow of amniotic fluids around the fetus and its position in the uterus change during the differentiation process. Thus the cells on the fingertip grow in a microenvironment that is slightly different from hand to hand and finger to finger.

The finer details of the fingerprints are determined by this changing microenvironment. A small difference in microenvironment is amplified by the differentiation process of the cells. There are so many variations during the formation of fingerprints that it would be virtually impossible for two fingerprints to be exactly alike. But, because the fingerprints are differentiated from the same genes, they are not totally random patterns either. The extent of variation in a physical trait due to a random development process differs from trait to trait.

By definition, identical twins can not be distinguished based on DNA. Typically, most of the

physical characteristics such as body type, voice, and face are very similar for identical twins and automatic recognition based on face and hand geometry will most likely fail to distinguish them. Although the minute details in the fingerprints of identical twins are different, a number of studies have shown significant correlation in the fingerprint class (i.e., whorl, right loop, left loop, arch, tented arch) of identical twin fingers; correlation based on other generic attributes of the fingerprint such as ridge count, ridge width, ridge separation, and ridge depth has also been found to be significant in identical twins.

2.3 History of Fingerprints

Humans have used fingerprints for personal identification for a very long time [6]. Fingerprints have been found on ancient Babylonian clay tablets, seals, and pottery. They have also been found on the walls of Egyptian tombs and on Minoan, Greek, and Chinese pottery as well as on bricks and tiles in Babylon and Rome. Some of these fingerprints were deposited unintentionally by workers during fabrication; sometimes the fingerprints served as decoration. However, on some pottery, fingerprints were impressed so deeply that they were likely intended to serve as the equivalent of a brand label. The world's first Fingerprint Bureau was opened in Calcutta (Kolkata) in 1897, after the Council of the Governor General approved a committee report (on 12 June 1897) that fingerprints should be used for classification of criminal records. Modern fingerprint matching techniques were initiated in the late 16th century. Henry Fauld, in 1880, suggested scientifically for the very first time that the fingerprints are unique. At the same time, Sir William Herschel asserted that he had practiced fingerprint identification for about 20 years. This discovery established the foundation of modern fingerprint identification. In late 19th century, Sir Francis Galton conducted an extensive study of fingerprints. He introduced the minutiae features for fingerprint classification in 1888. The discovery of uniqueness of fingerprints caused an immediate decline in the prevalent use of anthropometric methods of identification and led to the adoption of fingerprints as a more efficient method of identification. An important advancement in fingerprint identification was made in 1899 by Edward Henry, who (with his two assistants from India) established the famous "Henry System" of fingerprint classification : an elaborate method of indexing fingerprints very much tuned to facilitating the

human experts performing (manual) fingerprint identification. In early 20th century, fingerprint identification was formally accepted as a valid personal identification method by law enforcement agencies and became a standard procedure in forensics . Fingerprint identification agencies were setup worldwide and criminal fingerprint databases were established. With the advent of livescan fingerprinting and availability of cheap fingerprint sensors, fingerprints are increasingly used in government and commercial applications for positive personnel identification.

2.4 Fingerprint Sensing and Storage

Based on the mode of acquisition, a fingerprint image may be classified as off-line or live scan. An off-line image is typically obtained by smearing ink on the fingertip and creating an inked impression of the fingertip on paper. The inked impression is digitized by scanning the paper using an optical scanner or a high-quality video camera. A live-scan image, on the other hand, is acquired by sensing the tip of the finger directly, using a sensor that is capable of digitizing the fingerprint on contact.

A special kind of off-line images, extremely important in forensic applications, are the so-called latent fingerprints found at crime scenes. The oily nature of the skin results in the impression of a fingerprint being deposited on a surface that is touched by a finger. These latent prints can be "lifted" from the surface by employing certain chemical techniques.

The live-scan devices may be based on one of the following sensing schemes.

2.4.1. 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 as shown (Figure 2.2).

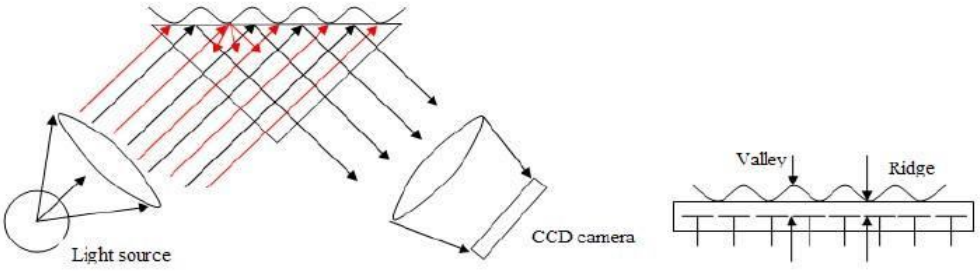


Figure 2.2: (a) General schematic for an FTIR based optical sensor (b) Schematic of a capacitive sensor

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 theoptics involved.

2.4.2. 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 valleys corresponds to smaller capacitance. This variation is converted into an 8-bit gray scale digital image. Most of the electronic devices featuring fingerprint authentication use this form of solid state sensors due to its compactness. However, sensors that are smaller than 0.5”x0.5” are not useful since it reduces the accuracy recognition.

2.4.3. 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. These sensors tend to be very bulky and contain moving parts making them suitable only for law enforcement and access control applications.

2.4.4.Thermal Sensors:

These are made up of pyroelectric 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.

2.5 Fingerprint Features

The pixel intensity values in the fingerprint image are typically not invariant over the time of capture and there is a need to determine salient features of the input fingerprint image that can discriminate between identities as well as remain invariant for a given individual . Thus the problem of representation is to determine a measurement (feature) space in which the fingerprint images belonging to the same finger form a compact cluster and those belonging to different fingers occupy different portions of the space (low intra-class variation and high inter-class variations).

A good fingerprint representation should have the following two properties: saliency and suitability. Saliency means that a representation should contain distinctive information about the

fingerprint. Suitability means that the representation can be easily extracted, stored in a compact fashion, and be useful for matching. Saliency and suitability properties are not generally correlated. A salient representation is not necessarily a suitable representation.

Image-based representations, constituted by raw pixel intensity information, are prevalent among the recognition systems using optical matching and correlation- based matching. However, the utility of these systems may be limited due to factors such as brightness variations, image quality variations, scars, and large global distortions present in the fingerprint image. Furthermore, an image-based representation requires a considerable amount of storage. On the other hand, an image-based representation preserves the maximum amount of information, makes fewer assumptions about the application domain, and therefore has the potential to be robust to wider varieties of fingerprint images. For instance, it is extremely difficult to extract robust features from a (degenerate) finger devoid of any ridge structure.

The fingerprints, when analyzed at different scales, exhibits different types of features. At the global level, the ridge line flow describes a pattern similar to one of those shown in Figure 1.5. Singular points, called loop and delta (denoted as squares and triangles, respectively in Figure 1.5), are a sort of control points around which the ridge lines are "wrapped". Singular points and coarse ridge line shape are very important for fingerprint classification and indexing but their distinctiveness is not sufficient for accurate matching. External fingerprint shape, orientation image, and frequency image also belong to the set of features that can be detected at the global level.

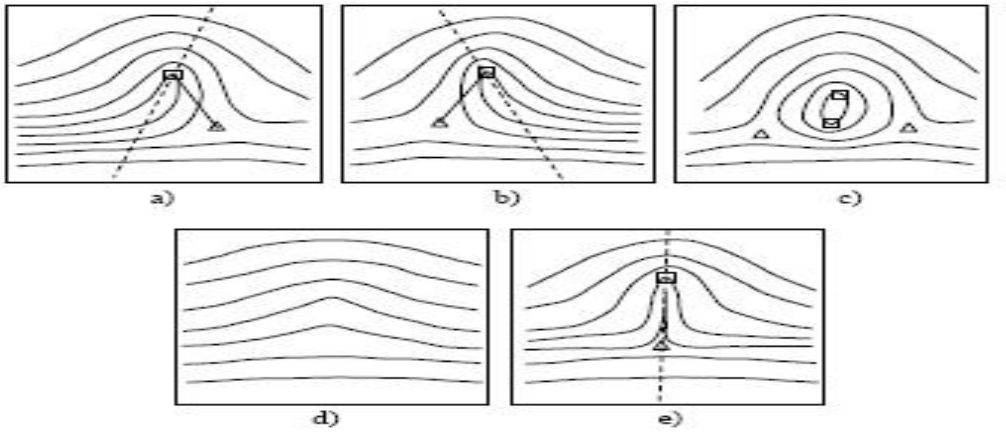
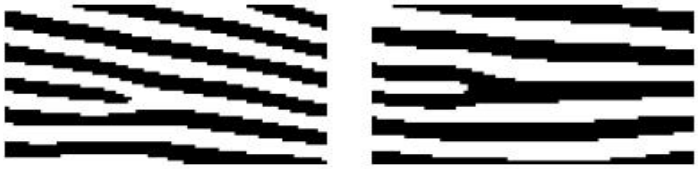


Figure 2.3 Fingerprint patterns as they appear at a coarse level: a) left loop; b) right loop; c) whorl; d) arch; and e) tented arch; squares denote loop-type singular points, and triangles delta type singular points.

At the local level, a total of 150 different local ridge characteristics, called minute details, have been identified .These local ridge characteristics depend heavily on the impression conditions and quality of fingerprints and are rarely observed in fingerprints. The two most prominent ridge characteristics, called minutiae (see Figure 1.6), are: ridge termination and ridge bifurcation.

A ridge ending is defined as the ridge point where a ridge ends abruptly. A ridge bifurcation is defined as the ridge point where a ridge forks or diverges into branch ridges.



(a) Ridge ending **(b) Bifurcation**

Figure 2.4: Example of a ridge ending and a bifurcation.

Minutiae in fingerprints are generally stable and robust to fingerprint impression conditions. Although a minutiae-based representation is characterized by a high saliency, a reliable automatic minutiae extraction can be problematic in low- quality fingerprints.

At the very-fine level, intra-ridge details can be detected. These are essentially the finger sweat pores (see Figure 1.7) whose position and shape are considered highly distinctive. However, extracting pores is feasible only in high-resolution fingerprint images (e.g., 1000 dpi) of good quality and therefore this kind of representation is not practical for most applications.

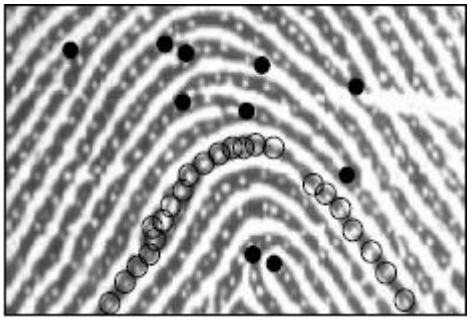


Figure 2.5 Minutiae (black-filled circles) in a portion of fingerprint image; sweat pores (empty circles) on a single ridge line.

CHAPTER 3

Project Overview

3.1 System Description

A fingerprint recognition system constitutes of fingerprint acquiring device, pre-processing of the features required for matching, feature extraction, post-processing of those features and matching with the templates present in the database. Pre-processing of the image includes histogram equalization, enhancement using FFT, binarization , ridge direction and detection of ROI (region of Interest). The steps of Feature Extraction are thinning, enhanced thinning, removal of spurious minutiae and extraction of minutiae. Post-processing includes numbering of true minutiae and saving these true minutiae as a template in the database for future use.

Now these steps will be discussed in the following sections.

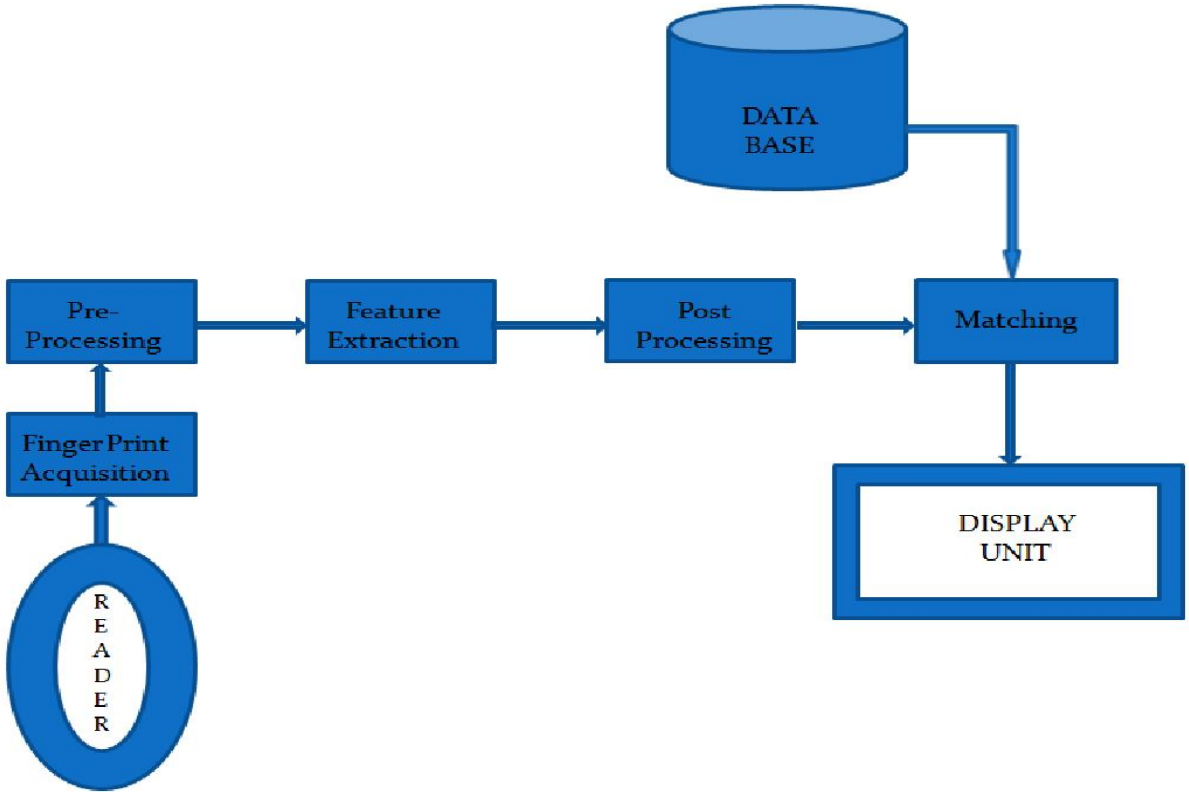


Figure 3.1 System Block Diagram

3.2 Acquisition of Fingerprint Image

There are two basic methods of acquiring a fingerprint image: inked (offline) and live scan (inkless). An inked fingerprint image is typically acquired by a trained professional obtaining an impression of an inked finger on a paper and the impression is then scanned using a flat bed document scanner. A livescan image, is acquired by sensing the tip of the finger directly, using a sensor that is capable of digitizing the fingerprint on contact. A special kind of offline images, are latent fingerprints which are found at crime scenes. The oily nature of the skin results in the impression of a fingerprint being deposited on a surface that is touched by a finger. Certain chemical techniques are applied to lift these latent prints from the surface. There are a number of livescan sensing mechanisms (e.g. optical frustrated total internal reflection, capacitive, thermal, pressurebased, ultrasound, etc.) that can be used to detect the ridges and valleys present in the fingertip.

Today's computational power is centered around using high speed processing devices like digital computers. The main parameters characterizing a digital fingerprint image are: resolution, area, number of pixels, geometric accuracy, contrast, and geometric distortion.

Fingerprint acquisition is the first and most important step of our project. For acquisition purposes we used device "Cross Match 300 LC USB scanner". It is a type of a live scan scanner used at the Universal Serial Bus port of computer.

3.3 Image Pre-processing

3.3.1 Enhancement and Histogram Equalization

A fingerprint image is one of the noisiest of image types. This is due predominantly to the fact that fingers are our direct form of contact for most of the manual tasks we

perform: finger tips become dirty, cut, scarred, creased, dry, wet, worn, etc. The image enhancement step is designed to reduce this noise and to enhance the definition of ridges against valleys. Fingerprint Image enhancement is to make the image clearer for easy further operations. Since the fingerprint images acquired from sensors or other Medias are not assured with perfect quality, those enhancement methods, for increasing the contrast between ridges and furrows and for connecting the false broken points of ridges due to insufficient amount of ink, are very useful for keep a higher accuracy to fingerprint recognition.

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information.

The enhanced image after FFT requires the improvements because it might connect some falsely broken points on ridges and to remove some spurious connections between ridges which require later detection and removal

3.3.2 Binarization

Fingerprint Image Binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows are white.

A locally adaptive binarization method is performed to binarize the fingerprint image. Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs

3.3.3 ROI extraction by Morphological operations

Two Morphological operations called ‘OPEN’ and ‘CLOSE’ are adopted. The ‘OPEN’ operation can expand images and remove peaks introduced by background noise. The ‘CLOSE’ operation can shrink images and eliminate small cavities.

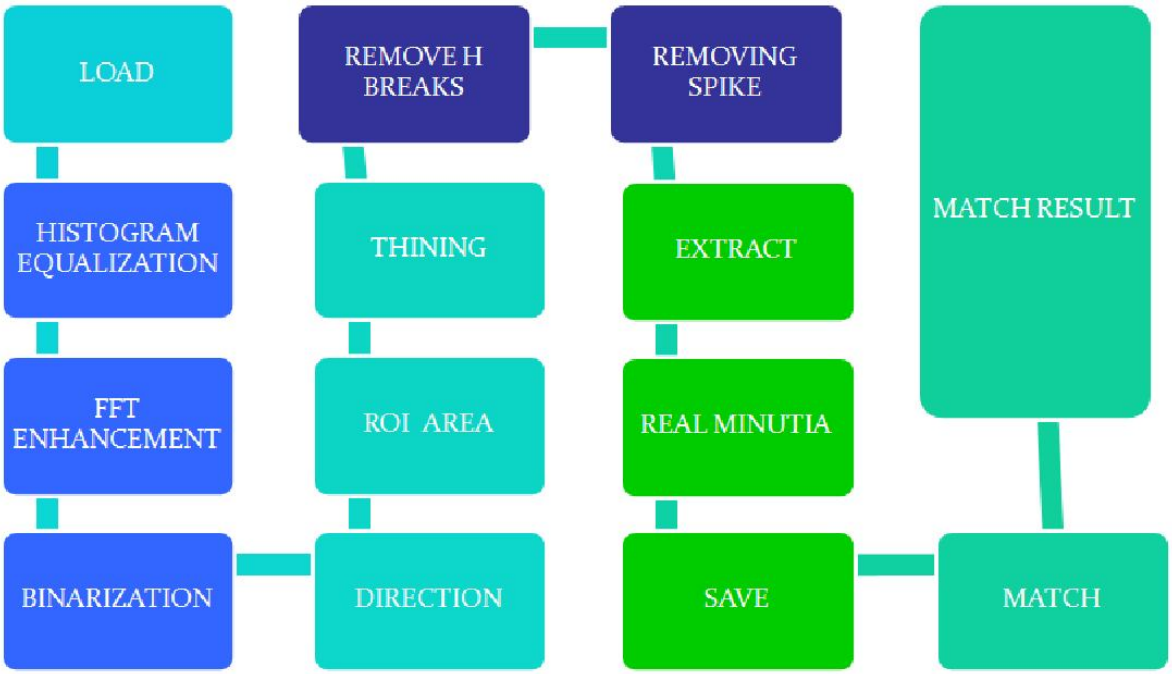


Figure 3.2 Block Diagram of Simulation

3.4 Minutiae Extraction

3.4.1 Fingerprint Ridge Thinning

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. It uses an iterative, parallel thinning algorithm. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3). And finally removes all those marked pixels after several scans. In my testing, such an iterative, parallel thinning algorithm has bad efficiency although it can get an ideal thinned ridge map after enough scans. [2] uses a one-in-all method to extract thinned ridges from gray-level fingerprint images directly. Their method traces along the ridges having maximum gray intensity value.

3.5 Minutiae Post-processing

3.5.1 False Minutiae Removal

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

3.5.2 Minutiae Matching

Given two set of minutia of two fingerprint images, the minutia match algorithm determines whether the two minutia sets are from the same finger or not.

An alignment-based match algorithm partially derived from the [1] is used in our project. It includes two consecutive stages: one is alignment stage and the second is match stage.

1. Alignment stage. Given two fingerprint images to be matched, choose any one minutia from each image, calculate the similarity of the two ridges associated with the two referenced minutia points. If the similarity is larger than a threshold, transform each set of minutia to a new coordination system whose origin is at the referenced point and whose x-axis is coincident with the direction of the referenced point.

2. Match stage: After we get two set of transformed minutia points, we use the elastic match algorithm to count the matched minutia pairs by assuming two minutia having nearly the same position and direction are identical.

CHAPTER 4

Fingerprint Acquisition

4.1 Introduction

There are two basic methods of acquiring a fingerprint image: inked (offline) and live scan (inkless). An inked fingerprint image is typically acquired by a trained professional obtaining an impression of an inked finger on a paper and the impression is then scanned using a flat bed document scanner. A livescan image, is acquired by sensing the tip of the finger directly, using a sensor that is capable of digitizing the fingerprint on contact. A special kind of offline images, are latent fingerprints which are found at crime scenes. The oily nature of the skin results in the impression of a fingerprint being deposited on a surface that is touched by a finger. Certain chemical techniques are applied to lift these latent prints from the surface. There are a number of livescan sensing mechanisms (e.g. optical frustrated total internal reflection, capacitive, thermal, pressurebased, ultrasound, etc.) that can be used to detect the ridges and valleys present in the fingertip.

Today's computational power is centered around using high speed processing devices like digital computers. The main parameters characterizing a digital fingerprint image are: resolution, area, number of pixels, geometric accuracy, contrast, and geometric distortion.

4.2. Image Capture Devices

We organize image capture devices into three categories: optical, solid-state, and other. There is yet another category, fingerprint acquisition via inking, which is the traditional

mode of criminal fingerprint capture. It is evident that this is inappropriate for fingerprint verification due to the inconvenience involved with ink, the need for subsequent digitization, and perhaps the stigma of this type of capture. The type of image acquisition for fingerprint verification is also called "live-scan fingerprint capture". Optical fingerprint capture devices have the longest history and use of these categories, dating back to the 1970s. These operate on the principal of frustrated total internal reflection (FTIR). A laser light illuminates a fingerprint placed on a glass surface (platen). The reflectance of this light is captured by a CCD array (solid-state camera). The amount of reflected light is dependent upon the depth of ridges and valleys on the glass and the finger oils between the skin and glass. The light that passes through the glass into valleys is not reflected to the CCD array, whereas light that is incident upon ridges on the surface of the glass (more precisely, the finger oils on the ridges that constitute the ridge-to-glass seal) is reflected. Innovations in optical devices have been made recently, primarily in an effort to reduce the size of these devices. Whereas an optical sensor was housed in a box about 6x3x6 inches as recently as the mid-1990s, smaller devices have recently appeared that are in the order of 3x1x1 inches. Different optical technologies than FTIR have also been developed. For instance, fiber optics has been proposed to capture the fingerprint. A bundle of optical fibers is aimed perpendicularly to the fingerprint surface. These illuminate the fingerprint and detect reflection from it to construct the image. Another proposal is a surface containing an array of microprisms mounted upon an elastic surface. When a fingerprint is applied to the surface, the different ridge and valley pressures alter the planar surfaces of the microprisms. This image is captured optically via the reflected light (or absence of it) from the microprisms. Solid-state sensors have appeared on the marketplace recently, though they have been proposed in the patent literature for almost two decades. These are microchips containing a surface that images the fingerprint via one of several technologies. Capacitive sensors have been designed to capture the fingerprint via electrical measurements. Capacitive devices incorporate a sensing surface composed of an array of about 100,000 conductive plates over which is a dielectric surface. When the user places a finger on this surface, the skin constitutes the other side of an array of capacitors. The measure of voltage at a capacitor drops off with the distance between plates, in this case the distance to a ridge (closer) or a valley (further). Pressure-sensitive surfaces have been proposed where the top layer is of an elastic, piezoelectric material to conform to

the topographic relief of the fingerprint and convert this to an electronic signal. Temperature sensitive sensors have been designed to respond to the temperature differential between the ridges touching the surface of the device and the valleys more distant from them.

Ultrasonic scanning falls into the final category of fingerprint capture technologies. An ultrasonic beam is scanned across the fingerprint surface much like laser light for optical scanners. In this case, it is the echo signal that is captured at the receiver, which measures range, thus ridge depth. Ultrasonic imaging is less affected by dirt and skin oil accumulation than is the case for optical scanning, thus the image can be a truer representation of the actual ridge topography. Two of the three most important factors that will decide when fingerprint verification will be commercially successful in the large-volume personal verification market are low cost and compact size.

A functionality that has not been available before solid-state sensors is locally adjustable, software-controlled, automatic gain control (AGC). For most optical devices, gain can be adjusted only manually to change the image quality. Some solid-state sensors, however, offer the capability to automatically adjust the sensitivity of a pixel or row or local area to provide added control of image quality. AGC can be combined with feedback to produce high quality images over different conditions. For instance, a low-contrast image (e.g., dry finger) can be sensed and the sensitivity increased to produce an image of higher contrast on a second capture. With the capability to perform local adjustment, a low-contrast region in the fingerprint image can be detected (e.g., where the finger is pressed with little pressure) and sensitivity increased for those pixel sensors on a second capture.

Optical scanners also have advantages. One advantage of larger models is in image capture size. It is costly to manufacture a large, solid-state sensor, so most current solid-state products have sub-1 inch square image area, whereas optical scanners can be 1 inch or above. However, this advantage is not true for some of the smaller optical scanners. The small optical scanners also have smaller image capture areas because a larger area would require a longer focal length, thus larger package size. Optical scanners are subject to linear distortion at the image edges when larger image capture area is combined with smaller package size.

4.3 Cross Match Verifier 300 LC USB Device

Fingerprint acquisition is the first and most important step of our project. For acquisition purposes we used device “Cross Match 300 LC USB scanner”. It is a type of a live scan scanner used at the Universal Serial Bus port of computer.

Cross Match Verifier 300 LC USB is an optical USB 2.0 fingerprint scanner. The scanner features a large 1.2" x 1.2" platen area, fast frame rate and an infrared filter to improve ambient light rejection. Verifier 300 LC is suitable for high-traffic desktop applications, as well as for integrating into kiosks or similar machines as it has a lightweight lexan case and a rugged sensor.

The Verifier 300 LC (Lexan Case) is a single fingerprint capture device that delivers accurate and reliable results for identification, verification, and registration programs. Cross Match's Verifier products have been deployed in more than 5,000 applications around the world in a wide array of projects including Child ID programs, physical and logical access control projects, border entry/exit control and national ID and registration programs.

The Verifier 300 LC is available with a universal serial bus (USB) and is easily integrated into high demand applications, such as school time and attendance, hospital patient record verification and correctional facility access control. A kiosk-ready version of the Verifier 300 LC is also available to simplify integration.

The Crossmatch Verifier product line is known for superior image quality, durability, and low maintenance requirements. Verifiers are ideal for demanding applications, border and port control, hospital patient record verification, correctional facility access control and desktop enrollments.

Software developers can use this device with various Fingerprint SDKs to develop customized fingerprint matching software solutions. This USB fingerprint scanner is widely used for fingerprint recognition, fingerprint verification, fingerprint authentication & fingerprint scanning applications. Verifier 300 USB fingerprint scanner is an ideal reader for most fingerprint security systems.

Figure 4.1`: Cross Match Verifier 300 LC USB Device

4.3.1 Features of Cross Match Verifier 300 LC USB Device

Some features of Cross Match Verifier 300 LC USB Device are discussed as below.

- Generous platen area (1.2" x 1.2")
- USB connection eliminates the need for an Image Capture Board
- Lightweight (1lb) (.45 kg)

- Available with integrated USB cable
- Low maintenance requirements
- Durable and portable
- Consistent forensic-quality flat fingerprint images
- Improved illumination can capture forensic-quality fingerprints from stained, marked or dark fingers
- Patented a spherical lenses
- I/R filter to improve ambient light rejection
- Supports: Fingerprint recognition, fingerprint verification, fingerprint authentication, fingerprint scanning & fingerprint matching applications.

Specifications of Cross Match 300 LC USB Device are summarized in Table 4.1 as shown below.

Resolution	500 ppi ± 1%
Linearity and Rectilinearity	Less than one pixel (average)
Platen Area	1.2" x 1.2" (30.5 mm x 30.5 mm)

Output (Digital)	Universal Serial Bus (USB 2.0)
Power (Digital)	5 V DC (supplied by PC)
Operating Temperature Range	0^{o}F to 104^{o}F (-18^{o}C to 40^{o}C)
Humidity Range	10-90% non-condensing, splash-resistant
Weight	1 pound (.45 kg)
Dimensions (H x L x W)	2.45" x 6.38" x 3.25" (62 mm x 162 mm x 83 mm)
Operating System	Windows XP/2000

Table 4.1 : Specifications of Cross Match 300 LC USB Device

4.3.2 System Requirements

System requirements of Cross Match Verifier LC USB 300 Device are as mentioned below.

1. One of the following operating systems : Windows XP, Windows 2000
2. USB SDK V4.0 or later
3. 1 GHz or higher Pentium IV compatible CPU
4. 256 MB RAM
5. 50 MB of available disk space

4.3.3 Applications

It is useable in many applications. Some of them are listed below.

1. Biometric Point of Sale Machines
2. Fingerprint Based Computer Login
3. Biometric Computer Logon
4. Web Based Fingerprint Recognition Systems
5. Fingerprint Access Control
6. Fingerprint Time and Attendance

7. Domain Controller

8. Biometric File Encryption

9. PC/workstation security

10. Network/enterprise security

11. Internet content security

12. E-commerce

13. Electronic transactions

CHAPTER 5

Image Enhancement

5.1 Fingerprint Image Enhancement

A fingerprint image is one of the noisiest of image types. This is due predominantly to the fact that fingers are our direct form of contact for most of the manual tasks we perform: finger tips become dirty, cut, scarred, creased, dry, wet, worn, etc. The image enhancement step is designed to reduce this noise and to enhance the definition of ridges against valleys. Fingerprint Image enhancement is to make the image clearer for easy further operations. Since the fingerprint images acquired from sensors or other Medias are not assured with perfect quality, those enhancement methods, for increasing the contrast between ridges and furrows and for connecting the false broken points of ridges due to insufficient amount of ink, are very useful for keep a higher accuracy to fingerprint recognition.

Two operations of image enhancement are discussed here, out of these two the latter case is adopted for my project with less computational complexity and increased efficiency.

The first operation for this purpose is combination of the adaptive matched filter and adaptive thresh holding. There is a useful side to fingerprint characteristics as well. That is the "redundancy" of parallel ridges. Even though there may be discontinuities in particular ridges, one can always look at a small, local area of ridges and determine their flow. We can use this "redundancy of information" to design an adaptive, matched filter. This filter is applied to every pixel in the image. Based on the local orientation of the ridges around each pixel, the matched filter is applied to enhance ridges oriented in the same direction as those in the same locality, and decrease anything oriented differently. The latter includes noise that may be joining adjacent ridges, thus flowing perpendicular to the local flow. These incorrect "bridges" can be eliminated by use of the matched filter. Thus, the filter is adaptive because it orients itself to local ridge flow. It is matched because it should enhance – or match – the ridges and not the noise.

In second operation two Methods are adopted in my fingerprint verification system: the first one is Histogram Equalization; the next one is Fourier Transform.

5.2 Histogram Equalization:

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. The original histogram of a fingerprint image has the bimodal type [Figure 5.1], the histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced [Figure 5.2].

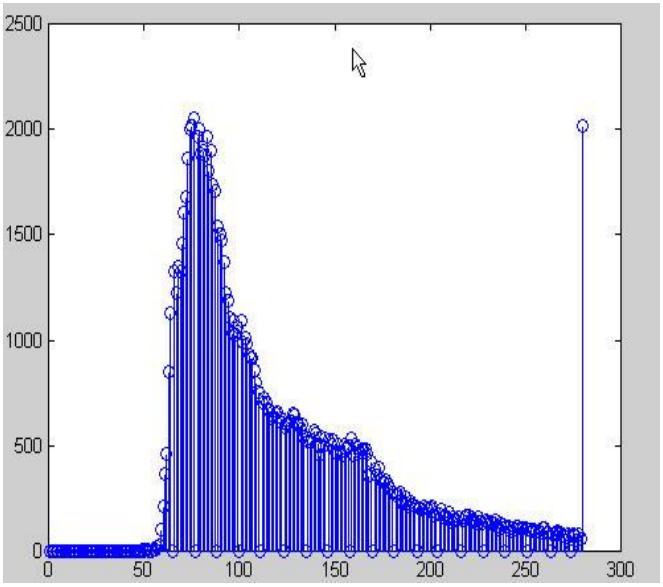


Figure 5.1 the Original histogram of a fingerprint image

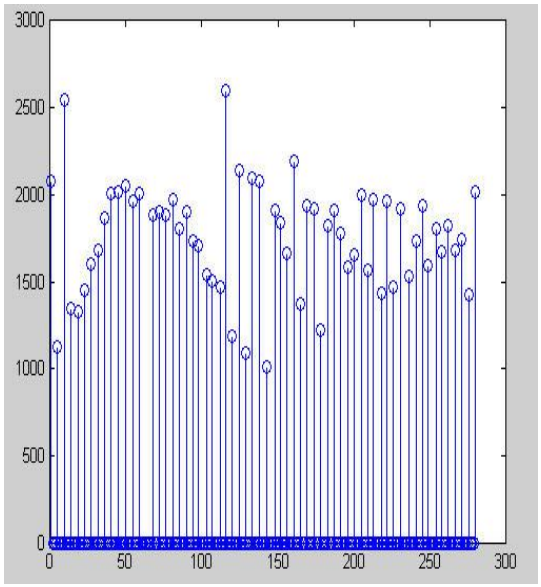


Figure 5.2 Histogram after the Histogram Equalization

The right side of the following figure [Figure 5.3] is the output after the histogram equalization.

Figure 5.3 Histogram Enhancement. Original Image (Left). Enhanced image (Right)

5.3 Fingerprint Enhancement by Fourier Transform

We divide the image into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to:

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times \exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \quad \ldots\ldots\ldots\ldots 5.1$$

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

In order to enhance a specific block by its dominant frequencies, we multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original FFT = abs(F(u,v)) = |F(u,v)|.

Get the enhanced block according to

$$g(x,y) = F^{-1}\left\{F(u,v) \times |F(u,v)|^{k}\right\} \quad \ldots\ldots\ldots\ldots 5.2$$

where $F^{-1}(F(u,v))$ is done by:

$$f(x,y)=\frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}F(u,v)\times\exp\left\{j2\pi\times\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\} \quad \ldots\ldots\ldots\ldots 5.3$$

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

The k in formula 5.2 is an experimentally determined constant, which we choose k=0.45 to calculate. While having a higher "k" improves the appearance of the ridges, filling up small holes in ridges, having too high a "k" can result in false joining of ridges. Thus a termination might become a bifurcation. Figure 5.4 presents the image after FFT enhancement.

Figure 5.4 Fingerprint enhancement by FFT
Enhanced image (left), Original image (right)

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 shown image at the left side of figure 5.4 is also processed with histogram equalization after the FFT transform. The side effect of each block is obvious but it has no harm to the further operations because I find the image after consecutive binarization operation is pretty good as long as the side effect is not too severe.

CHAPTER 6

Finger Print Image Preprocessing

6.1 Fingerprint Image Binarization

Fingerprint Image Binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows are white.

A locally adaptive binarization method is performed to binarize the fingerprint image. Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs [Figure 6.1].

Figure 6.1 the Fingerprint image after adaptive binarization
Binarized image (left), Enhanced gray image (right)

6.2 Fingerprint Image Segmentation

In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information. Then the bound of the remaining effective area is sketched out since the

minutias in the bound region are confusing with those spurious minutias that are generated when the ridges are out of the sensor.

To extract the ROI, a two-step method is used. The first step is block direction estimation and direction variety check [1], while the second is intrigued from some Morphological methods.

6.2.1 Block direction estimation

Estimate the block direction for each block of the fingerprint image with WxW in size (W is 16 pixels by default). The algorithm is:

1. Calculate the gradient values along x-direction (g_x) and y-direction (g_y) for each pixel of the block. Two Sobel filters are used to fulfill the task.
2. For each block, use Following formula to get the Least Square approximation of the block direction.

$$tg2ß = 2 \sum \sum (g_x * g_y) / \sum \sum (g_x^2 - g_y^2)$$ for all the pixels in each block.

The formula is easy to understand by regarding gradient values along x-direction and y-direction as cosine value and sine value. So the tangent value of the block direction is estimated nearly the same as the way illustrated by the following formula.

$$tg2\theta = 2\sin\theta \cos\theta / (\cos^2\theta - \sin^2\theta)$$

After finished with the estimation of each block direction, those blocks without significant information on ridges and furrows are discarded based on the following formulas:

$$E = \{2 \sum \sum (g_x * g_y) + \sum \sum (g_x^2 - g_y^2)\} / W*W*\sum \sum (g_x^2 + g_y^2)$$

For each block, if its certainty level E is below a threshold, then the block is regarded as a background block. The direction map is shown in the following diagram. We assume there is only one fingerprint in each image.

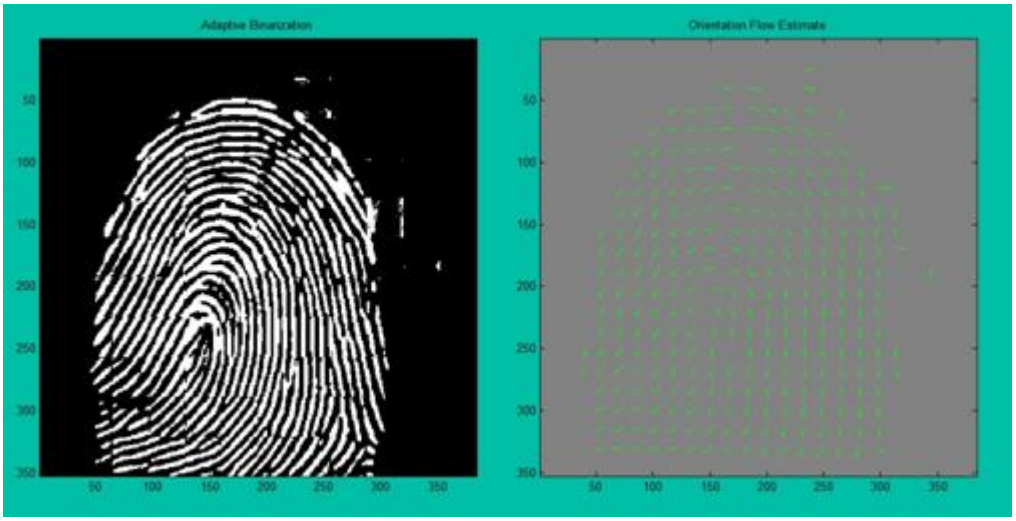


Figure 6.2 Direction map.
Binarized fingerprint (left), Direction map (right)

6.2.2 ROI extraction by Morphological operations

Two Morphological operations called 'OPEN' and 'CLOSE' are adopted. The 'OPEN' operation can expand images and remove peaks introduced by background noise [Figures 6.3a, 6.3b, 6.3c, 6.3d]. The 'CLOSE' operation can shrink images and eliminate small cavities [Figure 6.3].

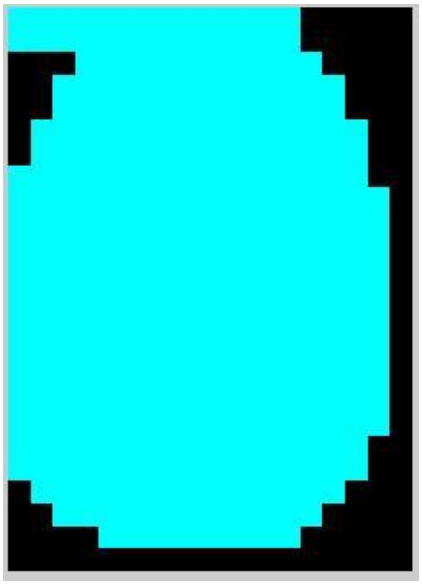


Figure 6.3a Original Image Area

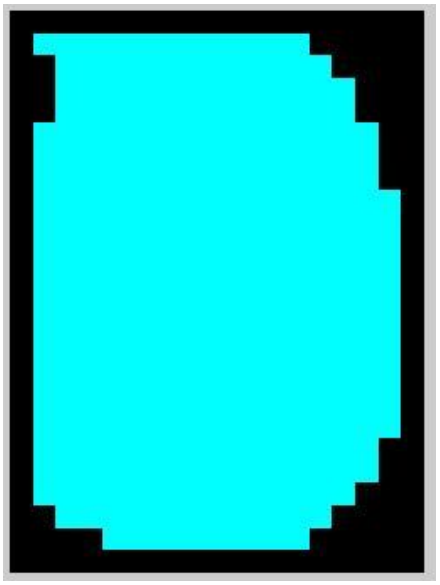


Figure 6.3b After CLOSE operation

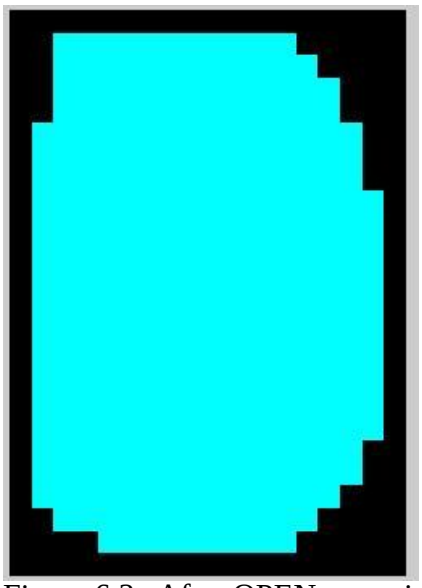


Figure 6.3c After OPEN operation

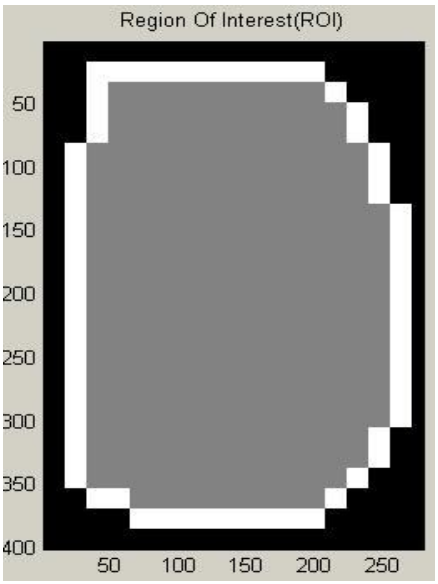


Figure 6.3d ROI + Bound

Figure 6.3d shows the interest fingerprint image area and its bound. The bound is the subtraction of the closed area from the opened area. Then the algorithm throws away those leftmost, rightmost, uppermost and bottommost blocks out of the bound so as to get the tightly bounded region just containing the bound and inner area.

CHAPTER 7

Feature Extraction

7.1 Fingerprint Ridge Thinning Techniques

Thinning is the process of reducing the thickness of each line of patterns to just a single pixel width. The requirements of a good thinning algorithm with respect to a fingerprint are:

1. The thinned fingerprint image obtained should be of single pixel width with no discontinuities.
2. Each ridge should be thinned to its centre pixel.
3. Noise and singular pixels should be eliminated.
4. No further removal of pixels should be possible after completion of thinning process.

7.1.1 Parallel thinning algorithm

[13] Uses an iterative, parallel thinning algorithm. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3). And finally removes all those marked pixels after several scans. Parallel thinning algorithm:

1) 2=<N(p1)<=6 T(p1) = 1

p2 * p4 * p6 = 0 p4 * p6 * p8 = 0

2) 2=< N(p1) <= 6 T(p1) = 1

p2 * p4 * p8 = 0 p2 * p6 * p8 = 0

P9	P2	P3
P8	P1	P4
P7	P6	P5

N(p) sum of Neighbors

T(p) Transition sum from 0 to 1 and 1 to 0

7.1.2 Thinning from Gray-level

[14] Uses a one-in-all method to extract thinned ridges from gray-level fingerprint images directly. Their method traces along the ridges having maximum gray intensity value. However, binarization is implicitly enforced since only pixels with maximum gray intensity value are remained. The advancement of each trace step still has large computation complexity although it does not require the movement of pixel by pixel as in other thinning algorithms.

7.1.3 Morphological thinning

The Morphological thinning function in software does the thinning. With n = Inf, thins objects to lines. It removes pixels so that an object without holes shrinks to a minimally connected

stroke, and an object with holes shrinks to a connected ring halfway between each hole and the outer boundary. When used with the 'thin' option, bw morphological uses the following algorithm:

1. Divide the image into two distinct subfields in a checkerboard pattern.
2. In the first sub iteration, delete pixel *p* from the first subfield if and only if the conditions G_1, G_2, and G_3 are all satisfied.
3. In the second sub iteration, delete pixel *p* from the second subfield if and only if the conditions G_1, G_2, and G_3' are all satisfied.

Condition G1:

$$X_H(p) = 1$$

where

$$X_H(p) = \sum_{i=1}^{4} b_i$$

$$b_i = \begin{cases} 1 \text{ if } x_{2i-1} = 0 \text{ and } (x_{2i} = 1 \text{ or } x_{2i+1} = 1) \\ 0 \text{ otherwise} \end{cases}$$

$x_1, x_2, \ldots, x_8$ are the values of the eight neighbors of p, starting with the east neighbor and numbered in counter-clockwise order.

Condition G2:

$$2 \le \min\{n_1(p), n_2(p)\} \le 3$$

where

$$n_1(p) = \sum_{k=1}^{4} x_{2k-1} \vee x_{2k}$$

$$n_2(p) = \sum_{k=1}^{4} x_{2k} \vee x_{2k+1}$$

Condition G3:

$$(x_2 \vee x_3 \vee \bar{x}_8) \wedge x_1 = 0$$

Condition G3':

$$(x_6 \vee x_7 \vee \bar{x}_4) \wedge x_5 = 0$$

The two sub iterations together make up one iteration of the thinning algorithm. When the user specifies an infinite number of iterations (n=Inf), the iterations are repeated until the image stops changing.

7.2 Selected Thinning Technique

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. In our testing parallel thinning algorithm has bad efficiency although it can get an ideal thinned ridge map after enough scans. The second method to extract thinned ridges from gray-level fingerprint images directly has large computation complexity although it does not require the movement of pixel by pixel as in other thinning algorithms. Thus the third method is bid out which uses the built-in Morphological thinning function. The thin ridge map is then filtered by other three morphological operations to remove some H breaks, isolated points and spikes.

7.3 Minutia Marking

After the fingerprint ridge thinning, marking minutia points is relatively easy. But it is still not a trivial task as most literatures declared because at least one special case evokes my caution during the minutia marking stage.

In general, for each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch [Figure 7.1]. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending [Figure7.2].

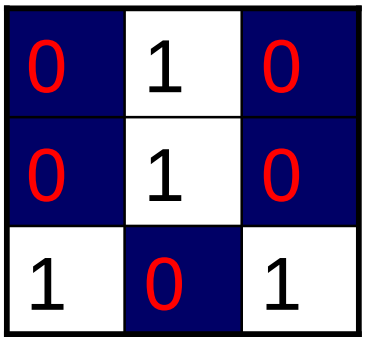


Figure7.1 Bifurcation

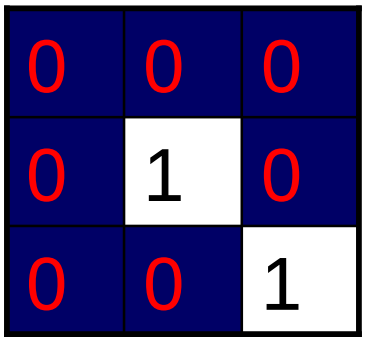


Figure 7.2 Termination

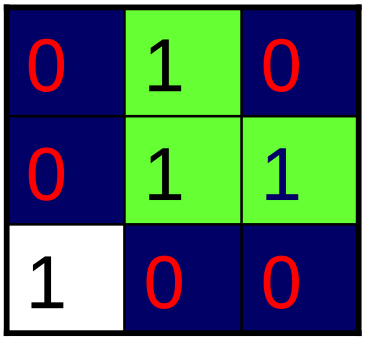


Figure 7.3 Triple counting branch

Figure 7.3 illustrates a special case that a genuine branch is triple counted. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3x3 window, so the two pixels will be marked as branches too. But actually only one branch is located in the small region. So a check routine requiring that none of the neighbors of a branch are branches is added.

Also the average inter-ridge width D is estimated at this stage. The average inter-ridge width refers to the average distance between two neighboring ridges. The way to approximate the D value is simple. Scan a row of the thinned ridge image and sum up all pixels in the row whose value is one. Then divide the row length with the above summation to get an inter-ridge width. For more accuracy, such kind of row scan is performed upon several other rows and column scans are also conducted, finally all the inter-ridge widths are averaged to get the D.

Together with the minutia marking, all thinned ridges in the fingerprint image are labeled with a unique ID for further operation. The labeling operation is realized by using the Morphological operation.

CHAPTER 8

Minutiae Purification

Minutiae purification, validation or sometimes refer to as the post processing is important as the amount of false minutiae extracted during the minutiae extraction phase, highly effects on the performance and efficiency of the matching algorithm. Noise, image artifacts created because of thinning process contribute towards the appearance of false minutiae. In minutiae purification stage, not only the false minutiae are detected and removed but the remaining minutiae are also validated to be genuine ones. Figure 8.1 shows typical false minutiae structures encountered most frequently. N. Ratha [29] has proposed a set of rules which operate on the skeleton image for the purpose of minutiae validation. Like a ridge ending that is connected to a bifurcation point and is less than a certain distance away is deleted. This rule corresponds to the removal of a spike structure shown in figure 8.1(d). A novel approach proposed by Tico [30] works in the neighborhood of minutiae in a thinned image by incorporating the validation of different type of minutiae in a single algorithm. It checks the validity of each minutia by scanning the local neighborhood around the minutiae and is able to cancel out the false minutiae on the basis of the configuration of the ridge pixels connected to the minutiae point under validation. This algorithm, however, only operates on the minutiae present inside the pattern area of the fingerprint image. Experiments have shown that the boundary effect and the contour minutiae are not removed with the above mentioned algorithm. To cater for the false minutiae on the borders and contour a simple method is often proposed in literature which is implemented in this work prior to the implementation of minutiae validation algorithm of Tico [30].

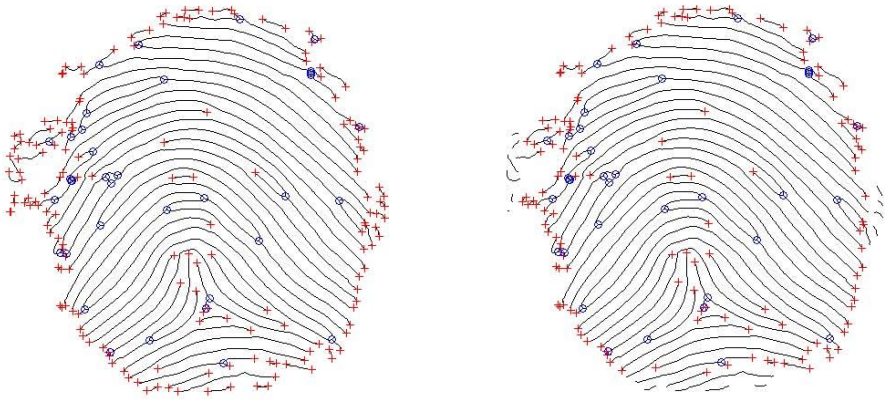
a) b) c) d)

Figure 8.1: False minutiae structures (a) Spur (b) Hole (c) Triangle (d) Spike

8.1 Border Minutiae Purification

Figure8.2(a) shows a skeleton of fingerprint image with ridge ending marked with a "plus" sign and bifurcations with a "circle". It is obvious that the number of false minutiae is alarmingly high. The false minutiae appearing on the border of the image are because of the impressions left by previous scans of fingerprints. These are removed by defining a threshold of distance and declaring all those minutiae point which lie closer to the border of the image. If this distance threshold is defined as thBD then the minutiae whose coordinates meet the following requirement are removed (Figure 8.2(b)). Where xi and yi are the x and y coordinates of the i^{th} minutiae, H and W are the height and width of the fingerprint image respectively.

$$x_i \le th_{BD} \mid y_i \le th_{BD} \mid x_i \ge W - th_{BD} \mid y_i \ge H - th_{BD} \rightarrow 8.1$$

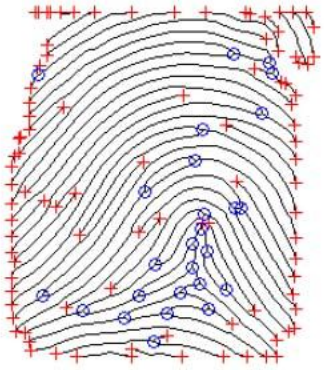


(a) (b)

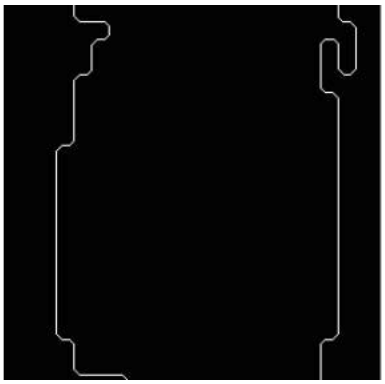
Figure 8.2: (a) Thinned fingerprint image showing all minutiae. (b) Minutiae closer to border has been removed.

8.2 Contour Minutiae Purification

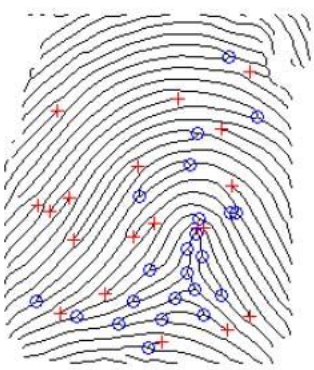
Image of the fingerprint, by its very nature, is oval shaped in nature. The contour of a fingerprint image is extracted by calculating the perimeter of the segmented fingerprint image. The segmented image of the fingerprint is a binary image containing foreground and background only. The foreground or the fingerprint area is represented by a binary "1" and the background is represented with a binary "0". A pixel is part of the perimeter if it is nonzero and it is connected to at least one zero valued pixel. The default connectivity is 4 for two dimensions; however MATLAB Image Processing Tool Box (IPT) function "bwperim" may be used with 8 connectivity (Figure 8.3(b)). This function returns a binary image containing only the perimeter pixels ("1" valued) of objects in the input binary image. For each pixel in binary contour image, the distance transform assigns a number that is the distance between that pixel and the nearest nonzero pixel. "bwdist" function of MATLAB Image Processing Tool Box uses the Euclidean distance metric by default and out puts the distance transform image (Figure 8.3(d)). Distance transform image has pixel values "0" exactly on the contour and the values of the pixels increases as the distance from the contour increases in both directions i.e. inwards and outwards. If xi and yi are the x and y coordinates of the i^{th} minutiae, thCD is threshold of distance from contour, and DT is distance transform of the contour image, then all those minutiae which satisfy condition DT (xi, yi) $\leq$ thCD are removed.

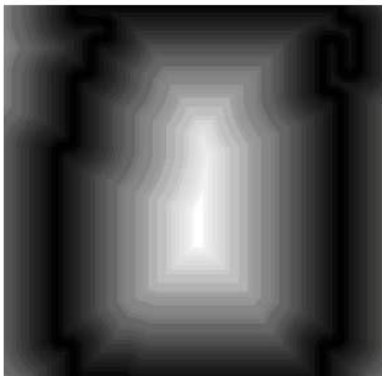


(a)



(b)



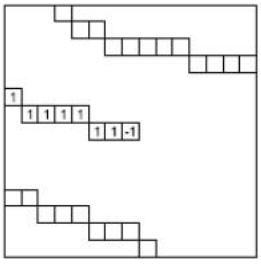


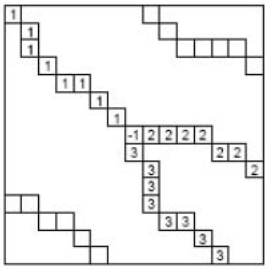
(c) (d)

Figure 8.3: Contour minutiae purification (a) Thinned image with false minutiae (b) Contour information of the same fingerprint (c) Thinned fingerprint image with contour minutiae cleaned (d) Distance Transform of the contour image of (b)

8.3 Minutiae Purification Based on Neighborhood

Despite having performed minutiae cleanup at the image border and contour, many false minutiae structure are still found inside the main pattern area of the fingerprint image. Most common type of false minutiae structures are shown in Figure 8.1. A novel approach for the validation of minutiae is the post processing algorithm. This approach not only segregates the false minutiae but also checks the validity of remaining genuine minutiae. It tests the validity of each minutiae point by scanning the skeleton image and examining the local neighborhood around the minutiae.





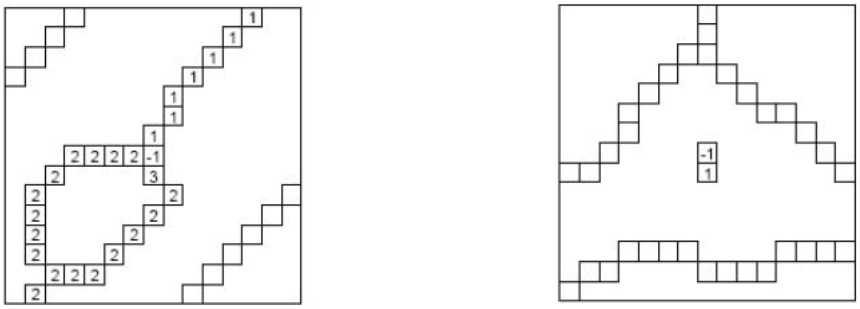
(a) (b)

Figure 8.4: Example of a valid ridge ending and bifurcation

The algorithm is applied separately on all candidate ridge ending and bifurcation minutiae. The common portion of the algorithm creates and initializes an image M of size W ×W , where M corresponds to a W ×W neighborhood centered on the candidate minutiae xi, yi in the skeleton image. Center pixel of M is set to "1" where as all other pixels are set to "0". W has been defined to be equal to twice the average ridge distance of the fingerprint image under consideration.

8.3.1 Post Processing for Ridge Bifurcation

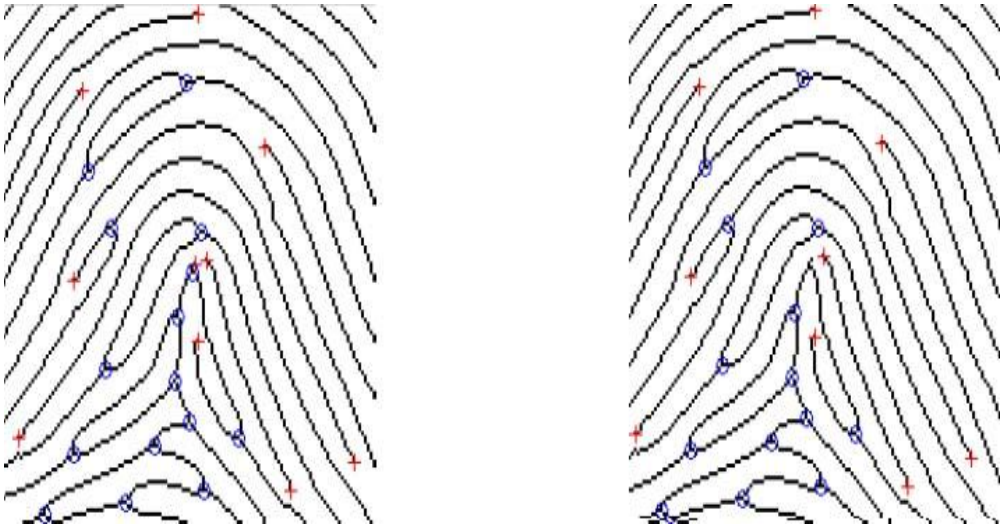
After initializing M, the algorithm searches for the 8connectivity from the center pixel (as in original thinned image) and label the three connected components (legs) with



(a) (b)

Figure 8.5 Example of canceling out false minutiae (a) for a hole (b) for a spur

"1", "2" and "3" in a manner as shown in figure 8.4(b). A full scan is made along the border of M and the number of transitions from 0 to 1 (T01), 0 to 2 (T02) and 0 to 3 (T03) are recorded. If T01 = 1andT02 = 1andT03 = 1 then the candidate minutiae is validated and the algorithm moves on to next bifurcation. Effectiveness of above algorithm is explained with the help of Figure 8.5(a) and 8.5(b) showing hole and spur structures being detected. A practical example is shown in Figure 8.6 in which the mentioned algorithm has successfully detected and cleaned two wrong minutiae formed because of a short ridge structure on a high curvature ridge.



(a) (b)

Figure 8.6 A practical example of canceling out false minutiae

8.4 False Minutia Removal

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

Seven types of false minutia are specified in following diagrams:

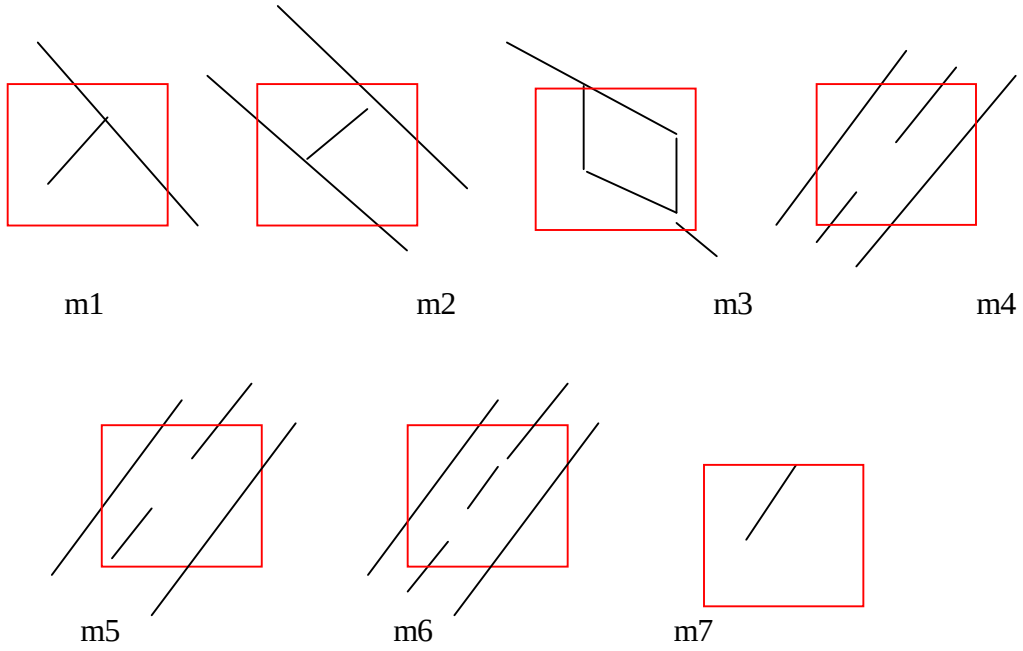


Figure 8.7 False Minutia Structures. m1 is a spike piercing into a valley. In the m2 case a spike falsely connects two ridges. m3 has two near bifurcations located in the same ridge. The two ridge broken points in the m4 case have nearly the same orientation and a short distance. m5 is alike the m4 case with the exception that one part of the broken ridge is so short that another termination is generated. m6 extends the m4 case but with the extra property that a third ridge is found in the middle of the two parts of the broken ridge. m7 has only one short ridge found in the threshold window.

[4] only handles the case m1, m4,m5 and m6. [9] and [2] have not false minutia removal by simply assuming the image quality is fairly good. [13] has not a systematic healing method to remove those spurious minutia although it lists all types of false minutia shown in Figure 8.7 except the m3 case.

Our procedures in removing false minutia are:

1. If the distance between one bifurcation and one termination is less than D and the two minutia are in the same ridge (m1 case). Remove both of them. Where D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.

2. If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations. (m2, m3 cases).

3. If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that no any other termination is located between the two terminations. Then the two terminations are regarded as false minutia derived from a broken ridge and are removed. (Case m4, m5, m6).

4. If two terminations are located in a short ridge with length less than D, remove the two terminations (m7).

Our proposed procedures in removing false minutia have two advantages. One is that the ridge ID is used to distinguish minutia and the seven types of false minutia are strictly defined comparing with those loosely defined by other methods. The second advantage is that the order of removal procedures is well considered to reduce the computation complexity. It surpasses the way adopted by [13] that does not utilize the relations among the false minutia types. For example, the procedure3 solves the m4, m5 and m6 cases in a single check routine. And after procedure 3, the number of false minutia satisfying the m7 case is significantly reduced.

8.5 Unify terminations and bifurcations

Since various data acquisition conditions such as impression pressure can easily change one type of minutia into the other, most researchers adopt the unification representation for both termination and bifurcation. So each minutia is completely characterized by the following parameters at last: 1) x-coordinate, 2) y-coordinate, and 3) orientation.

The orientation calculation for a bifurcation needs to be specially considered. All three ridges deriving from the bifurcation point have their own direction, [9] represents the bifurcation orientation using a technique proposed in [14]. [3] Simply chooses the minimum angle among the three anticlockwise orientations starting from the x-axis. Both methods cast the other two directions away, so some information loses. Here we propose a novel representation to break a bifurcation into three terminations. The three new terminations are the three neighbor pixels of

the bifurcation and each of the three ridges connected to the bifurcation before is now associated with a termination respectively [Figure 8.8].

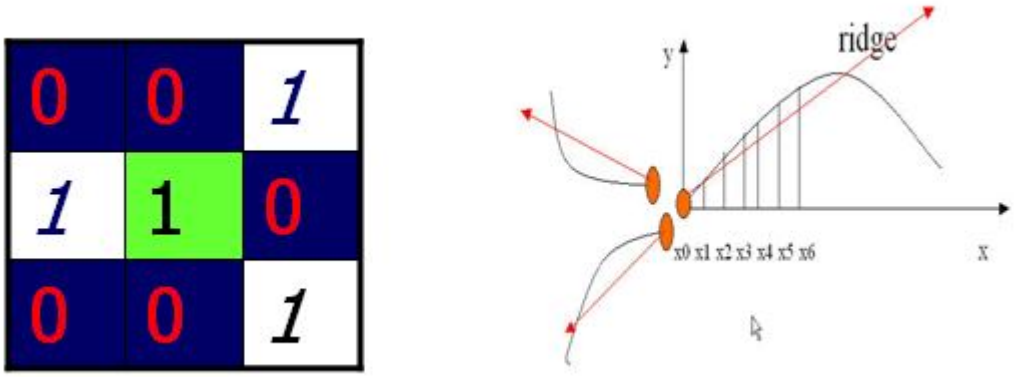


Figure 8.8 A bifurcation to three terminations
Three neighbors become terminations (Left)
Each termination has their own orientation (Right)

And the orientation of each termination (tx,ty) is estimated by following method:

Track a ridge segment whose starting point is the termination and length is D. Sum up all x-coordinates of points in the ridge segment. Divide above summation with D to get sx. Then get sy using the same way.

Get the direction from:

$$\text{atan}((sy-ty)/(sx-tx)).$$

CHAPTER 9

Minutiae Match

9.1 Minutiae Matching

Given two set of minutia of two fingerprint images, the minutia match algorithm determines whether the two minutia sets are from the same finger or not. An alignment-based match algorithm partially derived from the [1] is used in our project. It includes two consecutive stages: one is alignment stage and the second is match stage.

1. Alignment stage: Given two fingerprint images to be matched, choose any one minutia from each image; calculate the similarity of the two ridges associated with the two referenced minutia points. If the similarity is larger than a threshold, transform each set of minutia to a new coordination system whose origin is at the referenced point and whose x-axis is coincident with the direction of the referenced point.
2. Match stage: After we get two set of transformed minutia points, we use the elastic match algorithm to count the matched minutia pairs by assuming two minutia having nearly the same position and direction are identical.

9.1.1 Alignment Stage

1. The ridge associated with each minutia is represented as a series of x-coordinates (x_1, x_2…x_n) of the points on the ridge. A point is sampled per ridge length L starting from the minutia point, where the L is the average inter-ridge length. And n is set to 10 unless the total ridge length is less than 10*L.

2. For each fingerprint, translate and rotate all other minutia with respect to the reference minutia according to the following formula:

$$\begin{pmatrix} xi\_new \\ yi\_new \\ \theta i\_new \end{pmatrix} = TM * \begin{bmatrix} (xi - x) \\ (yi - y) \\ (\theta i - \theta) \end{bmatrix},$$

Where (x, y,θ) is the parameters of the reference minutia, and TM is

$$TM = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The following diagram illustrates the effect of translation and rotation:

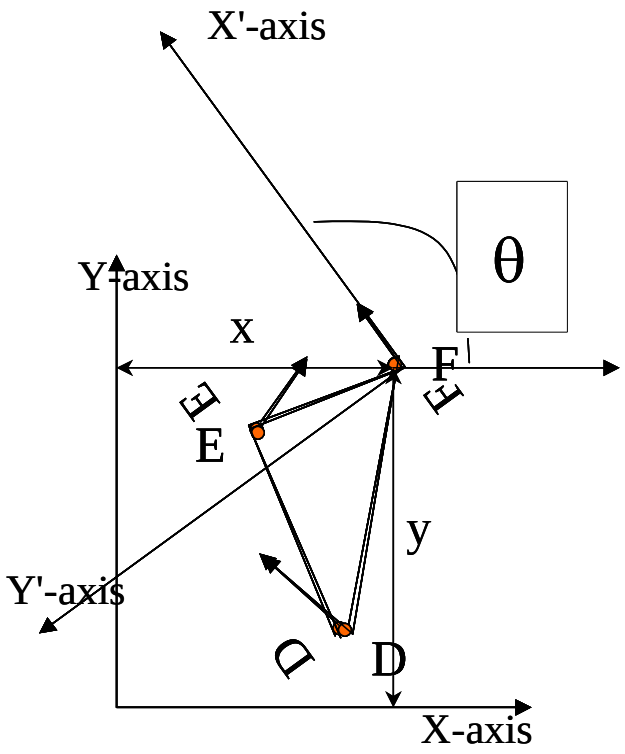


Fig9.1 The new coordinate system is originated at minutia F and the new x-axis is coincident with the direction of minutia F. No scaling effect is taken into account by assuming two fingerprints from the same finger have nearly the same size.

Our method to align two fingerprints is almost the same with the one used by [1] but is different at step 2. Lin's method uses the rotation angle calculated from all the sparsely sampled ridge points. Our method use the rotation angle calculated earlier by densely tracing a short ridge start from the minutia with length D. Since we have already got the minutia direction at the minutia

extraction stage, obviously my method reduces the redundant calculation but still holds the accuracy.

Also Lin's way to do transformation is to directly align one fingerprint image to another according to the discrepancy of the reference minutia pair. But it still requires a transform to the polar coordinate system for each image at the next minutia match stage. Our approach is to transform each according to its own reference minutia and then do match in a unified x-y coordinate. Therefore, less computation workload is achieved through our method.

9.2 Local Matching

As already have been discussed, different matching approaches have certain advantages/shortcomings. Keeping in view the utilization of the developed algorithm, similarity in the local structural neighborhood is considered for in depth study. The proposed algorithm is divided into levels depending upon the depth of local structure in consideration. At the course level, local or course matching is performed which is purely dependant on the local structural similarity only. Our proposed matching algorithm is divided into hierarchical structure consisting of local matching, validation and calculation of similarity score. Local matching stage of the algorithm picks i^{th} minutiae in template fingerprint along with it's k neighbors to form a secondary feature vector (SFV). This SFV is compared with the SFV of j^{th} minutiae of input fingerprint. The algorithm proceeds in this manner and compares all minutiae of template fingerprint against all minutiae of input fingering. A cost/feature distance is the outcome of a comparison between two minutiae/SFVs belonging to separate fingerprints. This comparison of SFVs is discussed in detail in the coming sections. First stage in local matching algorithm is to select minutiae in immediate neighborhood of central minutiae for the formation of a SFV.

9.2.1 Selection of Secondary Features

A simplified secondary feature is shown in Figure 9.2. The selection, order and the number of neighboring minutiae in a secondary feature vector is of paramount importance. In earlier approaches a fixed number of neighboring minutiae are considered in the immediate neighborhood for the formation of SFV, two in most of the cases. However,

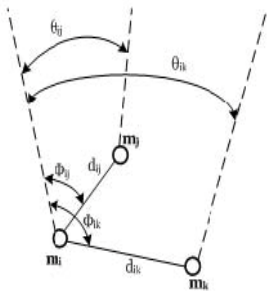
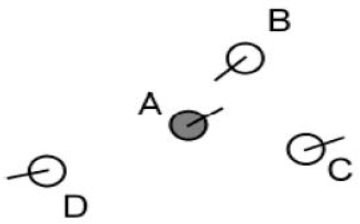


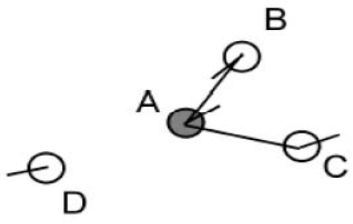
Fig9.2 Secondary features

the structure of a secondary feature changes significantly due to the addition of a false minutiae or missing minutiae closer to a central minutiae(see Figure 9.3). A spurious or missing minutiae causes the disappearance of a genuine secondary feature, while at the same time introduces a false secondary feature(Figure 9.3(c) and Figure 9.3(d)). This structural variation in a localized secondary feature vector is main contributor to the error cases of a matching algorithm especially when the number of minutiae on a fingerprint is less. Figure 9.3 shows a genuine secondary feature with 2 neighbors along with the effect of spurious and missing minutiae.

To address this problem a scheme based on the adaptive neighborhood grouping based on certain rules is proposed. We make a secondary feature vector having the contribution of p neighbors around a central minutiae by considering k nearest neighbors such that k > p. A similar approach has been proposed in [1] but they have used a



(a)



(b)

(c) (d)

Figure 9.3: (a) Four synthetic minutiae (b) A genuine secondary feature with 2 neighbors (c) False secondary feature because of spurious minutiae X (d) False secondary feature if a valid minutiae C is missing

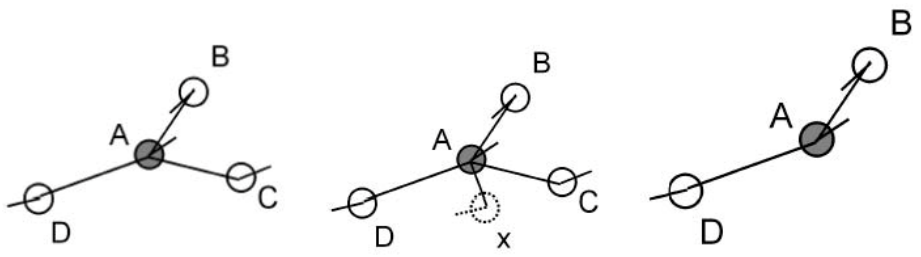
fixed number of p neighbors on the contrary we propose to adjust not only the value of p but also the value of k. This way for every minutiae in the fingerprint we can have h secondary feature vectors.

$$h = \binom{k}{p} = \frac{k!}{p! \times (k-p)!}$$

An example of a secondary feature vector with p = 2 is described in expression 9.1

$$[ri0, ri1, \theta i0, \theta i1, \varphi i0, \varphi i1, ni0, ni1, ti, t0, t1] \quad \ldots\ldots\ldots \quad (9.1)$$

Considering a total of M minutiae in a fingerprint image, the resulting number of secondary features would then be $M \times h$. By associating more secondary features to a central minutia in a permutated manner the influence of spurious and missing minutiae is almost reduced to nil in most of the cases as shown in Figure 9.4. Depending upon the size of the fingerprint in terms of number of minutiae, the value of k and p are adjusted accordingly. By doing experimentations we have come up to a heuristic rule for finding the number of minutiae in neighborhood and in secondary feature vector. When the number of minutiae in a fingerprint is more than 40, k is set to 6; if the number of minutiae is less than 20, then k is set to 10; otherwise the k is set to 8. p is set to half of k in every rule.



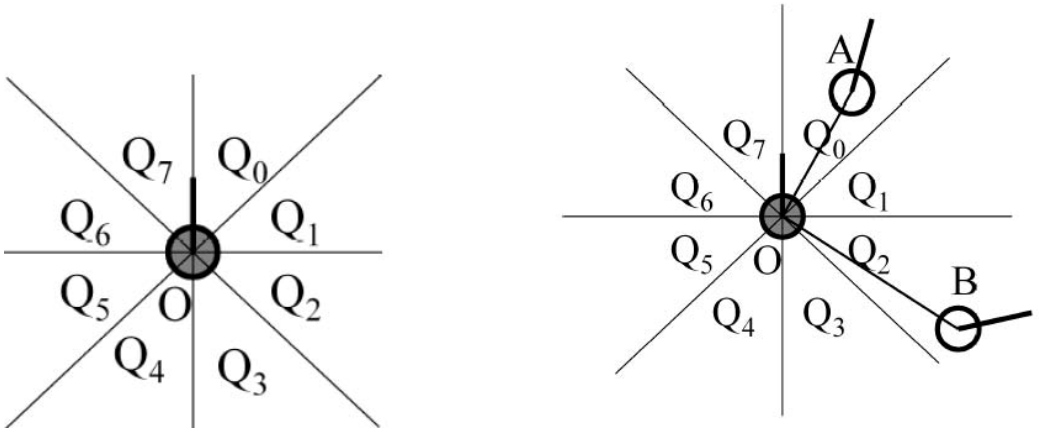
(a) (b) (c)

Figure 9.4: (a) Genuine secondary feature with p = 2 (b) Influence of spurious minutiae; secondary features remain intact(c) Influence of missing minutiae; part of genuine secondary features still available for matching

Placement of p neighbors in SFV is done by arranging them in the increasing order of their radial distance from the ridge direction of the central minutiae.

9.2.2 Indexing of Secondary Features

Every minutiae in a fingerprint is associated with an angle which is the direction of the ridge on which the minutiae is placed. This ridge direction is used to index the neighboring minutiae in 8 quadrants of 45 degrees each by aligning the quadrants with the ridge direction of the central minutiae. Secondary features formed as a result of the neighboring minutiae in quadrant number 1 (Q1) of the template image only needs to be matched against the secondary features in the Q1 of the central minutiae in a query image. However in order to cater for the nonlinear deformation in the fingerprint images, every secondary feature is labeled with the quadrant in which it resides in addition to the label of the nearby quadrant(see Figure 9.5). The purpose of indexing is to avoid time consuming and unnecessary matching of SFVs which do not correspond to the SFV of the mating minutiae in configuration(shape). In this manner while performing the matching, only those SFVs which fall in the same quadrant are taken to the next level and checked for their relative placement with respect to the tolerance boxes.



(a) (b)

Figure 9.5: (a) The eight quadrants Q0 to Q7 of a central minutiae aligned to its ridge direction (b) An example of secondary feature with the label Q0Q2, Q0Q3, Q1Q2 and Q1Q3

9.2.3 Tolerance Boxes

Distortions are inevitable when mapping a three dimensional fingertip onto a two dimensional scanner surface. Vertical forces, shear pressures and impression conditions contribute towards the distortion effect. A tolerance box is defined as a two dimensional box whose size, shape and placement is defined by three variables namely difference of orientations, distance and the angle of the line joining central and neighboring minutiae(see Figure 9.6). These tolerance boxes further localize the position of the input minutiae with respect to the template minutiae in same quadrant by coinciding both central minutiae. It checks if both the minutiae are placed close enough within the same quadrant.

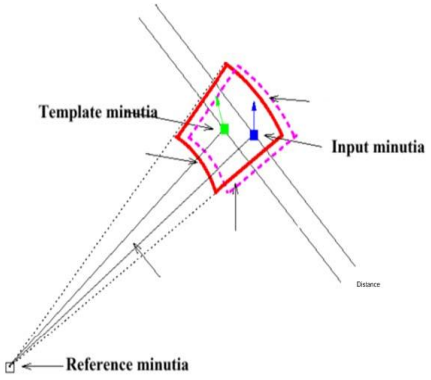


Fig. 9.6 Description of Tolerance Boxes

CHAPTER 10

Database

Databases consist of software-based "containers" that are structured to collect and store information so users can retrieve, add, update or remove such information in an automatic fashion. Database programs are designed for users so that they can add or delete any information needed. The structure of a database is tabular, consisting of rows and columns of information. Over many years general-purpose database systems have dominated the database industry. These offer a wide range of functions, applicable to many, if not most circumstances in modern data processing.

10.1 Database management systems

A database management system (DBMS) consists of software that organizes the storage of data. A DBMS controls the creation, maintenance, and use of the database storage structures of social organizations and of their users. It allows organizations to place control of organization wide database development in the hands of Database Administrators (DBAs) and other specialists. In large systems, a DBMS allows users and other software to store and retrieve data in a structured way.

Database management systems are usually categorized according to the database model that they support, such as the network, relational or object model. The model tends to determine the query languages that are available to access the database. One commonly used query language for the relational database is SQL, although SQL syntax and function can vary from one DBMS to another. A common query language for the object database is OQL, although not all vendors of object databases implement this, majority of them do implement this method. A great deal of the internal engineering of a DBMS is independent of the data model, and is concerned with managing factors such as performance, concurrency, integrity, and recovery from hardware failures. In these areas there are large differences between the products.

A relational database management system (RDBMS) implements features of the relational model. In this context, Date's "Information Principle" states: "the entire information content of

the database is represented in one and only one way. Therefore, there are no explicit pointers between related tables." This contrasts with the object database management system (ODBMS), which does store explicit pointers between related types. Caution should be used when using the following information in a historical context. For example, Pick is a legacy (multivalued) RDBMS, which does not use the SQL model.

10.2 Types of Database

10.2.1Operational database

These databases store detailed data needed to support the operations of an entire organization. They are also called subject-area databases (SADB), transaction databases, and production databases. For example:

- customer database
- personal database
- inventory database
- accounting database

10.2.2 Analytical database

Analytic databases (a.k.a. OLAP- On Line Analytical Processing) are primarily static, read-only databases which store archived, historical data used for analysis. For example, a company might store sales records over the last ten years in an analytic database and use that database to analyze marketing strategies in relationship to demographics.

On the web, you will often see analytic databases in the form of inventory catalogs such as the one shown previously from Amazon.com. An inventory catalog analytical database usually holds descriptive information about all available products in the inventory.

Web pages are generated dynamically by querying the list of available products in the inventory against some search parameters. The dynamically-generated page will display the information about each item (such as title, author, ISBN) which is stored in the database.

10.2.3 Data warehouse

A data warehouse stores data from current and previous years — data extracted from the various operational databases of an organization. It becomes the central source of data that has been screened, edited, standardized and integrated so that it can be used by managers and other end-user professionals throughout an organization. Data warehouses are characterized by being slow to insert into but fast to retrieve from. Recent developments in data warehousing have led to the use of a Shared nothing architecture to facilitate extreme scaling.

10.2.4 Distributed database

These are databases of local work-groups and departments at regional offices, branch offices, manufacturing plants and other work sites. These databases can include segments of both common operational and common user databases, as well as data generated and used only at a user's own site.

10.2.5 End-user database

These databases consist of a variety of data files developed by end-users at their workstations. Examples of these are collections of documents in spreadsheets, word processing and even downloaded files.

10.2.6 External database

These databases provide access to external, privately-owned data online — available for a fee to end-users and organizations from commercial services. Access to a wealth of information from external database is available for a fee from commercial online services and with or without charge from many sources in the Internet.

10.2.7 Hypermedia databases on the web

These are a set of interconnected multimedia pages at a web-site. They consist of a home page and other hyperlinked pages of multimedia or mixed media such as text, graphic, photographic images, video clips, audio etc.

10.2.8 Navigational database

In navigational databases, queries find objects primarily by following references from other objects. Traditionally navigational interfaces are procedural, though one could characterize some modern systems like XPath as being simultaneously navigational and declarative.

10.2.9 Document-oriented databases

Document-oriented databases are computer programs designed for document-oriented applications. These systems may be implemented as a layer above a relational database or an object database. As opposed to relational databases, document-based databases do not store data in tables with uniform sized fields for each record. Instead, they store each record as a document that has certain characteristics. Any number of fields of any length can be added to a document. Fields can also contain multiple pieces of data.

10.2.10 Real-time databases

A real-time database is a processing system designed to handle workloads whose state may change constantly. This differs from traditional databases containing persistent data, mostly unaffected by time. For example, a stock market changes rapidly and dynamically. Real-time processing means that a transaction is processed fast enough for the result to come back and be acted on right away. Real-time databases are useful for accounting, banking, law, medical records, multi-media, process control, reservation systems, and scientific data analysis. As computers increase in power and can store more data, real-time databases become integrated into society and are employed in many applications.

CHAPTER 11

Performance Evaluation and Results

11.1 Introduction

The response of a matcher in a fingerprint recognition system is typically a matching score s (without loss of generality, ranging in the interval [0, 1]) that quantifies the similarity between the input and the database template representations.The score in the algo is represented in percentage. The closer the score is to l, the more certain is the system that the two fingerprints come from the same finger; the closer the score is to 0, the smaller is the system confidence that the two fingerprints come from the same finger. The system decision is regulated by a threshold T_D : pairs of fingerprints generating scores higher than or equal to T_D are inferred as matching pairs (i.e., belonging to the same finger); pairs of fingerprints generating scores lower than T_D are inferred as nonmatching pairs (i.e., belonging to different fingers).

A typical biometric verification system commits two types of error: mistaking biometric measurements from two different fingers to be from the same finger (called false match) and mistaking two biometric measurements from the same finger to be from two different fingers (called false nonmatch). Note that these two types of errors are also often denoted as false acceptance and false rejection; a distinction has to be made between positive and negative recognition; in positive recognition systems (e.g., an access control system) a false match determines the false acceptance of an impostor, whereas a false nonmatch causes the false rejection of a genuine user. On the other hand, in a negative recognition application (e.g., preventing users from obtaining welfare benefits under false identities), a false match results in rejecting a genuine request, whereas a false nonmatch results in falsely accepting an impostor attempt. However, the use of false acceptance rate (FAR) and false rejection rate (FRR) is more popular and largely used in the commercial environment.

11.2 Classification Errors

To access the performance of a Biometric System it can be analyzed in the frame work of testing hypothesis [1]. Let the stored biometric template of a person be pattern $P' = S(B')$ and the acquired input for recognition be represented by pattern $P = S(B)$. Then the null and alternate

hypotheses are given by Equation 11.1 and 11.2 respectively.

H_0: B = B', The Claimed Identity is Correct (11.1)

H_1: B ≠B', The Claimed Identity is Not Correct (11.2)

Certain measure of similarity S = sim(P, P') is often defined and H_0 is decided if s ≥ T_D and H_1 is decided if s < T_D where T_D is the decision threshold. The measure of similarity s is often referred to as the matching score. When P = P', s is referred to as the matching score and B and B' are called the matching pair. When P ≠P', s is referred to as the non matching score and B and B' are called the non matching pair. With regards to expression 11.1 and 11.2, the decision H_0 when H_1 is true gives a false acceptance whereas the decision H_1 when H_0 is true results in a false rejection. The False Acceptance Rate (Proportion of non matching pairs resulting in False Acceptance) and False Rejection Rate (Proportion of matching pairs resulting in False Rejection) together characterize the accuracy of recognition system for a given decision threshold. Varying the threshold tradeoff between FAR and FRR.. In Figure 11.1 FAR is the area under the H_1 density function to the right of the decision threshold and FRR is the area under H_0 to the left of the decision threshold. The Equal Error Rate corresponds to a point at some threshold (T_{EER}), where FAR = FRR i.e. where the areas marked under the two curves are equal.

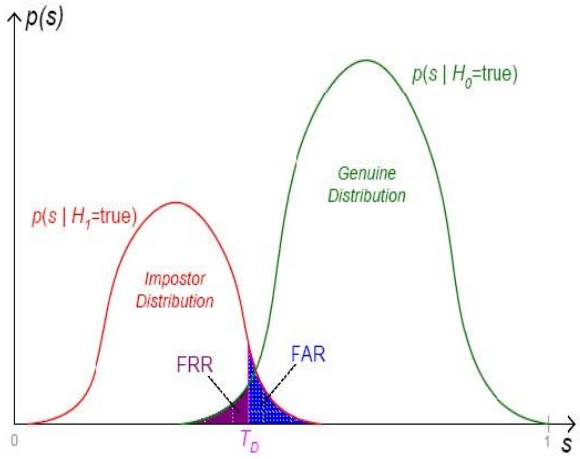
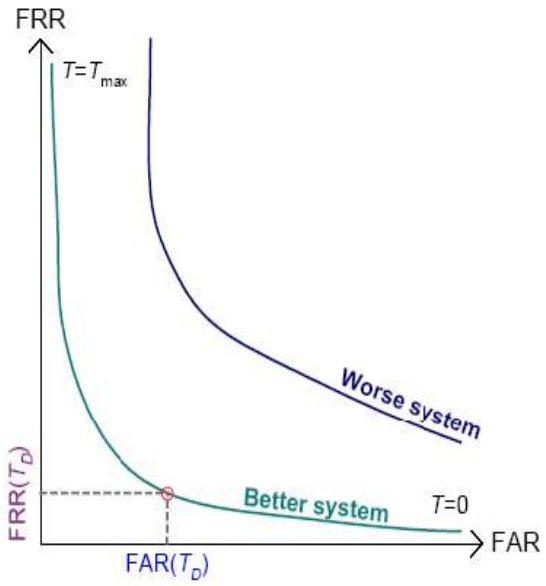


Figure11.1: Imposter and genuine distributions

Rather than showing the error rates in terms of probability densities it is often desirable to report

the system accuracy using a Receiver Operating Curve (ROC).

An ROC is a mapping $T_D \rightarrow$ (FAR, F RR)(Figure 11.2).



$ROC(T_D) = (FAR(T_D)), (FRR(T_D))$ (5.3)

Figure11.2: Receiver operating curve

It is important to note here that in a typical recognition system all information contained in the probability distribution functions is also contained in the ROC. If T_D approaches to zero, FAR goes to maximum that is 1 and FRR goes to 0; and by setting $T_D = T_{max}$ FAR goes to zero and FRR goes to 1. System can be operated at a certain threshold value to achieve desired FAR against a certain FRR.

11.3 Experimentation Results

My program tests all the images without any fine-tuning for the database. The experiments show my program can differentiate imposturous minutia pairs from genuine minutia pairs in a certain confidence level. Furthermore, good experiment designs can surely improve the accuracy

as declared by [5]. Further studies on good designs of training and testing are expected to improve the result. Here is the diagram for Correct Score and Incorrect Score distribution:

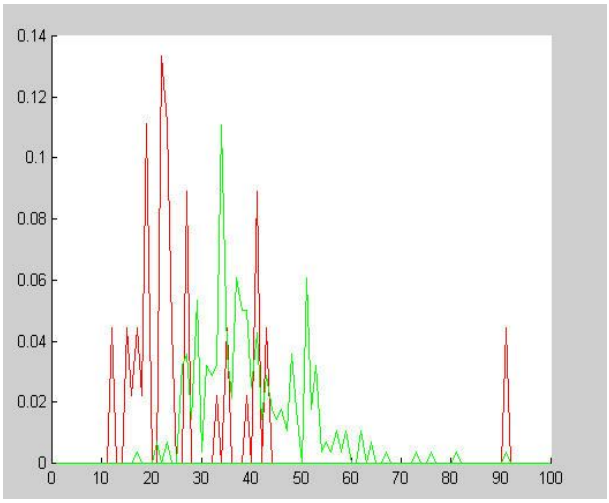


Figure 11.3 Distribution of Correct Scores and Incorrect Scores
Red line: Incorrect Score
Green line: Correct Scores

It can be seen from the above figure that there exist two partially overlapped distributions. The Red curve whose peaks are mainly located at the left part means the average incorrect match score is 25. The green curve whose peaks are mainly located on the right side of red curve means the average correct match score is 35. This indicates the algorithm is capable of differentiate fingerprints at a good correct rate by setting an appropriate threshold value.

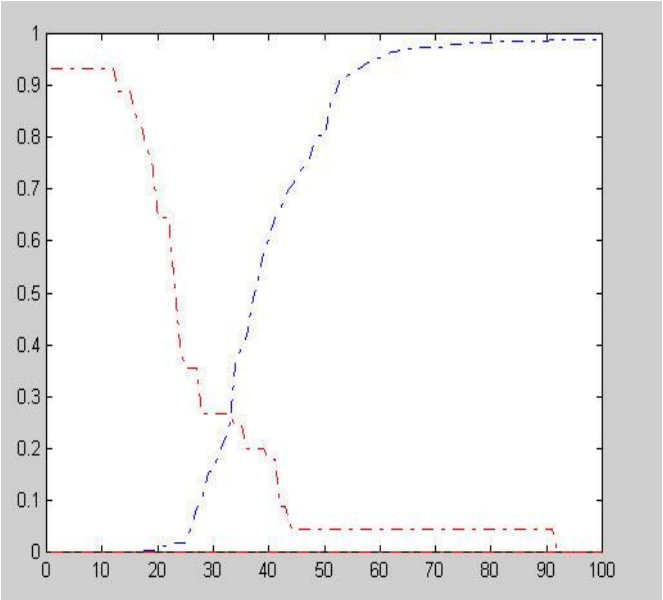


Figure 11.4 FAR and FRR curve

Blue dot line: FRR curve
Red dot line: FAR curve

The above diagram shows the FRR and FAR curves. At the equal error rate 25%, the separating score 33 will falsely reject 25% genuine minutia pairs and falsely accept 25% imposturous minutia pairs and has 75% verification rate. The high incorrect acceptance and false rejection are due to some fingerprint images with bad quality and the vulnerable minutia match algorithm.

11.4 Analysis and Comparison of Results

Initially all known matched fingerprints are passed through the matching algorithm to obtain a distribution of genuine scores, similarly all known nonmatch fingerprints are passed through the matching algorithm to obtain a distribution of imposter scores.It can be seen from the FRR and FAR curves of Figure 11.4 that the algorithm is reasonably capable of discriminating imposter cases, however there are certain genuine matching which result in lower scores and are contributing towards slightly higher error rates. In order to analyze the cause of lesser score a few cases were identified and analyzed in depth for identification of the exact cause of lesser score. Upon this analysis it was revealed that the genuine cases giving less score are basically partial images; the amount of overlap between two prints being matched is not enough.

Fig.11.5 partial match images

Though in most of the cases the minutiae available in the overlapped region have been identified correctly by the algorithm, yet the similarity score is less because the calculation of

similarity considers total number of minutiae in the print. One such case of partial match is shown in Figure 11.5. In order to validate the fact that the partial cases are the main cause of higher error rates.

CHAPTER 12

Conclusion

12.1 Overview

The theory behind the fingerprint matching based on minutiae, especially considering the structure in local neighborhood, was in detail studied. My project has combined many methods to build a minutia extractor and a minutia matcher. The combination of multiple methods comes from a wide investigation into research paper. Also some novel changes like segmentation using Morphological operations, minutia marking with special considering the triple branch counting, minutia unification by decomposing a branch into three terminations, and matching in the unified x-y coordinate system after a two-step transformation are used in my project. Also a program coding with MATLAB going through all the stages of the fingerprint verification is built. It is helpful to understand the procedures of fingerprint verification. And demonstrate the key issues of fingerprint verification.The tests showed that the system is capable of distinguishing the genuine fingerprints apart from the imposter fingerprints. The system has proved to be robust towards translation, rotation and/or missing and spurious minutiae between the matched fingerprints. A considerable improvement has been made in terms of computational efficiency by hierarchal nature of the algorithm.

12.2 Contribution and Objectives Achieved

A research has been carried out in the area of fingerprint matching based on minutiae. Features like ridge counts between minutiae and their types have also been used for calculating a degree of similarity between two minutiae. An in depth study of the theory of fingerprints have been carried out. Use of fingerprints as biometric identifier for personnel verification has been modeled. By implementing the complete performance evaluation, matching and feature extraction stages, a high degree of confidence in Matlab programming has been achieved. Having studied and implemented the feature extraction stage has given an extra understanding of the image processing concepts like segmentation.

12.3 Limitations

The performance of matching algorithm is highly dependent on the conditions while

enrollment and robustness of the enhancement and feature extraction algorithm. Noisy, distorted and fingerprint images with scars are a challenge for image enhancement and feature extraction stages. These problems contaminate the minutiae information in terms of false minutiae which not only increases the computations for matching algorithm but also adversely effects the matching score and ultimately the error rate.

12.4 Future Work

As future work, it is proposed that current research work in fingerprint matching should be extended to deal with a scenario of matching the partial fingerprints. This can be achieved by combining the proposed matching algorithm with textural information available in the fingerprint image. The textural information as proposed in [2,3,4] can be used to yield the results incase a partial fingerprint is matched against another partial fingerprint image in combination with the proposed matching algorithm. In addition to that, number of minutiae actually contributing; minutiae available in overlap or common region of the two fingerprints be used to determine the similarity score.

BIBLIOGRAPHY

[1]. N. K. Ratha, A. W. Senior, and R. M. Bolle, "Automated biometrics," in ICAPR'01: Proceedings of the Second International Conference on Advances in Pattern Recognition. London, UK: SpringerVerlag, 2001, pp. 445–474.

[2] A. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbankbased fingerprint matching," IEEE Transactions on Image Processing, vol. 9, no. 5, pp. 846–859, May 2000.

[3] A. Jain, A. Ross, and S. Prabhakar, "Fingerprint matching using minutiae and texture features," in Proceedings of International Conference on Image Processing, vol. 3, 2001, pp. 282–285 vol.3.

[4] C.H. Park, J.J. Lee, M. Smith, S. il Park, and K.H. Park, "Directional filter bankbased fingerprint feature extraction and matching," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 74–85, Jan. 2004.

[5] C. Lin, J. Liu, J. Ostenberg, and J. Nicol, "Fingerprint comparison i: Similarity of fingerprints," Journal of Forensic Sciences, vol. 27, no. 2, pp. 290–304, 1982.

[6] N. Ratha, S. Chen and A.K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, pp. 1657-1672, November 1995.

[7] Alessandro Farina, Zsolt M.Kovacs-Vajna, Alberto leone, Fingerprint minutiae extraction from skeletonized binary images, Pattern Recognition, Vol.32, No.4, pp877-889, 1999.

[8] Lee, C.J., and Wang, S.D.: Fingerprint feature extration using Gabor filters, Electron. Lett., 1999, 35, (4), pp.288-290.

[9] Lin Hong. "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.

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

[11] A. Wahab, S. Chin, and E. Tan, "Novel approach to automated fingerprint recognition," Vision Image and Signal Processing, vol. 145, no. 3, pp. 160–166, June 1998.

[12] L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. Intelligent biometric techniques in fingerprint and face recognition. 1999, the CRC Press.

[13] A. N. Marana and A. K. Jain "Ridge-Based Fingerprint Matching Using Hough Transform" ,Proc. of BSCGIP, pp. 112-119, 2005.

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