Fingerprint Matching Using Descriptors

A Dissertation submitted to the University of Hyderabad in partial fulfillment of the degree of

MASTER OF TECHNOLOGY

in

Information Technology

by

ROJA SUJATHA GOLLA

Department of Computer and Information Sciences

School of Mathematics, Computer and Information Sciences

University of Hyderabad
(P.O.) Central University, Gachibowli
Hyderabad – 500 046
Andhra Pradesh
India

CERTIFICATE

This is to certify that the dissertation entitled "**Fingerprint matching using Descriptors**" submitted by **Roja sujatha G.** bearing Reg. No **09MCMB26** in partial fulfillment of the requirements for the award of Master of Technology in Information Technology is a bonafide work carried out by him under my supervision and guidance.

The dissertation has not been submitted previously in part or in full to this or any other University or Institution for the award of any degree or diploma.

Associate Professor, IDRBT.
Signature of the Supervisor

Head of the Department

Dean of the School

DECLARATION

I **Roja Sujatha. G** hereby declare that this Dissertation entitled "**Fingerprint matching using descriptors** ", submitted by me under the guidance and supervision of **Dr. Mahil Carr, Associate Professor, IDRBT**, is a bonafide work. I also declare that it has not been submitted previously in part or in full to this University or other University or Institution for the award of any degree or diploma.

Date: Name : **Roja Sujatha. G**

Signature of the Student:

Regd. No. **09MCMB26**

ACKNOWLEDGEMENTS

I wish to express my sincere thanks to my advisor, Dr. Mahil Carr, Associate Professor, IDRBT, Hyderabad, who generously supported and guided me throughout my project, IDRBT for providing me with the infrastructure and technical support that I needed for this project. The project would not have been possible without his assistance.

I also thank Mr. B. Sambamurthy, Director, IDRBT, Prof. T. Amaranath, Dean, School of MCIS, Prof. Arun Agarwal, Head of the Department (DCIS), and University of Hyderabad for extending their cooperation.

The guidance of all the faculty members of IDRBT and the Department of Computer and Information Sciences, University of Hyderabad has been precious and timely I would like to thank all people who have helped and inspired me during my study.

Roja Sujatha.G

09MCMB26
University of Hyderabad and IDRBT
Hyderabad
E-mail: rojasujatha07@gmail.com

ABSTRACT

Biometrics such as fingerprint, face and voice print offers means of reliable personal authentication that can address these problems and is gaining citizen and government acceptance. Fingerprints were one of the first forms of biometric authentication to be used for law enforcement and civilian applications. This study is of banking applications. Most of the fingerprint matching algorithms have been developed using minutiae based matching. We extracted minutiae from NBIS software provided by NIST. In this thesis, we introduced a novel matching algorithm based on descriptors and minutiae. In this algorithm we used two descriptors: orientation based descriptor, minutiae based descriptor. First, we extracted the minutiae and next the descriptors around each minutia are established for template and input fingerprint images. The similarity value for orientation based descriptor, minutiae based descriptor is computed and similarity value is combined by using product rule. The effectiveness of the proposed algorithm is tested on a public database FVC2002 DB1, DB2 and FAR, FRR is computed

TABLE OF CONTENTS

CHAPTER 1

1 INTRODUCTION

Fingerprinting has it's roots in the early 1800s when a professor of anatomy at the University of Breslau first wrote a paper discussing fingerprint patterns. However, it wasn't until years later when a man by the name of Francis Galton published a book discussing the matter that it was used to identify individual persons 1823 Jan Purkyne publishes thesis on fingerprint patterns. After that in 1880 Dr. Henry Faulds publishes his article on the subject in a science magazine and offers his ideas to the London police. The idea is rejected. In 1892 Sir Francis Galton publishes a statistical model of fingerprint analysis and discusses his theory that it could be used in forensic science. In 1892 An Argentine police officer makes the first criminal fingerprint identification in a murder case. Crimes In 1893, the Home Ministry Office, UK, accepted that no two individuals have the same fingerprints. In 1901 The UK Fingerprint Bureau is created in Scotland Yard. In 1956 Alphonse Bertillon first conceived and then industriously practiced the idea of using body measurements for solving. Fingerprint training procedures were time-intensive and slow. Law enforcement agencies were the earliest adopters of the fingerprint recognition technology, more recently, however, increasing identity fraud has created a growing need for biometric technology for person recognition in a number of non-forensic applications. Biometric recognition refers to the use of distinctive physiological (e.g. fingerprints, face, retina, iris) and behavioral (e.g. gait, signature) characteristics, called biometric identifiers (or simply biometrics) for automatically recognizing individuals. Perhaps all biometric identifiers are a combination of physiological and behavioral characteristics and they should not be exclusively classified into either physiological or behavioral characteristics. For example, fingerprints may be physiological in nature but the usage of the input device (e.g., how a user presents a finger to the fingerprint scanner) depends on the person's behavior. Thus, the input to the recognition engine is a combination of physiological and behavioral characteristics. A fingerprint consists of the features

and details of a fingertip. There are three major fingerprint features: the arch, loop and whorl. Each finger has at least one major feature. The smaller or minor features (or minutiae) consist of the position of ridge ends (ridges are the lines that flow in various patterns across fingerprints) and of ridge bifurcations (the point where ridges split in two). Enrolment and acquisition can be done by sensors reading the tip of the finger directly and in real-time. A fingerprint scan contains a lot of information but scanners normally focus only on getting an image of the information that is essential for matching. Getting a high quality image of the fingerprint is very important for accurate fingerprint recognition, but also feature extraction plays a crucial role. It consists of converting the fingerprint image into a usable and comparable format that does not require lots of storage space. 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.

CHAPTER 2

2. BIOMETRICS

2.1 HISTORY OF BIOMETRICS

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). Biometrics is becoming an interesting topic now in regards to computer and network security, however the ideas of biometrics have been around for many years. In the 14th century portuguese explorer Joao de Barros reported the use of biometrics. He described the practice of chinese merchants of stamp children´s palmprints and footprint to distinguish from one another The real biometric system was created in 1870 by french anthropologist Alphonse Bertillion and turned biometrics a distinguished field of study. He developed an identification system (Bertillonage) based on detailed records of body measurement, physical description and photographs. It began to fail when it was discovered that many people share the same anthropologic measures. The first classification method for fingerprints was developed in 1892 by Sir. Francis Galton. The features used by Galton´s method were the minutiae that are still used nowadays. Some years later in 1896, Sir Edward Henry General Inspector of the Bengal police, began to use Galton´s method to replace the anthropometrics system for identification of criminals. Henry created a method to classify and store fingerprint that lets a quick searching of records. Later, that method was introduced by Henry in London for the first British fingerprint file. However the idea of biometrics as a field of study with useful identification applications was there and interest in it has grown. Today we have the technology to realise the aims, and to refine the accuracy of biometric identification, and therefore the possibility of making it a viable field

2.2 BIOMETRIC SYSTEM

A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system.

Identification (1:N) – The system identifies the end user from his/her biometric sample by associating it with his/her particular reference template based on a database search among the reference templates of the entire enrolled. It is 1:N matching . For identification we need only fingerprint template for matching. In identification the processing time depends on the number of templates

Verification (1:1) – The system verifies the claimed identity of the user by comparing his/her biometric sample with one specific reference template, which is either physically presented by the user or pointed to in the database. It is 1:1 matching. For verification we need an ID and the template for matching. It is fast processing and involves only one matching

2.3 BIOMETRIC TECHNIQUES

2.3.1 Fingerprint

Fingerprint recognition consists of comparing a print of the characteristics of a fingertip or a template of that print with a stored template or print. A fingerprint consists of the features and details of a fingertip. There are three major fingerprint features: the arch, loop and whorl. The smaller features consist of the position of ridge ends (ridges are the lines that flow in various patterns across fingerprints) and of ridge bifurcations (the point where ridges split in three). Getting a high quality image of the fingerprint is very important for accurate fingerprint recognition, but also feature extraction plays a crucial role. Feature extraction is also needed because even a very precise fingerprint image will have distortions and false minutiae that need to be filtered out. The applications of fingerprint recognition are identification of criminals for law enforcement; prevent fraudulent enrolment, secure physical access is another popular application.

2.3.2 Iris:

The iris is the externally-visible, colored ring around the pupil. It is a physical feature of a human being that can be measured and thus used for biometric verification or identification through the process of iris recognition. The human iris is well protected as although it is externally visible, it is an internal part of the eye. It is not genetically and it is believed to be stable throughout life (barring accidents and surgical operations). An iris 'scan' is a high-quality photograph of the iris taken under near-infrared (near-IR) illumination. Iris recognition systems generally use narrow-angle cameras and ask the user to position their eyes correctly in the camera's field of view. The resulting photograph is analyzed using algorithms to locate the iris and extract feature information, in order to create a biometric template or 'Iris Code'. The major applications of iris recognition are: immigration control/border crossing (using verification, identification or watch-lists), aviation security, controlling access to restricted areas/buildings/homes, database/login access.

2.3.3 Voice:

Voice recognition technology is a means of using the unique characteristics of a person's voice including the rhythm of their vocal cords and the concavity of their mouth to create a "voice print" which is then used for identification purposes. Voice recognition is for an individual to produce an actual voice sample. The unique patterns of an individual's voice are produced by the vocal tract. To ensure a good quality voice sample, the individual usually recites some sort of text, which can either be a verbal phrase or a series of numbers. The individual usually has to repeat this number of times. The most common devices used to capture an individual's voice samples are computer microphones, mobile phones, and land line based telephones. The voice samples are converted from an analog format to a digital format for processing. The applications of voice recognition are: call center automation, and transaction processing via the telephone or computer, financial transactions, credit card processing

2.3.4 Face

Face recognition refers to an automated or semi-automated process of matching facial images. The image of the face is captured using a scanner and then analyzed

in order to obtain a biometric “signature”; different algorithms can be used for this and manufacturers have adopted various proprietary solutions The term, face recognition, is used as though it refers to a single type of technology but in fact it constitutes a heterogeneous group of technologies which all work with the face but use different scanning techniques. The applications of face recognition are : to screen the spectators that attended the Super Bowl game, to screen images from closed circuit television cameras for targeted offenders . Face recognition has also been tested in airports around the world, including Keflavik Airport Reykjavik, Logan Airport Boston, Palm Beach International Airport Florida and Sydney Airport.

2.3.5 Hand Geometry:

The geometric features of the hand such as the lengths of fingers and the width of the hand are measured to identify an individual. The hand geometry scanner looks for unique features in the structure of the hand. These unique features include the finger thickness, length, and width, the distances between finger joints, the hand’s overall bone structure, etc. The user first places his or her hand onto a platen. This platen consists of 5 pegs which help the user position their fingers properly in order to insure quality enrolment and verification templates. The hand geometry scanner consists of a charged couple device camera (CCD), as well as various reflectors and mirrors in order to capture various black and white pictures of the hand. The applications of hang geometry are: physical access entry applications, time and attendance, point of sale applications.

2.3.6 Vein:

Vein recognition is a Verification of a person's identity by recognizing the pattern of blood veins in the palm (number of veins, their position and the points at which they cross). The pattern of blood veins in the palm is unique to every individual, and apart from size, this pattern will not vary over the course of a person's lifetime. Using infrared light, this biometric measures the unique blood pattern of veins in the hand. Software then extracts the vein pattern and compares it against patterns already stored in a database. The major applications are: this technology was used by several Japanese banks (The Bank of Tokyo-Mitsubishi and Suruga Bank) for customer authentication at ATM's, room access security of the Department of

Planning, Information and Management, student ID system that combines contactless palm vein authentication technology and multi-functional smart cards.

2.3.7 Dynamic Signature:

Dynamic signature recognition captures the distinct behavioral characteristics of an individual's signature including shape, speed, stroke, pen pressure and timing information. Signature recognition technology consists primarily of a pen and a specialized writing tablet, which are then connected to a local or central computer for template processing and verification. A signature cannot be too long or too short. If a signature is too long, there will be too much behavioral data presented, and as a result, it will be difficult for the signature recognition system to identify consistent and unique data points. If a signature is too short, there will not be enough data present, and as a result, this will lead to a higher False Accept Rate The applications are: Chase Manhattan Bank (the first known bank to adopt signature recognition technology), the Internal Revenue Service for verification purposes in tax returns that have been filed online, and Charles Schwab & Company for new client applications.

2.3.8 Gait

Gait recognition is recognizing individuals by their distinctive walk, captures a sequence of images to derive and analyze motion characteristics. A person's gait can be hard to disguise because a person's musculature essentially limits the variation of motion, and measuring it requires no contact with the person. However, gait can be obscured or disguised if the individual, for example, is wearing loose fitting clothes. Preliminary results have confirmed its potential, but further development is necessary before its performance, limitations, and advantages can be fully assessed. Gait analysis is widely used in professional sports training to optimize and improve athletic performance.

2.3.9 Multimodal

Multimodal biometric technology uses more than one biometric identifier to compare the identity of the person. Therefore in the case of a system using say three technologies i.e. face mimic and voice. If one of the technologies is unable to identify, the system can still use the other two to accurately identify against

2.4 BIOMETRICS CHARACTERISTICS

Biometrics characteristics are often classed in three main categories:

1) Physiological biometrics is based on measurements and data derived from direct measurement of a part of the human body. Fingerprint, iris-scan, retina-scan, hand geometry, and facial recognition are leading physiological biometrics.

2) Behavioral characteristics are based on an action taken by a person. Behavioral biometrics, in turn, are based on measurements and data derived from an action, and indirectly measure characteristics of the human body. Voice recognition, keystroke-scan, and signature-scan are leading behavioral biometric technologies. One of the defining characteristics of a behavioral biometric is the incorporation of time as a metric the measured behavior has a beginning, middle and end.
3) Chemical Biometrics is based on measuring chemical cues such as odor and the chemical composition of human perspiration.

2.5 ISSUES WITH BIOMETRICS

At present, many applications of biometric technologies exist both in the private and public sector. In both public and private sector the implementation of biometric applications are facing many challenges that need to be addressed. Issues with biometrics are security, privacy, interoperability etc. These issues need to be examined

2.5.1 Security

Biometric systems are more secure than traditional identification systems. But they only represent a secure identification process in that they provide a strong link between physical persons with their identity data. This means that the integrity of the linking process must be high. This will depend on the secure operation of each one of the four stages of a biometric identification process (enrolment, storage, acquisition, matching). In addition it cannot rely on secrecy, since most biometric

features are either self-evident or easily obtainable. On the other hand, since biometrics are only a part of the system, it is not enough to secure the biometric system if the rest of the process remains open to circumvention. In the end, the notion of a biometric identifier being absolute proof of identity has to be discarded. Biometric identification systems are subject to errors and circumvention and thus are not perfect.

2.5.2 Privacy

While the use of a biometric technology is not an invasion of privacy, in many cases the way the digital data is produced, stored, compared and possibly linked to other information about the individual, may raise a set of concerns. Although these are concerns the existing legal framework for Data protection can handle the widespread diffusion of biometrics into the commercial sphere may challenge the legal framework in ways that will have a negative impact on user acceptability. For example should the habit of sharing biometric data among private sector entities proliferate, then it is likely that users may find that the current data protection frame is unable to protect them adequately. Currently, any individual has the option of changing identity if the need arises (e.g. witness protection programme). This becomes harder or even impossible when identity is tied up with the physical self.

2.5.3 Cost

Costs vary between technologies and also between low-end and high-end equipment within any one technology. It is the purpose and scale of an application that determine costs. Thus costs will depend on the choice of open- or closed-system architecture, type of application, centralized or decentralized storage, whether encryption is used as a means of data protection, and the decision of where in the system matching takes place. Moreover, enhanced market competition or market distortions will also impact on costs, as will regulatory decisions on interoperability, standards and intellectual property rights. Real costs include overall system security (at all biometric stages) as well as those of the fall-back system which is an indispensable element of any proper biometric application

2.5.4 Interoperability

Interoperability across geographical borders and business sectors, across processes, devices and systems is beneficial to its diffusion. National interests in maintaining control and vendor resistance (aspiring to future market dominance due to lock-in effects) are natural barriers to interoperability. There is significant work being done at national and international levels to develop standards, which will be useful in promoting open systems development and interoperability. Technical interoperability is likely to be achieved in the near future but interoperability of processes may be more challenging especially when biometrics becomes more widely diffused in society. When systems become more interoperable, the need for building safeguards against abuse grows as well. Moreover, since individuals have many different biometrics at their disposal, there is the possibility for different applications to make use of different biometrics, in the sense that limited interoperability may create barriers and thus protect against abuse. Such systems may still be compatible at the data transmission level and thus it may still be possible to cross-check information as to who was identified and where.

CHAPTER 3

3. FINGERPRINTS

3.1 HISTORY OF FINGERPRINTS

Fingerprints have been scientifically studied for a number of years in our society. Sir William Herschel, in 1859, discovered that fingerprints do not change over time and that each pattern is unique to an individual. With these findings, he was the first to implement a system using fingerprints and handprints to identify an individual in 1877. At the time, his system was a simple one-to-one verification process. By 1896, police forces in India realized the benefit of using fingerprints to identify criminals, and they began collecting the fingerprints of prisoners along with their other measurements with a growing database of fingerprint images, it soon became desirable to have an efficient manner of classifying the various images. Between 1896 and 1897, Sir Edward Henry developed the Henry Classification System, which quickly found worldwide acceptance within a few years. This system allows for logical categorization of a complete set of the ten fingerprint images for a person. By establishing groupings based on fingerprint pattern types, the Henry System greatly reduces the effort of searching a large database. Until the mid-1990s, many organizations continued to use the Henry Classification System to store their physical files of fingerprint images [International Biometric Group, 2003]. As fingerprints began to be utilized in more fields, the number of requests for fingerprint matching began to increase on a daily basis. At the same time, the size of the databases continued to expand with each passing day. Therefore, it soon became difficult for teams of fingerprint experts to provide accurate results in a timely manner. In the early 1960s, the FBI, Home Office in the United Kingdom, and Paris Police Department began to devote a large amount of resources in developing automatic fingerprint identification systems. These systems allowed for an improvement in operational productivity among law enforcement agencies. Today, automatic fingerprint recognition technology can be found in a wide range of civilian applications

3.2 FINGERPRINT MATCHING TECHNIQUES

3.2.1 Minutiae-Based

There are several categories of fingerprint matching techniques. One such category employs methods to extract minutiae from the fingerprint images, and then compares this data to the previously stored template data sets. In most cases, the minutiae details are stored as sets of points in the two-dimensional plane. For each minutia, the x- and y-coordinates indicating its location within the image are recorded. Other stored parameters may include the orientation angle of each minutiae as well as the specific type of minutiae located. Generally, minutiae based methods require a significant amount of preprocessing to produce accurate results. There are a variety of methods in use today for extracting the minutiae from a fingerprint.

3.2.2 Image-Based

Image-based techniques are another significant category of fingerprint matching. These processes are appealing because they do not require a significant amount of pre-processing to produce acceptable results. In most cases, the only pre-processing methods that are applied area binarization and thinning phase. Therefore, imaged-based techniques have a better computational efficiency than the standard minutiae-based techniques. Also, for low quality fingerprint images, image-based techniques produce better results than minutiae extraction methods, where it may be difficult to reliably extract the actual minutiae points An important component for image-based matching is dealing with rotation. Since the input image might be oriented differently than the template image, it is necessary to apply a rotational correction to achieve the best results.

3.2.3 Ridge Feature-Based

In many images, minutiae extraction may be difficult to conduct in an efficient manner. A low quality image containing a large amount of noise presents problems for minutiae-extracting algorithms. In such a case, other options to acquire meaningful data from a fingerprint become necessary. Analyzing various ridge features provides this versatility. There are several features that are commonly examined in today's systems, ranging from fairly basic to more advance. The basic ridge features, however, are obtainable from any quality image. Since minutiae-

based methods require an image of good quality, ridge features offer an alternative for poor images. Furthermore, ridge feature-based techniques do not have to be limited to images of poor quality. Instead, they can be used in conjunction with minutiae-based techniques for images of good quality. With more data to be used in the matching process, the accuracy and robustness of a system would undoubtedly increase

3.3 ADVANTAGES OF FINGERPRINT

Fingerprints were accepted formally as valid personal identifier in the early 20th century and have since then become a de-facto authentication technique in law-enforcement agencies worldwide. Fingerprints have several advantages over other biometrics, such as the following:

3.3.1 High universality:

It means that each person should have the biometric. 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

3.3.2 High distinctiveness:

Even identical twins who share the same DNA have been shown to have different fingerprints, since the ridge structure on the finger is not encoded in the genes of an individual. Thus, fingerprints represent a stronger authentication mechanism than DNA. Furthermore, there has been no evidence of identical fingerprints in more than a century of forensic practice. There are also mathematical models that justify the high distinctiveness of fingerprint patterns.

3.3.3 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.

3.3.4 Easy collectability:

The process of collecting fingerprints has become very easy with the advent of online sensors. These sensors are capable of capturing high resolution images of the finger surface within a matter of seconds. This process requires minimal or no user training and can be collected easily from co-operative or non co-operative users. In contrast,

other accurate modalities like iris recognition require very co-operative users and have considerable learning curve in using the identification system.

3.3.5 High performance:

Fingerprint recognition achieves high 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.

3.3.6 Wide acceptability:

Fingerprint is which the people are willing to accept a particular biometric identifier in their daily lives.

3.4 CLASSIFICATION OF FINGERPRINTS

Plain Arch Tented Arch Ulnar Loop Radial Loop

Double Loop Whorl Plain Whorl Central Pocket Loop Whorl

Accidental Whorl

Fig 3.4.1 Classification of fingerprints

Plain Arch

In plain arch the ridges enter on one side of the impression and flow or tend to flow out the other side with a rise or wave in the center

Tented Arch

Tented arches are similar to plain arches with the exception that the ridges in the center form. They approach loop type of the pattern possessing two of the basic characteristics of the loop.

Ulnar Loop:

Ulnar loops are types of patterns in which the loop flow in the direction of the little fingers. It is also called as slant loop

Radial Loop

Radial loop are types of pattern in which the loops floe in the direction of thumbs

Double Loop Whorl

The double loop whorl consists of two separate loop formations, with two separate and distinct sets of shoulders and two deltas

Plain Whorl

A plain whorl has two deltas and at least one ridge making a complete circuit, which may be spiral or oval, or any variant of the circle. An imaginary line drawn between two deltas must touch or cross at least one of the recurving ridges within the pattern area.

Central Pocket Loop Whorl

The Central pocket loop whorl consists of one or more recurving ridges, or an obstruction at a right angle to the inner line of flow, with two deltas between which an imaginary line would cut or touch no recurving ridge within the pattern area. The inner line of flow of central pocket loop whorl is determined by drawing an imaginary line between the inner delta and the center of the innermost recurve or looping ridge

Accidental Whorl

The accidental whorl is a pattern with two or mare deltas, and a combination of two or more different types of patterns exclusive of the plain arch. This classification also include those exceeding unusual patterns which may not be placed by definition into any other classes.

3.5 PARAMETERS OF FINGERPRINT

3.5.1 Resolution

This indicates the number of dots or pixels per inch (dpi). 500 dpi is the minimum resolution for scanners and is met by many commercial devices 250 to 300 dpi is probably the minimum resolution that allows the extraction algorithms to locate the minutiae in fingerprint patterns. Minutiae play a primary role in fingerprint matching since most of the algorithms rely on the coincidence of minutiae to declare whether the two fingerprint impressions are of the same finger .The same fingerprint portion sub-sampled at different resolutions; decreasing the resolution results in a greater difficulty in resolving ridges from valleys and isolating minutiae points. Images acquired at 200 to 300 dpi are often matched through correlation techniques which seem to tolerate lower resolutions better.

3.5.2 Area

The size of the rectangular area sensed by a fingerprint scanner is a fundamental parameter. The larger the area, the more ridges and valleys are captured and the more distinctive the fingerprint becomes. An area greater than or equal to 1 x 1 square inches permits a full plain fingerprint impression to be acquired. In most of the recent fingerprint scanners aimed at non-AFIS market, area is sacrificed to reduce cost and to have a smaller device size. Small-area scanners do not allow a whole fingerprint to be captured, and the users encounter difficulties in representing the same portion of the finger. This may result in a small overlap between different acquisitions of the same finger, leading to false non-match errors.

3.5.3 Number of pixels

The number of pixels in a fingerprint image can be simply derived by the resolution and the fingerprint area. A scanner is working at r dpi over an area of height (h) x width (w) $inch^2$ has rh x rw pixels.

3.5.4 Dynamic range

This denotes the number of bits used to encode the intensity value of each pixel. Color information is not considered useful for fingerprint recognition and therefore almost all the available fingerprint scanners acquire grayscale images. The FBI standard for pixel bit depth is 8 bits, which yields 256 levels of gray. No definitive study has been conducted to show how recognition performance decreases when bit depth is

decreased. However, it is understood that some degree of bit depth above 1 bit is necessary for good performance of many feature extraction algorithms.

3.5.5 Geometric Accuracy

This is usually specified by the maximum geometric distortion introduced by the acquisition device, and expressed as a percentage with respect to x and y directions. Most of the optical fingerprint scanners introduce geometric distortion which, if not compensated, alters the fingerprint pattern depending on the relative position of the finger on the sensor surface.

3.5.6 Gray Level Quantization and Gray Range

The gray level quantization denotes the maximum number of gray levels in the output image and is related to the number of bits used to encode the intensity value of each pixel. The gray range is the actual number of gray levels used in an image disregarding the maximum given by the gray level quantization.

3.5.7 Gray level uniformity and input/output linearity

The gray level uniformity is defined as the gray level homogeneity measured in the image obtained by scanning a uniform dark or light gray patch. the input/output linearity quantifies the deviation of the gray levels from a linear mapping when the input pattern is transformed into an output image

3.5.8 Spatial frequency response

It denotes the ability of an acquisition device to transfer the details of the original pattern to the output image for different frequencies. It is measured through Modulation Transfer Function or Contrast Transfer Function

3.5.9 Signal to noise Ratio

It quantifies the magnitude of the noise with respect to the magnitude of the signal. The signal magnitude is related to the gray range in the output image and the noise can be defined as the standard deviation of gray levels in uniform gray patches

3.5.10 Image Quality

It is not easy to precisely define the quality of a fingerprint image, and it is even more difficult to decouple the fingerprint image quality from the intrinsic finger quality or status. In fact, when the ridge prominence is very low (especially for manual workers and elderly people), when the fingers are too moist or too dry, or when they are incorrectly presented, most of the scanners produce poor quality images.

3.6 DETAILS OF FINGERPRINT

A fingerprint is the feature pattern of one finger and it is unique. (see Fig 3.6.1)

Fig 3.6.1 Fingerprint Image

A fingerprint pattern is comprised of a sequence of ridges and valleys. In a fingerprint image, the ridges appear as dark lines while the valleys are the light areas between the ridges. A cut or burn to a finger does not affect the underlying ridge structure, and the original pattern will be reproduced when new skin grows. Fingerprints are distinguished by minutiae, are the abnormal points on the ridges. There are various minutiae points on a fingerprint (see Fig 3.6.2)

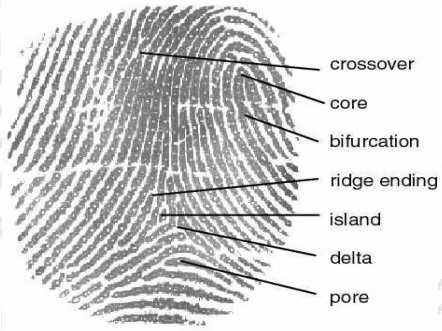


Fig 3.6.2: Properties of fingerprint

Core

Core is the topmost point on the innermost recurving ridgeline of a fingerprint. Generally, the core is placed upon or within the innermost recurve of a loop.

Delta

Delta is that point on a ridge at or nearest to the point of divergence of two type lines, and located at or directly in front of the point of divergence.

Ridge Ending

Ridge endings are the point where the ridges end abruptly(see Fig 3.6.3)

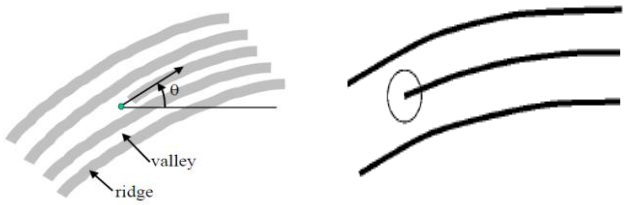


Fig : 3.6.3 Ridge Ending

Ridge Bifurcation

Ridge bifurcation is the point where three ridges are divided into different branches(see Fig 3.6.4)

Fig 3.6.4 Ridge Bifurcation

Island: Closed path is commonly referred as Island

Pore: Smallest point in the fingerprint

Crossover: It is a point where four ridges are divided into different branches

For most of the fingerprint matching algorithms ridge endings and ridge bifurcations are used. We extracted x-coordinate, y-coordinate and θ of ridge endings and bifurcations where θ is the orientation of the ridge

CHAPTER 4

4. LITERATURE REVIEW

4.1.FINGERPRINT MINUTIAE EXTRACTION BASED ON PRINCIPAL CURVES

Duoqian Miao , Qingshi Tang, Wenjie Fu proposed a new fingerprint minutiae extraction algorithm based on the principal curves . To obtain the principal curves they used the principal graph algorithm proposed by Kegl , which can be served as the skeletons of a fingerprint . The principal curves obtained from the principal graph algorithm are smoother than the ones obtained from thinning algorithm, and the minutiae extracted by the proposed algorithm are more efficient.

Definition of principal curves and principal graph algorithm

The smooth curve f(t) is a principal curve if and only if:

(1) f(t) does not intersect itself,

(2) f(t) has finite length inside any bounded subset of R^d,

(3) f(t) is self-consistent, i.e $f(t) = E[X|t_\tau(X) = \tau]$.

Principal graph algorithm consists of three steps:

Initialization

Fitting-smoothing

Restructuring

(1) Initialization: A thinning algorithm is adopted to obtain the approximate skeletons of a graph. The skeleton is denoted by G_{vs}, which consists of two sets V and S, where $V = \{v_1, v_2. . . v_n\}$ Rd is a set of vertices, and $S = \{(v_{i1}, v_{j1}), . . . , (v_{ik}, v_{jk})\} = \{S_{i1j1}, . . . , S_{ikjk}\}$ is a set of edges.

(2) Fitting-smoothing: The objective of this step is to adjust the smoothness of G_{vs} and to make it better fit the graph. Given a dataset $X_n = \{x_1 1, x_2, . . . , x_n\}$, this step minimizes a penalized distance function $E(G) = \Delta(G) + \lambda P(G)$ to optimize G_{vs}. The first component $\Delta(G)$ is the expected squared distance between points in X_n and G_{vs}, while the second component P(G) is a penalty function on the

average curvature of the graph. The smaller the value of $\Delta(G)$ is, the better the graph fits these data. The smaller the value of P(G) is, the smoother the graph is. In this step, a projection step is done first. After the projection step, the data points are partitioned into ‘‘the nearest neighbor region’’ according to the segment or vertex they project. Finally the vertex optimization step is performed to adjust the positions of vertexes and segments for finding a local minimum of E(G).

(3) Restructuring: This step complements and perfects the fitting-smoothing step. It uses geometric properties of the skeleton graph to modify the configuration of the vertices and edges. The goal of the step is to eliminate or rectify imperfections of the initial skeleton graph such as removing short branches and short loops.

Minutiae extraction based on principal curves

A minutiae extraction algorithm is proposed based on principal curves generalized by principal graph algorithm. From the enhanced fingerprint image two ridges are chosen as samples (Fig. 4.1.1): one is a simple ridge, and the other is a complex ridge. Then principal graph algorithm is used to obtain principal curves of the ridges. They analyzed a simple ridge shown in Fig 4.1.2a. Fig 4.1.2 is the principal curve of the ridge shown in Fig 4.1.1.

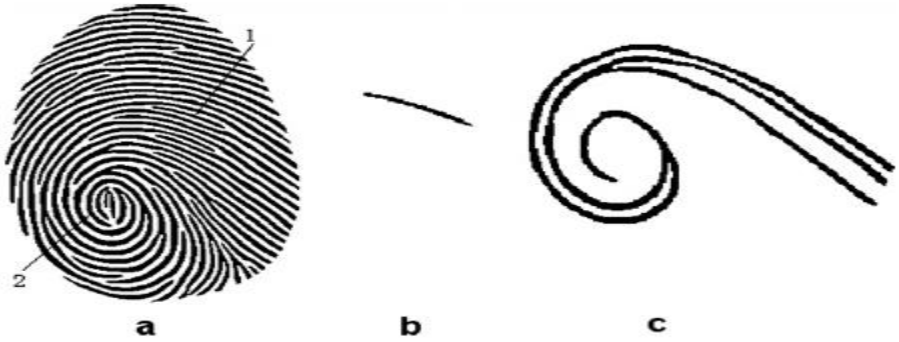


Fig 4.1.1 : a)Enhanced fingerprint image b) simple ridge c) complex ridge

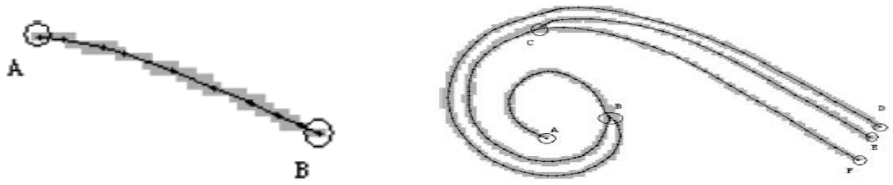


Fig 4.1.2 : a) Principal curve of a simple ridge b) Principal curve of complex ridge

The ridge consists of a single principal curve named AB (Note: Points A and B are two endings of this principal curve). The principal curve AB is a data set, and the first point and last point are two endings of principal curve. So we can analyze endings of principal curves first and then extract the fingerprint minutiae. complex ridge consists of 5 principal curves named AB , BC , BD , CE , CF . Each principal curve is a dataset, with the first and last point of dataset being the two endings of each principal curve. Based on the analysis, they proposed an algorithm to extract fingerprint minutiae from principal curves, which contains the following steps:

(1) Finding principal curve: After enhancing the image of a fingerprint, use the principal graph algorithm to get this fingerprint's skeleton which includes a set of principal curves.

(2) Extracting: Check the first point and the last point of each principal curve: if a single point is only in one dataset, then it is regarded as an ending of a simple ridge. If a point is found in three datasets, then it is regarded as an ending of a ridge bifurcation.

(3) Filtering: In this step, filter the ridge endings and ridge bifurcations obtained in the extraction step.

4.2 FINGERPRINT MINUTIAE EXTRACTION FROM SKELETONIZED BINARY IMAGES

Alessandro Farina, Zsolt M. Kovacs-Vajna, Alberto Leone proposed a new fingerprint minutiae extraction algorithm from skeletonised binary images The algorithm proposed in this paper works on the skeleton image obtained from a binarized version of the fingerprint image . New topological validation algorithms are presented to classify reliable endpoints and bifurcations: they are removed if topological requirements are not satisfied, they are classified as less reliable minutiae if requirements are not fully satisfied, else they are considered as highly reliable minutiae. This paper consists of several stages like pixel codification , pre-filtering , skeleton enhancement , minutiae validation , topological validation and final codification as shown in below Fig 4.2.1.

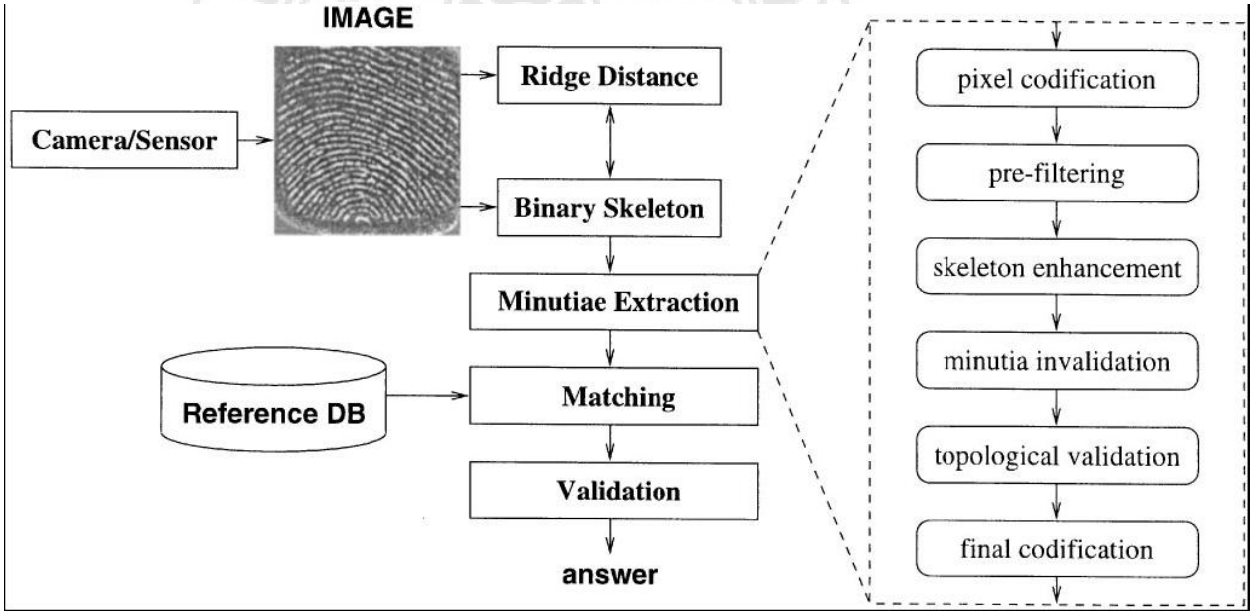


Fig 4.2.1 : General structure of an AFIS and details of minutiae extraction block

1) **Pixel codification**: This stage performs minutiae classification and removal of unclassified configurations. The skeleton image is processed in order to obtain a codified image the value of each pixel represents the number of outgoing branches in the corresponding pixel of the skeleton image

2) **Pre-filtering:** Pre-filtering is necessary to remove spurious minutiae without reducing the number of details useful for the identification. Pre-filtering scans the

codified image (row by row from top-left to bottom-right) In this phase an endpoint next to another minutia is deleted. Adjacent bifurcations are removed and those where one or more crosses are detected in their neighborhood. Crosses are removed if another cross is detected in their neighborhood.

3) **Skeleton enhancement:** Skeleton enhancement is for ridge repair by connecting endpoints identified as ridge breaks, elimination of bridges, spurs and short ridges. Two endpoints can be connected, if they are assumed to belong to the same ridge. The ridge repair algorithm has three steps: (i) Search of facing endpoints, (ii) Best endpoint selection and (iii) Ridge reconstruction

4) **Minutiae invalidation:** Minutiae originated by bridges and spurs are invalidated, once these configurations have been recognized. Close minutiae are also removed. Bridges and spurs islands are eliminated

5) **Topological validation :** It consists of bifurcation validation and endpoint validation

Bifurcation validation (Fig4.2.2)

For each valid bifurcation:

1) Compute the three branch directions on $N_{bv1}=3\lambda/2$ points;

2) If a minutia is found within $N_{bv2}=\lambda$ points: invalidate this bifurcation and go further;

3) Move along each branch for $N_{bv3}=\lambda/2$ points and verify that a lateral edge is present within$N_{bv4}=3\lambda/2$ points

4) If a lateral ridge is not found: invalidate this bifurcation and go further;

5) If lateral ridges are found: mark the bifurcation as a less reliable bifurcation;

6) Define a rectangular area ABCD with(Fig :4.2.2b)

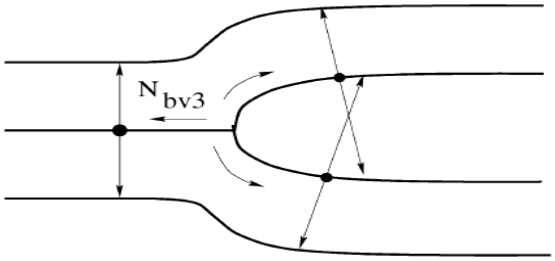
$AB=3\lambda/2$,

$AD=4\lambda$;

7) Move along the lateral ridges from the left intersections with the rectangle P0 and P1 to the right intersections P2 and P3;

8) If an endpoint is found: invalidate this bifurcation and go further;

9) If P2 and P3 are reached: mark the bifurcation as reliable.



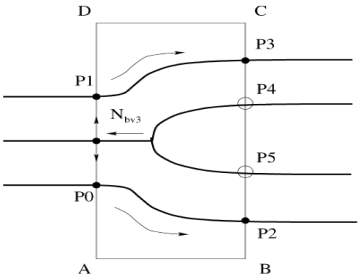


Fig : 4.2.2 a)Bifurcation Validation **4.2.2 b) Reliability Determination**

End point validation

For each valid endpoint:

1) Evaluate the endpoint direction defined as the direction of the broken ridge over Nr=λ points;
2) If the direction cannot be evaluated for the existence of a minutia within Nr points: invalidate the endpoint and go further;
3) Move along the endpoint ridge for N_{ev1}=λ/2 points;
4) Search orthogonally to the endpoint ridge direction for the neighboring ridges;
5) If within N_{ev2}=3λ/2 points the ridges are not intercepted: invalidate the endpoint and go further;
6) Define a rectangular area ABCD (Fig. 4.2.3) with:

   AB=3λ/2 and AD=3λ,
7) Lateral ridges are scanned from P0 and P1 to the exit from the rectangle (points P2 and P3) or a minutia occurrence;
8) If a lateral ridge crosses the rectangle in DC or AB, while the other crosses the rectangle in BC: mark the endpoint as a less reliable endpoint;
9) If a minutia is found: invalidate the endpoint and go further;
10) If both lateral ridges cross the rectangle in BC:

a) if the lateral ridges are not convergent: mark the endpoint as a less reliable endpoint else mark the endpoint as a highly reliable endpoint;

b) if a ridge is detected between P2 and P3: invalidate the endpoint

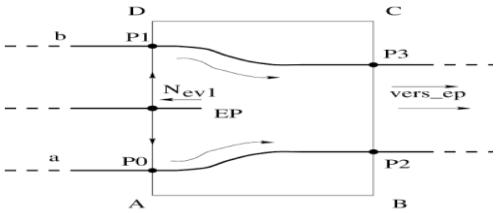


Fig 4.2.3 Endpoint validation

6) **Final codification:** The reliable and less reliable minutiae are determined

4.3 FINGERPRINT IMAGE POST PROCESSING

Marius Tico, Pauli Kuosmanen proposed a new algorithm for fingerprint image post processing This post processing algorithm detects and cancel false minutiae which are included in false minutia structures like spikes, holes, bridges, ladder structures, and spurs. The algorithm analyzes the neighborhood of each candidate minutia in order to decide whether the minutia is false or not . False minutiae structures are encountered in the minutiae . There are different types of false minutiae structures like bridge , ladder , spur ,hole etc. as shown in the below fig. The bridge and ladder structures; usually occur between close ridges. Very wide ridges may generate hole structures and very wide valleys may generate spurs

Fig 4.3.1 False minutiae structures

This algorithm operates directly onto the thinned ridge map image testing the validity of each candidate minutia. The candidate minutiae are detected in a single scan of the

thinned ridge map image using a 3 x 3 window. Each ridge pixel (value 1) is classified based on the number of 0 to 1 transitions met when making a full clockwise trip along its 8 neighborhood pixels. If there is only 1 such transition then the pixel is classified as a candidate ridge ending. If the number of transitions is 3 then, the pixel is classified as a candidate ridge bifurcation. In all other cases the pixel is not included into the candidate minutiae set. The number of candidate minutiae detected as above is much larger than the number of genuine minutiae in the fingerprint image. Most of the (Candidate minutiae have no meaningful correspondence into the fingerprint image, they being associated with different false minutia structures. The post processing algorithm presented in the following tests the validity of each candidate minutia by analyzing the thinned ridge map image in a W x W neighborhood of that minutia.

Algorithm for image post processing

For each candidate minutia (ridge ending or ridge bifurcation):

1. Create and initialize with 0 an image *L* of size *W* x *W*. Each pixel of *L* corresponds to a pixel of the thinned image which is located in a *W* x *W* neighborhood centered in the candidate minutia.
2. Label with -1 the central pixel of *L* (Fig4.3.2a). This is the pixel corresponding to the candidate minutia point in the thinned ridge map image.

3. If the candidate minutia is a ridge ending then:

(a) Label with 1 all the pixels in *L* which correspond to pixels connected with the candidate ridge ending in the thinned ridge map image .

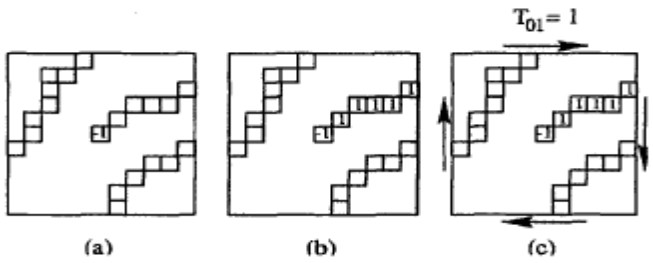


Fig 4.3.2 End point validation

(b) Count the number of 0 to 1 transitions (T_{01}) meet when making a full clockwise trip along the border of the *L* image

(c) If $T_{01} = 1$, then validate the candidate minutia as a true ridge ending.

4. If the candidate minutia is a ridge bifurcation then:

(a) Make a full clockwise trip along the 8 neighborhood pixels of the candidate ridge bifurcation, and label in L with 1, 2 and 3 respectively the three connected components met during this trip (Fig4.3.3).

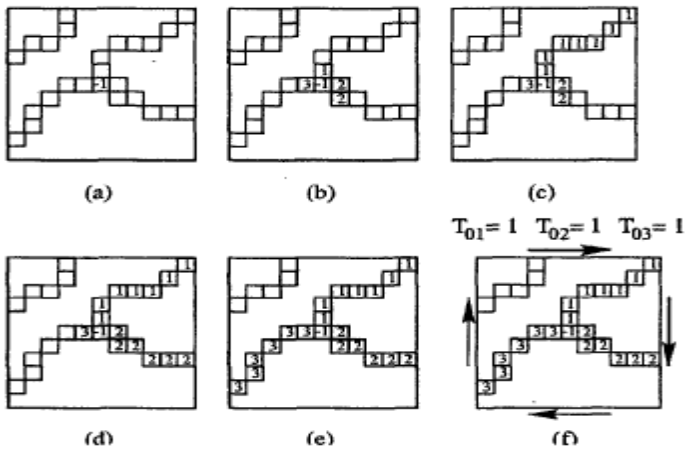


Fig 4.3.3 Bifurcation validation

(b) For each L = 1,2,3 (Fig 4.3.3 c,d,e), label with L all pixels in L which:

i. have the label 0;

ii. are connected with an L labeled pixel;

iii. correspond to 1 valued pixels in the thinned

(c) Count the number of 0 to 1, 0 to 2 and 0 to 3 transitions met when making a full clockwise trip along the border of the L image. The above three numbers are denoted by T_{01}. T_{02} and T_{03} respectively as shown in Fig 4.3.3 f.

(d) If $T_{01} = 1 \wedge T_{02} = 1 \wedge T_{03} = 1$, then validate the candidate minutia as a true ridge bifurcation

4.4 FINGERPRINT MATCHING FOR REAL TIME SYSTEMS

Ying Jie et.al 2005 [11] proposed a new fingerprint minutiae matching algorithm, which is fast, accurate and suitable for the real time fingerprint identification system. In this algorithm they used the core point to determine the reference point and used a round bounding box for matching. They used the fingerprint core to determine the reference point, which simplified the calculating processes. If two minutiae points are reference pair, the distances to the core points should be close.

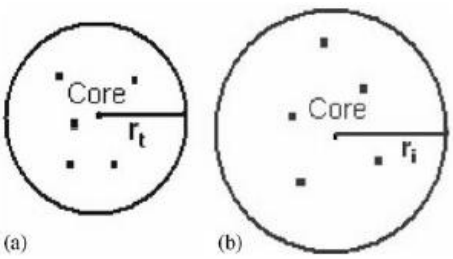


Fig 4.4.1. Reference area near core. (a) Template fingerprint. (b) Input fingerprint

Firstly, they took the core as the center of the template and input fingerprints, respectively. Then they selected a round area around the core. In these two areas, ensure that L same type minutiae points are included, e.g., all the minutiae are ridge endings. If the quality of the image is better, then L is smaller. The radii of the two round areas are r_t and r_i, respectively. Then we use the larger area as the reference area. That is, the radius of the reference area is determined by $r_c = \text{Max}(r_t, r_i)$.

After the reference minutia point pair is determined, convert each minutia point in the template minutiae set and input minutiae set into polar coordinate system. For a minutia point (x_i, y_i ,d_i ,r_i) conduct the conversion.

$$r_i = \sqrt{(x_i - x_r)^2 - (y_i - y_r)^2}$$

$$\theta_i = arctan((y_i - y_r)/(x_i - x_r)) + rot_i$$

$$\alpha_i = d_i - d_r$$

$$t_i = t_i$$

The minutia point in polar coordinate system is denoted as (r_i , θ_i , α_i , t_i), where r_i is radial distance, θ_i is radial angle, α_i is the minutia direction in polar coordinate system and t_i is the minutia type. For input fingerprint minutiae set conversion, rot_i is the difference angle of reference points calculated for input minutiae points, which is zero for the template minutiae points. Minutiae matching algorithm for real time system has the following steps

1. Determine reference area.
2. Choose P_i and Q_i points in the area as reference points and go to step (3). If all possible reference points are considered, go to step (6).
3. Convert each minutia point in template minutiae set and input minutiae set into polar coordinate system with respect to the corresponding reference points.

4. Sort the template minutiae set and input minutiae set by radial angle with increasing order.

5. Match the minutiae points in template minutiae set and input minutiae set in sequence. Firstly, select a bounding box around template minutia point. The bounding box will be introduced below. If there is a same type minutia point of the input minutiae set location in the bounding box, and its direction is close to the direction of the template minutia point in a threshold value, then we consider the two minutiae points match successfully and the score Score[i][j] is increased by one. If all minutiae points in template minutiae set are considered, go to step (2).

6. For all reference minutiae point pairs, find the maximal score value Score[i][j] and use it as the matching score of the template fingerprint and the input fingerprint. If the matching score is higher than a threshold value, then the input fingerprint can be considered to come from the same finger as template fingerprint.

4.5 FINGERPRINT MATCHING USING RIDGES

Jianjiang Feng, Zhengyu Ouyang, Anni Cai proposed a new fingerprint matching algorithm based on ridges A novel fingerprint matching algorithm is presented, which establishes both the ridge correspondences and the minutia correspondences between two fingerprints. First N initial substructure (including a minutia and adjacent ridges) pairs are found by a novel alignment method. Based on each of these substructure pairs, ridge matching is performed by incrementally matching ridges and minutiae, and then a matching score is computed. By this algorithm they established the ridge correspondences and the minutia correspondences between two fingerprints. The algorithm consists of three stages: preprocessing, alignment, and matching. In the preprocessing stage, ridges are extracted from the thinned image and sampled equidistantly, and relations between ridges and minutiae are established.

1) Preprocessing

1.1. *Feature extraction* : Matching algorithm is based on two types of features: minutiae and ridges. For a given grayscale fingerprint image, First the directional field is computed and the fingerprint is segmented into the foreground region and the background region. Then directional filtering is performed to improve the image

quality, and the enhanced image is binarilized and thinned to produce the ridge image. At last minutiae are detected on the ridge image.

1.2. *Ridge representation*: In order to make the ridge structures simple and consequently the matching algorithm easier, an operation, called clearup,is performed: (i) closed ridges are disconnected at an arbitrary point; (ii) ridges associated with bifurcations are split into three ridges; (iii) short ridges are removed

1.3. *Relations between ridges*: Adjacent relations between ridges are important constraints for ridge matching. The relations between points of adjacent ridges represent the relations between ridges since each ridge has been represented by a set of sampled points. For a point, a_i, on a ridge, draw a line segment centered at a_i, normal to the local ridge direction, with a length of w_1 pixels. On each side of the ridge, the nearest point to a_i on the first ridge intersected by the line segment is regarded as a neighboring point of a_i .A neighboring point of a_i is classified as a left or right neighboring point by checking its position when moving along ($a_{i-1} \rightarrow a_i \rightarrow a_{i+1}$). An example is given in below Fig 4.5.1

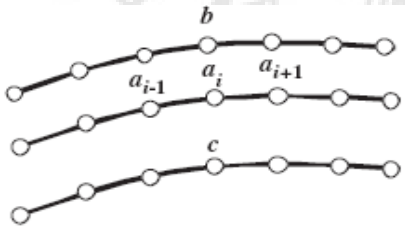


Figure 4.5.1: b and c are the left and the right neighboring points of a_i

2) Alignment

The objective of the alignment process is to recover the transformation between two fingerprints by some means and to align them as well as possible. After that, the ambiguity of correspondence is reduced greatly and the search for the best correspondence will be less complex.

2.1. Substructure

A substructure is constructed with the following way. First, each minutia is classified into termination or bifurcation by counting the number of ridges in a 3 × 3 window centered at this minutia. If the number is 1, the minutia is a termination; if

the number is 3, it is a bifurcation. For a termination, in addition to the ridge that the termination belongs to, two more adjacent ridges are included (see Fig. 4.5.2a). For a bifurcation, in addition to the three ridges that the bifurcation belongs to, two more adjacent ridges are also included (see Fig. 4.5.2 b).

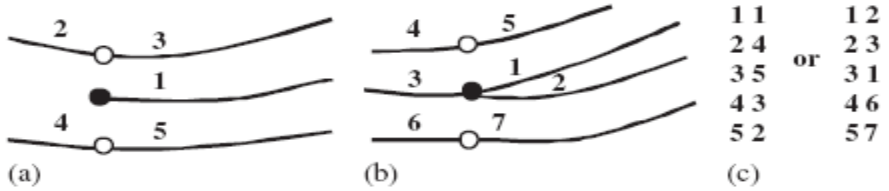


Fig 4.5.2 a) Substructure of termination b)substructure of bifurcation c) two possible correspondences between ridges when a termination is matched to a bifurcation.

Each adjacent ridge is split into two sub-ridges by a neighboring point of the minutia, which is called the projection point of the minutia, and each sub-ridge is assigned a label. The ridges of a substructure are labeled according to the order: first, the ridge that the minutia belongs to, and then the adjacent sub-ridges of the minutia. The three ridges that the bifurcation belongs to are labeled by checking the relative directions between the ridges. The adjacent sub-ridges of the minutia are labeled by checking the relative positions and the relative directions of the sub-ridges with respect to the minutia. Figs. (4.5.2 a) and (4.5.2 b) show examples for labeling of substructures of termination and bifurcation respectively. The necessary condition for a match of two substructures is that their minutiae are of the same type and their corresponding ridges have the same labels, or their minutiae are of different types, but their ridge labels have one of the two possible correspondences shown in Fig. (4.5.2 c).

2.2. Similarity between substructures

The objective of this step is not to compute a similarity degree between two substructures, but to give a binary decision if these two substructures are possibly matched. For each pair of corresponding ridges, r_1 and r_2, which both contain more than four sampled points, the similarity degree of them is computed as follows. Let $p_{1,1}$ and $p_{2,1}$ be the starting points of r_1 and r_2, $p_{1,2}$ and $p_{2,2}$ be the endpoints of r_1

and r_2. Assume the shorter one of two ridges is r_1, $p_{1,2}$ is the i^{th} point counting from $p_{1,1}$ and q is the i^{th} point counting from $p_{2,1}$. Then the similarity degree between the two ridges is $sr = 1 - |d1 - d2|/ \max(d1, d2)$, where d_1 denotes the Euclid distance between $p_{1,1}$ and $p_{1,2}$, and d_2 the Euclid distance between $p_{2,1}$ and q. Assume that the similarity degrees of n pairs of ridges are computed for a pair of substructures. These two substructures are regarded as possibly matched, if the following two conditions are both satisfied:

$$\begin{cases} sr_i > \sigma_1, \forall i \in [1, 2, \ldots, n], \\ (1/n) \sum_{i=1}^{n} sr_i > \sigma_2 2 \end{cases}$$

Where σ_1 and σ_2 are two thresholds and $\sigma_1 < \sigma_2$

2.3. Support from other substructure pairs

To compute the support of a substructure pair, which is possibly matched, from other substructure pairs, we perform a fast match for minutiae associated with each pair of corresponding ridges in these two substructures, and take the total number of matched minutiae as the support degree. For each pair of corresponding ridges in the substructure pair m1,1 and m2,1, we search the two lists of associated minutiae for matched minutiae (see Fig. 5). Take a pair of ridges as example (the wider ridges in Fig. 5). Two associated minutiae, m1,2 and m2,2, are said to be matched if the lengths (in terms of the number of sampled points) of the two sub-ridges between two pairs of reference points (minutiae or projection points) differ less than 3, and the two subridges are correspondent ridges in the substructure pair m1,2 and m2,2. In Fig. 5, in addition to m1,2 and m2,2 that are matched, m1,3 and m2,3 are also matched. The substructure pairs with the top N degrees of support will be selected as the initial substructure pairs for matching.

3. Matching

Given an initial substructure pair obtained in the alignment stage, we will gradually match other ridges and minutiae.A list, MRList, is used to store matched ridges, and another one, MMList, is used to store matched minutiae. The algorithm repeatedly generates candidate ridge pairs (CRP) and matches them, until no more ridges can be matched. A CRP consists of the ridge numbers, segment numbers, and candidate

point pairs (CPP) of the two ridges (or subridges). A priority queue, CRPQueue, is used to store CRPs. The CRP with more CPPs will have higher priority value. The matching algorithm is described as follows.

(1) Generate CRPs for the initial substructure pair. Estimate the affine transformation between the two substructures. Push CRPs, the estimated transformation and priority values into CRPQueue.

(2) If CRPQueue is empty, go to step 9; otherwise, pop up the first CRP, crp, in CRPQueue.

(3) Check the validity of crp. If invalid, then generate new CRPs and push the new CRPs into CRPQueue, and then go to step 2.

(4) Match crp using dynamic programming matching algorithm. If there is no matched portion between these two ridges, go to step 2.

(5) Store the matched portion and set the statuses of points to 0. The remaining portions are considered as new sub-ridges and the statuses of points are set to the new segment number.

(6) Generate CRPs from the newly matched ridges, and push CRPs, the current transformation and priority values into CRPQueue.

(7) Search the newly matched ridges for matched minutiae. If matched minutiae are found, for each minutia (substructure) pair, generate CRPs, compute the transformation and priority values based on the newly matched substructures, and push them into CRPQueue.

(8) Go to step 2.

(9) Compute the matching score.

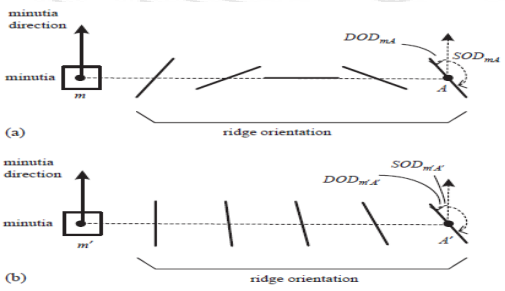
4.6 FINGERPRINT MATCHING BASED ON GLOBAL ALIGNMENT OF MULTIPLE REFERENCE MINUTIAE

En jhu et al. 2005 [13] proposed a minutia matching method based on global alignment of multiple pairs of reference minutiae. These reference minutiae are commonly distributed in various fingerprint regions. When matching, these pairs of reference minutiae are to be globally aligned, and those region pairs far away from

the original reference minutiae will be aligned more satisfactorily. Experiment shows that this method leads to improvement in system identification performance.

They extract local relative orientations (LROs) around a minutia. LRO is a kind of local feature around a minutia, and it can help to match two minutiae. LROs for a minutia are extracted at some sampling points around the minutia, and each LRO value is corresponding to a sampling point. The LRO is computed by algebraically summing the difference between adjacent ridge orientations from the minutia to the sampling point when tracking along the line connecting the two points. They call this the summed orientation difference (SOD). SOD differs from the direct orientation difference (DOD) between the minutia and the sampling point. Fig 4.6.1 gives out two examples of SOD and DOD**.** Fig. 4.6.1 contains a minutia *m* and a corresponding sampling point *A*. Fig. 4.6.2 contains a minutia m^1 and a corresponding sampling point A^1. Fig.4.6.1 shows that *A* and A^1 have the same DOD ($DOD_{mA} = DOD_{m^1A^1}$), but have different SOD ($SOD_{mA} \neq SOD_{m^1A^1}$). This is caused by the way by which the ridge orientation changes from the minutia to the sampling point. SOD can indirectly record this way, but DOD is not able to.

The sampling points for a minutia are selected from two lines which are orthogonal to each other and cross at the minutia. And one of the two lines is parallel with the direction of minutia. On each line, there are $2N + 1$ sampling points (including the minutia point), *N* points on each side of the minutia. The distance of two adjacent



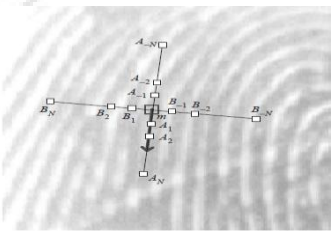


Fig 4.6.1.Two examples of SOD and DOD. **Fig 4.6.2. Orientation sampling points around a minutia**.

Sampling points of the same line is a constant *l*, which is called step length. Evidently, if the step length is small, the SOD between two adjacent sampling points of the same line is equal to the DOD between them. So the SOD at a certain point can be computed from the SOD of the previous point and the DOD between the two

points. For example $SOD_{mA2} = SOD_{mA1} + DOD_{A1A2}$. They denote LROs around a minutia as $D_\alpha = \{\alpha_i|_{i=-N}^{N}\}, D_\beta = \{\beta_i|_{i=-N}^{N}\}, \alpha_0 = 0, \beta_0 = 0$, α_i and β_i are in fact SOD values at point A_i and B_i , respectively, relative to the corresponding minutia. At last each minutia will consist of these characteristics (1) Coordinates (2) Direction (3) LRO (4) Sorting index This matching algorithm describes in detail the minutiae pattern matching process based on alignment of MRM, including (1) obtaining MRM, (2) alignment of MRM, (3) minutiae pairing, and (4) matching score computation

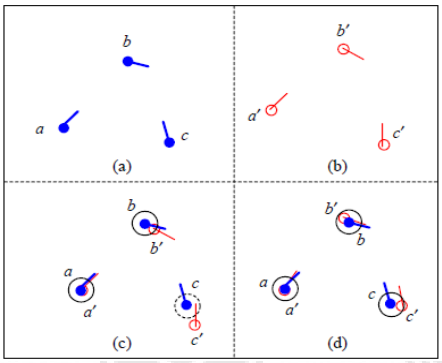


Fig 4.6.3 (a) minutiae set of the template (b) minutiae set of the query (c) Alignment based on a pair minutiae (d) alignment based on two pairs of minutiae

CHAPTER 5

FINGERPRINT MATCHING USING DESCRIPTORS

Fingerprint matching consists of two main parts

1. Fingerprint Minutiae Extraction
2. Fingerprint Matching

First we will discuss with Fingerprint Extraction and in the next section we discuss elucidate the fingerprint matching algorithm.

5.1 FINGERPRINT MINUTIAE EXTRACTION USING MATLAB

After the fingerprint ridge thinning, marking minutia points is relatively easy. The concept of Crossing Number (CN) is widely used for extracting the minutiae. 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 If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending ,i.e., if Cn(P) = = 1 it's a ridge end and if Cn(P) = = 3 it's a ridge bifurcation point, for a pixel P.

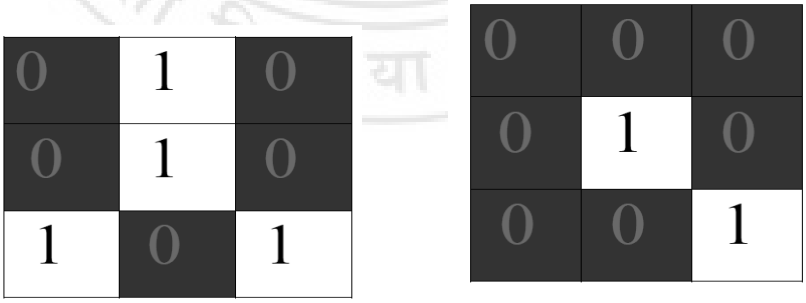


Fig 5.1.1 a) Bifurcation b) Termination

Taking the input as a gray scale image the minutiae can be extracted from the image

Fig 5.1.2 a) Input gray scale image **b) Image after binarization**

c) Fingerprint image after thinning **d) Image after minutiae extraction**

5.2 FINGERPRINT MINUTIAE EXTRACTION USING NBIS

For fingerprint extraction, we used NBIS 3.2.0 (National Biometric Image Software from http://www.itl.nist.gov/iad/894.03/nigos/nigos.html).It is open source software provided by NIST *(*National Institute of Standards and Technology). It incorporates new algorithms, a modular design, dynamic allocation, and flexible parameter control, which provide a framework for supporting future enhancement and adaptation of the technology. NBIS consists of different packages like 1. PCASYS: is a neural network based fingerprint pattern classification System, 2. MINDTCT is a fingerprint minutiae detector; 3. NFIQ is a neural network based fingerprint image quality algorithm, 4. NFSEG is a fingerprint segmentation system useful for segmenting four-finger plain impressions, 5. BOZORTH3 is a minutiae based

fingerprint matching system. We used MINDTCT package to extract minutiae. The algorithms and software parameters have been designed and set to optimally process images scanned at 19.69 pixels per millimeter (ppmm) (500 pixels per inch) and quantized to 256 levels of gray.

STEPS INVOLVED IN FINGERPRINT MINUTIAE EXTRACTION

5.2.1 Input fingerprint image file

Mindtct inputs a fingerprint image and automatically detects minutiae on the fingerprint. . The application can read files in ANSI/NIST, WSQ, JPEGB, JPEGL, and IHEAD formats. Mindtct has an option that will allow it to enhance very low contrast images. If the option is selected, mindtct will evaluate the histogram of the input image. If the image is a very low contrast image, it is enhanced to improve the contrast otherwise it is not modified.

5.2.2 Generate image quality maps

Because the image quality of a fingerprint may vary, especially in the case of latent fingerprints, it is critical to be able to analyze the image and determine areas that are degraded and likely to cause problems. Several characteristics can be measured that are designed to convey information regarding the quality of localized regions in the image. These include determining the directional flow of ridges in the image and detecting regions of low contrast, low ridge flow, and high curvature. Direction map represents area of the image with sufficient ridge structure Low Contrast map represents the area of low contrast. The low flow map marks the that could not be assigned a dominant ridge flow. The high curve map marks blocks that are in high curvature areas of the fingerprint

.

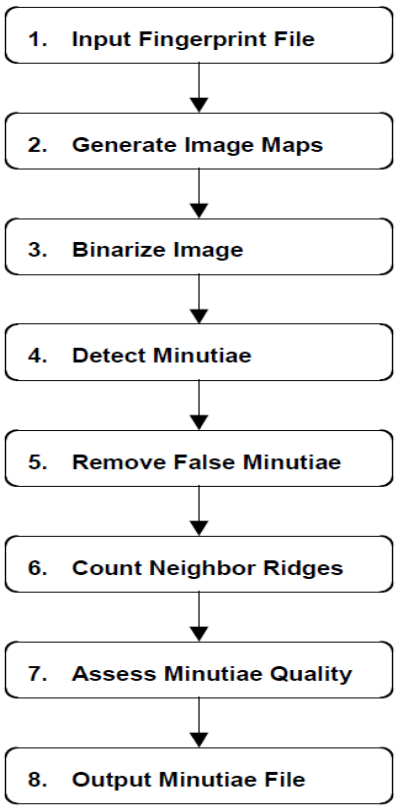


Fig 5.2.1 steps involved in Fingerprint Minutiae Extraction

5.2.3 Binarize Image

The minutiae detection algorithm in this system is designed to operate on a bi-level (or binary) image where black pixels represent ridges and white pixels represent valleys in a finger's friction skin. To create this binary image, every pixel in the gray scale input image must be analyzed to determine if it should be assigned a black or white pixel. This process is referred to as image binarization. A pixel is assigned a binary value based on the ridge flow direction associated with the block the pixel is within. If there was no detectable ridge flow for the current pixel's block, then the pixel is set to white. If there is detected ridge flow, then the pixel intensities surrounding the current pixel are analyzed within a rotated grid. This grid is defined in the global control structure, with column width set to 7 pixels and row height set to 9 pixels. With the pixel of interest in the centre, the grid is rotated so that its rows are parallel to the local ridge flow direction. Gray scale pixel intensities are accumulated along each rotated row in the grid, forming a vector of row sums. The binary value to be assigned to the centre pixel is determined by multiplying the centre row sum by the number of rows in the

grid and comparing this value to the accumulated gray scale intensities within the entire grid. If the multiplied centre row sum is less than the grid's total intensity, then the centre pixel is set to black; otherwise, it is set to white.

Fig 5.2.2. (a) Original image (b) Binarize image

It is desirable to preserve as much image information and ridge/valley structure as possible so that minutiae are not missed, and yet it is undesirable to accentuate degraded areas in the image to the point of introducing *false* minutiae. Significant effort has been invested to promote both robust and reliable binary images, and yet the current system tends to produce a considerable number of false minutiae. This is particularly troublesome when processing latent fingerprint images.

5.2.4 DETECT MINUTIAE

This step methodically scans the binary image of a fingerprint, identifying localized pixel patterns that indicate the ending or splitting of a ridge. The patterns searched for are very compact. Candidate ridge endings are detected in the binary image by scanning consecutive pairs of pixels in the image looking for sequences that match this pattern. Pattern scanning is conducted both vertically and horizontally. There are two patterns representing candidate ridge endings, the rest represent various ridge bifurcations. A secondary attribute of appearing/disappearing is assigned to each pattern. This designates the direction from which a ridge or valley is protruding into the pattern.(see Fig 5.2.3)

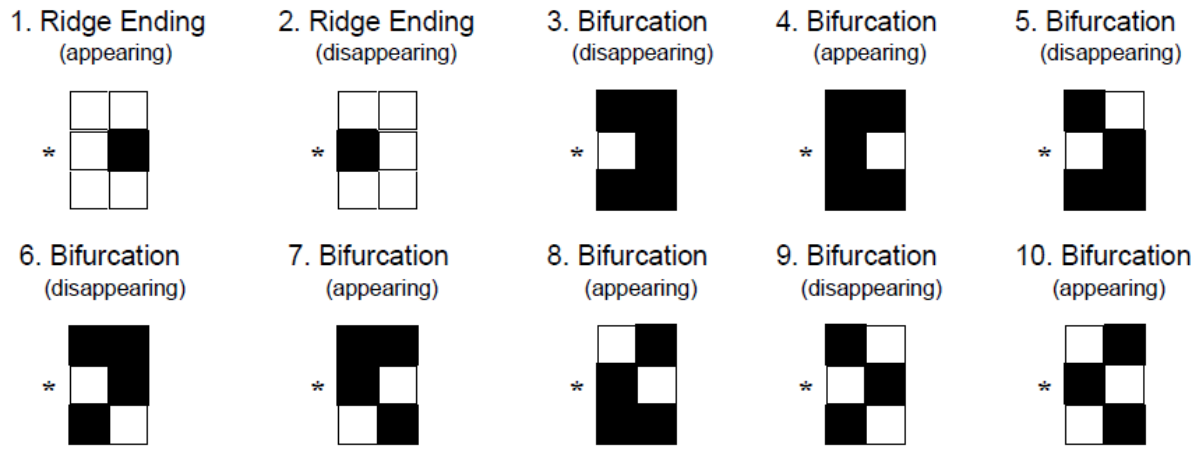


Fig 5.2.3. Pixel patterns used to detect minutiae.

5.2.5 REMOVE FALSE MINUTIAE

Using the patterns, candidate minutiae points are detected with as few as six pixels. This facilitates a particularly greedy detection scheme that minimizes the chance of missing true minutiae; however, many false minutiae are included in the candidate list. Because of this, much effort is spent on removing the false minutiae. These steps include removing islands, lakes, holes, minutiae in regions of poor image quality, side minutiae, hooks, overlaps, minutiae that are too wide, and minutiae that are too narrow (pores).

5.2.6 COUNT NEIGHBOUR RIDGES

Fingerprint minutiae matchers often use information in addition to just the points themselves. Ancillary information usually includes the minutia's direction, its type, and it may include information pertaining to minutiae neighbors. Beyond a minutia's position, direction, and type, there are no standard neighbor schemes. Different AFIS systems use different neighbor topologies and attributes. One common attribute is the number of intervening ridges (called ridge crossings) between a minutia and each of its neighbors.

5.2.7 ASSESS MINUTIA QUALITY

Even with the lengthy list of removal steps above, false minutiae potentially remain in the candidate list. A robust quality measure can help manage this in that false minutiae should be assigned a lower quality than true minutiae. Through dynamic thresholding, a tradeoff between retaining false minutiae and throwing away true minutiae may be determined. To this end, mindtct computes and reports minutiae qualities.

5.2.8 OUTPUT MINUTIAE FILE

Upon completion, mindtct, takes the resulting minutiae and outputs them to a file. The resulting minutiae can be accessed in the text file <filename>.min. A number of other output files are produced. These include a file for each of the image maps and a log file listing all the detected minutiae and their associated attributes. All of these are text files and are created by mindtct in the current working directory with fixed file names. The direction map is stored in <filename>.dm; the low contrast map is stored

in < filename>.lcm; the low flow map is stored in < filename>.lfm; the high curve map is stored in < filename>.hcm; and the quality map is stored in < filename>.qm. The maps are represented by a grid of numbers, each corresponding to a block in the fingerprint image. The last text output file, <filename>.min, contains a formatted listing of attributes associated with each detected minutiae in the fingerprint image. Among these attributes are the minutia's pixel coordinate location, its direction, and type.

5.3 FINGERPRINT MATCHING:

Here we used the descriptors for fingerprint matching

Fingerprint matching consists of two descriptors

1) Orientation based descriptor : which captures the orientation information around a minutia
2) Minutiae-based descriptor: which shows the relationship between a minutia and nearby minutiae.

   Both descriptors are combined to further increase the distinctiveness of minutiae.

Orientation based descriptor

Orientation based descriptors consist of ridge orientation information at some sampling points around a minutia, and the sampling points are defined by using sampling structure These sampling points are located on L circles centered at the minutia. Assume that the radius of the l^{th} circle is r_l and there are K_l sampling points distributed equally on the l^{th} circle (see Fig 5.3.1).

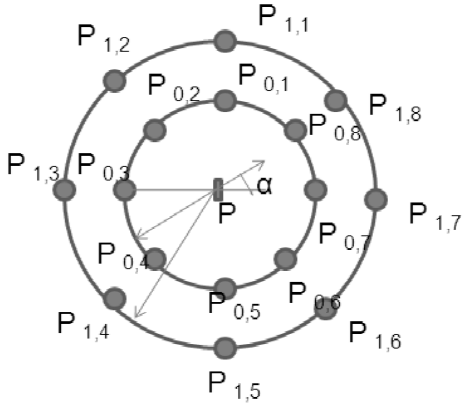


Fig 5.3.1 Distribution of sampling points

Using the minutia as origin and the direction of the minutia as the positive direction of *x* axis of polar coordinate system, the coordinate of the k^{th} sampling point on the l^{th} circle is defined as $\begin{cases} \rho_{l,k} = r_l \\ \theta_{l,k} = \frac{2\pi k}{k_l} \end{cases}$

In our experiments we used r_0 =26 , r_1=45 , k_0=k_1=8

The angle of minutiae is α and the orientation at sampling point is $\theta_{l,k}$. Then the relative orientation of $\theta_{l,k}$ with respect to α is computed as $\beta_{l,k}=\lambda(\theta_{l,k} - \alpha)$

$$\lambda(\alpha) = \begin{cases} \alpha - \pi \; if \; \alpha \geq \pi/2 \\ \alpha + \pi \; if \; \alpha < -\pi/2 \\ \alpha \; otherwise \end{cases}$$

The orientation based descriptor is represented as $D_o(p) = \left\{\{\beta_{l,k}\}_{k=0}^{K_l-1}\right\}_{l=0}^{L-1}$

Let $\alpha_{l,k}$ and $\beta_{l,k}$ denote the orientation based descriptors of two minutiae *p* and *q*, the similarity between them is computed as the mean value of the similarity of texture between valid corresponding sampling points So(p, q) = mean(so($p_{l,k}$, $q_{l,k}$)), where $p_{l,k}$, $q_{l,k}$ are sampling points of minutiae p and q , so($p_{l,k}$, $q_{l,k}$) is the similarity between the sampling points of minutiae p and q. Then the similarity between the sampling points is computed as $s_o(p_{l,k}, q_{l,k}) = e^{-|\lambda(\alpha_{l,k}-\beta_{l,k})|/(\frac{\pi}{16})}$

Minutiae based descriptor

Minutiae Based Descriptors shows the relationship between the minutiae and neighbouring minutiae Given a minutia p, its minutiae-based descriptor is defined as follows.

A minutia p' is called a neighbouring minutia of p, if the distance between p and p' is less than a predefined threshold r (50 pixels in our experiments) Let N(p) denote the set of neighbouring minutiae of p, and n_p denote the size of N(p). The minutiae-based descriptor of p is defined as $D_m(p) = \{(x_i, y_i, \theta_i)\}_1^{np}$, where (x_i, y_i , θ_i) are the x, y coordinate and angle of the i^{th} neighbouring minutia.. Let $D_m(q) = \{(x_i, y_i, \theta_i)\}_1^{nq}$ denote the descriptor of another minutia q. The similarity between $D_m(p)$ and $D_m(q)$ is defined as $s_m(p, q) = \frac{m_p+1}{M_p+1} \cdot \frac{m_q+1}{M_q+1}$

where m_p and m_q represent the number of matching minutiae of N(p) and N(q), respectively, and M_p and M_q represent the number of minutiae of N(p) and N(q) respectively.

Algorithm for minutiae based descriptor

1) Input: Take two minutiae files
2) For input fingerprint

   For each minutiae

   Calculate the Euclidean distance from all other minutiae

   If Euclidean distance <50

   Consider it as a neighborhood minutia for reference minutiae

   Calculate the number of neighbor minutiae for each minutia

   Display the distance value
3) For template fingerprint

   For each minutiae

   Calculate the Euclidean distance from all other minutiae

   If Euclidean distance <50

   Consider it as a neighborhood minutia for reference minutiae

   Calculate the number of neighbor minutiae for each minutia

   Display the distance value
4) To compare Input fingerprint and Template fingerprint find

a) if any of the Euclidean distance from minutiae to neighboring minutiae for both the fingerprint are equal and

b) No of neighbors minutiae >3

   Take those minutiae as reference for translation and rotation

   Apply translation and rotation to the input fingerprint

5) Translation

   Take the difference between X coordinates of fingerprint

   Computing Average difference in X (mean).

   Add the mean value for each X coordinate of input fingerprint

   Take the difference between Y coordinates of fingerprints

   Compute Average difference Y (mean)

   Add the mean value for each Y coordinate of input fingerprint

6) Rotation

   Take the difference between theta values of fingerprints

   Compute mean

   Add the mean value for each theta value of input fingerprint

7) Performing rotation and translation to Input fingerprint

8) Take the differences between the x ,y , theta value of template fingerprint image and transformed fingerprint image If the difference lies between threshold value Take it as matching minutiae (5<threshold<20).

9) Compute the Similarity score

Similarity score(S_m) = $s_m(p,q) = \frac{m_p+1}{M_p+1} \cdot \frac{m_q+1}{M_q+1}$

Combining minutiae descriptors

Since orientation-based descriptors and minutiae-based descriptors capture contemporary information, we further improve the discriminating ability of descriptors by combining two descriptors using the product rule, $s_c = s_o \cdot s_m$, where s_c, s_o and s_m represent the similarity of combined, orientation based and minutiae-based descriptors, respectively.

CHAPTER 6

Results

The experiments reported here have been conducted on the public domain collection of fingerprint images, DB1_B, DB2_B in FVC2002 (http://bias.csr.unibo.it/fvc2002). It comprises 80 fingerprint images of size 388×374 pixels captured at a resolution of 500 dpi, from 10 fingers. Each finger has eight impressions.
There are two types of matching; genuine matching and imposter matching.

Genuine Matching: It is the matching between two same fingerprint images

Imposter Matching: It is the matching between two different fingerprint images

We have two types of measurements to measure the efficiency for fingerprint matching algorithm. They are False Acceptance Rate (False Match rate) and False Non-Match rate (False Rejection Rate). False Acceptance is more severe than False Rejection because the system should not show an unauthorized user as an authorized user.

6.1 FALSE ACCEPTANCE RATE (FAR) OR FALSE MATCH RATE (FMR)

The false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

$$\text{False Acceptance Rate} = \frac{number\ of\ \ false\ Acceptances}{total\ number\ of\ \ attempts} \times 100\ \%$$

6.2 FALSE REJECTION RATE (FRR) OR FALSE NON-MATCH RATE (FNMR)

The false rejection rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an

authorized user. A system FRR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.

$$\text{False Rejection Rate} = \frac{number\ of\ \ false\ Rejections}{total\ number\ of\ \ attempts} \times 100\ \%$$

We computed FAR and FRR to get the efficiency of matching algorithm. We computed the FAR , FRR on FVC 2002 database DB1_B. The results are shown in the below table

Database	**Image size**	**FAR**	**FRR**
FVC2002 DB1	**388 x 374**	**0.08**	**0.132**
FVC2002 DB2	**388 x 374**	**0.062**	**0.109**

Comparison of proposed algorithm with others

Algorithms	**FAR**	**FRR**
On-line fingerprint Verification By Jain, A., Hong, L. and Bolle.	**0.084**	**0.17**
Fingerprint Matching Algorithm Based on Tree Comparison by Abinandhan Chandrasekaran Dr.Bhavani Thuraisingha	**0.035**	**0.1195**
Effective Algorithm for fingerprint matching by Ying HAO ,Tienie TAN	**0.01**	**0.15**

CHAPTER 7

Conclusion

Most of the fingerprint matching algorithms have been developed using minutiae based matching. In this project we proposed a novel fingerprint matching algorithm using descriptors and minutiae. For minutiae extraction we used NBIS software provided by NIST. The proposed fingerprint matching algorithm consists of two descriptors a) Orientation based descriptor: which captures the orientation information around the minutiae, minutiae based descriptor: shows the relationship between minutiae and nearby minutiae First, we extracted the minutiae and next the descriptors around each minutiae are established for template and input fingerprint images. The similarity value for orientation based descriptor, minutiae based descriptor is computed and similarity value is combined by using product rule and. The effectiveness of the proposed algorithm is tested on a public database FVC2002 DB1, DB2 and FAR, FRR is computed. Combined descriptor is much more discriminating than any single descriptor.

References

1. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition.* New York, NJ: Springer-Verlag.

2. Duoqian, M., Qingshi, T., & Wenjie, F. (2007). Fingerprint minutiae extraction based on principal curves. *Pattern Recognition Letters,* 28, 1009–1014.

3. Alessandro, F., Zsolt, M., K., & Alberto, L. (1998). Fingerprint minutiae extraction from skeletonized binary images. *Pattern Recognition,* 32, 877-889.

4. Jiea, Y., Fanga, Y. Y. Renjiea, Z., & Qifab, S. (2005) Fingerprint minutiae matching algorithm for real time system. *Pattern Recognition, 39,* 143 – 146.

5. Tico, M., & Kuosmanen. P. *(2000)* Algorithm for fingerprint image post processing. *IEEE,* 1735-1739.

6. Feng, J. (2007). Combining minutiae descriptors for fingerprint matching. *Pattern Recognition, 41,* 342-352.

7. Zhu, E., Yin, J., & Zhang, G. (2005) Fingerprint matching based on global alignment of multiple reference minutiae. *Pattern Recognition, 38,* 1685 – 1694.

8. Feng, J., Quyang, Z., & Cai, A. (2006). Fingerprint matching based on ridges. *Pattern Recognition, 39,* 2131 – 2140.

9. Stan, Z. L., & Jain, A. K. (2009) *Encyclopedia of Biometrics.* Springer.

10. Tico, M., & Kuosmanen, P. (2003). Fingerprint matching using an orientation based minutia descriptor. *Pattern Analy Mach Intell vol, 25,* 1009–1014.

11. Jain, A. K. Hong, L. & Bolle, R. (1997) On-line fingerprint verification. *Pattern Anal. Mach. Intell, 19,* 302–314.

12. Benhammadi, F., Amirouche, M. N., Hentous, H., Beghdad, K. B., & Assian, M. (2007). Fingerprint matching from minutiae texture maps. *Pattern Recognition, 40,* 189-197.

13. Chen, Z., & Kuo, C. H. (1991). A Topology-Based Matching Algorithm for Fingerprint Authentication. *Int. Carnahan Conf. on Security Technology*, 25, 84-87.

14. Qi, J., & Wang, Y. (2005). A robust fingerprint matching method. *Pattern Recognition, 38,* 1665-1671.

15. Zhu, En., Yin, J., & Zhang, G. (2005). Fingerprint matching based on global alignment of multiple reference minutiae. *Pattern Recognition, 38,* 1685-1694.

16. Nalini, K., Ratha, K. K., Chen, S., & Jain. A.K.(1996). A real time matching system for large database. *Pattern Analysis and machine intelligence, 18,* 799-813.

17. Jain, A. K., prabhakar, S., Hong, L., & Pankanti, S. (2000). Fiterbank-based fingerprint matching. *IEEE Transactions on Image Processing*, 9, 846-859.'

18. Watson, C. I., Garris, M. D., Tabassi, E., Charles, L., Wilson. R., McCabe, M., Janet, S., & Kenneth K. User's Guide To NIST Biometric Image Software.

19. Jia, J., Cai, L., Lu, P., & Liu X. (2007). Fingerprint matching based on weighting method and the SVM. *Neurocomputing, 70,* 849–858.

20. Tong, X., Liu, S., Huang, J., & Tang, X. (2008). Local relative location error descriptor-based fingerprint minutiae matching. *Pattern recognition letters, 29,* 208-294.

21. Tong, X., Huang, J., Tang, X., & Shi, D. (2005). Fingerprint minutiae matching using the adjacent feature vector. *Pattern recognition letters, 26,* 1337-1345.

22. http://fingerprint.nist.gov/NBIS

23. http://bias.csr.unibo.it/fvc2002/download.asp