Skeleton-based Fingerprint Minutiae Extraction

By

ZHAO Feng

A Thesis Submitted in Partial Fulfillment

of the Requirements for the Degree of

Master of Philosophy

in

Information Engineering

June 2002


香港中文大學
圖書館系統
27 MAR 2003
UNIVERSITY
LIBRARY SYSTEM
THE CHINESE UNIVERSITY OF HONG KONG

Abstract

With identity fraud in our society reaching unprecedented proportions and with an increasing emphasis on the emerging automatic personal identification applications, biometrics-based verification or identification is receiving a lot of attention. Biometrics, which refers to automatic personal identification based on distinctive physiological (e.g., fingerprints, face, retina, iris) or behavioral (e.g., gait, signature) characteristics, relies on "something that you are or you do" to make a positive personal identification with a high degree of confidence. It is inherently more reliable and more capable in distinguishing between an authorized person and a fraudulent imposter than traditional token-based or knowledge-based methods. Among all the biometric technologies, fingerprint-based identification system has received the most attention because of the long history of fingerprints and their extensive use in forensics.

Fingerprint minutiae are essentially ridge endings and ridge bifurcations that constitute a fingerprint pattern. Accurate automatic fingerprint minutiae extraction is critical for minutiae matching in an automatic fingerprint identification system. Primarily, there are two major approaches to fingerprint minutiae extraction: skeleton-based method and gray scale image-based method. The former approach extracts the minutiae from the skeleton of the fingerprint image. The skeleton is computed by thinning the binary image, which is obtained by adaptive thresholding of the input gray scale fingerprint image. The latter approach extracts the minutiae directly from the gray scale fingerprint image based on a ridge line following algorithm that follows the ridge lines in the fingerprint image until an ending or a bifurcation occurs. In this thesis, our objective is to develop a novel skeleton-based fingerprint minutiae extraction method.

We propose to use the fingerprint valley instead of ridge for the binarization-thinning process to extract fingerprint minutiae. We first use several preprocessing steps on the binary image in order to eliminate the spurious lakes and dots, and to reduce the spurious islands, bridges, and spurs in the skeleton image. By removing all the bug pixels introduced at the thinning stage, our

algorithm can detect a maximum number of minutiae from the fingerprint skeleton using the Rutovitz Crossing Number. This allows the true minutiae preserved and false minutiae removed in later post-processing stages. Finally, using the intrinsic duality property of fingerprint image we develop several post-processing techniques to efficiently remove the spurious minutiae. Especially, we define an *H*-point structure to remove several types of spurious minutiae including bridge, triangle, ladder, and wrinkle all together.

The performance of our proposed skeleton-based fingerprint minutiae extraction algorithms has been quantitatively evaluated in terms of "goodness index", which compares the automatically extracted minutiae with the minutiae obtained from the same fingerprint by a human expert. Experimental results clearly demonstrate the effectiveness of the new algorithms.

摘要

隨著身份詐騙現象日益嚴重，人們越來越看中最新出現的自動身份識別系統在日常生活中的應用，尤其是基於生物特徵的驗證或識別。所謂生物識別，是指基於人體所獨具的生理特徵〔譬如：指紋，人臉，視網膜，虹膜等〕或行爲特徵〔譬如：步態，簽名等〕的自動身份識別，它依賴於人體所具備的或所做的，提供可靠的身份識別。在分辨合法用戶和非法入侵者的有效性方面，生物識別比傳統的基於符號或基於認知的識別方法更加可靠。在所有的生物技術中，指紋識別系統越來越受到人們的重視，因爲指紋有着悠久的應用歷史，並且被廣泛用於司法鑒定。

指紋圖案主要由端點和交叉點兩種特徵構成。在自動指紋識別系統中，精確地自動提取指紋特徵對於指紋匹配尤爲重要。目前，主要有兩種指紋特徵提取的方法：基於細化圖的方法及基於灰度圖的方法。前一種方法從指紋的細化圖中提取特徵。此方法利用自適應二值化方法由指紋的灰度圖計算其二值化圖，然後由二值化圖得到指紋的細化圖。後一種方法從指紋的灰度圖中直接提取特徵，此方法利用 ridge line 跟蹤算法跟蹤指紋灰度圖中的 ridge line，直至遇到端點或交叉點，即指紋特徵點。在此論文中，我們的目標是設計一種新的基於細化圖的指紋特徵提取方法。

與眾不同的是，我們用指紋中的 valley 代替 ridge 進行二值化和細化操作來提取指紋特徵。我們首先對指紋的二值化圖進行預處理，以便去掉細化圖中的假特徵點，如 lakes，dots，同

時去掉另外一些假的特徵點，如 islands，bridges 和 spurs 等。然後，我們去掉細化過程中導致的一些 bug pixels。接着，我們用 Rutovitz Crossing Number 概念，從細化圖中最大可能地提取指紋特徵。此舉使得真正的特徵點得以保留，並使錯誤的特徵點在其後的 post-processing 階段得以有效去除。最後，利用指紋固有的二元性特性，我們設計了一些 post-processing 的算法用來有效地去除假的特徵點。尤其值得一提的是，我們定義了一種 H-point 結構，以便去除几種類型的錯誤特徵，包括 bridge，triangle，ladder 和 wrinkle。

我們通過比較由算法自動提取的指紋特徵和由手工標出的特徵，得到其性能指標〔goodness index〕，對我們所提出的基於細化圖的指紋特徵提取算法進行性能評估。實驗結果表明我們的新算法行之有效。

To My Family

Acknowledgments

Here I would like to acknowledge all the people who had assisted me during the two years of my graduate studies at the Chinese University of Hong Kong. I am most grateful to my supervisor, Dr. Xiaoou Tang, for his professional and personal advice, guidance and help on my research. He has provided me with numerous valuable ideas, insights, encouragement, and comments. He has been very understanding and supportive. I am very fortunate to have him as my advisor.

I would like to thank Feng Lin, Ph. D. candidate, for his useful discussion and help; Xiaogang Wang, M. Phil. Candidate, for his numerous suggestions, discussions, and help; Bo Luo, M. Phil. Candidate, for his useful discussion and help in programming. Special thanks to Zhifeng Li, Lifeng Sha, Hua Shen, Tong Wang and others in the multimedia laboratory for their numerous discussions and encouragement.

My sincere thanks go to all the members of my family, especially my parents for their never-fading love, care, understanding and encouragement, and to my girlfriend, Lilian, for her support, understanding and love. I could not have accomplished anything without their support and love. I owe my life and every achievement to them.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Automatic Personal Identification

- Is this person who he or she claims to be?
- Is this person authorized to enter this facility?
- Is this individual entitled to access the privileged information?
- Is the given service being administered exclusively to the enrolled users?
- Has this applicant been here before?
- Does this employee have authorization to perform this transaction?

Questions such as these are asked millions of times every day by hundreds of thousands of organizations in financial service, health care, electronic commerce (e-commerce), government, etc. All these questions are dealing with the same security issue — how to correctly and reliably identify an individual.

With the advent of electronic banking, e-commerce, and smart cards, with identity fraud in our society reaching unprecedented proportions and with an increasing emphasis on the privacy and security of information stored in various databases, automatic personal identification has become a very important topic. Automatically associating an identity with an individual is called automatic personal identification. It is now needed in a wide range of civilian applications involving the use of passport, cellular telephone, automatic teller machine (*ATM*), and driver license, etc.

Traditionally, automatic personal identification approaches have been widely used in two major types [1, 2, 3, 8]: (*i*) knowledge-based, (*ii*) token-based. The former approaches use "something that you know" such as password and personal identification number (*PIN*) to make a personal identification; the latter approaches use "something that you have" such as passport, credit card, ID card, and key to make a personal identification. These traditional personal identification approaches are very simple and can be easily integrated into different systems

with a low cost. However, they are prone to fraud because *PINs* may be forgotten or guessed by the impostors and tokens may be lost or stolen. Moreover, these traditional approaches cannot distinguish between an authorized person and an impostor who fraudulently acquires the "token" or "knowledge" of the authorized person. Therefore, they are not sufficiently reliable to satisfy the security requirements of our increasingly electronically interconnected information society.

1.2 Biometrics

Biometrics, which refers to automatic personal identification based on distinctive physiological (e.g., fingerprint, face, retina, iris) or behavioral (e.g., gait, signature) characteristics [1, 4, 5, 6], relies on "something that you are or you do" to make a positive personal identification with a high degree of confidence. It is inherently more capable and more reliable in distinguishing between an authorized person and a fraudulent imposter than traditional token-based and knowledge-based methods, because the biometric characteristics cannot be easily misplaced, forgotten, stolen, or forged. Moreover, the person to be identified needs to be physically present at the point of identification. Thus, biometrics provides us a solution for the security requirements of our increasingly electronically interconnected information society and will become the dominant automatic personal identification technique in the near future [1, 2, 3, 8]. So what does this mean? It means that in the very near future, passwords, *PINs*, and keys will disappear and be replaced by biometric identifiers like your fingerprints.

1.2.1 Objectives

The objectives of biometrics are:

- User convenience (e.g., money withdrawal without *ATM* cards and *PINs*);
- Reliable security (e.g., difficult to fraudulent access);
- Higher efficiency (e.g., lower overhead for computer password maintenance).

1.2.2 Operational Mode

On the one hand, a biometric system can be operated in two modes: (*i*) verification mode (one-to-one) and (*ii*) identification mode (one-to-many). A biometric system operating in verification mode either accepts or rejects a person's claimed identity (Am I whom I claim I am?) by comparing the captured biometric characteristics with his or her own biometric template stored in the system database or on the cards such as the smart card. While a biometric system operating in identification mode establishes an individual's identity (Who am I?) without a claimed identity by searching the entire template database.

On the other hand, a biometric system can be either (*i*) an online system or (*ii*) an offline system. An online system requires that a verification or identification should be performed quickly and need an immediate response; an offline system usually does not require that a verification or identification should be performed immediately and allows a relatively long response.

1.2.3 Requirements

What biological measurements qualify to be a biometrics? Any human physiological or behavioral characteristic can be used as a biometric characteristic to make personal identification provided that it has the following desirable properties [1, 2, 8]:

- Universality, which means that each person should have the characteristic;
- Uniqueness, which indicates that no two persons should be the same in terms of the characteristic;
- Permanence, which means that the characteristic should be invariant with time;
- Collectability, which indicates that the characteristic can be measured quantitatively.

In a practical biometric system, there are some other important issues that should be considered [2, 8], including:

- Performance, which refers to the achievable identification accuracy, speed, robustness, the resource requirements to achieve the desired identification accuracy and speed, as well as the working or environmental factors that affect the identification accuracy and speed;

- Acceptability, which indicates to what extent people are willing to accept a particular biometrics in their daily life;
- Circumvention, which refers to how easy it is to fool a biometric system by fraudulent techniques.

A practical biometric system should satisfy the following requirements [2, 8]:

- ✓ An acceptable identification accuracy and speed with a reasonable resource requirements;
- ✓ Not be harmful to the subjects;
- ✓ Be accepted by the intended population;
- ✓ Be sufficiently robust to various fraudulent techniques.

1.2.4 Performance Evaluation

Primarily, the performance of a biometric system is specified in terms of two error rates:

- False acceptance rate (*FAR*), which is defined as the probability that an impostor is accepted as a genuine user;
- False reject rate (*FRR*), which is defined as the probability that a genuine user is rejected as an impostor.

Clearly, *FAR* and *FRR* are dual of each other. A smaller *FAR* usually leads to a larger *FRR*, and vice versa. There is a trade-off between the two error rates and both of them cannot be reduced simultaneously based on the operating point (threshold in the decision rule) alone. The performance of a biometric system in performing automatic personal identification is usually specified in terms of its *FAR*. Therefore, the decision scheme should establish a decision boundary, which minimizes the value of *FRR* for a desired value of *FAR*. Different biometric applications dictate different *FAR* and *FRR* requirements. For example, access to a secure military installation requires a very low *FAR* at the expense of a higher *FRR*, but access to an *ATM* terminal desires a very low *FRR*.

1.2.5 Biometric Technologies

Currently, a number of biometric technologies have been either widely used or under intensive investigation include the following [1, 2, 8, 9, 10, 11, 12, 13, 14, 15]:

1. Physiological characteristics:
    - Face;
    - Fingerprint;
    - Hand geometry;
    - Hand vein;
    - Iris;
    - Retina;
    - Ear shape;
    - Body odor;
    - DNA;
    - Facial thermogram.
2. Behavioral characteristics:
    - Signature;
    - Gait;
    - Keystroke dynamics;
    - Voice.

Each biometric technology has its own advantages and disadvantages. No single biometrics is expected to effectively meet the needs of all the verification and identification applications [2]. A brief comparison of these fourteen different biometric technologies mentioned above is provided in Table 1.1.

Table 1.1 Comparison of biometric technologies [4].

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retina	High	High	Medium	Low	High	Low	High
Ear shape	Medium	Medium	High	Medium	Medium	High	Medium
Body odor	High	High	High	Low	Low	Medium	Low
DNA	High	High	High	Low	High	Low	Low
Facial thermogram	High	High	Low	High	Medium	High	High
Signature	Low	Low	Low	High	Low	High	Low
Gait	Medium	Low	Low	High	Low	High	Medium
Keystroke dynamics	Low	Low	Low	Medium	Low	Medium	Medium
Voice	Medium	Low	Low	Medium	Low	High	Low

To a certain extent, all these biometric technologies satisfy the requirements mentioned in section 1.2.3 and have been used in practical biometric systems [2, 8, 9, 15] or have the potential to become a valid biometric technique [2]. But most of them are not accepted in forensics as indisputable evidence of identity. In fact, the only legally acceptable, readily automated, and mature biometric technology is the fingerprint identification technique.

Among all the biometrics (e.g., face, fingerprint, hand geometry, hand vein, iris, retina, ear shape, body odor, DNA, facial thermogram, signature, gait, keystroke dynamics, voice, etc.), the fingerprint-based identification is one of the most reliable and proven mature technologies.

1.3 Fingerprint

Fingerprints are graphical flow-like ridges and valleys present on the surface of human fingers [4], as illustrated in Figure 1.1. They have been widely used for personal identification for over one hundred years [7]. The validity of fingerprint identification has been well established. In fact, fingerprint technology is so common in personal identification that it has almost become the synonym of biometrics [9].

1.3.1 Applications

Tremendous success of the fingerprint-based identification technique in various law enforcement departments around the world, the availability of cheap and compact solid-state fingerprint scanners [17, 18], the availability of inexpensive computing power, the availability of robust fingerprint matchers, and the increasing identity fraud have all ushered in an era to use fingerprints for automatic personal identification in a number of commercial, civilian, and financial applications, involving:

1. *Network access*
   - Electronic banking, e-commerce, and securities trading;
   - Electronic shopping (retail point-of-sale authentication);
   - Information and service access (e.g., web, internet, intranet);
   - Computer network security;
2. *Physical access*

- High security areas;
- Authorities;
- Access control (e.g., building, office, home);

3. *Device access*
   - Cellular phone;
   - PC, laptop computer log-in;
   - Car (driver licenses);
   - TV access;
   - Smart card;
   - *ATM* card;
   - Weapon;
4. *Identification*
   - Identification systems;
   - Social security benefits (welfare office, employment office);
   - Immigration (passports);
   - Airport check-in;
   - Law enforcement (criminal identification, prison security).

—Wherever you use a key or a password, your fingerprint can replace it.

Figure 1.1 A sample fingerprint image (black areas: ridges; white areas: valleys).

1.3.2 Advantages of Fingerprint Identification

The advantages of using fingerprints are as follows:

- Fingerprint identification is one of the most reliable and well-understood personal identification technologies;

- The validity of fingerprint identification has long been established and justified;
- Fingerprint is the most commonly used biometric technology which has the potential to become the dominant biometric technology in the very near future.

Fingerprints also have a number of disadvantages, including:

- Approximately 4% of the population does not have fingerprints of good quality due to postnatal marks (e.g., scratches, cuts) or occupational marks (e.g., manual workers);
- The commercially available fingerprint sensors cannot properly scan fingerprints from dirty fingers;
- Fingerprints are not suited for certain applications (e.g., surveillance) since they cannot be captured without the user's knowledge.

1.3.3 Permanence and Uniqueness

Fingerprints are fully formed at about seven months after the fetus was born and do not change throughout the life of an individual except due to accidents such as bruises and cuts on the finger tips. This shows that the fingerprint details are permanent.

In 1893, the Home Ministry Office, UK, accepted the discovery that no two individuals have the same fingerprints (i.e., the fingerprints of human beings are unique) [7]. The uniqueness of a fingerprint can be determined by the overall pattern of ridges and valleys (global information) as well as the local anomalies called minutiae, which will be described in Section 2.4.

1.4 Thesis Overview

The rest of this thesis is organized as follows. Chapter 2 presents an extensive overview on fingerprint identification. Chapter 3 introduces our live-scan fingerprint database obtained by four commercially available fingerprint sensors. Chapter 4 reviews the fingerprint minutiae extraction techniques and presents our preprocessing techniques for the skeleton-based fingerprint minutiae extraction method. A very efficient post-processing algorithm is described in Chapter 5. Chapter 6 contains the conclusions of our research.

1.5 Summary

Accurate automatic personal identification is now needed in a wide range of civilian applications involving electronic banking, e-commerce, access control, and the use of passports, smart cards. Biometrics, which refers to identify an individual based on his or her distinctive physiological or behavioral characteristics, relies on "something that you are or you do" to make a positive personal identification with a high degree of confidence. It is inherently more capable and more reliable in distinguishing between an authorized person and a fraudulent imposter than traditional token-based and knowledge-based methods. Among all the biometric technologies, fingerprint-based identification is one of the most reliable and proven mature techniques. A critical step in automatic fingerprint identification is reliably extracting minutiae from the input fingerprint image. In this thesis, our objective is to develop a novel skeleton-based fingerprint minutiae extraction method.

Chapter 2

Fingerprint Identification

2.1 History of Fingerprints

Fingerprint identification is one of the most reliable and proven mature technologies and fingerprints have been widely used for personal identification for over one hundred years [7]. Scientific studies on fingerprint technology were first initiated at the end of sixteenth century [7]. English plant morphologist, Nehemiah Grew, was the first fingerprint pioneer. In 1684, he published the first scientific paper reporting his systematic study on the details of ridges, valleys, and pores in fingerprints [7]. From then on, more and more researchers have engaged in studying on fingerprints. Starting in 1809, Thomas Bewick began to use an engraving of his fingerprint as his trademark in a few books (see Figure 2.1). It is believed to be one of the most important milestones of the scientific study on fingerprint identification [7]. In 1823, Joannes Evanelista Purkinje illustrated and described nine fingerprint patterns (arch, tented arch, left loop, right loop, and five types of whorls) in his thesis [7]. It is the first fingerprint classification scheme. In 1880, Henry Faulds wrote a letter to *Nature*, first scientifically suggested the individuality of fingerprints based on his own observation [7]. He recognized that fingerprint patterns were variable, but concluded that ridge details were permanent and unchangeable. He was believed to be the first person to identify fingerprints found at crime scenes. At the same time, William Herschel asserted that he had been experimenting with fingerprints for about twenty years [7].

The foundations of modern fingerprint identification were established by the studies of Sir Francis Galton and Sir Edward Henry in the late nineteenth century. Golton's study extensively examined the details that reside in fingerprints and he introduced the concept of minutiae for fingerprint identification in 1888 [5, 7]. Galton drew two fundamentally important conclusions: (*i*) the fingerprint of a person is permanent, i.e., it preserves its characteristics and shape throughout

one's life; (*ii*) the fingerprints of individuals are unique. According to the experimental evidence, it was proven that no two persons have the same fingerprints; even identical twins have different fingerprints despite signs of similarity. These two conclusions were the building blocks of research in the field of fingerprints over the last 90 years. Henry's study examined the global structure of fingerprints, and in 1899, he (actually his two Indian employees Khan Bahadur Azizul Haque and Rai Bahadur Hem Chandra Bose) established the famous "Henry System" of fingerprint classification [5, 7], which was introduced at Scotland Yard in 1901. This classification method is a very effective method for fingerprint indexing and is still in use in most identification systems nowadays. By using the ideas presented above, fingerprints are first classified by the Henry classification system and exact matching is carried out by comparing Galton minutiae.

Figure 2.1 Trademarks of Thomas Bewick [7].

In the early twentieth century, fingerprint was formally accepted as a valid sign of identity by law enforcement agencies and fingerprint identification became a standard procedure in forensics [7]. Fingerprint identification agencies were setup worldwide and criminal fingerprint database were established [7]. They developed various fingerprint identification techniques, including latent fingerprint acquisition, fingerprint classification, and fingerprint matching. However, manual fingerprint identification is tedious, time-consuming, and expensive, as it needs to

be performed by professional fingerprint experts. With the rapid expansion of fingerprint database, manual fingerprint identification became infeasible, even a team of over 1,300 professional fingerprint experts was not able to provide timely response. Therefore, in the early 1960's, the Federal Bureau of Investigation (*FBI*) Home Office (UK) and the Paris Police Department initiated studies on automatic fingerprint identification systems (*AFIS*) [39]. They made great progress so that many commercial *AFISs* are currently in operation in law enforcement agencies all over the world. These systems have greatly improved the efficiency of these agencies and successfully reduced the cost of hiring and training professional fingerprint experts.

With the advent of live-scan fingerprinting and the availability of cheap fingerprint sensors, *AFIS* has been highly utilized in civilian and commercial applications for positive personal identification besides forensic applications. Therefore, automatic fingerprint identification technology is in great demand. A number of commercially available *AFISs* [16, 17, 18] have been developed and tested on large databases.

2.2 *AFIS* Architecture

An *AFIS* can be operated in either verification mode (one-to-one) or identification mode (one-to-many). The *AFIS* operating in verification mode either accepts or rejects an individual's claimed identity (Am I whom I claim I am?); while the *AFIS* operating in identification mode establishes the identity of an individual without claiming his or her identity information (Who am I?). An *ATM* application is a typical example for an *AFIS* operating in verification mode, while a police application is a typical example for an *AFIS* operating in identification mode. Sometime, the *AFIS* can operate in an intermediate mode: one-to-few mode. "One-to-few" is essentially a "one-to-many" situation with a small database, for instance, a building access control system for a 100-person company.

There is quite a significant difference between verification and identification in terms of search and match routines. Verification only requires a match against one reference template, so the computation time is much shorter. On the other hand, identification requires a very efficient matching routine, as a search within

millions of fingerprints has to be performed in a short period of time. Generally, more time is spent in the stages of minutiae extraction and post-processing in order to assure that the survived minutiae are true minutiae. Otherwise, the probability of false matches is higher.

A typical block schema of an *AFIS* is shown in Figure 2.2. It mainly consists of five components: (*i*) input module, (*ii*) preprocessing module, (*iii*) enrollment module, (*iv*) authentication module, and (*v*) system database. Here, authentication means either verification or identification.

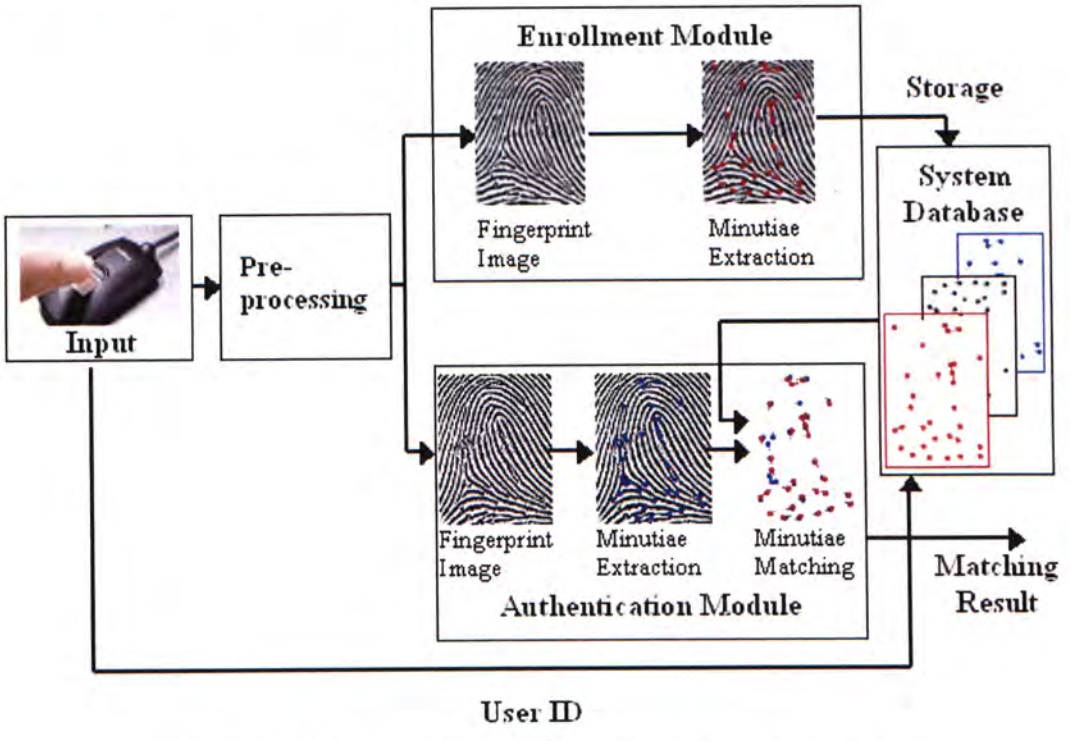


Figure 2.2 The block schema of an automatic fingerprint verification/identification system.

The input module consists of a high-resolution fingerprint sensor which captures the fingerprint images from the user. It also provides a mechanism for the user to indicate his or her identity (user ID). Typically, for the fingerprint sensor, the *AFIS* specifications require a resolution of 500 dpi (dot per inch), 8 bits per pixel (256 gray levels) for the acquired fingerprint images.

The acquired fingerprint image is subject to the preprocessing module which consists of general image enhancement and segmentation.

The enrollment module enrolls the fingerprint image of the user into the system database. When a fingerprint image is fed to this module, the minutiae extraction algorithm is applied to the input fingerprint image. The extracted minutiae can be

stored as a template on computer server, cellular phone, ID card, or *ATM* card. Minutiae extraction is a critical step, especially for enrollment. Subsequent matching will only be effective if the original reference minutiae template is clean and true, so special attention must be taken during enrollment.

The authentication module authenticates the identity of the user who intends to access the system. It can be organized into three steps: image acquisition, minutiae extraction and matching. During the authentication process, the user places his or her finger on the fingerprint sensor, thus a fingerprint image is scanned. Minutiae is extracted from the scanned fingerprint image and fed to the matching algorithm. If he or she claimed his or her user ID, the system operates in verification mode. The extracted minutiae are compared with the stored minutiae template of the claimed identity. If a match is made, the user is granted access; otherwise, the user will be rejected. If the user doesn't claim his or her user ID, the system operates in identification mode. The extracted minutiae are matched against all the minutiae templates stored in the system database and the matching result is a short list of the most likely candidates. The human expert makes the final decision of correct match by visual verification of this short list.

The system database consists of a collection of minutiae templates, each of which corresponds to an authorized user.

In an *AFIS*, you have to voluntarily touch the fingerprint sensor to show your actual agreement, which is quite different from face recognition. For example, you may be recognized without your approval. However, it is still possible to fool a fingerprint sensor. Since you leave your fingerprints everywhere (latent fingerprints), it is possible for some optical fingerprint sensors to be fooled by a copy of the latent fingerprint acquired using simple techniques, thus reducing the overall security of an *AFIS* system. To increase the security, several methods can be developed:

- ✓ Three-dimensional imaging technology;
- ✓ A sensor to detect a "living" effect such as electrical conductivity of the skin;
- ✓ A sensor that reads blood pressure through infrared sensors could detect that a finger is alive;
- ✓ Multiple fingers can be required even in a specific sequence, and a specific finger can be used to initiate a silent alarm;

✓ Several biometrics can be combined to increase the security.

2.3 Fingerprint Acquisition

Fingerprint acquisition is one of the critical processes in an *AFIS* and the quality of the acquired fingerprint images determines the performance of the entire system. The quality [20] refers to the clarity of ridges and valleys in the fingerprints. Distinct and well-separated ridges and valleys indicate a fingerprint of good quality. There are two primary methods of acquiring a fingerprint image: (*i*) inked (off-line process), (*ii*) live-scan (on-line process). An inked fingerprint image is typically acquired by scanning the impression of an inked finger on paper using a flat bed document scanner. The live-scan (inkless) fingerprint image is directly obtained from a finger by using a live-scan fingerprint sensor. In forensics, a special kind of inked fingerprints is called latent fingerprint (chance print), which is captured from the crime scene by dying the impression left by the suspect due to the presence of sweat pores in the fingertips, and then scanning the fingerprint. In this thesis, we concentrate only on live-scan fingerprints.

The inked fingerprints have the largest area of valid ridges and valleys with larger nonlinear deformations due to the inherent nature of the acquisition process. Acquisition of inked fingerprints is slow and cumbersome which is not feasible for an online *AFIS* and socially unacceptable. The live-scan fingerprints have a smaller fingerprint area with smaller nonlinear deformations because the sensor of small size only captures the ridges and valleys that are in contact with the acquisition surface. Both of them are scanned at a high resolution of 500 dpi. Latent fingerprints are partial fingerprints and are of poor quality. Figure 2.3 shows some fingerprint images acquired by different techniques.

The most popular sensing mechanism to obtain a live-scan fingerprint image is based on the optical frustrated total internal reflection (*FTIR*) technology [16]. When a finger is placed on one side of the prism, the ridges of the finger are in contact with the glass platen, while the valleys of the finger are not in contact with the glass platen. The rest of the imaging system essentially consists of an assembly of an LED light source and a CCD placed on the other side of the prism. The laser light source illuminates the glass at a certain angle and the camera is placed such that it can capture the laser light reflected from the glass. The light

that is incident on the plate at the glass surface touched by the ridges is randomly scattered, while the light incident on the glass surface corresponding to valleys suffers total internal reflection. Consequently, portion of fingerprint image formed on the imaging plane of the CCD corresponding to ridges are dark, and to valleys are white. Optical sensors are too large to be readily integrated in a number of applications (e.g., ID card, smart card, cellular phone). More recently, a number of different types of compact solid-state fingerprint sensors based on differential capacitance have become popular [17, 18]. The capacitance-based fingerprint sensors essentially consist of an array of electrodes. The fingerprint skin acts as the other electrode, thus to form a miniature capacitor. The capacitance from the ridges is higher than that from the valleys, which forms the basis of the capacitance-based sensors. The quality of the images acquired using these solid-state sensors is comparable to that of the images acquired using the optical sensors. These solid-state sensors are very small in size and they will become inexpensive in the very near future if manufactured in a large quantity. Another kind of fingerprint sensors is based on thermal sensing of temperature difference across the ridges and valleys in the fingerprint images [19].

(a) (b)

Figure 2.3 Examples of different types of fingerprints: (a) an inked fingerprint from NIST special database 4 (*NIST-4*); (b) a live-scan fingerprint captured by an optical fingerprint sensor ("StarTek FM100" by StarTek, Taiwan).

2.4 Fingerprint Representation

Fingerprints can be represented either by global information [21,22] or by local minutiae [10, 23]. The global representation of fingerprints is generally used for

indexing fingerprints (fingerprint classification). Two special types of features related to global representation are the singularity points (cores and deltas) [42], as illustrated in Figure 2.4. The core point is defined as the topmost point on the innermost recurving ridge and the delta point is defined as the center of a triangular region where three different direction flows meet.

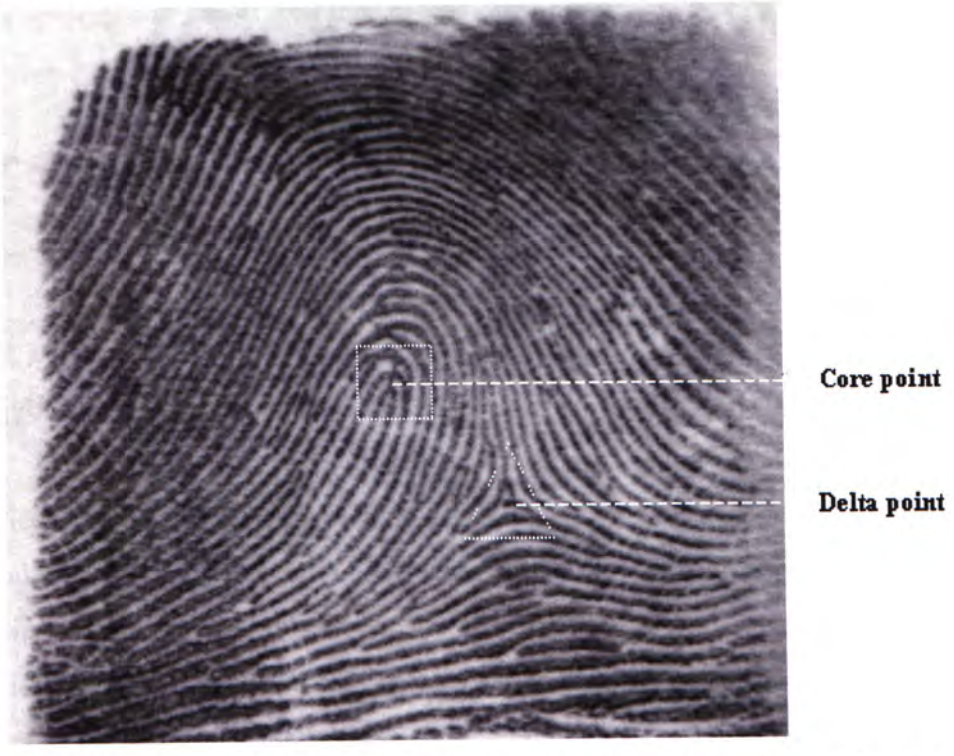


Figure 2.4 Illustration of the singularity points in a fingerprint image from *NIST-4*.

The most common representation used in fingerprint identification is the minutiae, because of the following reasons:

- Minutiae capture most of the individual information;
- Minutiae-based representation is storage efficient;
- Minutiae-based representation reduces the fingerprint matching problem to a point- or graph-matching problem.

Typically, there are two prominent types of minutiae (ridge endings and ridge bifurcations), as illustrated in Figure 2.5. A ridge ending is defined as the ridge point where a ridge ends abruptly. A ridge bifurcation is defined as the ridge point where a ridge forks or diverges into branch ridges.

Generally, a fingerprint is represented by the minutiae locations, minutiae types, and some attributes like minutiae orientation. Over one hundred years of study on fingerprints guarantees the uniqueness of minutiae-based representation for a large population of humans. A good quality fingerprint image typically has

about 40 to 100 minutiae [24], but a dozen of minutiae are considered sufficient to identify a fingerprint pattern [25].

Figure 2.5 Illustration of fingerprint minutiae ("x": ridge bifurcations; "o": ridge endings).

A less commonly used fingerprint feature is pores on the ridge surfaces that are also claimed to satisfy the uniqueness requirement [40, 41]. They can be used as auxiliary features in minutiae-based systems. A fingerprint is represented by the locations of pores and the local directions of the ridges at the pores locations. The pores-based representation also reduces the fingerprint matching problem to a point matching problem. The extraction of pores requires that the fingerprint image should be obtained at a high resolution of 1000 dpi.

2.5 Fingerprint Classification

Fingerprint classification refers to categorize a given fingerprint into one of the pre-specified categories based on the global ridge and valley structures. Fingerprint classification essentially provides us an indexing mechanism and plays an important role in fingerprint matching. This indexing mechanism significantly reduces the search time and computational complexity because the given fingerprint will only be matched against a subset of the fingerprints of the same class in the database, which may consists of millions of fingerprints. Since it is impossible for two fingerprint images of different classes to match with each other, fingerprint classification is viewed as fingerprint matching at a coarse level.

Generally, fingerprints are classified into five distinct classes, namely, arch (*A*), tented arch (*T*), left loop (*L*), right loop (*R*), and whorl (*W*), as illustrated in Figure 2.6. The natural distribution of these five classes is 0.037, 0.029 0.338, 0.317, and 0.279 for the classes *A*, *T*, *L*, *R*, *W*, respectively [36], which shows that the loop and whorl classes are very popular in our populations. Fingerprint classification is only effective in an *AFIS* operating in identification mode and is not an issue in an *AFIS* operating in verification mode.

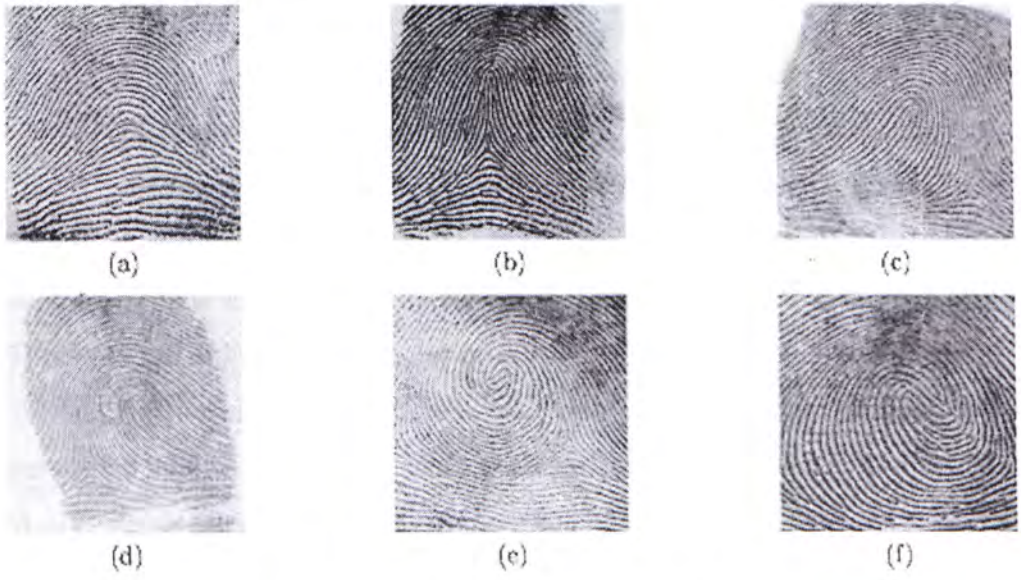


Figure 2.6 A coarse-level fingerprint classification of six categories: (a) Arch, (b) Tented arch, (c) Left loop, (d) Right loop, (e) Whorl, and (f) Twin loop. (Twin loop images are labeled as whorl in *NIST-4*.)

A number of approaches to fingerprint classification have been developed and can be categorized into the following categories:

- Knowledge-based approach [22], which performs the classification based on the number and relative locations of the detected singularity points;
- Structure-based approach [29], which employs both the geometric grouping and the global geometric shape analysis of fingerprint ridges to accomplish the classification;
- Neural network-based approach [36], which classifies the fingerprint images by a multilayer perceptron (*MLP*) network using the K-L transformed direction vectors as the input features;

- Frequency-based approach [30], which uses the frequency spectrum of the fingerprints obtained from the hexagonal Fourier transform for classification;
- Syntactic approach [31], which converts the fingerprint into a string of primitives and make classification based on this string;
- Statistical approach [21, 43], which uses a novel statistical representation (FingerCode) to make classification based on a two-stage classifier;
- Hybrid approach [32, 33, 34, 35], which combines more than two classifiers for fingerprint classification in order to improve the overall performance.

The *FBI* requirement of fingerprint classification is 1% error rate with a maximum of 20% reject rate. A state-of-the-art fingerprint classification algorithm [21] reports the following accuracies on 4,000 images in the *NIST-4* database:

A classification accuracy of 90% is achieved for the five-class problem and an accuracy of 94.8% for the four-class problem (arch and tented arch are merged into one class) after 1.8% of the fingerprint images are rejected during feature extraction stage. By incorporating a reject option at the classifier, the classification accuracy can be increased to 96% for the five-class classification task, and to 97.8% for the four-class classification task after a total of 32.5% of the images are rejected.

2.6 Fingerprint Matching

Fingerprint matching refers to use a similarity measure to determine whether or not two fingerprints are from the same finger. The similarity is determined based on the concept of correspondence in minutiae-based matching. A minutia m_i in the input fingerprint is considered as "corresponding" to the minutia m_j in the stored template if they represent the identical minutia scanned from the same finger. If the similarity (matching score) is greater than a certain predetermined threshold T, the input fingerprint matches the stored template fingerprint in the database; otherwise, they are not from the same finger.

Generally, a fingerprint matching process consists of three stages:

1. Two fingerprints to be matched are compared to determine whether or not they belong to the same class. If yes, go to stage 2, otherwise, it is impossible that these two fingerprints are from the same finger;
2. An alignment process is conducted in which several salient minutiae are first located and then an approximate alignment of the minutiae pattern is performed;
3. A matching process is applied in which the sum of the similarity between the corresponding minutiae pairs is evaluated, and finally, a decision is made based on the similarity.

Fingerprint matching has been approached from several different strategies:

The most commonly used matching approach is minutiae-based matching, which first locate the minutiae, and then match their relative placement between the input fingerprint and the stored template. There are two major approaches in minutiae-based matching: (*i*) point pattern-based matching and (*ii*) graph-based matching. The point pattern-based approaches [10, 28] consider the minutiae as a two-dimensional (*2-D*) point pattern. Two sets of minutiae are aligned and the sum of the similarity between the matched minutiae is calculated. Alignment plays an important role in point pattern-based matching and corresponds to enrollment (registration) in most of the *AFISs*. The graph-based approaches [26, 27] first construct a nearest neighbor graph from the fingerprint minutiae pattern, which codes the relative locations of minutiae, and then use an inexact graph-matching algorithm for matching. Alignment is not needed is graph-based matching.

Another matching approach is filterbank-based matching [44], which uses a bank of Gabor filters to capture both the local and global details in a fingerprint image as a compact fixed length FingerCode, and the matching is based on the Euclidean distance between the two corresponding FingerCodes.

2.7 Challenges

A number of commercial fingerprint identification systems [16, 17, 18] have been developed and tested on large databases, but most of them are still not able to meet the rigid performance requirements in many emerging civilian

applications. Fully automatic fingerprint identification is still a challenging problem. It currently faces the following challenges:

- Some information is lost when the three-dimensional fingerprint is scanned into a two-dimensional digital gray scale image;
- Different placements and pressures of the fingers on the fingerprint sensor may cause different fingerprint impressions and different deformations;
- In practice, due to variations in skin conditions (postnatal and occupational masks such as cuts, bruises on the fingers), fingerprint sensors, and non-cooperative attitude of subjects, a large number of scanned fingerprint images (about 10%) are of very poor quality. This leads to a significant number of spurious minutiae as well as missing minutiae, which greatly degrades the performance of fingerprint matching;
- It is difficult to develop an enhancement algorithm to robustly improve the quality of the fingerprint images of poor quality, thus to make it more suitable for minutiae extraction;
- It is difficult to design a reliable minutiae extraction algorithm to extract a robust representation due to the noise present in the fingerprint image;
- Fingerprint classification still remains a very hard task for both the human experts and the automatic systems. For example, approximately 17% of the fingerprint images in *NIST-4* belong to two different classes. On the other hand, only several fingerprint categories have been identified and the distribution of fingerprints into these categories is not uniform;
- It is difficult to propose a matching algorithm to reliably perform matching with a large number of fingerprints in real time. Quantitatively defining a reliable match measurement between two minutiae sets is still a difficulty.

2.8 Combination Schemes

Different approaches to the given task (e.g., fingerprint classification, fingerprint matching) may offer rather complementary information. This indicates

that a combination scheme is likely to improve the overall performance and applicability of a fingerprint identification system. The outputs of various approaches can be combined to obtain a decision which is more accurate than the decision made by any of the individual approach.

In addition, combination of multiple biometric characteristics has been shown to be very effective in improving the overall system performance [37]. For example, fingerprint verification is reliable but inefficient in database retrieval, while face recognition is fast but less reliable. A prototype biometric system which integrates face and fingerprint have been developed to overcome the limitation of fingerprint verification systems as well as face recognition systems [38]. The integrated system operates in the identification mode with an admissible response time and the identity established by the integrated system is more reliable than the identity established by the face recognition system. Thus, the integrated system meets both the response time and the accuracy requirements.

2.9 Summary

Among all the biometrics, fingerprint-based identification is one of the most reliable and proven mature technologies. Fingerprints are widely used for personal identification. The validity of fingerprint identification has been well established. In this chapter, we provide an overview of fingerprint identification including its long history. An *AFIS* is described along with the basic concepts involving fingerprint acquisition, fingerprint representation, fingerprint classification, and fingerprint matching. Various approaches to fingerprint classification and fingerprint matching have also been reviewed. In practice, fully automatic fingerprint identification is still a challenging problem. At the end of this chapter, we point out that the overall system performance can be improved by the combination schemes. Combination of multiple biometrics will be a very promising research topic.

Chapter 3

Live-Scan Fingerprint Database

3.1 Live-Scan Fingerprint Sensors

Four different fingerprint databases (hereinafter DB1, DB2, DB3, DB4) were collected by using the following live-scan sensors (see Figure 3.1):

- DB1: Optical sensor "StarTek FM100" by StarTek, Taiwan [16];
- DB2: Capacitive sensor "Precise 100SC" by Precise Biometrics, Sweden [17];
- DB3: Solid-state sensor "Veridicom" by Veridicom, CA [18];
- DB4: Thermal sensor "FingerChip™ FCD4B14" by ATMEL, CA [19].

Figure 3.1 Four different fingerprint sensors.

These commercially available live-scan fingerprint sensors are based on several different sensing mechanisms: (*i*) the StarTek FM100 is based on the optical frustrated total internal reflection (FTIR) technology, (*ii*) the Precise 100SC and the Veridicom are based on differential capacitance, (*iii*) FingerChip™ FCD4B14 is based on thermal sensing of temperature difference across the ridges and valleys in the fingerprint images. The sensing mechanisms have been described in Section 2.3.

3.2 Database Features

Totally, our fingerprint database (CUHK_DB) currently consists of over 30,000 fingerprint images and we are still in the process of enlarging it which will surely be a pretty large and practical fingerprint database. Table 3.1 summarizes the

global features of the four fingerprint databases and Figure 3.2 shows a sample image from each of them.

Table 3.1 The fingerprint database: CUHK_DB (15x15 mm = 0.6"x0.6", 0.4x14 mm = 0.02" x 0.55")

Data-base	Sensor Name	Sensor Type	Sensing Area	Image Size	Gray Levels	Image Type	Resolution	Database Size
DB1	StarTek FM100	Optical	15x15 mm	256x256	256	.bmp	500 dpi	14,220
DB2	Precise 100SC	Capacitive	15x15 mm	300x300	256	.png	500 dpi	11,000
DB3	Veridicom	Solid-state	15x15 mm	300x300	256	.tif	500 dpi	4,500
DB4	FingerChip	Thermal	0.4x14 mm	440x440	256	.bmp	500 dpi	500

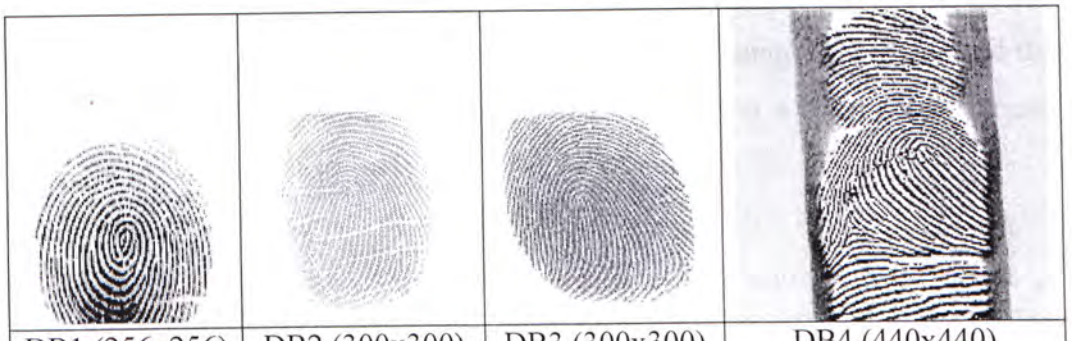


Figure 3.2 Examples of fingerprint images from DB1, DB2, DB3 and DB4. The four images are displayed at the same scale factor (35%) to demonstrate the different image size of each database.

To summarize, DB1 has the following features:

- The fingerprints were collected from 113 untrained volunteers;
- The subjects mainly consist of undergraduate and postgraduate students at the Chinese University of Hong Kong, and also their friends and relatives;
- Approximately 38% of the subjects are female, 80% of the subjects are under 25 years of age, 20% of the subjects are between the ages of 25 and 50;
- Up to ten fingers were collected for each volunteer (namely, right thumb, right index, right middle, right ring, right little, left thumb, left index, left middle, left ring, and left little in this order);
- For the first 31 volunteers, each finger was scanned in three directions including the vertical direction, left rotation between 0 to 15°, right

rotation between 0 to 15°, 10 fingerprint images for each direction (totally 31*10*3*10=9300 fingerprints); For the subsequent 82 volunteers, each finger was only scanned 6 times in the vertical direction (totally 82*10*6=4920 fingerprints);

- The volunteers were asked to lift their fingers between image acquisitions;
- The fingerprint core in each image was apparent, while the presence of deltas was not guaranteed due to the small sensing area of the sensor;
- The glass window of the sensor was systematically cleaned between image acquisitions;
- The acquired fingerprints were manually checked in order to assure that the maximum rotation is approximately in the range [-15°, 15°] and that each pair of impressions of the same finger has a nonnull overlapping area.

DB2 and DB3 were collected as follows:

- The fingerprints in DB2 were collected from 70 untrained volunteers;
- The fingerprints in DB3 were collected from 25 untrained volunteers;
- The subjects mainly consist of undergraduate and postgraduate students at the Chinese University of Hong Kong, and also their friends and relatives;
- Approximately 38% of the subjects are female, 80% of the subjects are under 25 years of age, 20% of the subjects are between the ages of 25 and 50;
- Up to ten fingers were collected for each volunteer;
- In DB2, ten fingerprints in the vertical direction were collected for the first 20 volunteers (totally 20*10*10=2000 fingerprints); and for the subsequent 50 volunteers, each finger was scanned in three directions including the vertical direction, left rotation between 0 to 15°, right rotation between 0 to 15°, 6 fingerprint images for each direction (totally 50*10*3*6=9000 fingerprints);
- In DB3, 18 images of each finger in three directions (i.e. vertical, left rotation and right rotation) were collected for 25 volunteers (totally 25*10*3*6=4500 fingerprints);

- The volunteers were asked to lift their fingers between image acquisitions;
- The presence of the fingerprint cores was guaranteed while the presence of deltas was not guaranteed;
- The sensor plate was not systematically cleaned between image acquisitions;
- The acquired fingerprints were manually checked in order to assure that the maximum rotation is approximately in the range [-15°, 15°] and that each pair of impressions of the same finger has a nonnull overlapping area.

DB4 has the following features:

- The fingerprints were collected from 8 laboratory members between the ages of 22 to 28 (one female);
- Up to ten fingers were collected for each member;
- Ten fingerprints in the vertical direction were collected for the first two members, and for the subsequent 6 members, each finger was scanned 5 times in the vertical direction (totally 2*10*10 + 6*10*5=500 fingerprints);
- FingerChip™ FCD4B14 is a sensor with silicon chips based on the thermal sensing technology and it may be the smallest sensor in the world. The volunteers only need to sweep their fingers along the sensor, a burst of slice images are captured and the complete fingerprint image is then reconstructed by mosaicking the multiple slices using proprietary software;
- The presence of the fingerprint cores and deltas was not guaranteed since no attention was paid on checking the correct finger position on the sensor;
- The sensor plate was not systematically cleaned between image acquisitions for no fingerprint mark left on the sensor;
- The acquired fingerprints were manually checked in order to assure that each pair of impressions of the same finger has a nonnull overlapping area;

- There are some fingerprint images with large distortion and reconstruction error due to the sweeping speed of the finger;
- There are some images with very low contrast due to the sensor's temperature close to the finger's temperature, i.e., the chip is sensitive to the temperature difference;
- Some images are captured by sweeping the finger in a reverse direction along the sensor, thus badly reconstructed.

Figure 3.3 and 3.4 show some sample images taken from DB1, DB2, DB3 and DB4, respectively.

Figure 3.3 Examples of fingerprint images from DB1. The top row is the sample images of right thumb, right index, right middle, right ring, and right little; the bottom row is the sample images of left thumb, left index, left middle, left ring, and left little, respectively, which are all taken from the same person.

3.3 Filename Description

The following is the description of the filename of the fingerprint images stored in the databases:

IDnnnDFI.FMT

| | | | | | | | | | |
| | | | | | | | * * *→ image format (".bmp", ".png", and ".tif"),
| | | | | | | *→ image number for the same finger (0~9, 0: first sample, … 9: tenth sample),
| | | | | | *→ finger number for the same person (0:right thumb, 1: right index, … 9: left little),
| | | | | *→ acquisition direction (V: vertical, L: left rotation, R: right rotation),
| | * * *→ individual number (one for each person, 000: first person, … 999: thousandth person),
* *→ identification.

For example, ID031V01.bmp means that this fingerprint image is the **Second** sample of the **First** finger (right thumb) of the 32nd person in **Vertical** direction.

Another example (ID032L83.bmp):

ID032	L	8	3.bmp
33rd person	**Left Rotation**	**9th finger**	**4th sample**

Generally, fingerprint images of all the fingers in the same direction have been stored in a specific directory. As all the fingerprint images have a different name, it is possible to put them all in the same directory without problem.

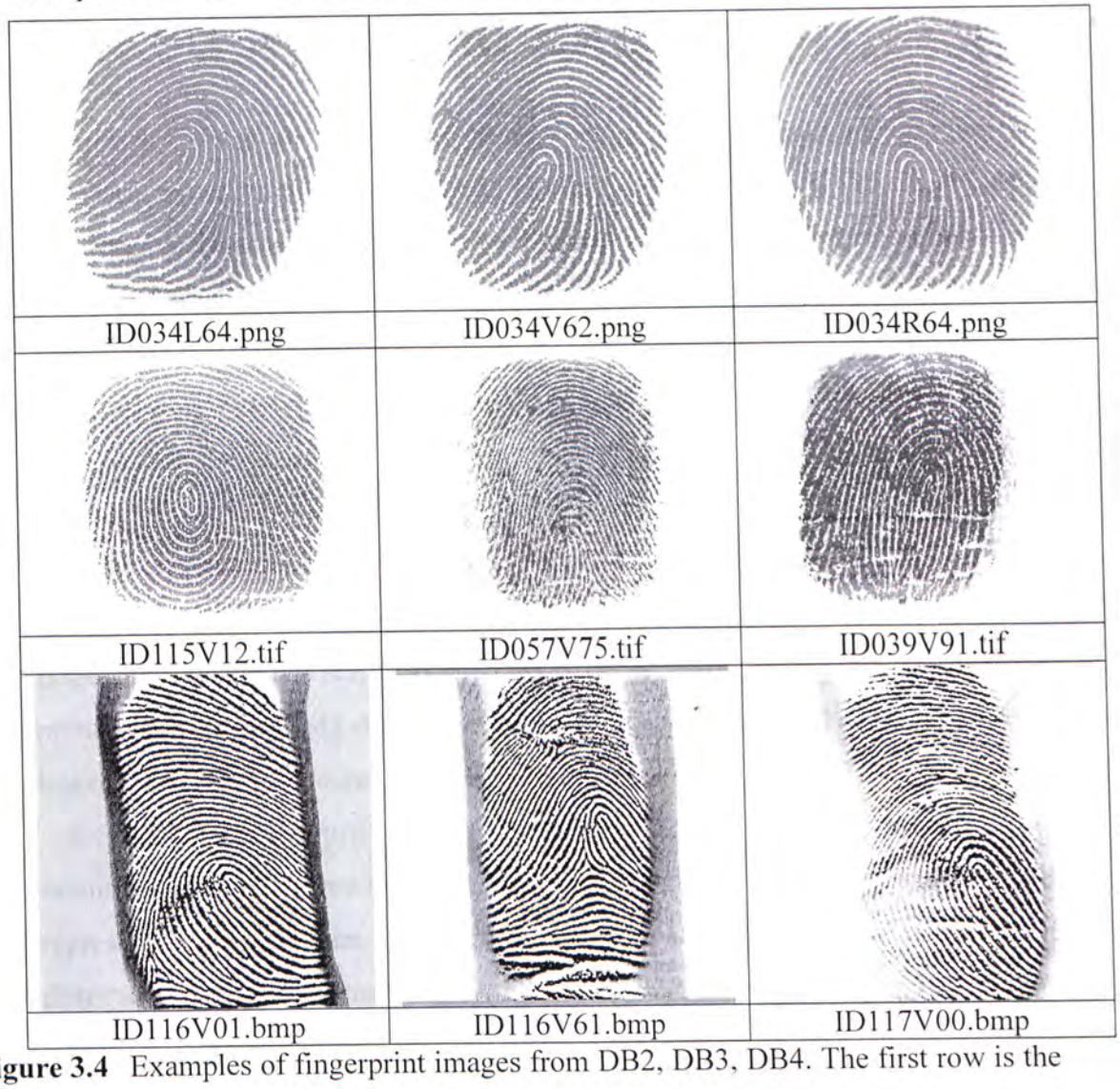


Figure 3.4 Examples of fingerprint images from DB2, DB3, DB4. The first row is the sample images in DB2 from the same finger in different directions. The second and the third rows are the sample images in DB3 and DB4 from different fingers and are roughly ordered by quality (left: high quality, middle: moderate quality, and right: low quality).

Chapter 4

Preprocessing for Skeleton-Based Minutiae Extraction

Primarily, there are two kinds of techniques for fingerprint recognition: (*i*) filterbank-based method [43, 44] and (*ii*) minutiae-based method [10, 23, 45, 46]. The filterbank-based algorithm uses a bank of Gabor filters to capture both the global and local information in a fingerprint as a compact fixed length FingerCode. The fingerprint matching is based on the Euclidean distance between the two corresponding FingerCodes. The widely used minutiae-based method first locates the minutiae points, and then matches their relative placement between the input fingerprint image and the stored template in the database.

In an automatic fingerprint identification system (*AFIS*), there are two most prominent types of minutiae which are used for their stability and robustness: (*i*) ridge endings and (*ii*) ridge bifurcations. A ridge ending is defined as the ridge point where a ridge ends abruptly. A ridge bifurcation is defined as the ridge point where a ridge forks or diverges into branch ridges.

Generally, a fingerprint pattern is represented by the minutiae locations, minutiae types, and some attributes like minutiae orientation. The minutiae-based representation is compact, amenable to matching algorithms, robust to noise and distortions, and easy to compute. Over one hundred years of study on fingerprints guarantees the uniqueness of minutiae-based representation for a large population of humans. In a fingerprint image of good quality, there are about 40 to 100 minutiae [24], but a dozen of minutiae are considered sufficient to identify a fingerprint pattern [25].

A good minutiae extraction algorithm should be both reliable and efficient. Reliability means that the minutiae extraction algorithm should (*i*) not create spurious minutiae, (*ii*) not miss true minutiae, and (*iii*) be precise in locating minutiae and computing minutiae orientation. However, reliable extraction of

minutiae from fingerprint images is a very hard task. Efficiency means that the minutiae extraction algorithm should be able to operate in "real-time" in the online applications such as *ATM* card security, smart card security, and access control. However, there is a trade-off between efficiency and reliability. In practice, the design strategy is to select a set of operations that are efficient in both speed and reliability.

4.1 Review of Minutiae-based Methods

Reliable extraction of minutiae from fingerprint images is a very difficult problem. Various approaches to automatic minutiae extraction have been proposed in the literature. Most of the techniques [10, 20, 45, 46, 47] extract the minutiae from the skeleton of the input fingerprint image. The skeleton is computed by thinning the binary image, which is obtained by adaptive thresholding of the gray scale fingerprint image.

An original technique based on a ridge-line following strategy is proposed in [23] to extract the minutiae directly from the gray scale fingerprint image. The minutiae are located by finding the intersection and excessive bending during the following. Although they claimed that the algorithm could perform better on noisy and low contrast images, it faces a problem on how to determine the thresholds of growing step and bending angle, which hinders its application for an automatic identification system. In addition, the robustness of this method with respect to image quality is questionable due to the fact that the gray-level ridge-line following algorithm may behave unpredictably when ridges and valleys are not well defined.

Besides, neural network-based approaches can be found in [48,49]. The neural network-based minutiae extraction algorithm extracts the minutiae from the fingerprint images via a multilayer perceptron (*MLP*) classifier. The back-propagation learning technique is used for its training, and the input to the *MLP* is a set of selected feature vectors. Unfortunately, the performances of these approaches have not been established.

In this thesis, we focus our attention on the skeleton-based minutiae extraction method.

4.2 Skeleton-based Minutiae Extraction

The skeleton-based minutiae extraction algorithm generally consists of the following main steps:

1. Use an adaptive thresholding algorithm to compute the binary image from the input gray scale fingerprint image;
2. Use a thinning algorithm to compute the fingerprint skeleton from the binary image;
3. Use Rutovitz crossing number to extract minutiae from the skeleton of fingerprint image;
4. Post-processing the minutiae set according to some heuristic rules.

There are two types of minutiae, ridge endings and ridge bifurcations. Ridges are generally used for minutiae extraction, since most previous researches assume that the ridges and valleys in the fingerprint have a similar width and are equally spaced. In fact, this may not always be true for various fingerprints collected by different scanners. For example, the fingerprint images we collected using an optical scanner (DB1, as described in Chapter 3) show that the average ridge width (typically 6 pixels) is larger than the average valley width (typically 3 to 4 pixels), as illustrated in Figure 4.1. Since a thinner binary image is easier for skeleton computation, we propose to use the valley instead of ridge for minutiae extraction. Accordingly, we use valley endings and valley bifurcations as fingerprint minutiae due to the intrinsic duality property of fingerprints [5].

In our algorithm, we first use several preprocessing steps on the binary image in order to eliminate the spurious lakes and dots, and to reduce the spurious islands, bridges, and spurs in the skeleton image. After the valley skeleton is extracted from the binary image, ideally, the width of the skeleton should be strictly one pixel. However, this is not always true, especially at the intersection points, thus producing spurious minutiae points. Therefore, we use a new algorithm to remove such pixels to improve minutiae extraction. By removing all the bug pixels introduced at the thinning stage, our algorithm can detect a maximum number of minutiae from the fingerprint skeleton using the Rutovitz Crossing Number. Finally, a very efficient post-processing algorithm is proposed to eliminate a significant number of spurious minutiae.

Figure 4.1 Fingerprint images acquired using the StarTek FM100 sensor (White areas: valleys; Black areas: ridges. The ridges are thicker than valleys.).

4.2.1 Preprocessing

By observation, most of the misconnections in the fingerprint skeleton images are introduced by the diagonal pixels in the binary image, as shown in Figure 4.2.

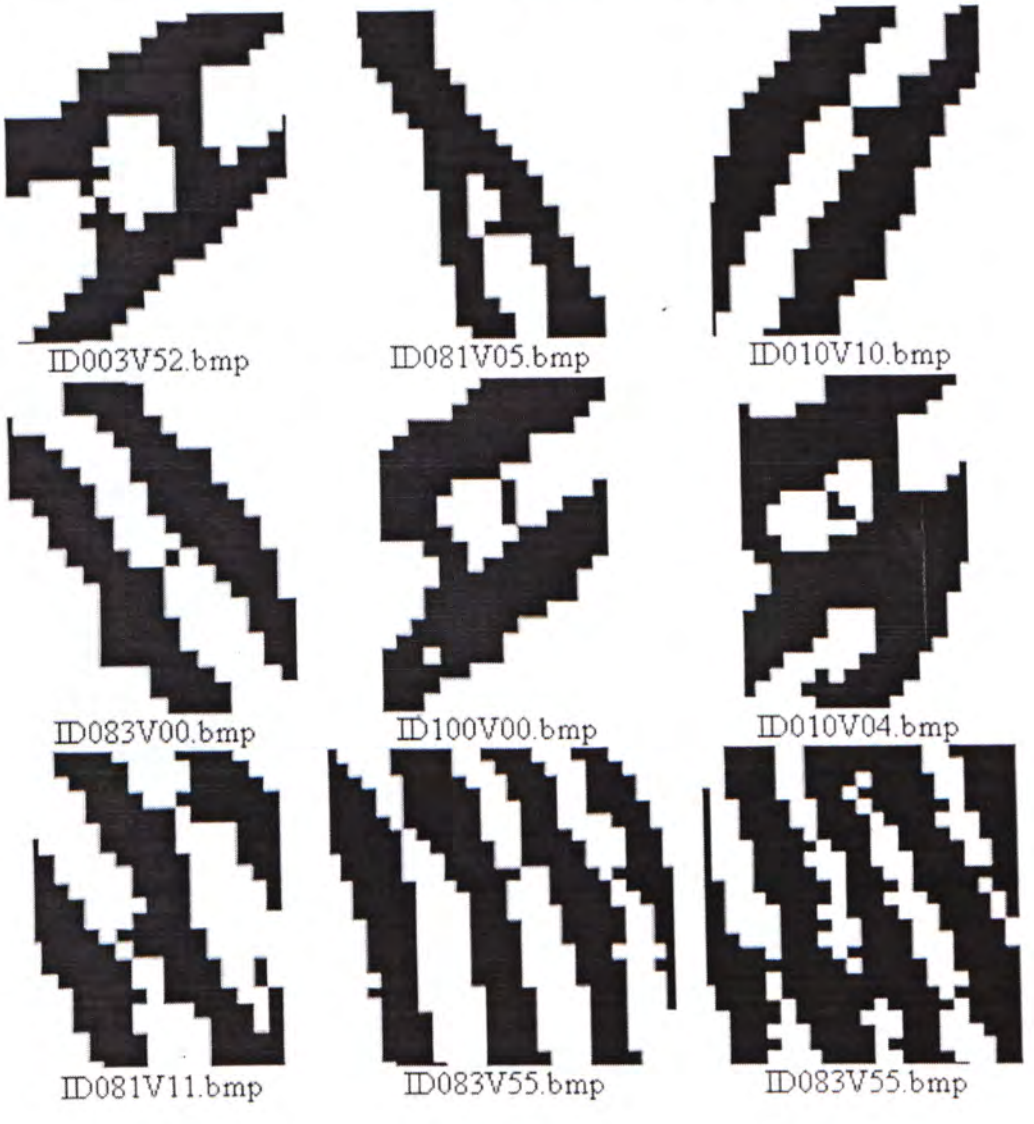


Figure 4.2 Examples of black diagonal pixels which introduce misconnected structures in the thinning image (Black: valley; white: ridge).

The diagonal pixels and the isolated regions, as illustrated in Figure 4.3 and Figure 4.4, introduce ridge lakes and valley lakes in the ridge skeleton image and valley skeleton image, respectively.

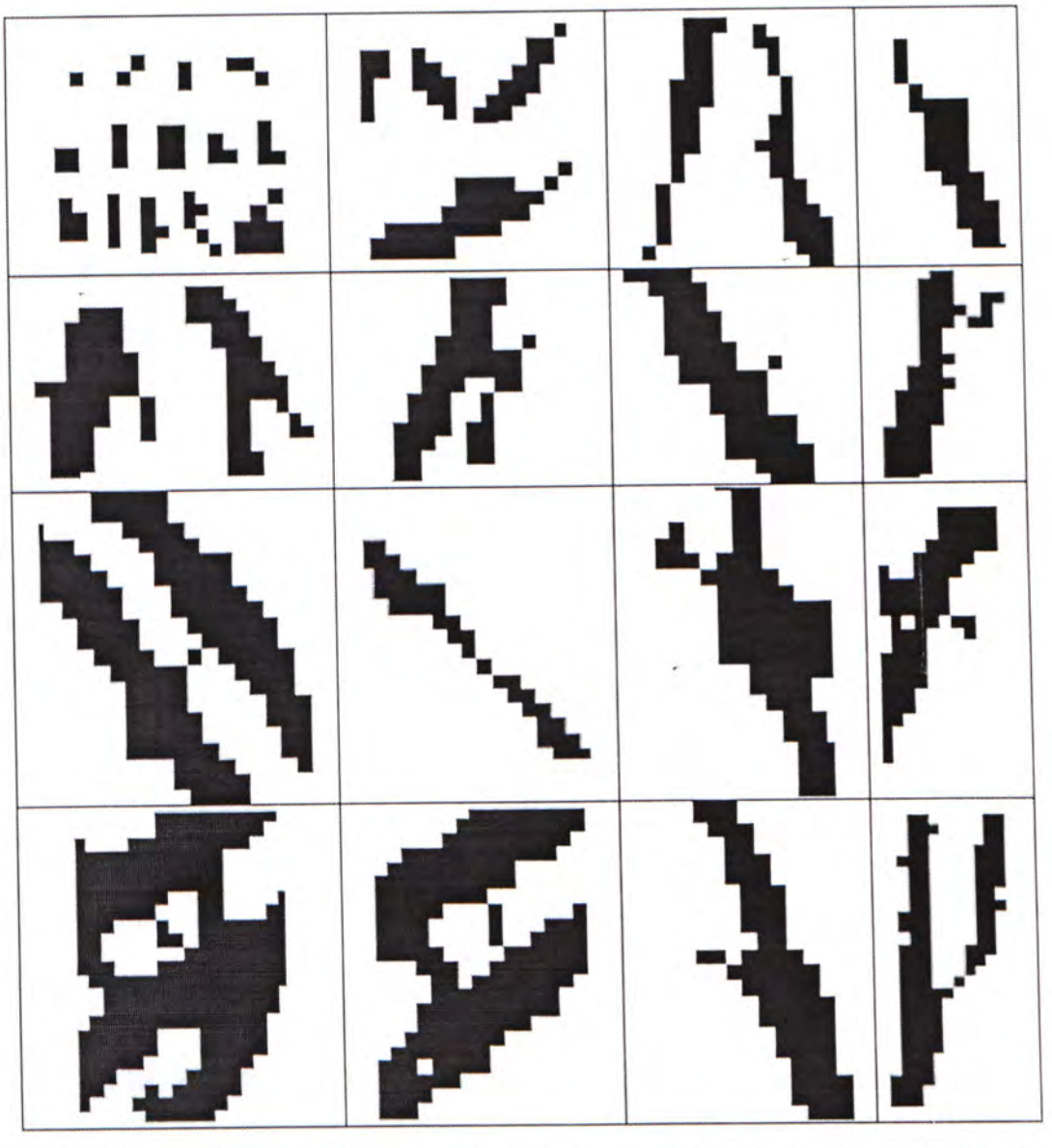


Figure 4.3 Examples of the isolated regions consisting of black pixels and the black diagonal pixels which introduce ridge lakes in the ridge skeleton images.

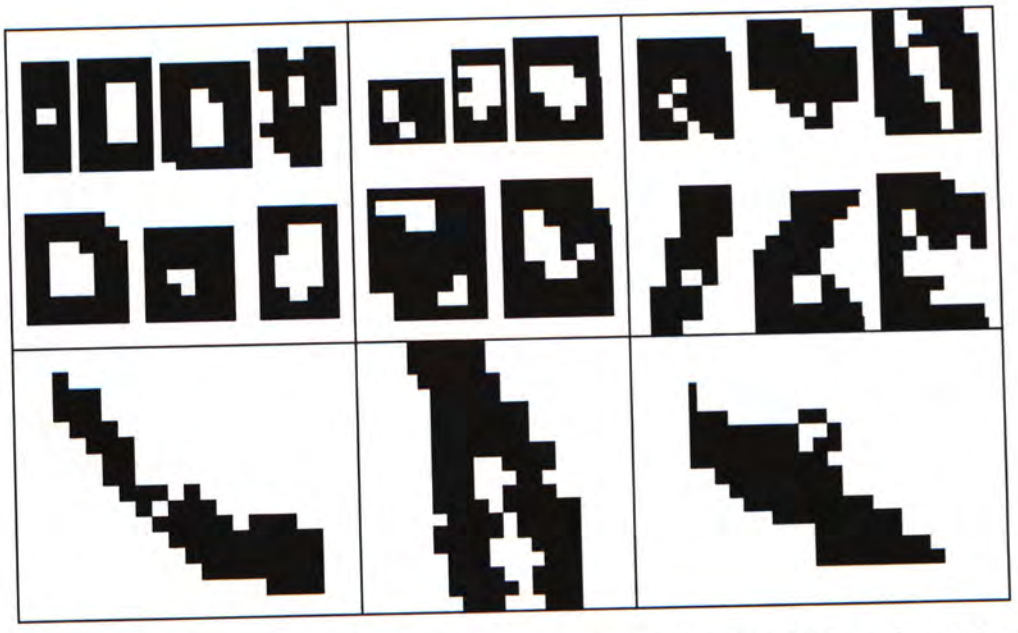
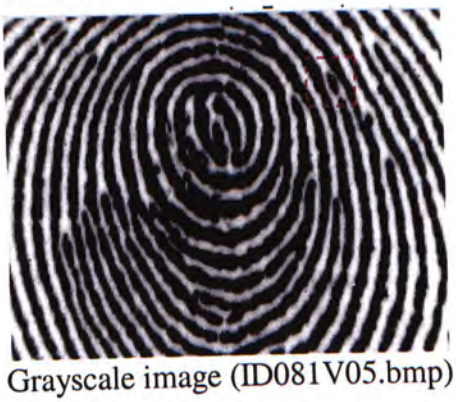


Figure 4.4 Examples of the isolated regions consisting of white pixels and the black diagonal pixels which introduce valley lakes in the valley skeleton images.

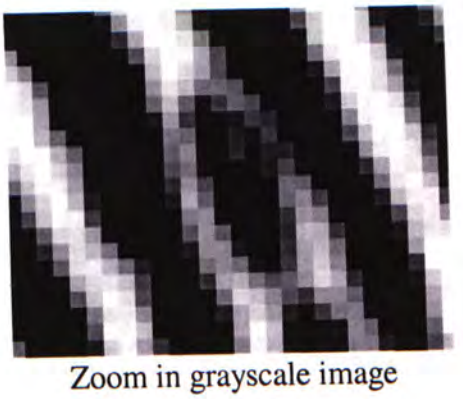
Therefore, we propose several preprocessing steps before thinning of the binary image:

1. Use a morphological operator to separate some linked parallel valleys, thus to eliminate some spurious bridges and spurs in the skeleton image;
2. Fill in the small holes with an area (number of pixels) below a threshold T_{a1}, thus to eliminate the spurious lakes in the skeleton image;
3. Remove the dots (isolated pixels) and the islands (short lines) with an area below a threshold T_{a2}, thus to eliminate the spurious lakes, dots, and some islands in the skeleton image.

The morphological operator does separate some misconnected valleys due to the binarization artifacts, as illustrated in Figure 4.5. The image "ID081V05.bmp" will be used for all the preprocessing effects illustration.

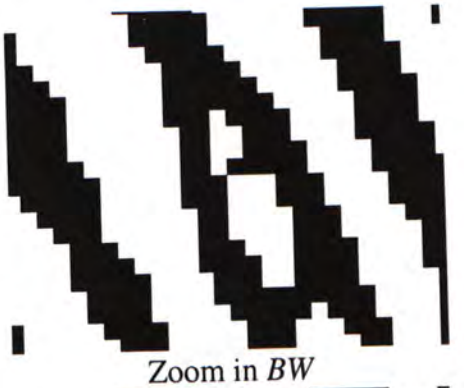


Grayscale image (ID081V05.bmp)



Zoom in grayscale image

Binary valley image (*BW*)



Zoom in *BW*

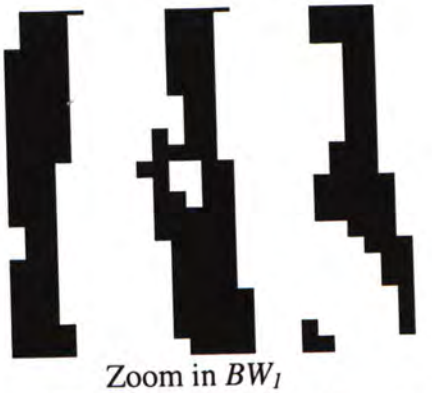
BW after morphological operation (BW_1)

Zoom in BW_1

Figure 4.5 An example showing the effect of the morphological operation on the binary image.

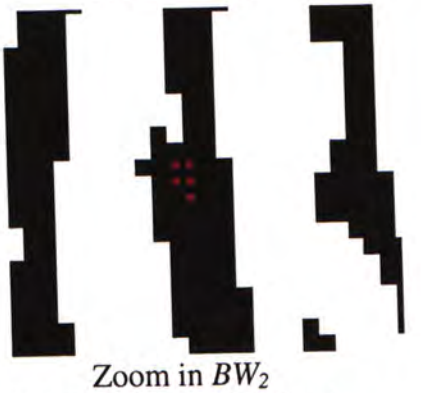
The results of step 2 and step 3 are shown in Figure 4.6 and Figure 4.7.

BW_1



Zoom in BW_1

BW1 after filling small holes (BW_2)



Zoom in BW_2

Figure 4.6 An example showing the effect of filling in the small holes in the binary image BW_1 (red dots represent the filled black pixels).

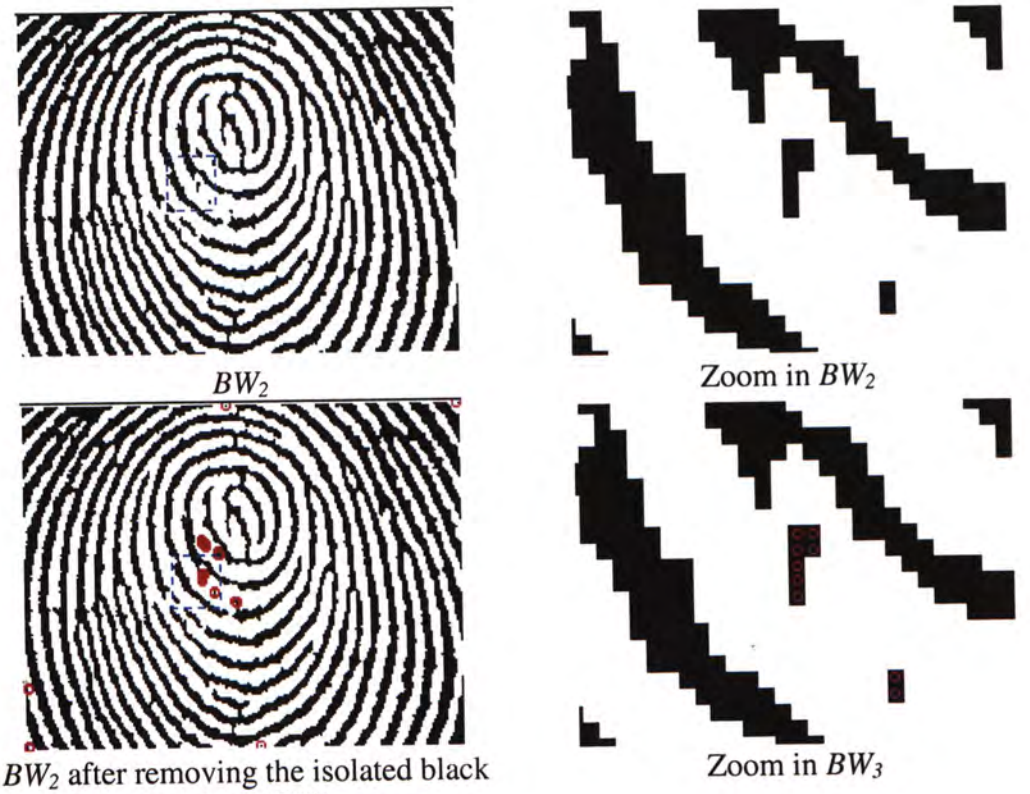


Figure 4.7 An example showing the effect of removing the isolated black regions in BW_2 (red circles: removed black pixels).

Figure 4.8 Preprocessing results at different processing steps. (Red cross: eliminated diagonal pixels; Red dots: filled pixels; Red circles: removed pixels).

The thresholds should be selected appropriately, if T_{a1} and T_{a2} are too small, the above spurious minutiae in the skeleton image will not be eliminated completely, if they are too large, the skeleton will be distorted. In our experiments, we set T_{a1}=11 and T_{a2}=9. Figure 4.8, 4.9 show the preprocessing results on the binary image and on the skeleton image, respectively. Some more examples illustrating the effects of the preprocessing steps are shown in Figure 4.10.

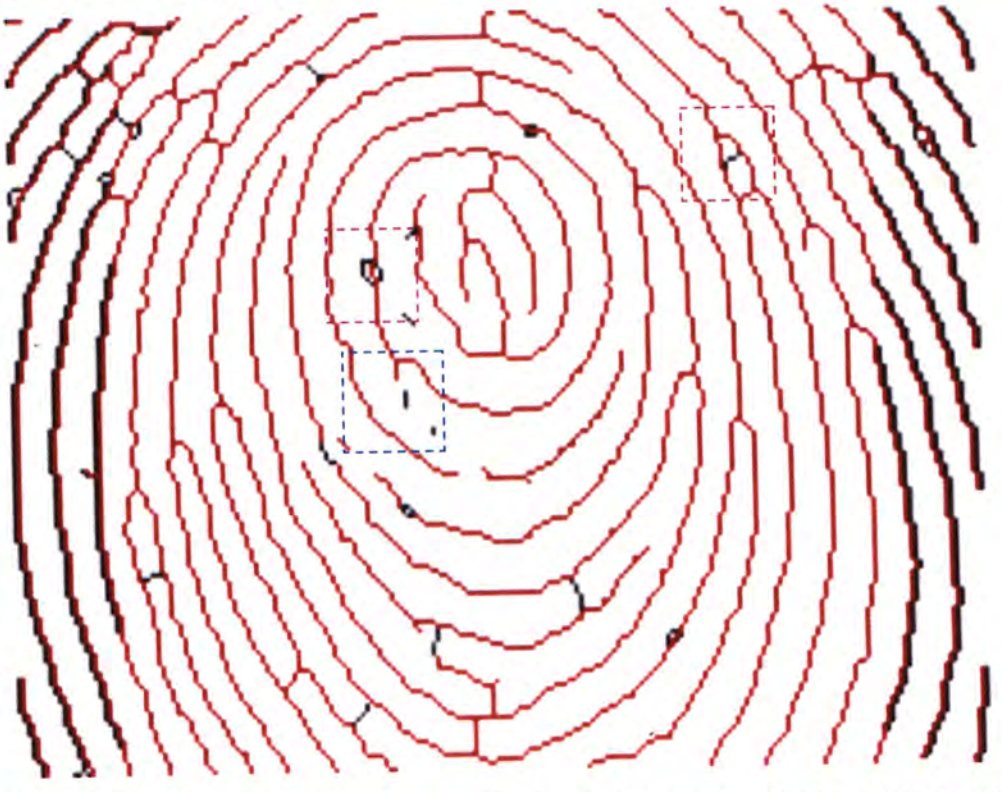


Figure 4.9 The valley skeleton image obtained from the binary image after preprocessing. Black curves represent the eliminated false minutiae structures (e.g., red rectangle: removed bridge; magenta rectangle: removed lake; and blue rectangle: removed island.)

From the results, we see that the morphological operation on the binary image separates the misconnections efficiently. Accordingly, without separating the misconnected valleys, the spurious minutiae such as triangle, bridge and ladder may not be removed by later post-processing algorithms which is based on the duality property of fingerprint images [5], because the bifurcation pairs have no dual ending pairs, as illustrated in Figure 4.11.

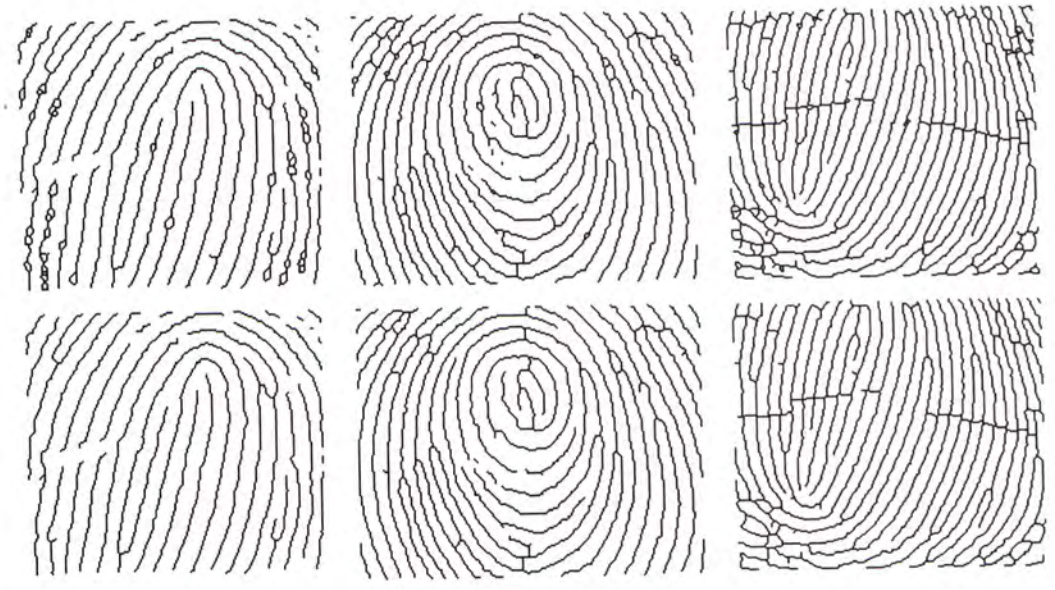


Figure 4.10 Examples showing the effects of the preprocessing steps. (Upper row: original skeleton images; lower row: skeleton images after preprocessing.)

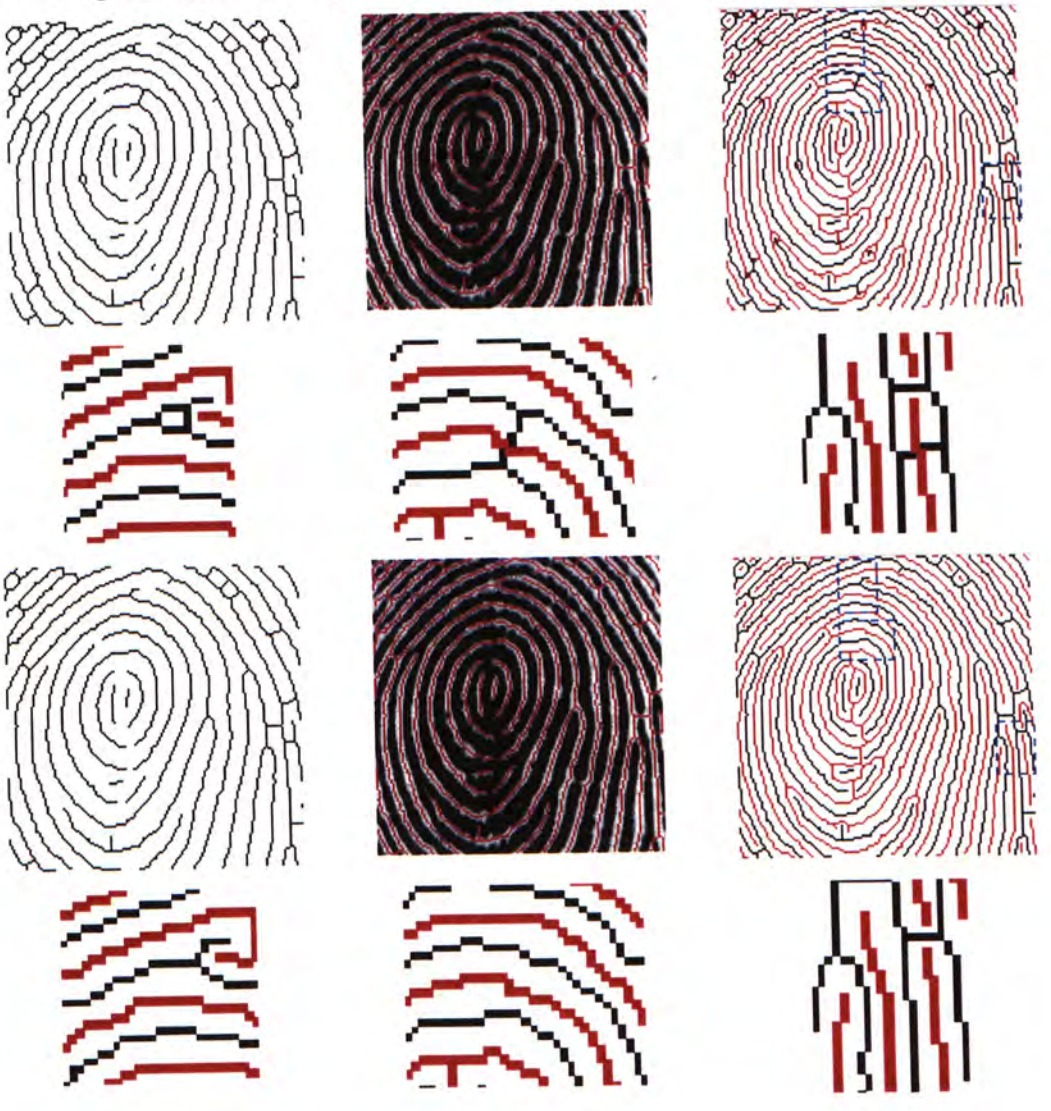


Figure 4.11 An example showing the effects of separating the misconnections for spurious triangle, bridge, and ladder, respectively. Row by row from top-left to bottom right: f_1) original valley skeleton; f_2) valley skeleton overlaying on the grayscale image; f_3) original valley skeleton (black) and its dual ridge skeleton (red); $f_{4\sim6}$) zoom in f_3) for spurious structures: triangle, bridge, and ladder, respectively; $f_{7\sim12}$) corresponding images to $f_{1\sim6}$ after preprocessing. The remaining spurious bridge in f_{12} will be removed in later post-processing stage using the duality property of fingerprint images.

4.2.2 Validation of Bug Pixels and Minutiae Extraction

The concept of Crossing Number (*CN*) is widely used for extracting the minutiae [10, 20, 45, 46, 47]. Rutovitz's definition [50] of crossing number for a pixel P is:

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

$$CN = \frac{1}{2}\sum_{i=1}^{8}\left|P_i - P_{i+1}\right|$$

where P_i is the binary pixel value in the neighborhood of P with P_i = (0 or 1) and $P_1=P_9$.

The skeleton image of fingerprint is scanned and all the minutiae are detected using the following properties of *CN*, as illustrated in Figure 4.12.

CN	*Property*
0	Isolated point
1	Ending point
2	Connective point
3	Bifurcation point
4	Crossing point

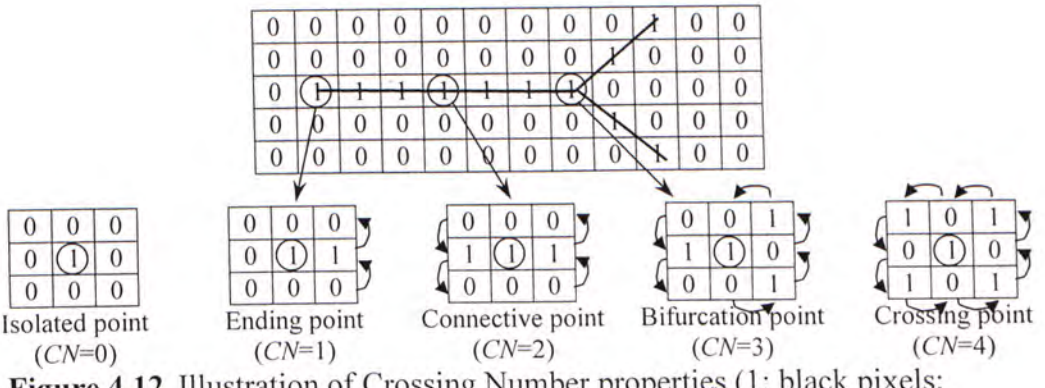


Figure 4.12 Illustration of Crossing Number properties (1: black pixels; 0: white pixels in the fingerprint skeleton image).

Ideally, the width of the skeleton should be strictly one pixel. However, this is not always true. Figure 4.13 shows some examples, where the skeleton has a two-pixel width at some bug pixel locations.

We define a bug pixel as the one with more than two 4-connected neighbors (marked by bold-italic ***1*** and ***0***). These bug pixels exist in the fork region where bifurcations should be detected, but they have CN =2 instead of CN >2. The existence of bug pixels may (*i*) destroy the integrity of spurious bridges and spurs, (*ii*) exchange the type of minutiae points, and (*iii*) miss detecting of true bifurcations, as illustrated in Figure 4.14. Therefore, before minutiae extraction, we develop a validation algorithm to eliminate the bug pixels while preserve the skeleton connectivity at the fork regions. By scanning the skeleton of fingerprint image row by row from top-left to bottom-right, we delete the first bug pixel encountered and then check the next bug pixel again for the number of 4-connected neighbors. If the number of 4-connected neighbors after the deletion of previous bug pixel is still larger than two, it will also be deleted; otherwise, it will be preserved and treated as a normal pixel. Some examples are shown in Figure 4.13. After this validation process, all the pixels in the skeleton satisfy the CN properties. Thus we can extract all the minutiae including true minutiae and false minutiae. The false minutiae can be eliminated at the post-processing stage.

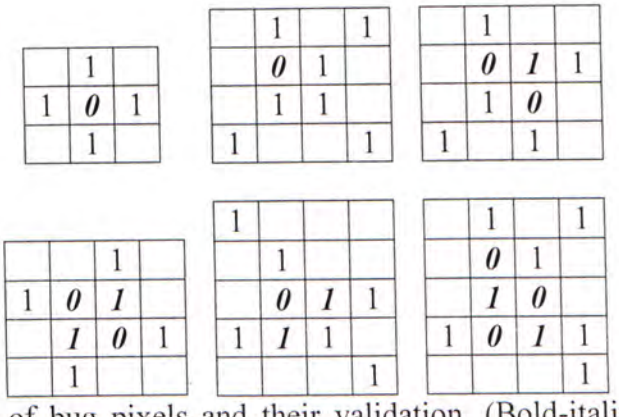
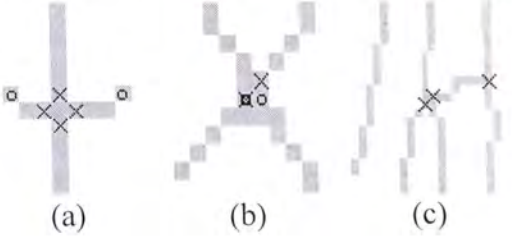


Figure 4.13 Examples of bug pixels and their validation. (Bold-italic 0: deleted bug pixels, bold-italic 1: preserved bug pixels that are changed to normal pixels.)



(a) (b) (c)

Figure 4.14 Without validating the bug pixels, we may have: (a) four bifurcations ("x") are missed; (b) two bifurcations are misdetected as two endings ("o"); (c) two bifurcations are missed including one true bifurcation.

4.3 Experimental Results

To evaluate the performance of our proposed skeleton-based minutiae extraction algorithm, we randomly select 35 fingerprint images of medium quality from our fingerprint database (as described in Chapter 3). In the experiments, the scanned fingerprint images (256 x 256, 256 gray level, 500 dpi) are cropped into 170 x 180 in size in order to remove the very noisy border areas. One benefit of reducing the fingerprint area is that there is less chance of spurious minutiae information.

The valley skeleton and ridge skeleton are first obtained from the valley image and its dual ridge image, respectively. The valley skeleton agrees rather well with the original valley image, while the ridge skeleton introduces a large number of spurious lakes and bridges. Consequently, the ridge skeleton will produce more spurious minutiae. Figure 4.15 shows a typical example.

(a) (b)

Figure 4.15 (a) Valley skeleton, (b) ridge skeleton (The skeleton is overlaid on the original gray scale fingerprint image).

The accuracy rates of applying the minutiae extraction algorithm on ridge skeleton and valley skeleton before and after preprocessing are reported in Table 4.1 and Table 4.2, respectively. In the tables, the total rate is calculated using the following formula:

$$Total \quad rate = \frac{E_t + B_t}{E_e + B_e}$$

Where E_t and B_t are the number of true endings and true bifurcations, E_e and B_e are the number of extracted endings and bifurcations.

Table 4.1 Accuracy rates for ridge minutiae extraction.

	Before preprocessing	After preprocessing
Ending	10.84 %	10.92 %
Bifurcation	20.24 %	51.32 %
Total rate	13.54 %	17.08 %

Table 4.2 Accuracy rates for valley minutiae extraction.

	Before preprocessing	After preprocessing
Ending	12.39 %	12.87 %
Bifurcation	16.35 %	26.58 %
Total rate	13.27 %	16.57 %

From the results, we can see that after preprocessing the accuracy rate of bifurcation is improved significantly, especially for the ridge skeleton. It demonstrates that the preprocessing algorithm does eliminate a large number of spurious lakes, bridges, spurs, which introduce false bifurcations. However, the accuracy rate of endings is only increased slightly since the preprocessing algorithm only eliminates some spurious islands that introduce false endings. In fact, the spurious dots also introduce false endings and are eliminated efficiently in the preprocessing stage. However, there are only a small number of dots in the skeleton image. The improvement of the accuracy rate of ridge bifurcation is greater than that of valley bifurcation. This shows that the ridge skeleton introduces more spurious minutiae. Some typical results of preprocessing are shown in Table 4.3 and Table 4.4. In addition, the computation speed for valley thinning is much faster than ridge thinning.

Table 4.3 Examples showing the number of extracted ridge minutiae.

Before preprocessing		After preprocessing	
Endings	Bifurcations	Endings	Bifurcations
157	37	152	4
167	39	163	9
58	51	58	20
89	34	80	10
93	75	87	27
152	60	146	8

Table 4.4 Examples showing the number of extracted valley minutiae.

Before preprocessing		After preprocessing	
Endings	Bifurcations	Endings	Bifurcations
77	52	56	44
121	115	89	65
78	142	64	110
64	186	62	110
80	112	77	55
68	163	55	123

Table 4.5 shows some typical results of validating the bug pixels. From the results, we can see that the bug pixels exist in the fork region where bifurcations should be extracted. Some fingerprint skeletons may have more bug pixels and some may have none.

Table 4.5 Number of minutiae before and after validating the bug pixels.

After preprocessing		After validating bug pixels	
Endings	Bifurcations	Endings	Bifurcations
67	47	67	47
87	27	87	27
55	123	55	125
62	110	62	118
77	55	75	57
106	20	93	27

Some examples are illustrated in Figure 4.16 showing the results of minutiae extraction. From the results, we can see that a maximum number of minutiae are extracted from the skeleton images including both genuine and spurious minutiae. This allows the true minutiae preserved and false minutiae removed in later post-processing stages.

4.4 Summary

In this chapter, we first review the most popular approaches to minutiae extraction from the fingerprint images. After that, we present a skeleton-based minutiae extraction method which uses the valley instead of ridge for minutiae extraction. In our method, we propose several simple and efficient preprocessing techniques on the binary image in order to eliminate the spurious lakes and dots,

and to reduce the spurious islands, bridges, and spurs in the skeleton image. Our minutiae extraction algorithm can detect all the minutiae, including both true and false minutiae, using the simple Crossing Number on the skeleton images after validating all the bug pixels introduced at the thinning stage. This allows the true minutiae preserved and false minutiae removed in later post-processing stages.

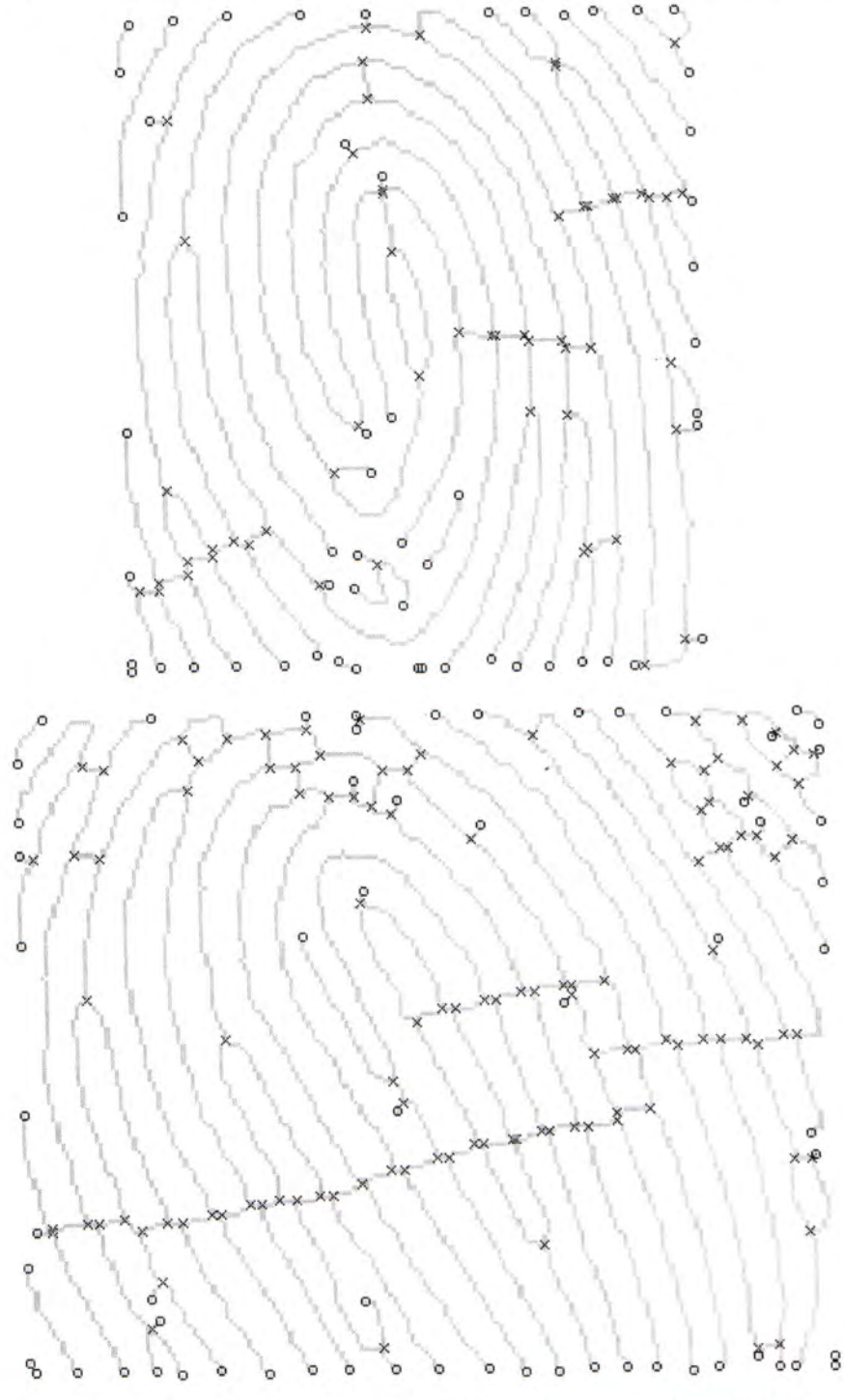


Figure 4.16 Examples showing the results of minutiae extraction before post-processing ("o": endings; "x": bifurcations).

Chapter 5

Post-Processing

Initially, a large number of spurious minutiae are extracted due to small ridge segments, ridge breaks, noisy links between parallel ridges, etc. Thus, it is necessary to scrutinize and validate the minutiae initially extracted and this is called post-processing.

Post-processing plays an important role in fingerprint minutiae extraction and fingerprint matching processes, but it is a very difficult problem.

5.1 Review of Post-Processing Methods

Most of the current post-processing algorithms [51, 52] eliminate the false minutiae by evaluating the statistical characteristics within an $M \times M$ matrix moving along the image pixel by pixel. Xiao and Raafat [53] develop a new post-processing algorithm using both the statistical and structural information to eliminate the false minutiae. However, the method relies heavily on pixel connectivity computation, which is very time-consuming. A neural network-based minutiae filtering technique, which operates directly on the gray scale images is proposed by Maio and Maltoni [54]. Each minutia, as detected by the algorithm [23] is normalized and then analyzed through a three-layer neural network classifier. This method can only eliminate false and type-exchanged minutiae, and the number of dropped (missing) minutiae is increased at the same time. In addition, the method relies greatly on the type and quality of training data.

In order to eliminate the spurious lakes, Kim et al. [55] propose a classical but complicated method based on a graph construction to detect the closed paths that form the lake. Farina et al. [47] propose to clean bridge based on ridge positions instead of directional maps used by conventional methods. They argue that evaluation of the directional maps is very time-consuming. Xiao and Raafat [53] remove bridge, triangle, and ladder by calculating the number of "connected" minutiae and their structural relations. Stosz and Alyea [41] propose to eliminate

wrinkle by analyzing the spatial relationship of the consecutive minutiae on the wrinkle. Hong et al. [59] define an objective function to detect wrinkle based on the observation that the spurious minutiae existing in a wrinkle are anti-aligned and the region between them is brighter than the average brightness of the image region. All these approaches rely extensively on pixel connectivity analysis one way or the other.

5.2 Post-Processing Algorithms

After preprocessing on the binary and skeleton images [56], we extract minutiae from the fingerprint skeleton image. However, due to various noise in the fingerprint image, the extraction algorithm produces a large number of spurious minutiae such as break, spur, bridge, merge, triangle, ladder, lake, island, and wrinkle, as shown in Figure 5.1. Therefore, reliably differentiating spurious minutiae from genuine minutiae in the post-processing stage is crucial for accurate fingerprint recognition. The aim of the post-processing stage is to eliminate these spurious minutiae. The more spurious minutiae are eliminated, the better the matching performance will be. In addition, matching time will be significantly reduced because of the reduced minutiae number. This is very important since the execution time is a critical parameter in an automatic fingerprint identification system (*AFIS*).

Taking full advantage of the duality property of fingerprint image [5], we develop several post-processing techniques to efficiently remove spurious minutiae. Especially, we define an *H*-point structure [58] to remove several types of spurious minutiae including bridge, triangle, ladder, and wrinkle all together. Experimental results clearly demonstrate the effectiveness of the new algorithms.

5.2.1 *H*-Point

For the various types of false minutiae illustrated in Figure 5.1, we use preprocessing algorithms [56] to eliminate lakes, dots, and a number of islands and spurs. For the rest of the false minutiae types, we observe that there is at least one bridge structure in such spurious minutiae as bridge, triangle, ladder and wrinkle. For the various types of breaks, there are also corresponding bridge structures in the duality image. We define a bridge structure and its corresponding

dual break in the duality image collectively as an *H*-point. If we can successfully remove the *H*-points in the image, we can eliminate most of the spurious minutiae.

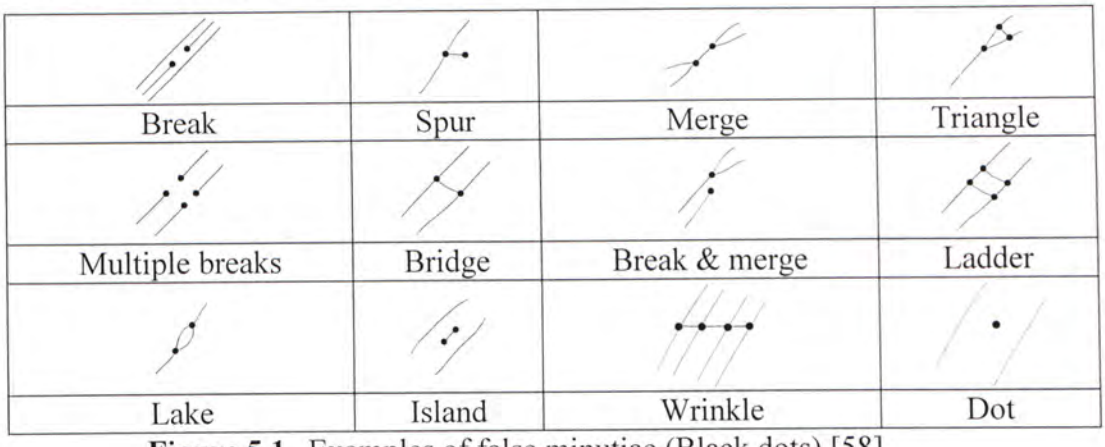


Figure 5.1 Examples of false minutiae (Black dots) [58].

5.2.2 Termination/Bifurcation Duality

To further explain the *H*-point definition, we need to first understand the duality definition. In a fingerprint image, for each ridge ending, there is generally a corresponding valley bifurcation and vice versa [5], with the only exception at the singularity points (cores and deltas) [57]. This is called the termination/bifurcation duality, as illustrated in Figure 5.2 a). Around a bridge structure, such a duality takes on the form of a bridge in the ridge (or valley) skeleton image and its corresponding dual break in the valley (or ridge) skeleton image, as shown in Figure 5.2 b). We define such a structure with two bifurcations and two corresponding endpoints (endings) as an *H*-point. In the following, we will present a simple procedure utilizing the duality property to eliminate the *H*-point.

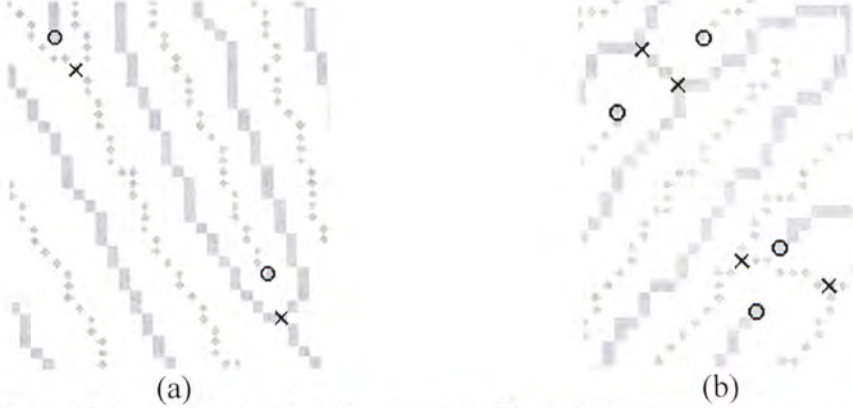
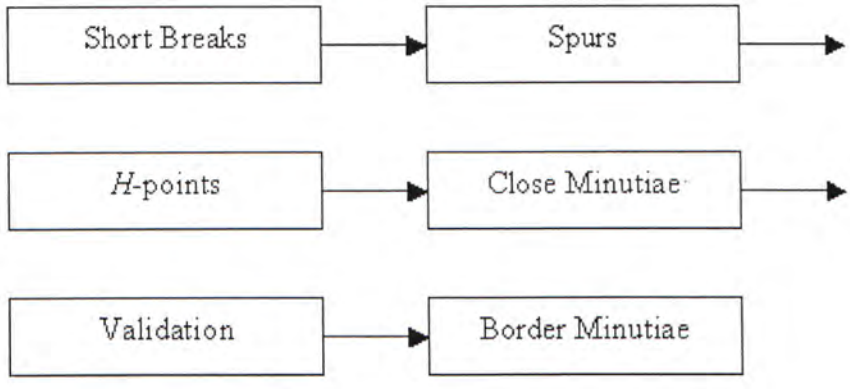


Figure 5.2 Illustration of ridge and valley duality. The solid gray squares represent the valley skeleton, and the solid gray diamonds represent the ridge skeleton. (a) The termination/bifurcation duality; (b) *H*-point examples: a valley bridge corresponds

to a ridge break in the dual skeleton image and vice versa ("o": endings; "x": bifurcations).

5.2.3 Post-Processing Procedure

Since any particular processing step will affect the performance of later steps, we have to be very careful of the processing order. To efficiently remove the spurious minutiae while retaining the true minutiae, we design several algorithms to remove the spurious minutiae in the following order:



In the first stage, we remove some short breaks based on the conventional definition of a break. If the endpoints of a break satisfy all the following conditions, they will be removed:

1. The distance between two endpoints is below a threshold T_1;
2. The difference between the orientation angles of two endpoints (Ang_1, Ang_2) is within an interval of $[\theta_1, \theta_2]$;
3. The difference between the orientation angle of the line connecting the two endpoints (Ang_3) and either angle of Ang_1 or Ang_2 is within an interval of $[\theta_3, \theta_4]$.

In order to calculate the orientation angle of an endpoint, we look for the 8-connected neighbors around the endpoint. During the tracing procedure, our algorithm keeps going forward even after encountering a bifurcation point so that the orientation of endpoint 2 is estimated as the "dashed" line instead of the "solid" line as illustrated in Figure 5.3. Thus the endpoints orientations satisfy the above orientation angle rules 2 and 3 (i.e., two endpoints almost face to each other). Otherwise, endpoints 1 and 2 cannot be connected. If that is the case, the bifurcation and endpoint *2* will be removed in the following spur elimination stage. As a result, the true bifurcation will be detected as an endpoint which results in

the type-exchanged error. Therefore, this strategy mainly helps to decrease the type-exchanged error due to the poor valley connectivity.

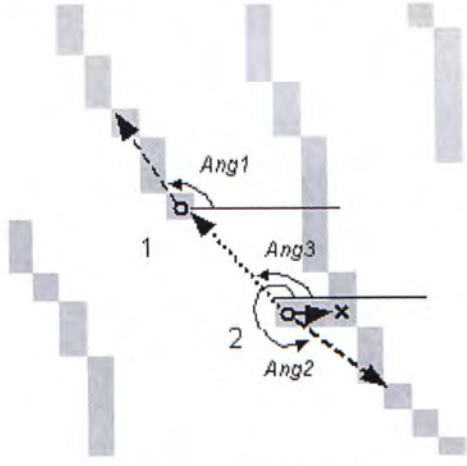


Figure 5.3 Keep tracing when meets a bifurcation point. ("o": endings; "x": bifurcation.)

In the second stage, we first label the connected pixels in the skeleton image. If the distance (D) between a bifurcation point and an endpoint is below the threshold T_2 and their labels are the same (i.e., they are connected), we again label the connected pixels within a small window ($2D+1$ x $2D+1$) centered around the bifurcation point or the endpoint. If their labels are still the same, we remove both of them for they form a genuine spur. Otherwise, they are retained (see Figure 5.4).

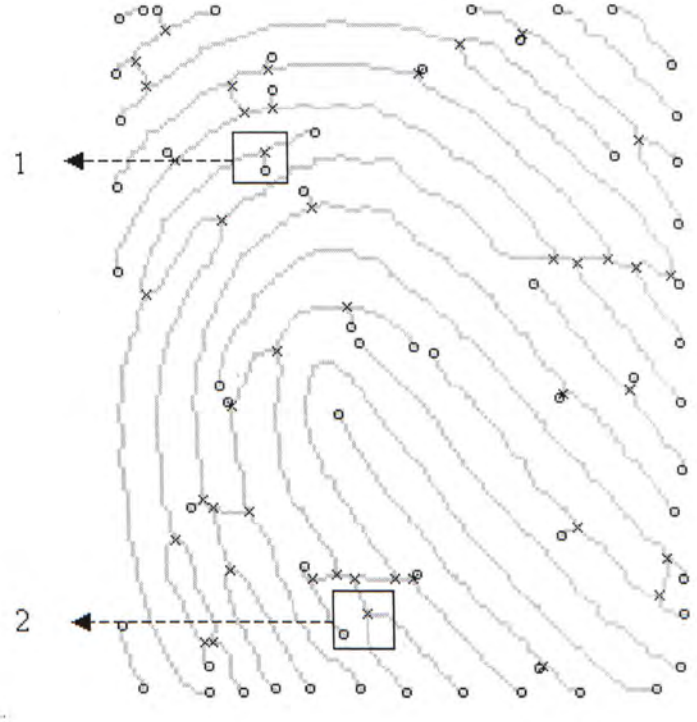


Figure 5.4 Examples showing the elimination of spurs. After relabeling the connected pixels within the square, the bifurcation and the endpoint inside square 1 still have the same labels, while those within square 2 have different labels.

In the third stage, the *H*-points are detected and eliminated. If a bridge in the ridge (or valley) skeleton image and a break in the valley (or ridge) skeleton image satisfy the following conditions, they form an *H*-point (see Figure 5.5):

1. The intersecting point lies between the two endpoints and the two bifurcation points;
2. The distance between the bridge midpoint M_2 and the break midpoint M_1 is within a threshold T_3;
3. The intersecting angle θ is within an interval of $[\theta_5, \theta_6]$.

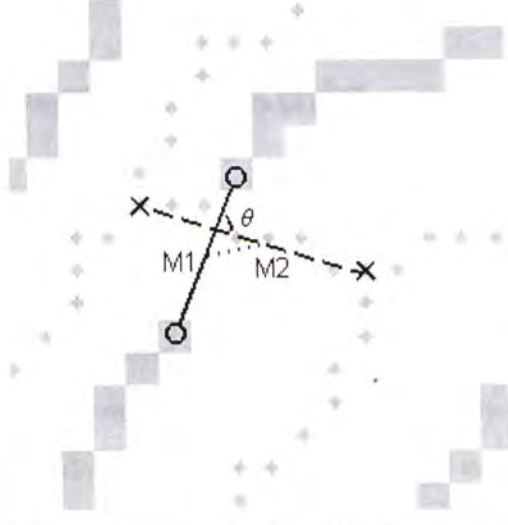
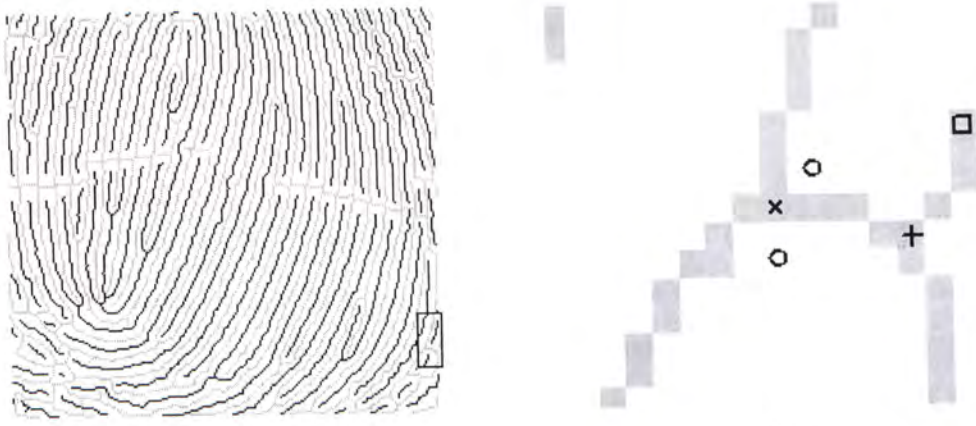


Figure 5.5 An example showing the elimination of *H*-point.

After eliminating those minutiae that are too close to each other, we further validate the remaining minutiae according to the duality property [5]. It is true that a true minutia has only one dual minutia in the dual skeleton image except for the singularity points which have no dual minutiae. Hence, we remove the minutia if it has more than one neighboring minutiae in the dual skeleton image, as illustrated in Figure 5.6. Finally, all the minutiae within a certain distance threshold T_4 from the image border are removed.

After post-processing, a large percentage of the spurious minutiae are eliminated, the remaining minutiae are treated as true minutiae which are used for later fingerprint matching.



(a) (b)

Figure 5.6 (a) Valley skeleton (gray) and its dual ridge skeleton (black), (b) Zoom in the rectangle. (After removing the spur ("+" and "□"), the remaining bifurcation ("x") is also eliminated for it has two neighboring endpoints in its dual skeleton image.)

5.3 Experimental Results

To evaluate the performance of our post-processing algorithms, we randomly select 35 fingerprint images of medium quality from our fingerprint database (DB1, as described in Chapter 3). In the experiments, the scanned fingerprint images (256 x 256, 256 gray level, 500 dpi) are cropped into 170 x 180 in size in order to remove the very noisy border areas. The valley skeleton and ridge skeleton are then obtained from both the valley image and its dual ridge image, respectively.

Table 5.1 gives the overall performance of the proposed post-processing algorithms. We can see that the false minutiae rate drops 56.5% after post-processing. The false and dropped minutiae rates are not as good as those reported in [23] (false = 8.52%, dropped = 4.51%), but the type-exchanged minutiae rate is much lower than that reported in [23] (exchanged = 13.03%).

Table 5.1 Post-processing performance (False minutiae rate for valley skeleton)

Before post-processing	After post-processing		
	False	Dropped	Type-exchanged
83.4 %	15.2 %	7.01 %	4.69 %

To further quantitatively evaluate the performance of our minutiae extraction algorithm we adopt the "goodness index" (*GI*) measurement, which compares the

extracted minutiae with the minutiae obtained from the same fingerprint by a human expert [45]. The goodness index is defined as:

$$GI = \frac{P - D - I}{T}$$

where P is the total number of paired minutiae, D is the number of deleted spurious minutiae (false and type-exchanged), I is the number of inserted missing minutiae (dropped), and T is the number of true minutiae. An extracted minutia m_1 is said to be paired with the true minutia m_2 marked by the human expert if m_1 lies within an *8x8* tolerance box centered around m_2. The maximum value of GI is 1, which means that all the extracted minutiae are paired with the true minutiae, and no spurious minutiae and missing minutiae are detected ($P=T$, $D=I=0$). A high value of GI indicates high quality of the extracted minutiae. The larger the value of GI is, the better the minutiae extraction algorithm will be. Table 5.2 presents the GI values for a representative subset of 10 scanned fingerprint images. The maximum and minimum values of GI for this dataset are 0.75 and 0.18, respectively. The average value is 0.50. The results outperform those presented in [45] and are comparable to those reported in [60].

Table 5.2 GI values for a dataset of 10 fingerprint images. (Parameters used in our experiments: T_1, T_2, T_3, T_4, θ_1, θ_2, θ_3, θ_4, θ_5, θ_6, are 9, 6, 2.5, 7 pixels, 145°, 225°, -25°, 25°, 65° and 115°.)

Fingerprint	P	D	I	T	GI
01	11	1	1	12	0.75
02	18	4	1	19	0.68
03	21	3	3	28	0.54
04	13	2	2	17	0.53
05	15	3	3	18	0.50
06	19	3	4	24	0.50
07	15	7	1	16	0.44
08	12	5	1	14	0.43
09	12	2	3	17	0.41
10	8	3	3	11	0.18

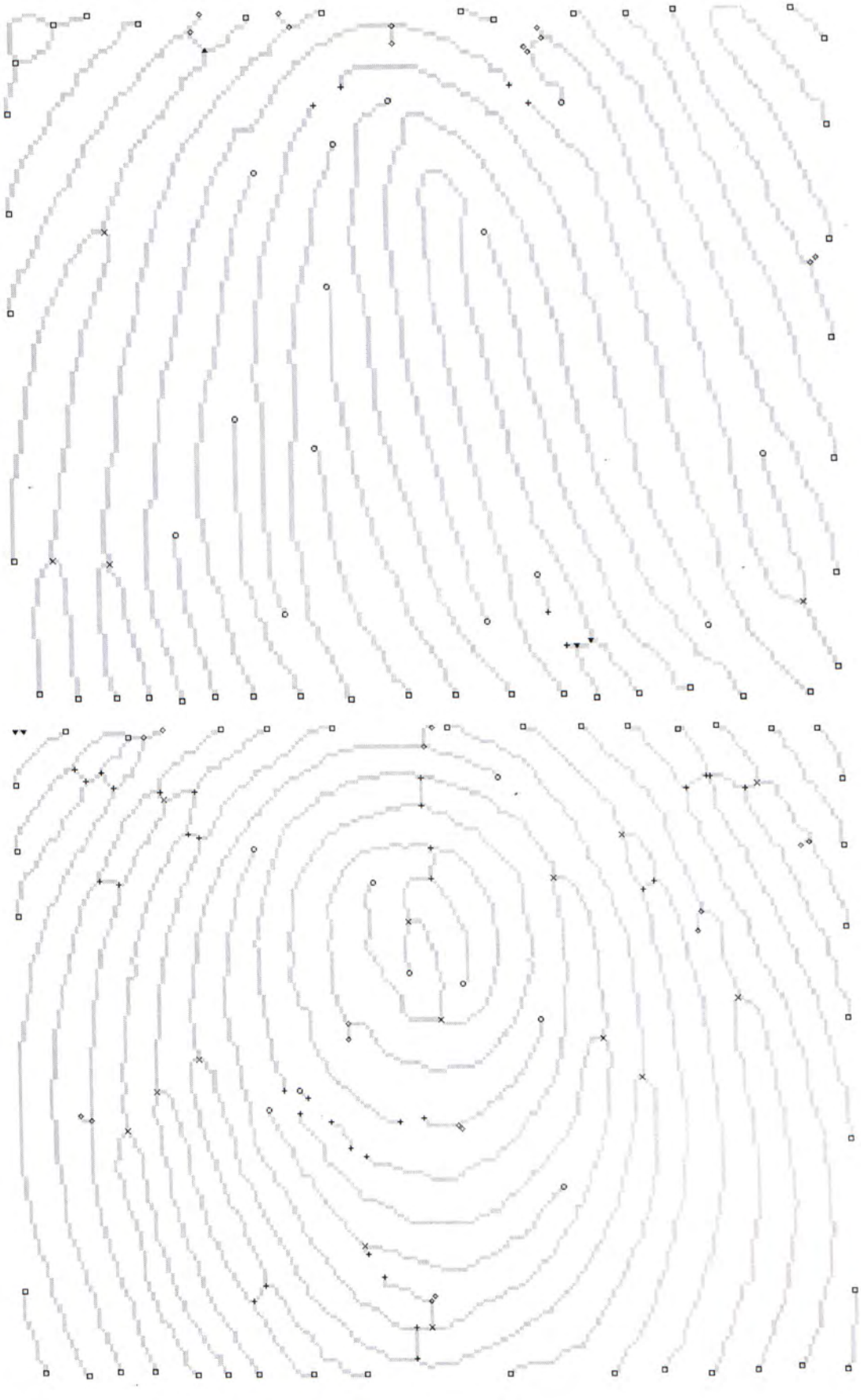
Figure 5.7 shows several typical results of our minutiae extraction and post-processing algorithms. As can be seen from the results, the survived minutiae after post-processing agree rather well with the minutiae marked by the human expert in regions where the valley structures are clear. False minutiae and dropped

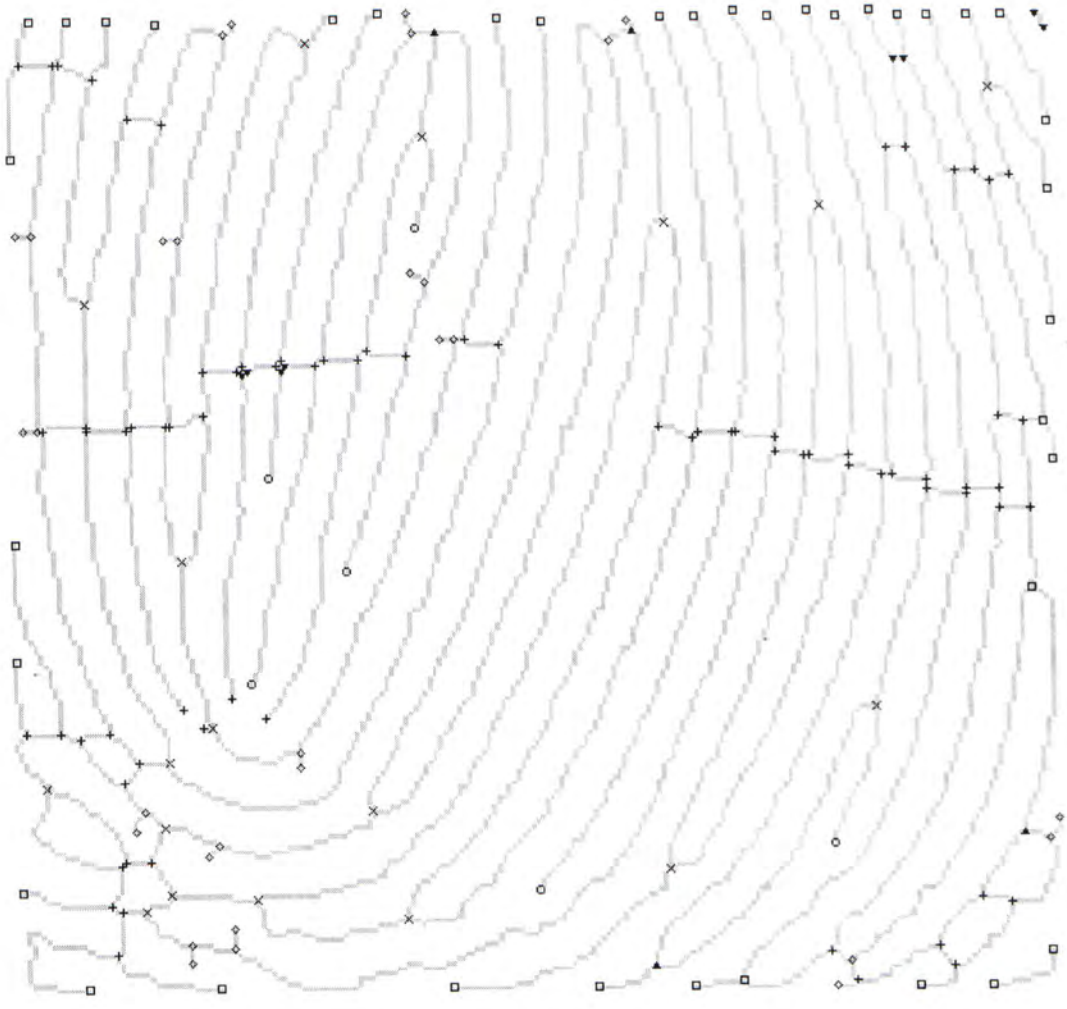
minutiae generally occur in the noisy regions near the border or on the scars, and type-exchanged minutiae occur in the areas where the valley connectivity is poor.

5.4 Summary

Due to different properties of fingerprint sensors and different conditions under which a fingerprint is scanned, the quality of a fingerprint image can vary greatly. For a fingerprint image of low quality, a large number of false minutiae may be extracted. Post-processing algorithms are generally needed to reduce the high false alarm rate. In this chapter, we review the current approaches to post-processing. All these approaches rely extensively on pixel connectivity analysis one way or the other, which is computationally expensive. In this work, using the duality property of fingerprint image we develop several post-processing techniques to efficiently remove spurious minutiae. Especially, we develop an efficient *H*-point elimination method to remove several types of spurious minutiae including bridge, triangle, ladder, and wrinkle all at once. The performance of our proposed algorithms has been evaluated in terms of "goodness index" (*GI*), which compares the automatically extracted minutiae with the minutiae obtained from the same fingerprint by a human expert. The high values of goodness index (*GI*) illustrate the effectiveness of our proposed post-processing method.

(a) (b)





(c)

Figure 5.7 Minutiae extraction example results: (a) Minutiae marked by a human expert; (b) Automatically extracted minutiae; (c) Post-processing results at different processing stages (Diamond (◊): eliminated spurs; Plus (+): eliminated *H*-points; Solid down triangle (▼): eliminated close minutiae; Solid up triangle (▲): eliminated minutiae by validation; Square (□): eliminated border minutiae; Circle (○): survived endings; X-mark (x): survived bifurcations.).

Chapter 6

Conclusions and Future Work

In this chapter, we will summarize the work we have done, and discuss the limitations of our current approaches.

6.1 Conclusions

In this thesis, we concentrate on the fingerprint minutiae extraction techniques, which is a core technology in the automatic fingerprint identification systems. Fingerprint minutiae extraction is very important, but to design a reliable and efficient minutiae extraction algorithm, which is robust to various fingerprint quality is still a challenging problem.

In this work, we develop a novel skeleton-based fingerprint minutiae extraction method. The main contributions of our research are:

- We propose to use the fingerprint valley instead of ridge for binarization-thinning process to extract minutiae from the fingerprint image;
- We develop several simple and efficient preprocessing techniques for minutiae extraction. It eliminates the spurious lakes and dots and a number of spurious islands, bridges, and spurs in the skeleton image;
- In order to improve the performance of minutiae extraction, we propose a new algorithm to remove the bug pixels existing in the fork regions where bifurcations should be detected. The bug pixels are introduced at the thinning stage;
- Our minutiae extraction algorithm can detect a maximum number of minutiae, including both genuine and spurious minutiae, using the simple Crossing Number (*CN*) on the skeleton images. This allows the true minutiae preserved and false minutiae removed in later post-processing stages;

- Taking full advantage of the intrinsic duality property of fingerprint image, we develop several post-processing techniques to efficiently remove the spurious minutiae in the skeleton image;
- Especially, we define an *H*-point structure to remove several types of spurious minutiae including bridge, triangle, ladder, and wrinkle all at once;
- A number of type-exchanged errors are corrected by connecting the short breaks based on the conventional definition of a break;
- The spurs and *H*-points are efficiently removed without using the time-consuming tracing algorithm, which is needed in most of the current approaches in the literature;
- Some false minutiae are further validated due to the duality property of fingerprint image. The fact is that a true minutia has only one dual minutia in the dual skeleton image except for the singularity points (cores and deltas) which have no dual minutiae. The spurious minutiae has more than one neighboring minutiae in the dual skeleton image;
- The performance of the proposed algorithms has been evaluated in terms of "goodness index" (*GI*), which compares the results of automatic extraction with manually extracted minutiae. The high values of goodness index (*GI*) illustrate the effectiveness of our proposed post-processing algorithms.

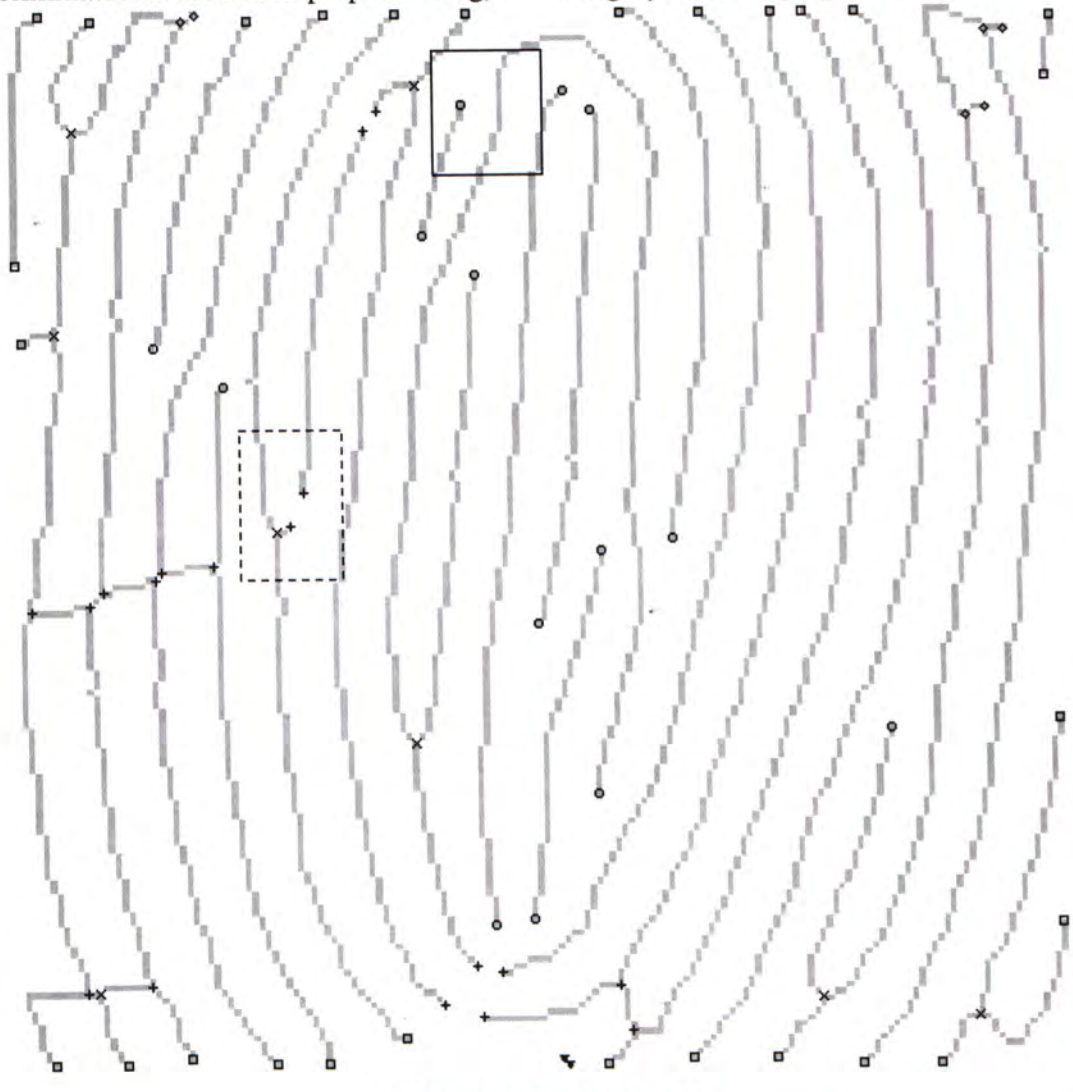
6.2 Problems and Future Works

6.2.1 Problem 1

In the preprocessing stage, although the morphological operator can correctly separate the misconnected parallel valleys, it may separate some truly connected valleys. Some of these valleys can be reconnected in later post-processing stages, but some of them will not be linked, and thus result in type-exchanged error, as illustrated in Figure 6.1. However, by observation, we see that most of these errors are due to the low quality of the fingerprint images, especially for the poor valley connectivity.

(a) Valley skeleton image (black curves: eliminated structures in preprocessing)

(b) Extracted minutiae overlaying on the gray scale fingerprint image.



(c) Post-processing results

Figure 6.1 An example showing the separated valleys which should not be separated. The valley skeleton within the solid rectangle is separated, thus the true bifurcation is detected as an ending which results in type-exchanged error; while the separated valley skeleton within the dashed rectangle is reconnected in the post-processing stages.

6.2.2 Problem 2

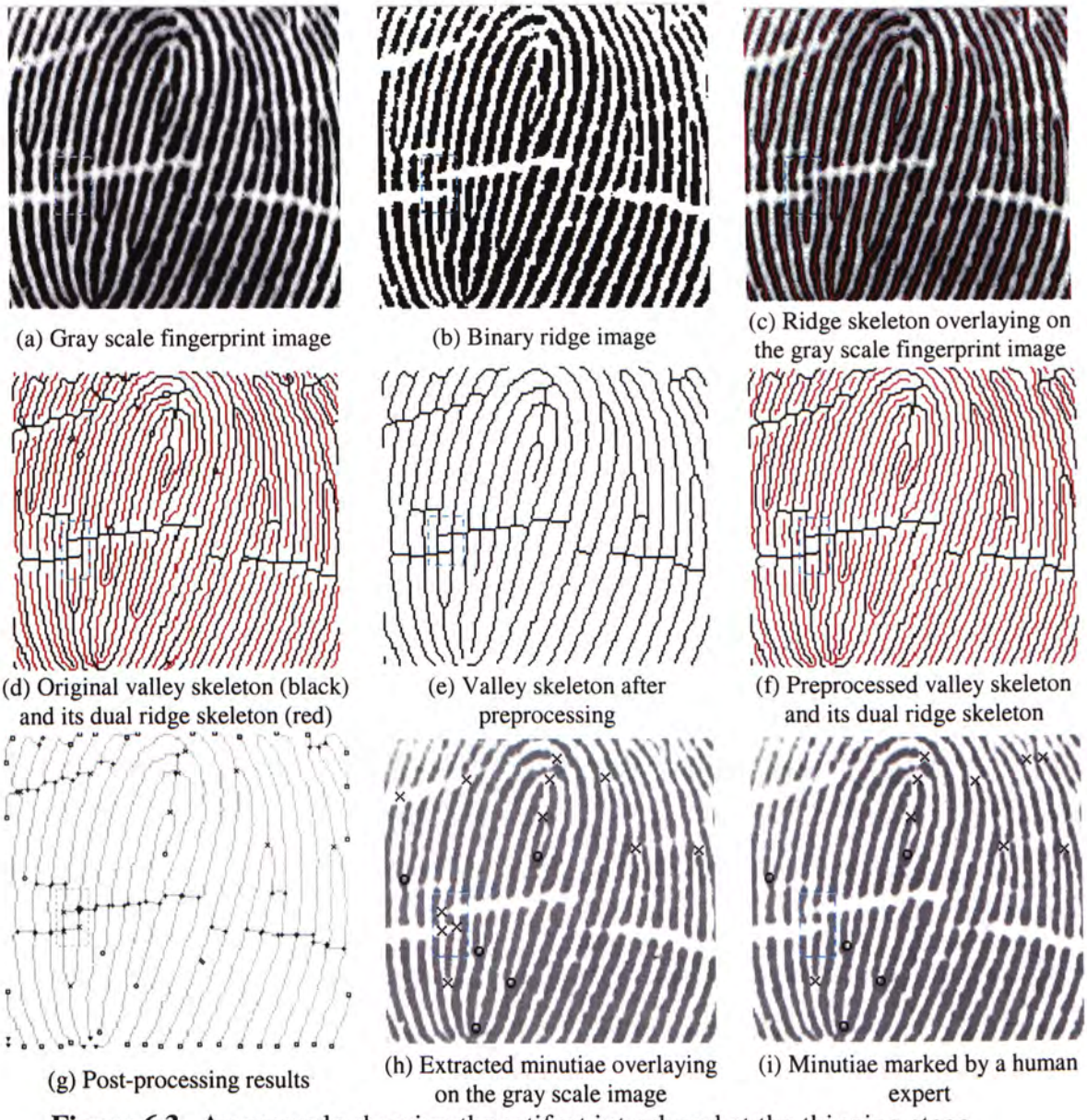
For the fingerprint images of poor quality, the binarization-thinning process may introduce some artifacts. Figure 6.2 shows some examples that result in type-exchanged errors.

(a) grays cale fingerprint images (b) preprocessed binary images (c) preprocessed valley skeletons

Figure 6.2 Examples showing the artifacts introduced at the binarization and thinning stages. (Top row: the true bifurcation is detected as a spurious ending; bottom row: the true ending is detected as a spurious bifurcation. Notice columns (b) and (c) that the preprocessing has no effect on the regions inside the cyan rectangles which result in type-exchanged errors.)

6.2.3 Problem 3

Another kind of artifact introduced at the thinning stage is illustrated in Figure 6.3. Due to the poor image quality, the very short ridge (black ridge within the cyan rectangle in Figure 6.3 a)) is eliminated during the thinning process (see Figure 6.3 c)). For the spurious ladder in the valley skeleton is not separated at the preprocessing stage (see Figure 6.3 e)), it has no dual ridge ending pairs (see Figure 6.3 f)), thus, it cannot be eliminated in later post-processing stages based on the duality property (see Figure 6.3 g)). Finally it introduces three spurious bifurcations (see Figure 6.3 h)).



(a) Gray scale fingerprint image

(b) Binary ridge image

(c) Ridge skeleton overlaying on the gray scale fingerprint image

(d) Original valley skeleton (black) and its dual ridge skeleton (red)

(e) Valley skeleton after preprocessing

(f) Preprocessed valley skeleton and its dual ridge skeleton

(g) Post-processing results

(h) Extracted minutiae overlaying on the gray scale image

(i) Minutiae marked by a human expert

Figure 6.3 An example showing the artifact introduced at the thinning stage.

6.2.4 Future Works

Problem 1 and problem 2 may introduce type-exchanged error, and problem 3 may introduce spurious minutiae. All these problems are due to the low quality of fingerprint images. To a certain extent, problem 1 and problem 3 are because of the preprocessing techniques. We notice that in Figure 6.3 e), the difference between the local orientation of the shorter edge and those of the two longer edges of an H-point is prominent, almost ninety degrees. In future work, we will first temporarily remove all the bifurcations in the H-points in order to separate the shorter edges from the longer edges, then apply the principle component analysis (PCA) method to compute the local orientations. If the difference between the

local orientations satisfies the predefined conditions, both of the two bifurcations belonging to an *H*-point will be removed. In this case, we may need to compute the valley skeleton image only, thus we believe that this new approach can eliminate the *H*-points more efficiently. Due to this new method, the morphological operations at the preprocessing stage may not be needed. Then problem 1 will be solved as well. In order to solve problem 2, we will investigate new adaptive thresholding and thinning algorithms or integrate the image enhancement algorithms to improve the quality of the fingerprint images.

In order to evaluate the robustness of the proposed algorithms, we will test our algorithms on a much larger dataset containing data from different sensors.

Bibliography

[1] B. Miller, "Vital signs of identity," *IEEE Spectrum*, vol. 31, no. 2, pp. 22-30, 1994.

[2] E. Newham, The Biometric Report, SJB service, New York, 1995.

[3] National Institute of Standards and Technology (NIST), Guideline for the Use of Advanced Authentication Technology Alternatives, Federal Information Processing Standards Publication 190, 1994.

[4] Anil K. Jain, Ruud Bolle, and Sharath Pankanti, Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.

[5] L.C. Jain, U. Halici, I. Hayashi, S.B. Lee, and S.Tsutsui (Eds.), Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press, 1999.

[6] David D. Zhang, Automated Biometrics: Technologies and Systems, Kluwer Academic Publishers, 2000.

[7] H. C. Lee and R. E. Gaensslen, Advances in Fingerprint Technology, Boca Raton: CRC Press, 1994.

[8] R. Clarke, "Human identification in information systems: management challenges and public policy issues," *Info. Technol. & People*, vol. 7, no. 4, pp. 6-37, 1994.

[9] S. C. Davies, "Touching big brother: how biometric technology will fuse flesh and machine," *Info. Technol. & People*, vol. 7, no. 4, pp. 60-69, 1994.

[10] A. K. Jain, L. Hong, S. Pankanti and R. Bolle, "An identity authentication system using fingerprints," *Proc. IEEE*, vol. 85, no. 9, pp. 1365-1388, 1997.

[11] Jr. J. Campbell, "Speaker recognition: a tutorial," *Proc. IEEE*, vol. 85, no. 9, pp. 1437-1462, 1997.

[12] V. Nalwa, "Automatic on-line signature verification," *Proc. IEEE*, vol. 85, no. 2, pp. 215-239, 1997.

[13] R. Wildes, "Iris recognition: an emerging biometric technology," *Proc. IEEE*, vol. 85, no. 9, pp. 1348-1363, 1997.

[14] J. Zhang, Y. Yan, and M. Lades, "Face recognition: eigenface, elastic matching, and neural nets," *Proc. IEEE*, vol. 85, no. 9, pp. 1423-1435, 1997.

[15] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 15, no. 11, pp. 1148-1161, 1993.

[16] StarTek products, http://www.startek.com.

[17] Precise Biometrics products, http://www.precisebiometrics.com.

[18] Veridicom products, http://www.veridicom.com.

[19] Atmel products, http://www.atmel.com/atmel/products/prod42a.htm.

[20] B. M. Mehtre, "Fingerprint image analysis for automatic identification," *Machine Vision and Applications*, vol. 6, pp. 124-139, 1993.

[21] A. K. Jain, S. Prabhakar, and L. Hong, " A multichannel approach to fingerprint classification," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 21, no. 4, pp. 348-359, 1999.

[22] Kalle Karu and Anil K. Jain, "Fingerprint classification," *Pattern Recognition*, vol. 29, no. 3, pp. 389-404, 1996.

[23] D. Maio and D. Maltoni, "Direct gray-scale minutiae detection in fingerprints," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 19 no. 1 , pp. 27-40, 1997.

[24] Lin Hong, Yifei Wan, and A. K. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 20, no. 8, pp. 777 –789, 1998.

[25] M. Electronic, "Automatic fingerprint identification," *IEEE Spectrum*, vol. 10, pp. 36-45, 1973.

[26] A. K. Hrechak and J. A. Mchugh, "Automated fingerprint recognition using structural matching," *Pattern Recognition*, vol. 23, no. 8, pp. 893-904, 1990.

[27] D. K. Isenor and S. G. Zaky, "Fingerprint identification using graph matching," *Pattern Recognition*, vol. 19, no. 2, pp. 113-122, 1986.

[28] A. Ranade and A. Rosenfeld, "Point pattern matching by relaxation," *Pattern Recognition*, vol. 12, no. 2, pp. 269-275, 1993.

[29] M. M. S. Chong, T. H. Ngee, L. Jun, and R. K. L. Gay, "Geometric framework for fingerprint classification," *Pattern Recognition*, vol. 30, no. 9, pp. 1475-1488, 1997.

[30] A. P. Fitz and R. J. Green, "Fingerprint classification using hexagonal fast Fourier transform," *Pattern Recognition*, vol. 29, no. 10, pp. 1587-1597, 1996.

[31] K. Rao and K. Black, "Type classification of fingerprints: a syntactic approach," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 2, no. 3, pp. 223-231, 1980.

[32] R. Cappelli, D. Maio, and D. Maltoni, "Combining fingerprint classifiers," *Proc. 1st MCS*, Cagliari, Italy, pp. 351-361, 2000.

[33] A. Senior, "A combination fingerprint classifier," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 23, no. 10, pp. 1165-1174, 2001.

[34] M. Kawawoe and A. Tojo, "Fingerprint pattern classification," *Pattern Recognition*, vol. 17, no. 3, pp. 295-303, 1984.

[35] B. G. Sherlock and D. M. Monro, "A model for interpreting fingerprint topology," *Pattern Recognition*, vol. 26, no. 7, pp. 1047-1055, 1993.

[36] C. L. Wilson, G. T. Candela, and C. I. Watson, "Neural network fingerprint classification," *J. Artificial Neural Networks*, vol. 1, no. 2, pp. 203-228, 1993.

[37] R. Brunelli and D. Falavigna, "Personal identification using multiple cues," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 17, no. 10, pp. 955-966, 1995.

[38] L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 20, no. 12, pp. 1295-1307, 1998.

[39] Federal Bureau of Investigation, The Science of Fingerprints: Classification and Uses, U.S. Government Printing Office, Washington, D. C., 1984.

[40] A. R. Roddy and J. D. Stosz, "Fingerprint features-statistical analysis and system performance estimates," *Proc. IEEE*, vol. 85, no. 9, pp. 1390 –1421, 1997.

[41] J. D. Stosz and L. A. Alyea, "Automatic system for fingerprint authentication using pores and ridge structure," *SPIE Proc. Automatic Systems for the Identification and Inspection of Humans*, vol. 2277, pp. 210-223, 1994.

[42] V. S. Srinivasan and N. N. Murthy, "Detection of singularity points in fingerprint images," *Pattern Recognition*, vol. 25, no. 2, pp. 139-153, 1992.

[43] A. K. Jain, S. Prabhakar, and S. Pankanti, "A filterbank-based representation for classification and matching of fingerprints," *Int. Joint Conf. Neural Networks*, vol. 5, pp. 3284-3285, 1999.

[44] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Trans. Image Processing*, vol. 9, no. 5, pp. 846-859, 2000.

[45] Nalini K. Ratha, Chen Shaoyun, and Anil K. Jain, "Adaptive flow orientation-based feature extraction in fingerprint images," *Pattern Recognition*, vol. 28, no. 11, pp. 1657-1672, 1995.

[46] A. K. Jain, L. Hong and R. Bolle, "On-line fingerprint verification", *IEEE Trans. Pattern Anal. Machine Intell.*, Vol. 19, No. 4, pp. 302-314, 1997.

[47] A. Farina, Z. M. Kovács-Vajna, and A. Leone, "Fingerprint minutiae extraction from skeletonized binary images," *Pattern Recognition*, vol. 32, no. 5, pp.877-889, 1999.

[48] M. T. Leung, W. E. Engeler, and P. Frank, "Fingerprint image processing using neural networks," *IEEE Proc. 10th Conf. Computer and Communication Systems*, vol. 2, pp.582-586, 1990.

[49] W. F. Leung, S. H. Leung, W. H. Lau, and A. Luk, "Fingerprint recognition using neural network," *Proc. IEEE Workshop, Neural Networks for Signal Processing*, pp. 226-235, 1991.

[50] D. Rutovitz, "Pattern recognition," *J. Roy. Statist. Soc.*, vol. 129, pp. 504-530, 1966.

[51] B. Moayer and K. S. Fu, "A tree system approach for fingerprint recognition," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. PAMI-8, no. 3, pp. 376 –387, 1986.

[52] L. O'Gorman and J. V. Nickerson, "An approach to fingerprint filter design," *Pattern Recognition*, vol. 22, no. 1, pp. 29-38, 1989.

[53] Q. Xiao and H. Raafat, "Fingerprint image postprocessing: a combined statistical and structural approach," *Pattern Recognition*, vol. 24, no. 10, pp. 985-992, 1991.

[54] D. Maio, D. Maltoni, "Neural network based minutiae filtering in fingerprints," *Proc. 14th Int. Conf. Pattern Recognition*, pp. 1654-1658, vol. 2, 1998.

[55] S. Kim, D. Lee, and J. Kim, "Algorithm for detection and elimination of false minutiae in fingerprint images," *Proc. 3rd Int. Conf., Audio- and Video-Based Biometric Person Authentication (AVBPA)*, Halmstad Sweden, pp. 235-240, 2001.

[56] Feng Zhao and Xiaoou Tang, "Preprocessing for skeleton-based fingerprint minutiae extraction," *The 2002 Int. Conf. on Imaging Science, Systems, and Tech. (CISST'02),* Las Vegas, Nevada, USA, June 24-27, 2002.

[57] K. Uchida, T. Kamei, M. Mizoguchi, and T. Temma, "Fingerprint card classification with statistical feature integration," *Proc. 14th Int. Conf. Pattern Recognition,* vol. 2, pp. 1833-1839, 1998.

[58] Feng Zhao and Xiaoou Tang, "Duality-based Post-processing for Fingerprint Minutiae Extraction," *The 2002 Int. Conf. on Information Security (sponsored by ACM),* Shanghai, China, July 10-13, 2002.

[59] L. Hong, A. Jian, S. Pankanti, and R. Bolle, "Fingerprint enhancement," *Proc. 3rd IEEE Workshop, Applications of Computer Vision (WACV '96)*, pp. 202 –207, 1996.

[60] D. Simon-Zorita, J. Ortega-Garcia, S. Cruz-Llanas, and J. Gonzalez-Rodriguez, "Minutiae extraction scheme for fingerprint recognition systems," *Proc. Int. Conf., Image Processing,* vol. 3, pp. 254-257, 2001.