Strategies for intelligent interaction management and usability of biometric systems

A Thesis Submitted to the University of Kent

For the Degree of Doctor of Philosophy (Ph.D.)

In Electronic Engineering

By

Qianqian Wu

March 2016

Acknowledgements

My thesis would have been impossible to finish without the assistance of others, and it is here that I would like to express my most sincere gratitude to them.

First and foremost, I would particularly like to articulate my deep gratitude to my supervisors Professor Michael Fairhurst, who gave me the opportunity to study for my PhD and was generous with his support, advice and constant support in the project work. At last few years, I have been through many difficult times. I believe without his help my project would have been impossible to achieve. Hence, I want to express my deepest appreciation to my supervisor again for greatly assisting me in many ways on various aspects of my work and my life.

I would like to express my heartfelt thanks to my husband, Xuejian Wang for giving me full support in my life, and always being there for me. Without him I would have many more stressful and worrisome moments.

Finally, last but not the least, I would like to thank all my colleagues in the department, especially friends of the Image and Information Engineering Research group of School of Engineering and Digital Arts of the University of Kent who improved my research experience by discussing and suggesting research issues related to my Ph.D. study.

Abstract

Fingerprint biometric systems are one of the most popular biometric systems in current use, which takes a standard measure of a person's fingerprint to compare against the measure from an original stored template, which they have pre-acquired and associated with the known personal identification claimed by the user. Generally, the fingerprint biometric system consists of three stages including a data acquisition stage, a feature extraction stage and a matching extraction. This study will explore some essential limitations of an automatic fingerprint biometric system relating to the effects of capturing poor quality fingerprint images in a fingerprint biometric system and will investigate the interrelationship between the quality of a fingerprint image and other primary components of a fingerprint biometric system, such as the feature extraction operation and the matching process. In order to improve the overall performance of an automatic fingerprint biometric system, the study will investigate some possible ways to overcome these limitations. With the purpose of acquisition of an acceptable quality of fingerprint images, three components/enhancements are added into the traditional fingerprint recognition system in our proposed system. These are a fingerprint image enhancement algorithm, a fingerprint image quality evaluation algorithm and a feedback unit, the purpose of which is to provide analytical information collected at the image capture stage to the system user. In this thesis, all relevant information will be introduced, and we will also show some experimental results obtained with the proposed algorithms, and comparative studies with other existed algorithms will also be presented.

Contents

List of Tables

List of Figures

Chapter 1

Introduction and background

Fingerprint recognition is one of the most widely used biometric technologies in current practical use. The study reported in this thesis will introduce relevant information about fingerprint biometrics and also each component of an automatic fingerprint biometric system will be presented in order to provide us with an overview its structure and configuration. Furthermore, the essential limitations of fingerprint biometric systems relating to the effects of a poor quality fingerprint image will be explored and some approaches to overcome these presented and evaluated.

This chapter will present the fundamental background and basis for the investigations and analysis reported later in this thesis. Section 1.1 will introduce some background information about traditional identity management systems and also explain why the development of biometric technology is very important. Section 1.2 will introduce an initial overall background survey of biometrics, which consists of five aspects including applications of biometrics, disadvantages of biometrics, characteristics of biometric modalities and biometric systems. Section 1.3 will present relevant information about fingerprints as a biometric modality, and also describes each component of an automatic fingerprint biometric system and the techniques involved. Section 1.4 will discuss research problems relating particularly to the effect which a poor quality fingerprint image has in a fingerprint biometric system. Section 1.5 will state the proposed solutions and the novel contributions of the project. Following this overall consideration of the problem to be addressed, the objective and aims, and the organisation of the study to be presented in this thesis will be explained in Section 1.6.

1.1 Introduction and background

Nowadays, fingerprint recognition systems have been widely used for verifying personal identity because fingerprint biometrics exhibit extremely useful properties, including reliable performance, inexpensive cost, east of use. According to a National Institute of Science and Technology (NIST) research report, the quality of fingerprint images should be predictive of recognition performance [1] [2]. Thus, the study to be reported in this thesis will address some important aspects of how to obtain fingerprint images with an improved level of quality by means of better user-system interaction, in order to improve system performance including accuracy, and error rates. The project has three objectives. Firstly, we will investigate issues around the effect of data quality, and propose one approach to improve the quality in the input fingerprint images by using a new fingerprint quality enhancement algorithm. Furthermore, the project will analyse fingerprint image defects by using a new fingerprint image quality evaluation algorithm from the point of view of five aspects to determine the particular factors which are likely to have generated a poor quality image. Finally, this project will develop a interface to guide the user interact with the biometric system more effectively in order to obtain a fingerprint image with an acceptable quality, which is a second approach to overcome the quality issue in a fingerprint recognition system.

Traditionally, to access secure physical areas or protect sensitive information, conventional identity management systems based on a personal identification number (PIN) or the possession of a particular artefact (such as a card or key) are used as a key/token to verify a person's identity. With the development and innovation of science and technology, nowadays, these traditional identity management systems have been applied in many areas for protecting personal information such as the mobile phone, bank information, and many others.

However, there are many negative influences which affect users' lives. First of all, a password can be hard to memorize (especially if a user employs a number of different passwords for different applications) and can sometimes be easily guessed or "cracked". For example, if the user uses the same personal identification number and

password for all systems, it obviously increases the risk for cracking a password. Otherwise, if the user sets a PIN for every isolated system, he might struggle to remember all passwords as the total number of the systems increases, which now has already become a troublesome issue because society is becoming more mobile and interconnected. For the convenience of memorizing, many users might set a simple password that is vulnerable to dictionary attack or even a simple knowledge-based guess. Also, the traditional identity management systems utilize knowledge or the use of a token to establish surrogate representations (i.e. a surrogate representation is a virtual identity which an individual established when he first uses a system, such as passwords and ID cards). Once the surrogate representations are lost, the user would lose access to the system completely until their identity is established again [3]. Besides that, the traditional identity management systems often make it difficult or impossible to control surrogate representations being shared among users, which further complicates the identity management task. A typical example is the sharing of access to online information services, such as an online library, magazine, and so on.

Over the past few decades, biometric techniques have attracted increasingly more attention for their superior characteristics in dealing with the aforementioned problems and meeting a variety of requirements of identity management, such as public security issues and bank transactions. It has reasonably been seen that biometrics is an important emerging discipline that attempts to identify and distinguish a person through the physical, chemical or behavioural measurement of the characteristics of an individual, such as fingerprint, voice print, iris, handwritten signature and face [4]. Figure 1.1 shows some examples of common biometric modalities, including fingerprint, ear, face, hand geometry, vein pattern, voice, keystroke pattern, signature, iris, plamprint, gait, facial thermogram [4].

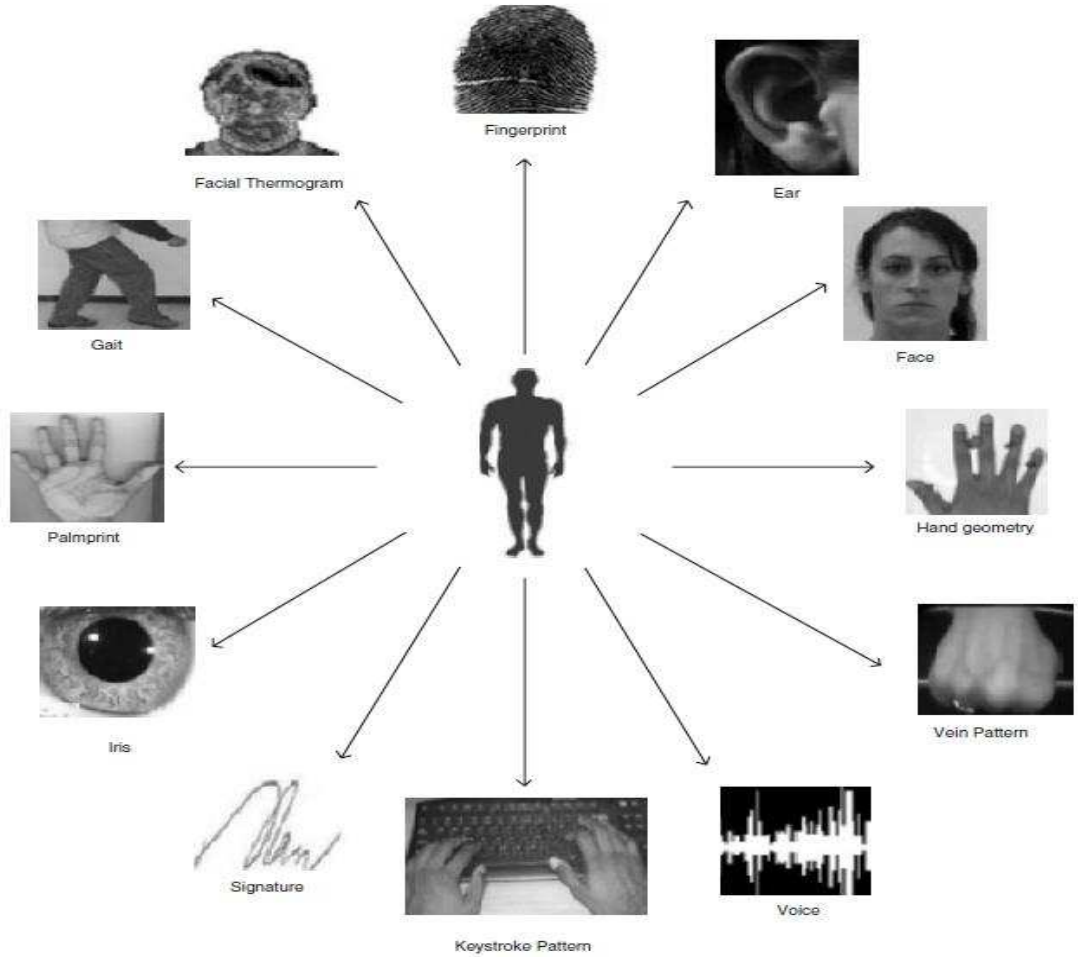


Figure 1.1: Examples of biometric trains (Taken from [4])

1.2 Biometrics

1.2.1 Applications of biometrics

As an emerging science and technology, biometrics has been intensively studied and developed over at least the past decade, and many of the biometric modalities now in use have gradually been accepted by the public and have applied increasingly in practice to provide solutions for various identity management related tasks. For hundreds of years, the handwritten signature has been used as a means of verifying

identity and also it has been a widely accepted means for providing authentication for legal documents, bank cheques and other formal transactions [5]. Face recognition has been used as means of virtual and physical access control (e.g. access to office buildings, mobile phones, personal computers, and nuclear power plants), law enforcement and surveillance (e.g. tracking down suspected individuals and post-event analysis in sensitive areas), and formalising official documents (e.g. driving license, passport, and national identity card) [6]. Dental biometrics and DNA have found application in forensic science, historical research, and medical science [7]. Iris and fingerprint recognition have been seen gradually more and more deployed as a measure for large scale identity management systems, such as border control and securing access of private information contained on a mobile phone. Generally speaking, the application of biometrics can be sorted into three categories: government security sector applications, forensic applications, and commercial and industrial application [8].

1.2.2 Some disadvantages of biometrics

Although biometrics can provide high security, bring convenience to users, and innovate traditional identity management technologies, there are still questions and issues which need to be resolved.

One of issues is that biometrics may not be superior to traditional identity verification mechanisms in all application contexts. For example, the deployment of biometrics on a very large scale is challenging. All biometric systems operate at a certain accuracy which is defined, for example, by the percentage of false matching rate of the system [9] as well as other measures. Assuming that we have a biometric system for verification of an individual's identity, which operates at 0.01% false matching rate, this simply implies that with 10,000 attempts of a brute force attack, the system can be broken by an imposter on average. The security level that such a biometric system provides is only equivalent to a 5 digit password machine, which obviously does not provide a high level of security for the user compared with more traditional alternatives.

Secondly, biometrics relies on measuring a unique biological characteristic of a person, which cannot be replaced if it has been compromised. For every individual, a desirable biometric measure is unique and invariant for a period of time (e.g. face and voice), or even for a whole lifetime (e.g. fingerprint and iris). Assume, for example, that we are using an access control system, which operates based on face biometrics, and one user's face biometrics have been compromised. It will be difficult for the system operator to establish a new identity in the system for the user since the user's face biometrics cannot be reset as easily as a password. This has led to a whole new area of research, and a further layer of processing in the event of biometric compromise. A good example of this is the use of the concept of revocability through the application of unidirectional transforms to raw biometric data [10].

Thirdly, an individual's biometrics are not necessarily as confidential as more abstract or hidden knowledge. Biometrics is something that we take wherever we appear. For example, a person's face biometrics can be remotely captured via high definition camera when visiting a shop or walking out of a building; the fingerprint of a person can been recovered and/or fabricated through a latent fingerprint left on anything touched; a person's voice biometrics can be easily recorded by a potential imposter. Despite the superior properties biometrics provides for a modern identity management system, there are also these issues we need to consider and resolve when designing and setting up a biometric system.

1.2.3 Characteristics of biometric modalities

By definition, biometrics-based processing can make use of any characteristic of an individual as long as it can be appropriately acquired, and that it satisfies the following requirements [4]:

- Universality: the selected characteristic should be possessed by every individual to be enrolled.

- Distinctiveness: no two persons should be the same in terms of two characteristic.
- Permanence: the chosen modality should be stable and invariant over a sufficient period of time.
- Collectability: the biometric trait should be measurable in a quantitative way, and should be repeatable.

It is well acknowledged that a good biometric identifier should meet the following demands associated with a biometric system [4]:

- Performance: it should provide satisfactory accuracy within a demanded time frame, and be robust enough for realistic application.
- Acceptability: the chosen biometric technology should be acceptable to the proposed community of users
- Circumvention: it should possess the ability to resist subversion by other means and be similarly resistant to forgery or imitation.

Generally, these requirements should be satisfied for all biometric systems. However, in practice, a good biometric modality will not necessarily completely satisfy all aspects in every respect, but must do so to a degree suitable for the intended actual requirement of the biometric system in a particular application scenario [8]. Figure 1.2 illustrates a review of most common biometric traits in these aspects.

Biometric characteristic	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Facial thermogram	H	H	L	H	M	H	L
Hand vein	M	M	M	M	M	M	L
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Ear	M	M	H	M	M	H	M
Hand geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Retina	H	H	M	L	H	L	L
Iris	H	H	H	M	H	L	L
Palmprint	M	H	H	M	H	M	M
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H
DNA	H	H	H	L	H	L	L

Figure 1.2: Provides a review and comparison of some common biometric traits which are rated in High, Medium, and Low categories, abbreviated as H, M and L respectively (Taken from [8]).

1.2.4 Biometric systems

An identity management system that is built based on biometric technologies, takes a standard measure of a person's biometric characteristic to compare against the measure from an original stored template (i.e. a template is the biometric data that the user enrolled in a biometric system, usually under supervision to guarantee integrity [3]), which they have pre-acquired and associated with the known personal identification claimed by the user.

Based on the recognition scheme, biometric systems can generally be sorted into two categories as either a verification systems or an identification system, which are described as follows [4]:

- A verification system: this type of biometric system basically verifies an individual's identity, which is equivalent to answering the following question that "is this person who he claim to be", by making a comparison of the biometric characteristic with the enrolled reference template in the system database, and then a decision is finalized through a similarity measure. Presuming that we adopted a similarity measure for the verification task, which calculates the distance/difference, which is represented as d, between the input sample and reference template. And then a threshold T, which represents the tolerance of the difference the system is operating at is created to supervise the verification process. If $d < T$, then the user is accepted into the system with the identity he has claimed, otherwise, the system rejects the user as an imposter [4], [11]. The verification system carries out a 1:1 comparison to confirm the user's identity.

- An identification system: an identification system addresses the question "who is this person". In the same way as with a verification system, the system also stores the users' biometric templates in the system database. When a user wants be recognized by the system, his biometric characteristic is exhaustively compared with all the existing users' biometric templates in the system database, and the system produces a list of similarity of which the user might be, and depending on the similarity measure the authentication is granted [4].

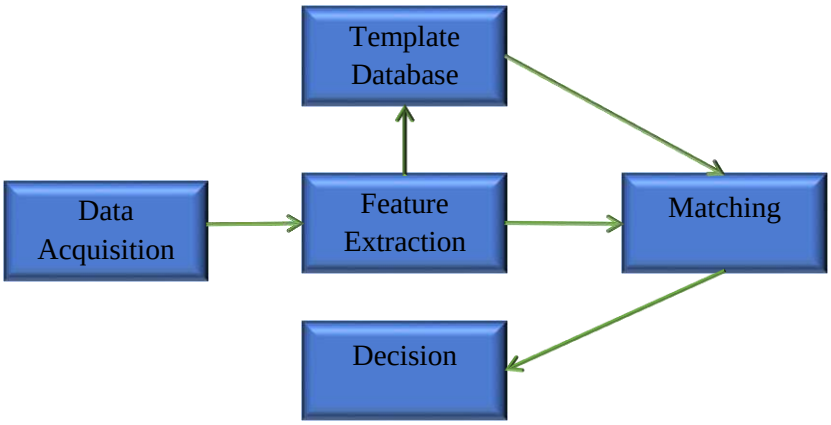


Figure 1.3: An example of fundamental components in a biometric system.

Depending on the functionality of each part of a biometric system, we can divide a biometric system into four main modules, consisting of a data acquisition module, a feature extraction module, a matching module, and a database module. Within each module, a set of related activities are performed. Figure 1.3 illustrates these fundamental components of a biometric system. The specification of all modules of a biometric system will be described in detail as follows [4]:

- The first unit is the data acquisition module, where a specific biometric sensor is used to capture the biometric data from the user in a regulated environment. For example, a high definition camera might be utilized to collect an iris image from a user. Besides that, depending on the awareness of the data collection process in a biometric system, data acquisition modules can be categorized into two different modules, which are called either an active data acquisition module or a passive data acquisition module. An active biometric collection process is in an application scenario that the user is fully aware of the data acquisition process, and the user might also be instructed and regulated to donate the sample in some application setup. For example, biometric samples such as iris, fingerprint, and signature recognition are generally acquired in an active data acquisition scheme. As for biometrics such as face, gait and voice,

a passive data acquisition scheme is usually more feasible. In that case, the user might have little or no awareness of the data acquisition process. Suspect tracking and screening in an airport environment is a typical example of biometric system with a passive data acquisition scheme. These two options are also sometimes referred to as overt and covert capture respectively.

- The second unit is the feature extraction module. Once a biometric data sample has been collected from a user, it generally needs to be pre-processed, and then a feature representation would be generated by applying the specified feature extractor. The quality of the input sample may also be controlled and regulated in the pre-processing stage, where data processing such as noise removal and histogram equalization for contrast enhancement (to give just two examples) are carried out.

- The third unit is the matching module, which compares the feature representation extracted from the input sample with the user's template stored in the template database. There are two different approaches in current use including the state of art classifier (e.g. support vector machine [12], neural network [13], hidden Markov model [14], naive Bayesian classifier [15]) and similarity measure (e.g. maximum likelihood estimation [16]). In the application context of a multi-modal biometric system (a multi-modal biometric system deploys two or more biometric modalities in its design, where each modality provides its own identity evidence), a decision fusion scheme is normally required to combine classification results produced by each classifier, and a decision is made based on the specified fusion scheme.

- The fourth unit is the template database, which stores all enrolled or updated users' biometric data. Normally, instead of storing the raw biometric data of a user, a biometric template database will store an extracted feature representation, which has been generated by a specified feature extractor, and for security reasons, the feature representation might be encrypted by means of

a specific algorithm[17]. Generally, the user needs to enrol his/her biometric data at first into a database in the form of a suitable template before the service being protected by the biometric system can be used. At the enrolment stage, several individual; biometric samples might be collected from the user and used to construct a reliable feature representation of the user either in a supervised or unsupervised environment. If appropriate, quality control measures might be deployed at the enrolment stage to ensure that the system acquires an acceptable biometric characteristic from the user. After the enrolment, a user profile is fully constructed and the original biometric template is stored in the template database. To keep the latest biometric information of a user, many biometric systems will update the biometric templates store in the template database after a given period of time or by setting up other updating mechanisms: supervised methods (e.g. clustering-based or editing based strategies) and semi-supervised methods (e.g. graph based, self-updating strategies) [18].

1.3 Fingerprint biometrics

1.3.1 Background to fingerprint biometrics

Unlike some of the biometric modalities developed more recently, such as ear, gait, hand vein, keystroke, facial thermograms, the uniqueness of the fingerprint was empirically observed and its value in human identity established a considerable time ago, so that its value in biometrics has developed and matured for over a hundred years [4]. It is believed that the earliest application of the fingerprint as a measure for identity verification can date back to as early as AD273 in China according to an archaeological investigation of sales contracts and regulation of trade at an archaeological site of Dun Huang [19]. The earliest research about the fingerprint was contributed by Nehemiah Grew, an English plant morphologist. He described some of the basic patterns on the human finger and foot skin although he did not notice its uniqueness and its potential application for verification or classification of identities of individuals in 1684 [20]. The early development of a fingerprint classification system was driven by the demand

for identity management (although this term was not then as established as now) of criminals. In 1884, fingerprint evidence helped the authorities to solve a murder case in Argentina, which later led to the practical adoption of the first fingerprint classification system [21]. In 1896, the first fingerprint classification system, which was named the Vucetichissimo system, was introduced by Ivan Vucetich, and was deployed to identify criminals in Argentina [22]. In 1901, another influential fingerprint classification system was developed and soon adopted by police forces all over the world, and which is named the "Henry classification system" [23]. In 1911, fingerprint evidence alone was used to convict someone accused of burglary [24]. This historical timeline of fingerprint technology development has demonstrated the fingerprint's individuality as a biometric trait and its long established acceptance by law enforcement authorities.

As noted above, the development of fingerprint biometrics was initially motivated primarily by the need of a method to verify the identity of a criminal in order to replace the traditional approaches for an identity verification. During the early period of use, fingerprint matching was mainly conducted through visual inspection of topologies of fingerprint patterns, which was based largely on the Henry classification system [24]. However, as the volume of recorded fingerprints of criminals increased, manual and visual matching of fingerprint methods soon became extremely time consuming and, infeasible, especially for identification tasks, which eventually led to the development of the automatic fingerprint identification system (AFIS). In the 1980s, an automated fingerprint identification system was created by the US Federal Bureau of Investigation, which had managed to extract the minutiae (minutiae are discussed in detail at Section 1.3.3.2 of this chapter) of a fingerprint automatically and derived a classification method based on minutiae patterns [24].

Nowadays, in addition to the traditional application of fingerprint biometrics in criminal screening and other identity management related applications made by the authorities, fingerprint biometrics have also been widely adopted and embraced for personal and commercial applications. For example, Samsung developed the

fingerprint-controlled door locks [25], and ClockRite has also introduced a fingerprint clocking system [26]. Furthermore, another development in the application of fingerprint biometrics is that a fingerprint biometric has been utilized in mobile phones to secure the access of mobile device and authorize the rapidly booming transactions and payments made on the mobile internet. Figure 1.4 illustrates some examples of personal and commercial applications of fingerprint biometrics.

(a) (b) (c)

Figure 1.4: Some examples of personal and commercial applications of fingerprints biometrics: (a) Samsung fingerprint door lock (Taken from [25]); (b) Fingerprint clocking system utilize fingerprint biometrics to assure the user is really he claims to be when clocking in and out (Taken from [26]); (c) IPhone 6s embedded with fingering sensor which assist establishing a digital ID for unlocking mobile phone and also for authorizing online payments (Taken from [27]).

Compared to many other biometrics, fingerprint biometrics have been shown to offer some superior properties, including time tested reliability, long established acceptance

by the authorities, fast growing acceptance by the public, thoroughly researched individualization, and flexible and economical deployment.

1.3.2 Automatic fingerprint biometric systems

An automatic fingerprint biometric system utilizes fingerprint biometrics to recognize or confirm an individual's identity. In the context of biometrics, the term "fingerprint" refers to the impression the friction ridge skin on a person's fingertip leaves when in contact with a surface. The fingerprint pattern is biologically developed and formed during the first few weeks of the embryo and persists through a lifetime [24]. The foundation of fingerprint biometrics was built on over a hundred years' empirical examination and observation of the uniqueness and individualization of one's fingerprint characteristics.

Similarly to any biometrics system, an automatic fingerprint biometric system could also be divided into two categories, defined as either a fingerprint verification system or a fingerprint identification system depending on the nature of the recognition task it carries out [4].

- A fingerprint verification system: this verifies that a user actually is the person he or she claims to be, by performing a one-to-one matching procedure. The system takes a fingerprint sample from the user, and compares it with fingerprint template of the claimed identity enrolled in the system. If the similarity measure between them is higher than a (task-dependent) defined threshold, the user is recognized as the genuine user. Vice versa, if this degree of match is not met, then he might be considered as an imposter, or a person attempting to break into the system without appropriate authorisation [4].

- A fingerprint identification system: in this case we search for a user's identity in a fingerprint identity database, and identify "who he really is" according to a similarity measure. The user is assigned the identity to which his sample has

the highest similarity to, providing the result of the similarity measure computation is higher than a defined threshold. Otherwise, he is declared unenrolled in the system if the result of the similarity measure computation is below the defined threshold [4].

Generally, the structure of an automatic fingerprint biometric system also includes three stages: data acquisition, feature extraction, and matching [4]. The detailed information about all these stages of an automatic fingerprint system is described in following section.

1.3.3 Fundamental components of an automatic fingerprint analysis system

1.3.3.1 Data acquisition stage

The data acquisition stage is the point at which the fingerprint images from the users are captured. This can be achieved either by means of a live scan of the fingerprint image produced by a digital fingerprint sensor or a scan of an offline collected fingerprint, such as a digital scan of a latent fingerprint lifted from a crime scene or a rolled fingerprint on a fingerprint card (a fingerprint card is a form that authorities (e.g. the police) use to record a person's personal information and fingerprints, and an example of a fingerprint card is shown in Figure 1.5) [24]. Some detailed information about different types of fingerprint sensors will be given below.

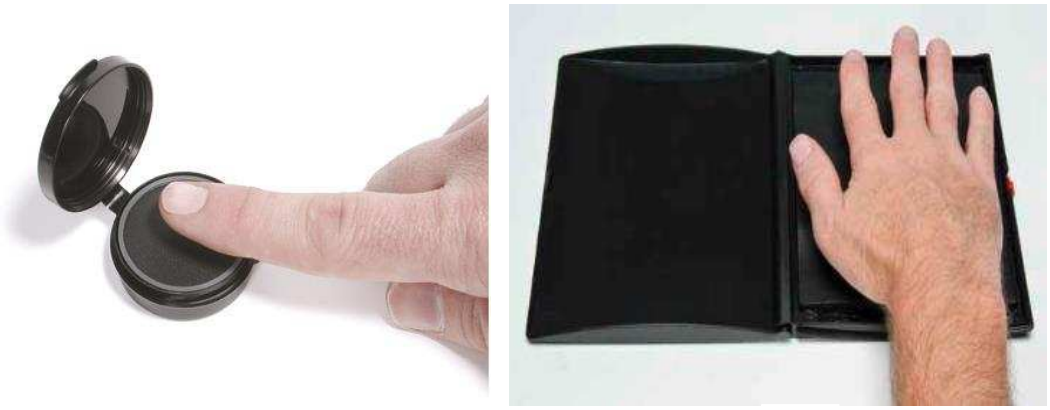
1.3.3.1.1 Sensing fingerprints

At the early stage of development of fingerprint acquisition technology, before computerised techniques were established, fingerprints were mainly acquired using an ink-based process [4], [24]. As the technology developed, the sensing and recording of fingerprints has been computerized. Typically, there are two types of fingerprint collection methods depending on the acquisition process adopted. These are online and offline scan approaches.

- Offline scan: there are two types of offline fingerprint collection methods. One is the historical ink technique-based fingerprint collection, and another one is the latent fingerprint collection [22]. The collected fingerprints by these two methods can be digitized through taking a scan or a photo. The traditional inked fingerprint is collected using specialized fingerprint collection equipment including ink roller, inking plate, fingerprint card, and a specialized ink as demonstrated in Figure 1.5. Firstly, a finger is uniformly smeared with specialized ink, then a rolled or dabbed fingerprint is collected on a fingerprint card, and in the end the fingerprint is digitized via a scanning device [22]. With the development of appropriate technology, micro-reticulated thermoplastic resin pads and ceramic inking pads have been generated as a new approach for collecting fingerprint which simplifies the collection process [22]. Figure 1.6 illustrates an example of a ceramic fingerprint pad and palm print pad separately. In addition, a latent fingerprint is another important type of fingerprint, which is a residual fingerprint that is left behind when a person touches an object or a surface. The latent fingerprint has a major application in forensics.

(a) (b)

Figure 1.5: An example of tradition fingerprint collection equipment and collection process. (a) Equipment required for inked technique based fingerprint collection. (b) An illustration of inked fingerprint collection procedure (Taken from [24]).



(a) (b)

Figure 1.6: (a): An example of ceramic fingerprint pad; (b): an example of palm print pad (Taken from [28]).

- Live scan: A live scan of a fingerprint collects the fingerprint from a person's fingertip by means of a digital fingerprint sensor [4], [24]. Various types of live scan mechanism have been utilized to design the fingerprint sensor for detecting ridges and valleys on the surface of the finger, and they generally can be assigned to three basic categories: optical (i.e. frustrated total internal reflection optical fingerprint sensor), solid-state (e.g. capacitive fingerprint sensor, thermal fingerprint sensor, pressure based fingerprint sensor), and ultrasound sensors [4] [29] [30]. Figure 1.7 illustrates some examples of different types of fingerprint sensors. Furthermore, depending on acquisition behaviour design, the fingerprint sensor can also be categorized into touch based, sweep based, and touchless sensors, which also lead to a difference in reconstruction of fingerprint images [4]. Generally, a touch based sensor is easier to use while a sweep based fingerprint sensor needs rather more intuition and practice to use it correctly. The sweep based fingerprint sensor was found to have a fail-to-acquire rate of 37.9% in collecting the well-known FVC2004 database [31]. Although the touch based sensor performs better than the sweep based sensor, it also suffers from the pressure vs physical distortion dilemma and latent fingerprint issues, which led to the development of touchless

fingerprint recognition systems [32], [33]. Various sensors will naturally generate different quality of fingerprint images, subject to the sensing mechanism and the interaction design they adopt.

Figure 1.7: Some examples of fingerprint sensors: (a): optical sensor (Taken from [34]); (b): ultrasound sensor (Taken from [35]); (c) capacitive sensor (Taken from [36]); (d) thermal sensor (Taken from [37]); (e) pressure sensor (Taken from [38]).

1.3.3.2 Key parameters of fingerprint sensors

The FBI has identified a set of important parameters of digital fingerprint sensors including resolution, physical area, number of pixels, geometric accuracy, gray-level quantization, gray-level uniformity, input/output linearity, spatial frequency response, and signal-to-noise ratio [4], [39]. By investigating the impact of these parameters, researchers have suggested that the acquisition area of the fingerprint sensor is the

most influential parameter over the performance of a fingerprint biometric recognition system [40], [41].

1.3.3.3 Feature extraction stage

The feature extraction stage is necessary to extract the fingerprint feature representation from a fingerprint image. After the fingerprint is successfully captured by the fingerprint sensor, the image is processed by the feature extractor to extract a representation of the fingerprint. This representation is linked to a personal identification number (i.e. the number used throughout the entire system as the digital identity of the user) and a personal profile, which contains fundamental information (e.g. gender, age, address) about the user when the user is enrolled in the system for the first time.

The dominant features which a fingerprint image contains relate to the ridges and valleys which are visually presented as dark areas (ridges) and light areas (valleys) in a gray level digital fingerprint image. The characteristics of a fingerprint image can be sorted into three levels in a hierarchical order [4], as follows:

- Level 1: at the global level, the ridge flow defines a pattern on a fingerprint such as loop, delta, and whorl [4]. Also, this can be further sorted into a more detailed typology such as left loop, right loop, whorl, arch, tented arch, as described in Henry's fingerprint classification system and illustrated in Figure 1.8 [4]. Generally, loop and delta points are named singular points, which is useful for fingerprint classification and indexing, but they are not adequate alone for accurate matching because of their lack of distinctiveness. Besides that, various other features also can be extracted at the global level, some examples of which are the external fingerprint shape, orientation image and frequency image [4]. More detailed information about the orientation image and frequency image will be described in Chapter 3.

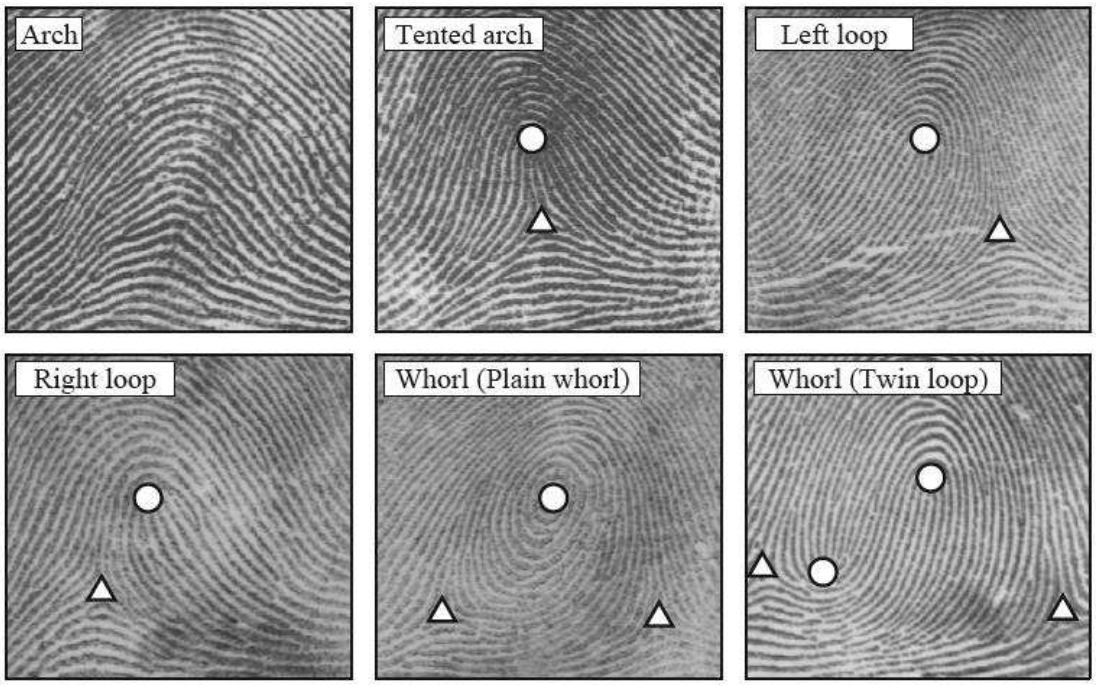


Figure 1.8: Examples of five basic types of fingerprints, including arch, tented arch, left loop, right loop, and whorl (Taken from [4]).

- Level 2: at the local level, there are around 150 types of low-level detail which can be observed in a fingerprint. However, some of these details are difficult to observe since their appearance can be highly dependent on the quality of the impression [42]. The two most common ridge patterns are ridge bifurcations and ridge endings, which are used as minutiae points because of their stability and robustness [4]. A ridge ending is defined as the place where a ridge terminates abruptly, while a ridge bifurcation is defined as the point where a ridge splits into branch ridges [43]. Figure 1.9 demonstrates an example of these different types of minutiae points.

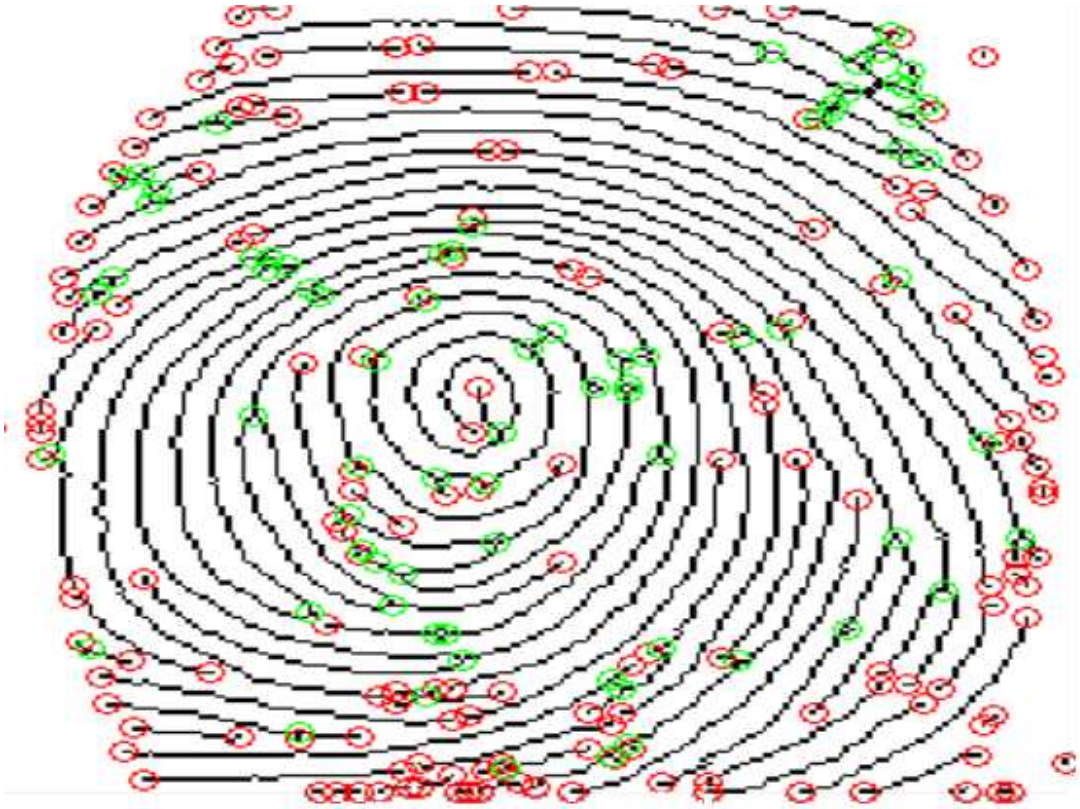


Figure 1.9: An example of the minutiae points detected on a fingerprint images. Green circles indicate a ridge bifurcation, while the red circles indicate a ridge ending (Taken from [44]).

- Level 3: at the very fine level, more intra-ridge characteristics of a fingerprint image can be detected including ridge width, shape, curvature, edge contour and pores. Among them, sweat pores are the most important, but these can be easily extracted only from fine high resolution fingerprint images [4].

According to the different scales of the feature extraction, three types of feature extraction algorithms can be derived which lead to the development of three categories of fingerprint representation techniques: (i) ridge pattern based, (ii) minutiae points based, and (iii) pores, local shape of ridge edges and other characteristic based feature representation [4].

1.3.3.4 Matching stage

The matching stage is the final processing stage, which compares the input fingerprint image from a user with the fingerprint template of the claimed identity enrolled in the system (in a verification scenario), and then returns result, usually in the form of match "score". However, fingerprint images captured even from the same finger can often appear significantly different because of the large variations caused by particular capture conditions, such as rotation of the finger on the sensor or other displacement, uneven pressure applied at the sensor, different skin conditions which can occur. As a result, to develop a fingerprint matching algorithm which can effectively handle all these different sorts of variation can be difficult and challenging [4].

Generally, most of the automatic fingerprint matching algorithms which have been proposed in the literature can quite effectively match good quality fingerprint images. However, matching low quality fingerprint images and incomplete lifted latent fingerprints remains very challenging. Currently, automatic fingerprint matching algorithms can be assigned into three categories: (i) correlation-based matching, (ii) minutiae-based matching, and (iii) non-minutiae based matching [4], which are described as follows:

- Correlation based matching: two fingerprint images are compared directly by the global pattern of ridges and valleys to investigate the degree of similarity between them. The disadvantages of this type of algorithm are that if the rotation and displacement of these two fingerprint cannot be determined, this matching algorithm will need to exhaustively compare the query fingerprint at all possible rotation and displacement positions, which is computationally intensive. Furthermore, non-linear distortion and noise contamination make impressions from the same finger exhibit a potentially significant difference, and, as a result, two global fingerprint patterns which are nominally the same cannot necessarily then be reliably correlated [4] [55].

- Minutiae based matching: this is the most popular matching technique in current use, which extracts minutiae from the two fingerprints and stores them as sets of minutiae points. The result of the matching comes from the similarity between these two minutiae feature sets. Although the minutiae pattern of each finger is unique, the performance of a minutiae feature extraction is significantly affected by the quality of the fingerprint image. A degraded fingerprint image will result in errors in the minutiae extraction process, which can lead to a number of problems, including a number of false minutiae which are detected and the strong possibility that some of the genuine minutiae are missed [4] [56] [57] [58].

- Non-minutiae based matching: this type of matching algorithm is utilized when the minutiae based matching algorithm is infeasible, particularly in extracting features from poor quality fingerprint images. In this case, matching solutions based on less distinctive features, such as the ridge patterns, (e.g. local orientation, frequency, ridge shape, and texture information), is adopted in the design of a matching algorithm, which can then be more reliable than using the minutiae themselves [4] [59].

1.4 Research problem

It is well known that most available fingerprint recognition systems use minutiae-based matching [4]. Minutiae characteristics are local discontinuities in the fingerprint pattern which represent two basic kinds of minutiae, one is the ridge ending and the other is ridge bifurcation. A ridge ending is defined as the place where a ridge terminates abruptly, while a ridge bifurcation is defined as the point where a ridge splits into branch ridges [60]. Figure 1.10 shows an example of a ridge ending and a bifurcation.

Figure 1.10: Examples of ridge ending and bifurcation.

Therefore, automatically and reliably extracting minutiae from fingerprint images is a critical part of the structure of an automatic fingerprint recognition system. However, there exist many difficulties in the minutiae extraction procedure since the performance of a minutiae feature extraction algorithm is significantly affected by the quality of the fingerprint image. Ideally, in a well-defined fingerprint image, the ridges can be easily detected and minutiae can be precisely located in the image as long as ridges and valleys change and flow in a locally constant direction. Figure 1.11(a) shows an example of an "ideal" fingerprint image. However, due to intrinsic (e.g., incorrect ridge frequency and orientation estimation) and extrinsic reasons (e.g., temporal or permanent cuts, dry/wet fingers, dirt, residual prints on the sensor surface, etc.), fingerprint images generally fall short of this ideal in practical applications [45]. Usually, a fingerprint image could be made up of regions of various qualities, either good, medium, or poor quality, where the ridges pattern might be noisy and contaminated (Figures 1.11(b) and (c)). Table 1.1 list the criteria of three categories in quality of fingerprint images [61].

(a) (b) (c)

Figure 1.11: (a) A good quality fingerprint; (b) a medium quality fingerprint degraded by ridge breaks; (c) a poor quality fingerprint including a lot of noise.

Quality	Factors
Good	Foreground is much bigger than background. The ridges can be easily detected. Most of the minutiae can be precisely located. The gray-value contrast between ridges and valleys is clear.
Medium	Foreground is bigger than background. Most of the ridges strutures can be easily detected. A fair amount of minutiae are visible. The gray-value contrast between and valleys is clear.
Bad	Foreground is smaller than background. The ridges strutures is completedly corrupted. Only a small number of minutiae are visible. The gray-value contrast between and valleys is poor.

Table 1.1: Definition of qualitative measurement of the quality of fingerprint images (Taken from [61]).

In general, degradations which affect the quality of fingerprint images can be assigned to three basic categories [4]:

- The ridges are not continuous since there are small gaps in the ridge, which is misleading;
- Parallel ridges are not well separated due to the presence of cluttering noise;
- Cuts, creases, and bruises are found to be present (usually) on the surface of the fingertip.

As a result, these three types of degradation can negatively interfere with the minutiae extraction process, which brings about the following problems [4]:

- A large number of false minutiae are detected,
- Some of the genuine minutiae are missed,
- The position and orientation information of the minutiae might be erroneously extracted.

As a summary, according to the literature referred to above about fingerprint recognition systems, we can find that extraction of a reliable minutiae feature from fingerprint images is a critical part in a fingerprint system, and it relies heavily on the quality of fingerprint images. However, for both intrinsic and extrinsic reasons, acquisition of an ideal fingerprint image can be a very difficult problem, which is suggested as a limitation of fingerprint systems. In order to acquire an acceptable quality of fingerprint image, two different solutions will be introduced, which will be presented in the next section.

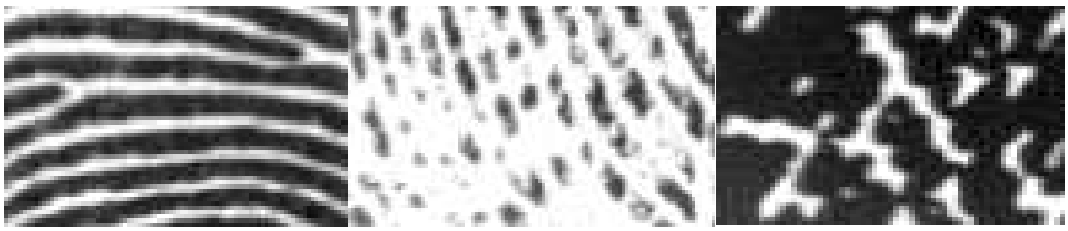
1.5 Contributions

1.5.1 Proposed solutions

With the purpose of acquisition of an acceptable quality of fingerprint images, three components/enhancements are added into the traditional fingerprint recognition system in our proposed system. These are a fingerprint image enhancement algorithm, a fingerprint image quality evaluation algorithm and a feedback unit, the purpose of which is to provide analytical information collected at the image capture stage to the system user.

Generally, for each fingerprint image, the fingerprint regions resulting from the segmentation can be divided into three categories (Figure 1.12) [4], [62]:

- Well-defined region, in which ridges and valleys are clearly separated so that a minutiae extraction algorithm is able to detect minutiae correctly.
- Recoverable region, in which minutiae cannot be easily detected because the clarity of ridges and valleys structures are corrupted due to a small amount of noise present in the fingerprint, arising from typical physical sources in the finger itself, such as cuts, creases, etc.
- Unrecoverable region, in which ridges and valleys are corrupted completely by a severe amount of noise and distortion which results in minutiae becoming completely unrecognisable.



(a) (b) (c)

Figure 1.12: Fingerprint regions (a): Well-defined region; (b): recoverable region; (c): unrecoverable region.

In general, an enhancement algorithm can work on the first two categories, and thus these two categories are classified as recoverable regions, while the last category is described as referring to unrecoverable regions [4]. Therefore, two solutions have been proposed based on the different kinds of classification of fingerprint regions, which are described below in greater detail. Figure 1.13 illustrates these two different solutions for acquisition of an acceptable quality of fingerprint images in a fingerprint recognition system.

- Solution 1: a fingerprint image enhancement algorithm is adopted as a solution to improve the quality of fingerprint images for facilitating the extraction of minutiae. Theoretically, an enhancement algorithm should be capable of removing noise and improving the clarity of the ridges and valleys in the structure of recoverable regions in the input fingerprint image to correctly identify the minutiae based on visual clues summarized by professional fingerprint inspectors such as local ridge orientation, ridge continuity, ridge tendency and etc., as long as ridges and valleys structures in a fingerprint image are not corrupted completely. In this work, the proposed fingerprint image enhancement algorithm is based on the idea of a contextual filter, which achieves higher accuracy than other algorithms which have been proposed. The detailed information about this algorithm is described further in Chapter 3.

- Solution 2: If the enhanced fingerprint image cannot be verified by the fingerprint recognition system, which may consist of a significant number of unrecoverable regions resulting in a fingerprint image enhancement algorithm is not the appropriate method to use here, and then a feedback process is proposed as another solution for acquiring a new fingerprint image with an acceptable quality. This process provides information to the user about the degradation of the current image, and offers an opportunity to provide a better image, usually through supporting an improved interaction between the user

and the sensor. More detailed information and analysis about this feedback unit is described in Chapter 5.

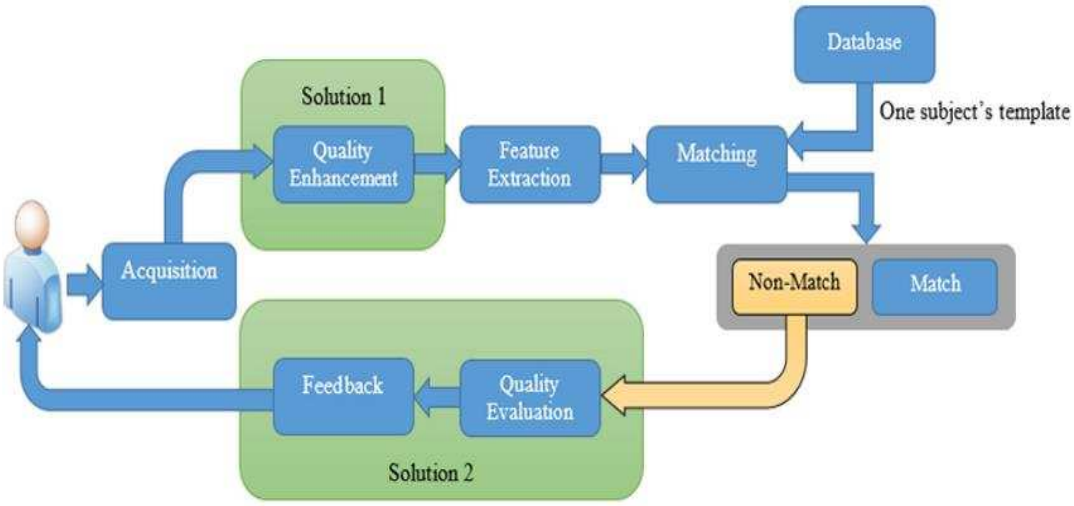


Figure 1.13: Two different solutions proposed for acquisition of an acceptable quality of a fingerprint image in a fingerprint recognition system.

As shown in Figure 1.13, in the study we report here, a fingerprint image should be evaluated by the proposed fingerprint image enhancement algorithm firstly (as described in Chapter 3), and then the enhanced fingerprint will be verified by the fingerprint recognition system to investigate whether the selected fingerprint can be matched with fingerprint template of the claimed identity or not. If this enhanced image cannot be matched, it means that it may be a poor quality fingerprint, and possibly consists of unrecoverable regions. In this case, the user will be asked to provide a new fingerprint image. In order to acquire a fingerprint with an acceptable quality, the input fingerprint will be evaluated using a quality check through the fingerprint image quality evaluation algorithm (as described in Chapter 4) for seeking the modifiability of input activity to assess fingerprint quality, which generated the poor quality data in the first place. And then the analytical results from the fingerprint

image quality evaluation algorithm will be embedded into the feedback unit (as described in Chapter 5). Finally, an appropriate guidance through the feedback unit will be provided to the user in a way which encourages the acquisition of a new fingerprint collection where the quality of the image is improved.

1.5.2 List of contributions

The key contributions of this thesis were described as follows.

- A new fingerprint quality enhancement algorithm have been proposed to improve the quality of fingerprint images, which consists of four steps including fingerprint image segmentation, local ridge orientation calculation, local ridge frequency estimation and Gabor filtering. In this work, novel methods were introduced in the first three steps (fingerprint image segmentation, local ridge orientation estimation and local ridge frequency estimation). In order to evaluate the proposed fingerprint enhancement algorithm, the FVC 2004 databases were used. According to the experimental results obtained, the proposed algorithm is found to effectively and efficiently improve the verification accuracy.

- A novel algorithm is introduced to evaluate the quality of fingerprint images from the point of view of five different aspects including valid area, dry/wet finger, worn ridge, and position deflection. Also, a new algorithm is proposed to estimate the fingerprint position deflection, which utilizes a new reliable and robust method to detect fingerprint singular points. Through a series of experiment and result analysis, the proposed algorithm has shown to be more accurate than other approaches.

- A feedback unit is suggested for a fingerprint recognition system, which provides the appropriate guidance to the user to guide the user to interact with the biometric sensor correctly by analyzing the input fingerprint image so as to

improve the usability of a fingerprint recognition system. Three different mechanisms are introduced to investigate whether the proposed feedback unit is able to improve the performance of the biometric system or not, and to also to seek the best mechanism for the fingerprint biometric system in terms of verification accuracy. Also, a new online fingerprint collection database was created specifically for evaluating the performance of the fingerprint biometric system.

1.6 Chapter conclusions and thesis organisation

In this chapter, an introduction has been presented an initial background to the biometrics field in general, which includes aspects such as the potential applications of biometrics, disadvantages of biometrics-based solutions, and the characteristics of biometric modalities and biometric systems. In addition, an information about the nature of the fingerprint itself has been presented, which provides us with a clear view of the fundamental information required to understand fingerprint biometrics. Also each component of a typical automatic fingerprint biometric system and the techniques involved in processing fingerprint data have been described, which provide an overview of the structure and configuration of a complete automatic fingerprint biometrics system.

Subsequently, some essential limitations of an automatic fingerprint biometric system have been clearly identified, which relate to the effects of capturing poor quality fingerprint images in a fingerprint biometric system. In order to improve the overall performance of an automatic fingerprint biometric system, it is necessary to extensively explore and investigate some ways to overcome these limitations. In this circumstance, the specific objectives of the study have been introduced in this chapter.

Finally, with the purpose of making the following chapters more cohesive and easier to follow, the organisation of this thesis can be described as follows:

- Chapter 2: Fingerprint databases

This chapter introduces fingerprint databases utilized throughout this study, comprising four offline databases, which are used to evaluate our proposed algorithms, especially in relation to the proposed fingerprint image enhancement algorithm (see Chapter 3) and the singular detection algorithm (see Chapter 4), and one online database, which we designed and collected in-house in order to evaluate our proposed algorithms and, in particular, in order to evaluate the feedback interaction strategies under consideration (see Chapter 5). This was necessary because we required detailed information about the nature of the interaction between specific users and the capture sensor, and an on-line evaluation of the characteristics of the captured sample, in order to provide and analyse the effects of feeding back an analysis to the user. Only then could we understand how our proposed approaches could lead to an improvement in processing performance. Obviously, this sort of data is not generally available, and so we had to collect relevant data for ourselves.

- Chapter 3: Fingerprint image enhancement

This chapter presents relevant information and background about the fingerprint image enhancement, and discusses some related work about a range of fingerprint image enhancement algorithms. Subsequently, the proposed new fingerprint enhancement algorithm is described, which consists of five steps including fingerprint image segmentation, local ridge orientation, local ridge frequency and Gabor filtering. For each step, relevant background and related research studies are introduced and analysed. Finally, some experimental results obtained with the proposed algorithm and comparative studies with other existing algorithms will also be introduced.

- Chapter 4: Fingerprint image quality assessment

This chapter will present a review of relevant background information about the effect of fingerprint image quality in an automatic fingerprint recognition system, and will also survey existing reported research studies which are concerned with fingerprint image quality evaluation algorithms. Subsequently, a new proposed fingerprint image

quality assessment algorithm will be described, which includes four independent sub-methods for analysing fingerprint image defects from the point of view of five aspects (i) valid area in the image, (ii) an image is taken from a wet finger, (iii) a dry finger, (iv) the existence in the image of worn ridges and (v) the effects of position deflection on the sensor.

- Chapter 5: Human-Biometric-Sensor Interaction Evaluation

This chapter will present a review of relevant background information about the effect of usability of the biometric system, and will survey existing reported research about approaches for the design of software agents in the biometric system. Subsequently, the design of a user feedback interface based on the three different mechanisms which have been proposed, will be described with detailed information about the characteristics of each mechanism. Finally, some experimental results will be reported and analysed in order to investigate whether the proposed feedback unit is able to improve the performance of the biometric system or not, and will compare the different mechanisms to seek the best practical strategy for improving the performance of a typical biometric system.

- Chapter 6: Final remarks

This chapter will provide a final overview and discussion of the study reported in the thesis, which includes two aspects: firstly, it will summarize all the contributions made in this thesis. Secondly, it will introduce some potential new ideas for the improvement of fingerprint-based recognition systems in the future.

It should be noted that this chapter provides only general background to the field of study. Because the work reported is somewhat diverse in nature, a decision has been taken to review the state of the art in detail in the relevant experimental chapters later in the thesis.

Chapter 2

Fingerprint databases

In this chapter, we will introduce the fingerprint databases utilized throughout this reported study, including a set of databases collected for the Fingerprint Verification Competition (FVC) carried out in 2002 and 2004. In addition, we also introduce an online fingerprint database which was designed and collected in-house, specifically for this study, in order to evaluate the proposed algorithms and, in particular, the feedback interaction strategies under consideration. Section 2.1 will present all the details and specification of the FVC databases and also explain the design and the data collection protocol of the in-house online fingerprint databases. Finally, section 2.2 is the brief conclusion of this chapter.

2.1 Fingerprint databases

In this study, five fingerprint databases are used for the experiments carried out: these are categorised as either offline or online databases, depending on whether the test computations are carried out based on the physical presence of the human user (online) or on pre-collected data (offline) [31]. In the work, four of the experimental databases are characterized as offline databases, which consist of the FVC 2002 DB1_A, FVC2004 DB1_A, FVC2004 DB2_A, and FVC2004 DB3_A databases, and one online database, which is that compiled in-house specifically for this project, and which are refer at simply as the "on-line database".

The specification of these databases is described and discussed as follows:

1. **Offline Databases - FVC databases**

   The Fingerprint Verification Competition (FVC) databases were planned and collected for a series of fingerprint verification competition campaigns, which were organized by various institutions including the Biometric Systems Lab, University of Bologna, Pattern Recognition and Image Processing Lab, Michigan State University, U.S., the National Biometric Test Center, and San Jose State University [4]. The purpose of the fingerprint verification competitions was to provide databases according to the same protocol for evaluating the performance of various state-of-the-art fingerprint recognition systems [31]. Currently, the FVC databases are among the most popular fingerprint image databases adopted for experimentation within the fingerprint research community. A significant proportion of researchers working on fingerprint-based biometric systems report their experimental results based on these databases when comparing their algorithms with algorithms developed by other researchers. Until now, the FVC databases include four different databases, relating to the years in which they were compiled, namely: FVC 2000, FVC 2002, FVC 2004 and FVC 2006.

In the FVC series of databases, the first three editions adopt the same protocol to collect fingerprint images, which utilized three different fingerprint scanners and one SFinGE synthetic generator to create four different databases, which are designated DB1, DB2, DB3 and DB4 [31].

In FVC 2000, two small- size and low – cost fingerprint sensors were used to collect the fingerprint images in DB1 and DB2 including an optical fingerprint sensor and a capacitive fingerprint sensor. And, a higher quality (large area) optical sensor was applied to collect the fingerprint images in DB3. Finally, a synthetic generator was used to synthesize new fingerprint images in DB4, which are similar to the fingerprint images acquired by the traditional "ink-technique". In addition, some rules were used to create these databases, which are described as follows. Firstly, if fingerprint images were considered completely intractable by a human expert, they could be discarded from the databases, while, in order to avoid an excessive degree of ease of matching algorithms, "perfect" fingerprint images were also removed from the databases [46].

In FVC 2002, three different fingerprint sensors were used. In DB1 and DB2, two different optical fingerprint sensor were employed, and fingerprint images of DB3 were collected by using a capacitive fingerprint sensor. As for each database, all fingerprint images were sorted by quality according to the NIST quality index [1] [2], and then the top-ten quality fingers were discarded. More detailed information about the FVC 2002 databases will presented in the following section [47].

In FVC 2004, in the same way as for the process of the FVC 2002 data collection, the fingerprint images were collected by using a different optical fingerprint sensor in DB1 and DB2, while a thermal fingerprint sensor was applied to collect fingerprint images in DB3. In this work, no fingerprint images were discarded with respect to quality of fingerprint images, whatever

the evaluation by a human expert or the NIST quality index. More detailed information about the FVC 2004 databases will be also described in the following section [48].

Compared with the above three editions of FVC, there is a different way to collect fingerprint images adopted in FVC 2006. The collection of fingerprint images was performed without deliberately introducing difficulties such as exaggerated distortion, rotation of the finger, wet/dry fingerprint image, etc. However, a wider variety of individuals were asked to donate their fingerprint, which included manual workers and elderly people. At the end, all fingerprint images were selected to create databases by choosing the most difficult images according to the NIST quality index [49].

Table 2.2 provides a brief summary of each of these FVC databases (see [4]), and the difficulties reported in Table 2.2 were received from analytical results of top performing participants, which is listed in Table 2.1. It should be noted that in FVC 2000, the FMR (False Match Rate) / FNMR (False Non-Match Rate) Errors were computed without FTE (Failure to Enroll) error, so that poor quality fingerprint images could be rejected at enrolment time, which affects the comparison results. This could be a challenge when comparing FVC 2000 databases with others [31]. Furthermore, FVC 2006 [49] has not been considered because it is not available in-house. Hence, in our work, only two databases are available.

	DB1	DB2	DB3	DB4
FVC2000	2.30%	1.39%	4.34%	3.38%
FVC2002	0.20%	0.17%	0.63%	0.16%
FVC2004	1.61%	2.32%	1.34%	0.81%
FVC2006	5.88%	0.05%	1.59%	0.39%

Table 2.1: EER (Equal Error Rates) of the top three performing algorithms for the FVC databases (Taken from [4]).

Competition	Number of Databases	Size of each Databases	Notes
FVC 2000 [46]	4	A: 100×8 B: 10×8	• Volunteers are mainly unhabituated students. • Two sessions, no quality check. • Low to Medium difficulty (DB1, DB2, DB4); Medium to High difficulty (DB3),
FVC 2002 [47]	4	A: 100×8 B: 10×8	• Volunteers are mainly unhabituated students. • Three sessions, no quality check. • Voluntarily exaggerated perturbations: displacement, rotation, wetness and dryness. • Low difficulty (DB1, DB2, DB3, DB4).
FVC 2004 [48]	4	A: 100×8 B: 10×8	• Volunteers are mainly unhabituated students. • Three sessions, no quality check. • Voluntarily exaggerated perturbations: distortion, wetness and dryness. • Medium difficulty (DB1, DB2, DB3, DB4).
FVC 2006 [49]	4	A: 100×8 B: 10×8	• Heterogeneous population also includes unhabituated manual workers and elderly people. • No quality check. • The Final databases were selected from a larger database by choosing the most difficult fingerprints according to a quality index. • High difficulty (DB1), Medium difficulty (DB3), Low difficulty (DB2, DB4).

Table 2.2: A summary of FVC databases. The size of each database is noted as 100 fingers and 8 impressions per finger (Taken from [4]).

In the present study, only two databases were used for the proposed algorithms. As noted in Table 2.2, we can see that the fingerprint images in FVC 2002 [47] were collected by including exaggerated movement and rotation of the finger which introduces the degradation (e.g. rotation and displacement of fingerprint) in the acquired fingerprint images. Thus, that is the best choice to use when investigating the performance of the proposed singular detection algorithm (i.e. this algorithm is used to detect core points of fingerprint images). As for the proposed fingerprint image enhancement algorithm, the FVC 2004 [48] database is the best to use when evaluating whether or not the proposed algorithm can improve the performance of the fingerprint recognition system, because, according to the difficulty reported in Table 2.1, this database is markedly more challenging than the FVC 2002 databases [50].

- **FVC 2002 Database [47]**

  The Second International Fingerprint Verification Competition (FVC 2002) is one of most popular public fingerprint image databases in current use. Four different databases were created, which are designated DB1, DB2, DB3 and DB4 and, for each database, a different fingerprint sensor is used for collecting data samples.

  In these databases [47], a total of 90 volunteers were asked to donate their fingerprints, which were randomly partitioned into three groups, associating to distinct database samples collected using a different fingerprint sensor. Figure 2.1 shows an image taken from each database of FVC 2002. Each individual providing data was required to donate four impressions of two fingers (index and middle finger) of both hands, and this is done in three separate sessions. In order to acquire fingerprints with a different quality, during the second session, participants were required to dislocate fingers at maximize differences of the finger placement (in impressions 1 and 2) and rotate the finger with maximum 35 degrees (in impressions 3 and 4); and for the third session, participants

enrolled their fingerprint under different conditions such as giving a sample from a dry (in impressions 1 and 2) print and from a wet finger (in impressions 3 and 4). Figure 2.2 shows an example of collected impressions under different conditions. The technical descriptions for each database are also listed in Table 2.3.

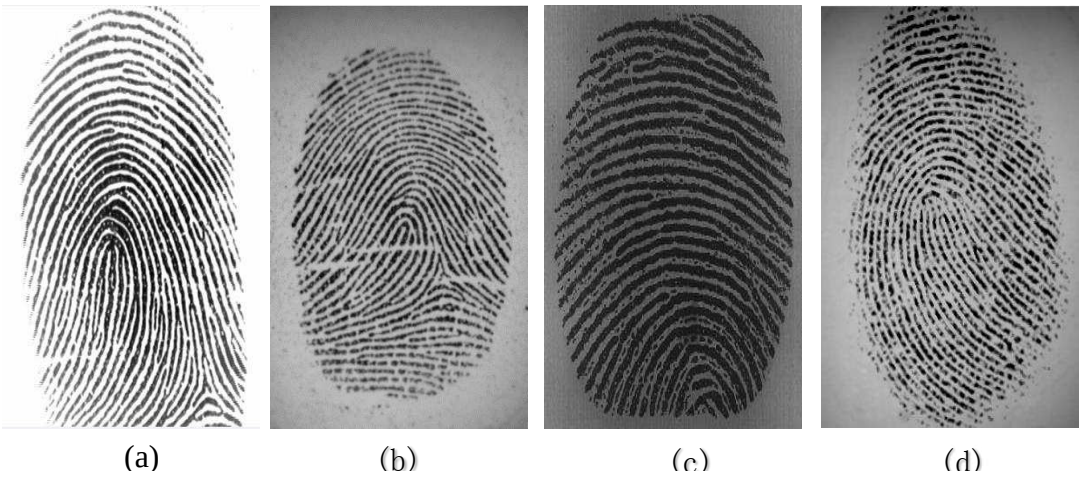


Figure 2.1: Examples of a fingerprint image from each database in FVC 2002 database. (a) DB1; (b) DB2; (c) DB3; (d) DB4.

Figure 2.2: Examples of a fingerprint image under different conditions in the FVC 2002 database. (a) displacement of the finger; (b) rotation of the finger; (c) a dry fingerprint; (d) a wet fingerprint.

	DB1	**DB2**	**DB3**	**DB4**
Sensor Type	Optical Sensor	Optical Sensor	Capacitive Sensor	SFinGe V2.51
Image Size	388 * 374	296*560	300*300	288*384
Set A	100*8	100*8	100*8	100*8
Set B	10*8	10*8	10*8	10*8
Resolution	500 dpi	569 dpi	500 dpi	500 dpi

Table 2.3: The technical descriptions of FVC2002. (Taken from [47])

As shown in Table 2.3, each database contains 110 fingers and 8 impressions per finger (880 fingerprint images in total), and it is divided into two subsets A and B. In our study, only FVC2002_DB1A database was used for evaluating the singular detection algorithm (detailed information will be provided in Chapter 4). In this database, 800 images of 100 fingers were captured with an optical sensor (specifically, the Touch View II sensor manufactured by Identix [51]).

- **FVC 2004 Database [48]**

  Since the FVC 2000 and FVC 2002 databases have received a significant amount of attention from both the academic community and commercial organizations, the FVC 2004 databases were collected for the purpose of evaluating the new and existing algorithms for comparison of fingerprint biometric systems [48], [31]. Table 2.4 shows the technical description of the FVC 2004 database.

	DB1	**DB2**	**DB3**	**DB4**
Sensor Type	Optical Sensor (CorssMatch V300)	Optical Sensor (Digital Persona U. are. U 4000)	Thermal Sweeping Sensor (Atmel FingerChip)	Synthetic Generator (SFinGe v3.0)
Image Size	640 × 480	328 × 364	300 × 480	288 × 384
Set A	100 × 8	100 × 8	100 × 8	100 × 8
Set B	10 × 8	10 × 8	10 × 8	10 × 8
Resolution	500 dpi	500 dpi	512 dpi	About 500 dpi

Table 2.4: Technical description of the FVC2004 database. (Taken from [31])

In this database, a total of 90 people were asked to donate images of their fingerprints [48]. In the same way as for the process of the FVC 2002 data collection, all volunteer participants were randomly divided into three different groups, each associated with a distinct fingerprint sensor. Each individual was required to donate four impressions of two fingers (index and middle finger) of both hands, and this is done in three separate sessions. In order to acquire fingerprints with a different image quality, during the first session, participants were asked to place the finger at a different vertical position (in impressions 1 and 2), and as for impressions 3 and 4 of the fingerprint, the users were requested to apply low and high pressure on the fingerprint sensor alternately. During the second session, users were asked to provide fingerprint images with the exaggerated skin distortion (in impressions 1 and 2), which occurred when a finger is moved on the surface of the fingerprint sensor and, as a consequence, a number of distortions could be generated on the fingerprint image [52]. And then, the participant was asked to donate the fingerprint by rotating the finger (a maximum of 35 degrees) in impressions 3 and 4. In the last session, fingerprints with different skin conditions were obtained. For impressions 1 and 2, they are dry fingerprints, and for impressions 3 and 4, they are wet fingerprints. Figure 2.3 illustrate an example of fingerprint images collected under different conditions, and Figure 2.4 shows an image from each database in FVC 2004.

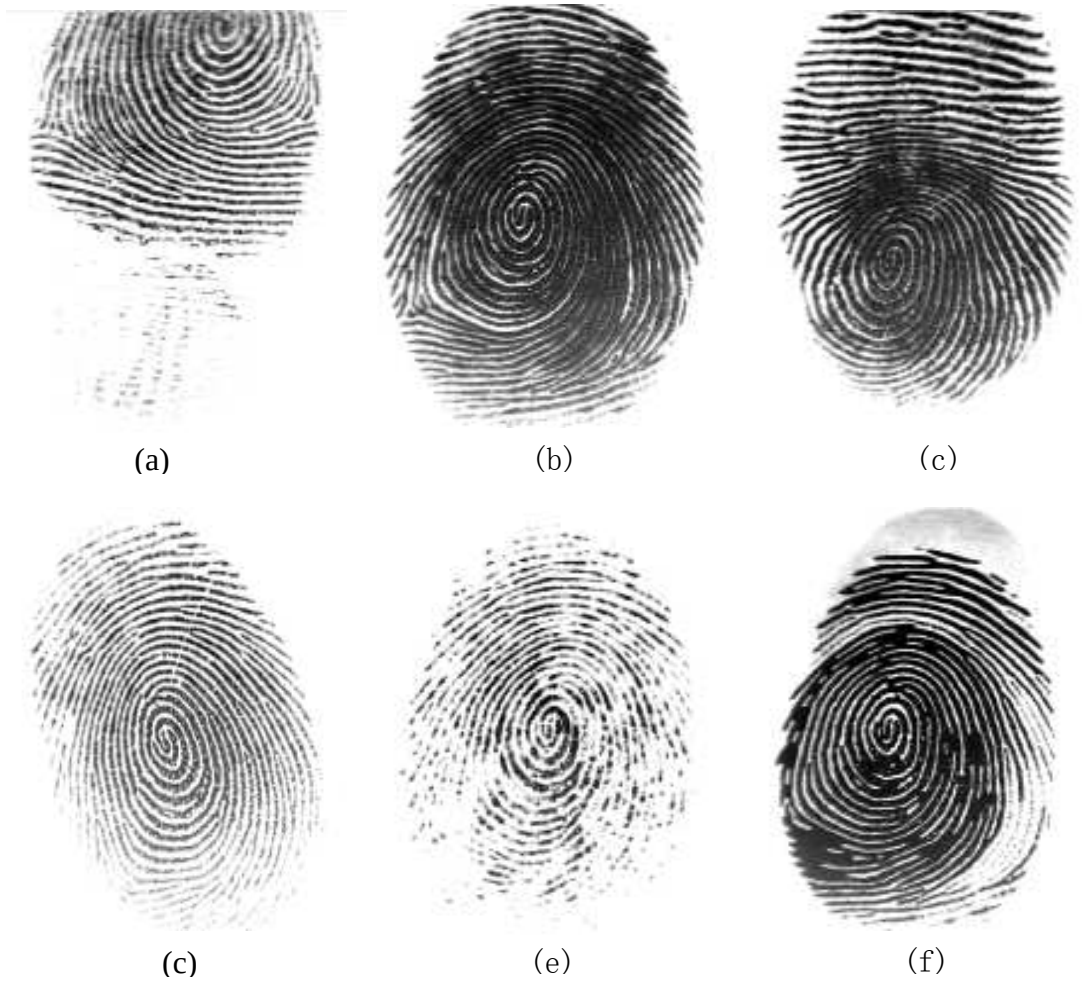


Figure 2.3: Examples of fingerprint images from the same finger collected under different conditions in the FVC 2004 database. (a) the displacement of the finger at a different vertical position; (b) a collected fingerprint with high pressure; (c) a collected fingerprint with skin distortion ; (d) rotation of the finger; (e) a dry fingerprint; (f) a wet fingerprint.

Figure 2.4: Examples of a fingerprint image from each database in the FVC 2004 database. (a) DB1; (b) DB2; (c) DB3; (d) DB4.

In this study, in order to better investigate the performance of the proposed fingerprint image enhancement algorithm, these three different databases were utilized, specifically FVC 2004 DB1_A, FVC 2004 DB2_A, FVC 2004 DB3_A. Fingerprint samples in these databases were collected using two different types of fingerprint sensors. These were an optical sensor and a thermal sweeping sensor (the descriptions of these two different types of fingerprint sensors are noted in Chapter 1). As shown in Table 2.4, the size of each database is the same, each containing 100 fingers and 8 impressions per finger (800 fingerprint images in total).

2. Online Databases – The online in-house collection database

With the purpose of evaluating the performance of the feedback unit, the online fingerprint collection database was created in-house, specifically for use in this study. In this database, all individuals were asked to donate samples of their fingerprints, but in this case using the different proposed feedback mechanisms (these will be described in detail in Chapter 5), which means users were receiving various different kinds of feedback to assist them to interact

with the fingerprint sensor during the acquisition process, in order to increase the chances of providing samples of acceptable quality in the fingerprint images. For this reason, the collection of this new database is essential, since, no current publicly available fingerprint databases contain samples comparable to those processed in this way, and are therefore not suitable for our work.

- **Overview of this database:**

  A total of 30 volunteers were recruited to participate in this data collection activity. For each subject, two images of four fingers (thumb, index, middle finger and ring finger) of both two hands were collected in two sessions, which resulted in a database of 960 fingerprint images. All of the volunteers in the databases were aged between 10 and 70. They come from different educational background and all have limited experience or no experience of interacting with a fingerprint sensor. Also, the majority of the participants are male, which comprises 80% of the database. As for these participants, they work in a Chinese brick factory. Their daily role involve carrying bricks with rough surface which wears their fingerprints and at the same time introduces a great amount of crease and cuts in their fingerprint. The reason for selecting these particular group of participant is because their fingerprint is usually worse than ordinary people, and through testing our algorithms on the data that is collect from these group of people will more realistically reflect the usability and effectiveness of our proposed algorithms on fingerprint images with poor quality. All participants fully completed the planned data collection sessions, which means that their fingerprint data is complete in our experimental setup.

  The volunteers were randomly assigned to test one of the three different feedback mechanisms under evaluation. Table 2.5 lists detailed information about the online collection database description including a brief description of each feedback mechanisms. As a result, three “sub-databases” are created, one for each feedback mechanism respectively. Each sub-database contains

320 images from 10 subjects. For each subject, 4 fingerprints were collected twice from both hands of the subject in each session, including thumb, index, middle and ring finger. The fingerprint image samples of this database vary considerably in quality because of the following three aspects: firstly, most of volunteers have little or no experience of working with fingerprint biometric systems; furthermore, the enrolled fingerprint images were acquired without any effort to control image quality; finally, the fingerprint sensor was not cleaned during collection, since the experimental setup was intended to simulate the condition of a fingerprint sensor in typical practical usage.

Database	Feedback Mechanism	Session 1 Numbers	Session2 Numbers	Total Numbers
DS1	1 display the user's previous failed sample.	16×10	16×10	320
DS2	2 display a specific and detailed analytical report.	16×10	16×10	320
DS3	3 provision of very detailed information including the previous failed fingerprint and the analytical results.	16×10	16×10	320

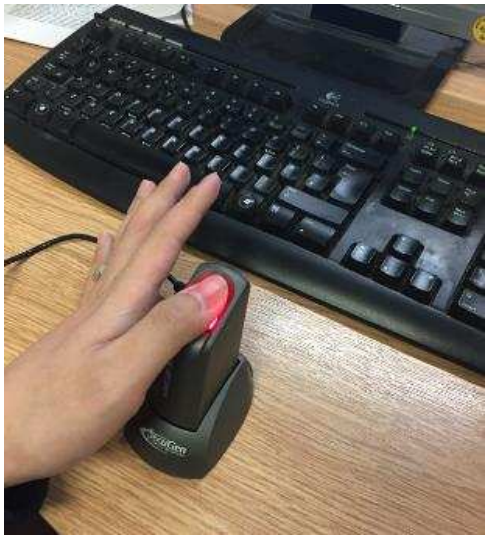
Table 2.5: Detail of the online collection sub-databases.

- **Data collection setup:**

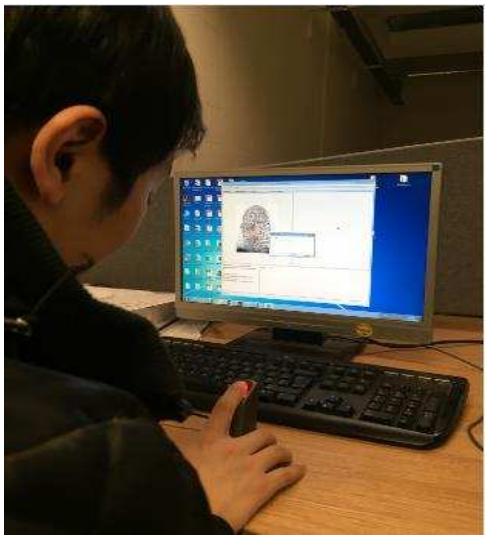
Environment: as shown in Figure 2.5, a fingerprint sensor was placed on the desk where the participant was seated while providing fingerprint samples, and a dry towel and damp wipes were also provided on the desk in order to achieve the transformation of the finger's skin condition as required by the experiment. For example: if the analytical result of processing the input fingerprint is shown to be that this is a wet/dry finger, then the dry/damp tissue (as appropriate) will be used to address the identified problem.

(a)

(b)



(c)



(d)

Figure 2.5: (a) A box of damp wipes; (b) a dry towel; (c) enrolment of fingerprint from an optical sensor; (d) an example of the user interacting with the sensor for the fingerprint enrolment by the VeriFinger 6.5 Algorithm Demo application.

Sensor: The SecuGen Hamster IV (Figure 2.6) sensor was utilized throughout data collection process, which is an optical sensor with an effective sensing area of 12.9mm*16,8mm. The fundamental parameters of the fingerprint sensor are given in Table 2.6.

Figure 2.6: The optical fingerprint sensor (SecuGen Hamster IV).

Name	**SecuGen Hamster IV**
Type	Optical Fingerprint Sensor
Image Resolution	508 DPI
Image Size	258 × 336 pixels
Platen Size	16.1 mm × 18.2 mm
Effective Sensing Area	12.9 mm × 16.8 mm
Operating Temperature	−20℃ ~65℃
Dimensions / Weight	27×40×73mm / 100g (without stand)

Table 2.6: The fundamental parameters of the fingerprint sensor (Taken from [53]).

Software: Participants were asked to enrol their fingerprints using the fingerprint recognition demo software (VeriFinger 6.5/ MegaMatcher 4.3 Algorithm Demo application) marketed by Neurotechnology [54]. For this application, four operational modes are included, which are described as follows:

- Enrolment: this mode can scan a fingerprint from a fingerprint device or enrol a fingerprint from a local disk using the "open file" button.

- Enrolment with feature generalization: this mode produces a feature representation of a finger from multiple fingerprints of the same finger.

- Verification: this mode can perform a one versus one verification procedure.

- Identification: this mode can be used in 1: N matching, which enrols one fingerprint image from the template and compares it with other multiple fingerprint images.

As for the process of the online collection database, only the mode of enrolment was utilised, which can extract features of the input fingerprint and then write this information to the database. The detailed steps of the fingerprint enrolment process are described as follows, and Figure 2.7 illustrates the VeriFinger 6.5 Algorithm Demo application's window with the mode of enrolment.

1) Connect the fingerprint sensor to the VeriFinger 6.5 application. If the connection is successful, the name of the selected fingerprint sensor was displayed in the bottom-left window.

2) Select Enrol from the menu of operation modes, and then scan a fingerprint from the selected fingerprint sensor. If this operation is successful, the input fingerprint image will be shown in the top left window, and the sub-windows will pop up for recording the ID of the enrolled fingerprint. At the same time, this fingerprint will be written to the database.

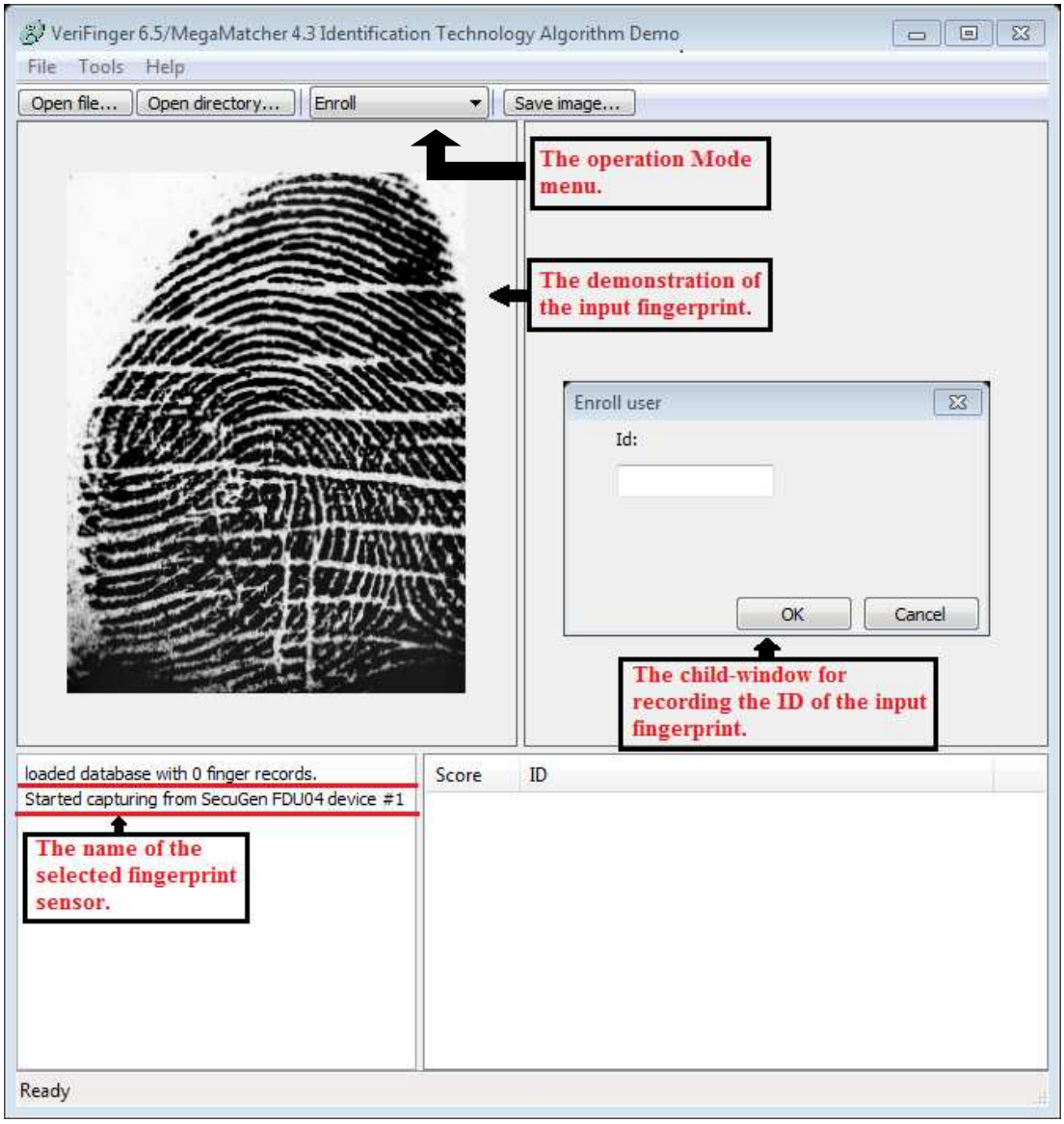


Figure 2.7: Illustration of the VeriFinger 6.5 Algorithm Demo application for collecting the fingerprint image from the selected fingerprint sensor.

- **Data collection procedures:**

  A total of four impressions are collected for each requested finger for each subject during two sessions of data collection, and the time lapse between the two sessions was at least one week.

  During the first session, each individual is randomly partitioned into one of two groups corresponding to the two feedback mechanisms defined for capturing fingerprint images. In the first session, impression 1 was collected without giving any guidance to the subject about how to interact with the sensor. Once the fingerprint was enrolled, the acquired fingerprint image was analysed by the selected feedback mechanism. Then, the user was guided to enrol again (impression 2) using the guidance generated by the feedback mechanism based on the analytical result of impression 1.

  The second session generated impression 3 and impression 4. The data collection procedure carried out in the second session is identical to those in the first session. Impression 3 was collected without any specified guidance, and then the selected feedback mechanism was activated to assist the user, in order to encourage better interaction with the fingerprint sensor when collecting impression 4.

  More details of the experimental work based on the acquired data, and a full specification of the different feedback mechanisms proposed can be found in Chapter 5.

2.2 Chapter conclusions

In this chapter, five fingerprint databases utilized have been described in this study, comprising four offline databases and one online database. The detailed information and specification of each database has been introduced, and also explained the reasons why and how a subset of these databases was selected for the experiments carried out (which will be reported fully in later chapters).

Initially, relevant statistical information about four offline databases was described in detail. For the purpose of evaluating the proposed singular detection algorithm (see Chapter 4), the FVC2002 DB1_A database was utilized. And for investigating the proposed fingerprint image enhancement algorithm (see Chapter 3), three offline databases were used, specifically FVC2004 DB1_A, FVC2004 DB2_A, and FVC2004 DB3_A.

Furthermore, in order to evaluate the influence of the fingerprint feedback processes for use in a fingerprint recognition system (see Chapter 5), a completely new online fingerprint collection database was created in-house specifically for the purposes of the study. Detailed information about this online database was presented in relation to the following aspects: Environment, equipment (the hardware and software) and data collection procedures.

In the following chapter, some detailed relevant information and background material about the fingerprint image enhancement algorithm have been introduced, and also a new and robust fingerprint image enhancement algorithm have been proposed to improve the performance of the overall fingerprint recognition system, which efficiently removes noise and improves the clarity of ridges and valleys structures of the input fingerprint image so as to improve the quality of fingerprint images.

.

Chapter 3

Fingerprint image enhancement

This chapter will present a new fingerprint image enhancement algorithm for improving fingerprint system performance, which efficiently removes noise and improves the clarity of ridge and valley structures of the input fingerprint image. The proposed algorithm is based on Gabor Filtering, and two essential parameters, Local ridge orientation and frequency, will be estimated by novel methods. Section 3.1 will introduce some background information about fingerprint image enhancement algorithms in general. Section 3.2 will discuss some previously reported research in this area. Section 3.3 will describe the new proposed algorithm in detail, which includes four steps: Segmentation, Local ridge orientation image estimation, Local ridge frequency estimation and Gabor filtering. Section 3.4 will show some experimental results obtained with the proposed algorithm, and comparative studies with other existed algorithms will also be introduced in this section. Finally, section 3.5 is the brief conclusion of this chapter.

3.1 Introduction

One approach to improving interaction between the user and a biometric system is to capture the image and then enhance it, in order to try and compensate for lack of quality in the raw data. In this chapter we will explore some ways in which this might be achieved, and we will introduce a new algorithm for image enhancement in fingerprint biometrics.

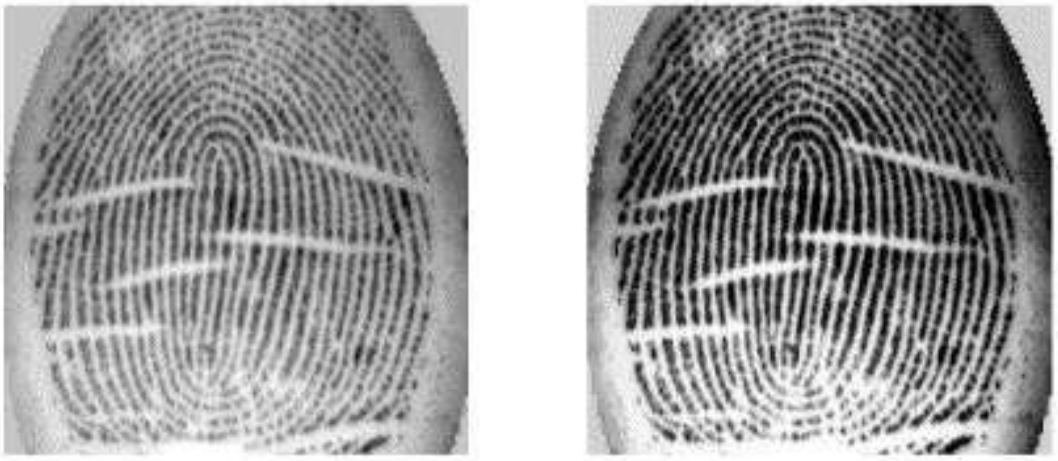
As mentioned in the previous chapter, a fingerprint recognition system consists of three fundamental modules, including the data acquisition module, the feature extraction module, and the matching module [4]. A fingerprint image is first captured by the data acquisition module, and then passed to the feature extraction module for generating a unique feature representation, and after that the representation is compared with the fingerprint template of the person whose identity is claimed. For automatic fingerprint recognition systems, there are two most prominent local ridge characteristics which are widely used, which are named minutiae points and which correspond to ridge endings and ridge bifurcations (as described in Chapter 1).

Minutiae based fingerprint matching algorithms are widely acknowledged as one of the most popular and mature approaches for designing a fingerprint recognition system. As a result, a reliable feature extraction unit is a prerequisite for a stable fingerprint recognition system. However, robustness of feature extraction is often degraded by the quality of the fingerprint image. The noise associated with poor quality images frequently gives rise to large variance in the ridge and valley structures of a fingerprint image which a feature extraction algorithm is based on. One of the most influential degradation factors that a fingerprint image is likely to display is the noise introduced during the fingerprint acquisition process. For instance, a wet fingerprint will often result in cluttered ridges in a fingerprint image; a dry fingerprint, on the other hand, will often generate low contrast and fragmented ridges in a fingerprint; a lifted latent fingerprint from a crime scene may contain much noise introduced by the surface of the object which the fingerprint was lifted from during the acquisition process; a fingerprint captured with inconsistent pressure or sudden movement will commonly

result in a blurred fingerprint. And after a feature extraction algorithm is applied, these various forms of degradation can result in large numbers of erroneous minutiae being detected, genuine minutiae being neglected, and incorrect minutiae information being extracted [4]. Therefore, building an automatic fingerprint image-enhancement algorithm into a fingerprint recognition system is necessary and essential, because this can remove noise and clarify the ridge and valley structures in the fingerprint image in order to significantly improve the quality of the captured fingerprint image.

The benefit of including an enhancement algorithm in the design of a fingerprint recognition system is, therefore, that it helps compensate for common noise occurring in the fingerprint images and improves the existing features in the image. The common enhancement algorithms are designed based on the local ridge orientation (described as the constant ridge direction in a local region), ridge continuity (described as the flow of the ridge direction change), and ridge tendency (ridge characteristics e.g. ridge to valley thickness). A variety of enhancement algorithms has been derived including pixel-wise enhancement, contextual filtering, and multi-resolution enhancement [4], which are descried in detail as follows.

- Pixel-wise enhancement: a pixel-wise enhancement technique operates either locally or globally to improve the contrast of a fingerprint image at pixel level. Although this type of technique does not necessarily achieve completely satisfactory results on its own for improving the quality of fingerprint images, this technique can be an important initial processing step within a state of the art enhancement algorithm [4]. Figure 3.1 illustrates an example of an enhanced image generated using the histogram equalization method, which is an example of a pixel-wise enhancement technique [63].



(a) (b)

Figure 3.1: (a) The original image (b) the enhanced image using the histogram equalization method (Taken from [63]).

- Contextual filtering: in contrast with most of fingerprint recognition systems which deploy a single filter for fingerprint image enhancement, a fingerprint biometric system which utilizes contextual filtering technique would select a suitable filter from a range of pre-computed filters, and then proceed to enhance the local region depending on the local context of a fingerprint images. Generally, the estimated local ridge orientation and local ridge frequency are used as parameters to create the contextual filter so that it can remove noise and clarify the ridge and valley structures in the corresponding local region of the fingerprint image [4]. Figure 3.2 illustrates an example of an enhanced image using the contextual filtering method based on Gabor filters [64].

(a) (b)

Figure 3.2: (a) The original image (b) the enhanced image using Gabor filters approach as suggested by Hong (Taken from [4][64]).

- Multi-resolution enhancement: This technique operates so as to divide the fingerprint image into regions corresponding to the different frequency bands, which is an efficient way to remove the noise in different regions. All the features in the region of the fingerprint image are filtered by a textural filter, and then all of the enhanced image regions are combined to obtain the whole image [4]. Figure 3.3 shows an example of an enhanced fingerprint image using a multi-resolution enhancement technique based on the wavelet-based textural filtering [65].

(a) (b)

Figure 3.3: (a) The original image; (b) the enhanced image using a multi-resolution enhancement method (Taken from [65]).

In general, the goal of an enhancement algorithm is to improve the quality of an input fingerprint image for facilitating the extraction of minutiae [4]. Ideally, an enhancement algorithm should be capable of removing noise and improving the clarity of ridges and valleys in the structure of the image. Besides that, another important factor to consider is that it should not introduce any incorrect features into the image.

In the work to be reported here, our approach is based on the adoption of contextual filters, which is one of the most widely used techniques for fingerprint image enhancement. Regarding this type of the image enhancement technique, two prominent features, the local ridge orientation and the local ridge frequency are utilized in the filters in order to efficiently remove the unacceptable noise and improve the clarity of the ridge and valley structures in the fingerprint image. Currently, several types of contextual filters have been introduced in the literature, which will be described in more detail in the next section of this chapter.

3.2 Related research

One of the most important fingerprint image enhancement algorithms is built based on a contextual filter where local orientation and ridge frequencies are used to adjust the filter so that it is well matched to the local context. Instead of adopting a single filter for image enhancement, a set of filters is created specifically for individual regions [4]. Within the context of fingerprint enhancement algorithms, the local ridge orientation and local ridge frequency are often regarded as the definition of the local context. Generally, the structure of the ridges and valleys is defined by local orientation and frequency which varies within the local region. Therefore, a filter which is tuned to work on the corresponding ridge frequency and orientation can compensate for the noise and at the same time preserve the genuine structure of the ridges and valleys.

Theoretically, the idea behind common contextual filters is similar [4]. First of all, depending on the ridge orientation, a low-pass filter is applied to fill in the gaps and pores in the local ridges. And then, a band-pass filter is applied orthogonally to the ridges to clarify the structure of the ridges and valleys and separate parallel linked ridges. Several common contextual filters have been reported in the literature of fingerprint enhancement, and these are described as follows:

- Sherlock, Monro, and Millard [66] presented a technique for fingerprint image enhancement which performs contextual filtering in the Fourier domain. The fingerprint image is convolved with the pre-computed filters. To reduce the total number of filters and to improve the algorithm's efficiency in terms of processing time, this algorithm neglects the variance of the ridge frequency across different regions of the fingerprint image and considers it as a single value, which is somewhat unrealistic in practice. Therefore, the algorithm only takes into account partial contextual information of a fingerprint image.

- Hong and Xinsheng [67] introduce a two-step approach for fingerprint image enhancement. Firstly, according to the first derivative and contrast of a fingerprint image, a fingerprint images is segmented, and then an orientation

estimation is applied to correct the local orientations, and in the end a binarisation process is applied.

- Hong, Wan, and Jain [64] introduced a Gabor filter-based fingerprint enhancement algorithm which utilizes full information of the local context, both local orientation and frequency. In addition, their algorithm identified the unrecoverable region in a fingerprint image which is beneficial in reducing the overall processing time of the fingerprint algorithm, since an unrecoverable region can be masked out in later processing and prevent the generation of spurious minutiae.

To add to this list, in our study we have developed a new fingerprint enhancement algorithm based on Gabor filtering, within which two parameters, local ridge orientation and frequency, have been specified by new methods. An experimental comparative study of a range of selected enhancement methods [68] [69] compared with our own work is described in the next section, using three different databases from the FVC2004 publicly available databases [48] [70], which contain fingerprint images of varying quality. All these databases were described in detail earlier in Chapter 2 of this thesis.

3.3 Technical approach

3.3.1 Segmentation

Segmentation is the first step of the proposed fingerprint image enhancement algorithm, which is used to select a region of interest (ROI) from a fingerprint image. A well selected region of interest (ROI) can increase both the performance and efficiency of the system. Nevertheless, if the region of interest selected is too small then a lot of features may be missed, resulting in poor performance at the fingerprint matching stage. Conversely, if a selected region of interest is too big then the feature extraction algorithm may extract a number of false features, which will reduce the accuracy of the fingerprint recognition system. The purpose of fingerprint image

segmentation is the process of separating the foreground region in the image from the background region. Generally, the foreground region is considered as the region of interest that an algorithm attempts to identify and separate from the background region because it includes the valid ridges and valleys. In contrast, the background region is the area outside of the region of interest, which contains invalid fingerprint information generated by the data acquisition stage. Therefore, with the purpose of improving the performance of the fingerprint enhancement algorithm, a fingerprint image segmentation algorithm is an essential step to remove the background region, and thus avoiding spurious features being extracted.

There are many approaches proposed in the literature for the segmentation of a fingerprint image. The pixel-wise segmentation method is one of most accurate approaches to segmenting fingerprint images, which was introduced by Bazen and Gerez [71]. Three features are computed for each pixel, including gradient coherence, intensity mean, and intensity variance, and then a supervised linear classifier is adopted to identify the foreground and background region. A final morphological approach is used to fill holes in both foreground and background and to regularize the external silhouette of the region of interest, which is proposed by Gonzales and Woods [72]. However, this method has some limitations when it is hard to separate the foreground and the background in the fingerprint image. In order to overcome the limitation of this method, Akram et al. [73] proposed a modified gradient based method, which estimates the local gradient values to detect a sharp variation in the pixel intensity of the background. However, according to test results, we find that this method cannot accurately segment the fingerprint image if the image represents an extremely dry fingerprint and the background is lighter than the foreground area, or the image is extremely wet and the background is darker than the fingerprint area. Figure 3.4 show some examples of test results, which shows the operation of the algorithm which cannot segment the fingerprint images correctly using Akram's method. With the aim of resolving these problems, we therefore proposed a new algorithm, which is related to the gray level range measure and more traditional techniques including the mean

and variance based method[4]. The steps for this algorithm are described below in greater detail.

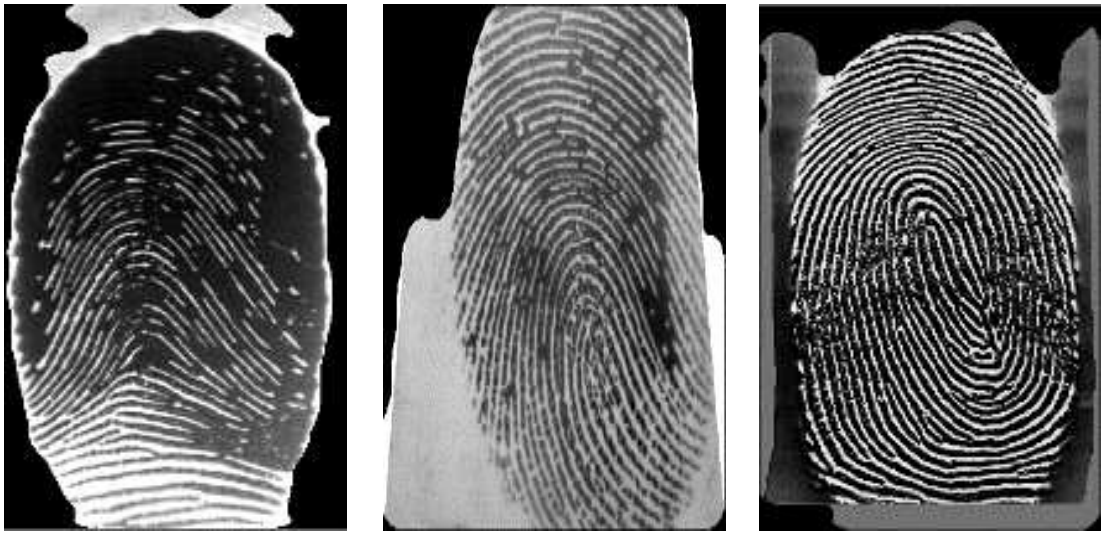


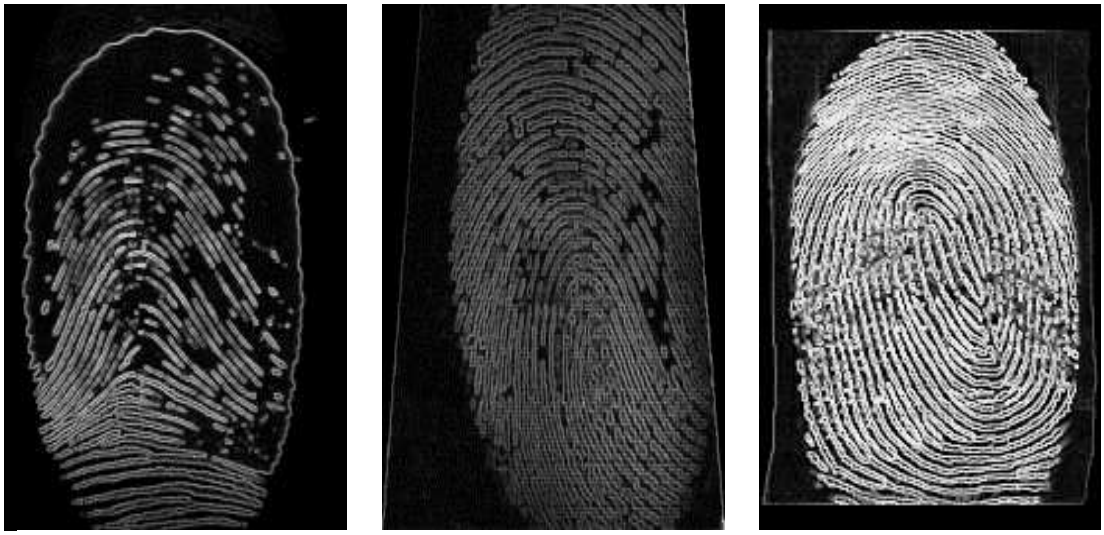
Figure 3.4: Some examples of segmented images uisng the Akram's method: (a) a segmented image from FVC 2004_DB1_A; (b) a segmented image from FVC 2004_DB2_A; (c) a segmented image from FVC 2004_DB3_A.

A: First-Stage: Obtain the filtered image $I(i,j)$ using gray level range method:

1) The gray level range method is utilized to compute the local intensity range in the local region in order to investigate the local intensity change in that region, which is calculated using equation 3.3.1.1

$$I(i,j) = \max(x) - \min(x) \qquad (3.3.1.1)$$

In the above expressions, x is the pixel intensity of the region. The region is defined by a 3 by 3 matrix, which is the finest window size for this operation. In general, a finer window size will result in a more accurately filtered image. Figure 3.5 illustrate some examples of filtered fingerprint images using the gray level range method.



(a) (b) (c)

Figure 3.5: (a) A filtered image from FVC 2004_DB1_A; (b) a filtered image from FVC 2004_DB2_A; (c) a filtered image from FVC 2004_DB3_A.

B: Second-Stage: Segment the filtered image $I(i,j)$ using the Mean and Variance method:

1) Divide the filtered image $I(i,j)$ into non-overlapping blocks with size W × W. In our case, W=8 as suggested by [74].

2) Compute the mean values M_I for the filtered image $I(i,j)$ using equation 3.3.1.2.

$$M_I = \frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}} I(i,j) \qquad (3.3.1.2)$$

3) Calculate the standard deviation value std_I using equation 3.3.1.3.

$$std_I = \sqrt{\frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}}(I(i,j) - M_I)^2} \qquad (3.3.1.3)$$

4) Generate the mask, ROI2. Compute the average value of the filtered image G as threshold, if M_I is higher than the threshold, this block is marked as foreground; otherwise it is considered as a background block.

5) Generate the mask, ROI3. Compute the average value of standard deviation from the filtered image G as threshold, if std_I is higher than the threshold, this block is marked as foreground; otherwise it is considered as a background block.

6) Generate the region of interest image (ROI). If either $ROI2$ or $ROI3$ is equal to 0, this block is marked as a background block; otherwise it belongs to a foreground block. After that, the morphological operations, dilation and erosion, are applied to eliminate holes in the both the foreground and background. Some examples of segmented image are illustrated in Figure 3.7.

(a) (b) (c)

Figure 3.6: Examples of a fingerprint image from each database in the FVC 2004. (a) DB1_A; (b) DB2_A; (c) DB3_A.

(d) (e) (f)

Figure 3.7: Examples of the segmented image using the proposed segmentation algorithm on Figure 3.6. (a) segmentation on Figure 3.6 (a); (b) segmentation on Figure 3.6 (b); (c) segmentation on Figure 3.6 (c).

3.3.2 Estimation of local ridge orientation

An estimation of fingerprint orientation fields is an essential step in the fingerprint enhancement algorithm, which represents one of the intrinsic properties of a fingerprint image, and potentially can have a critical impact on almost all subsequent processes [64]. This is defined as:

"Let [x,y] be a generic pixel in a fingerprint image. The local ridge orientation at [x,y] is the angle θ_{xy} that the fingerprint ridges, crossing through an arbitrary small neighbourhood centred at [x,y], form with the horizontal axis. Because fingerprint ridges are not directed, θ_{xy} is an un-oriented direction lying on $[0\ldots180^{\circ}]$." [4]

Different approaches have been published in the literature for computing the local ridge orientation, and these can be categorized as gradient-based approaches [75], [76],

filter-based approaches [77], and model-based approaches [78], [79], [80], [81], [82]. Filter-bank based approaches have the capability to avoid noise, but the results are not always very accurate because of the limited number of filters. Besides that, computational expense is another argument against these algorithms. Model-based approaches consider the global constraints and regularity of the orientation field except for the areas around the singular points, so these approaches have to estimate the position of singular points first. However, it is well known that accurate extraction of singular points is a challenging problem, especially for poor quality fingerprint images [83]. Comparing the two kinds of methods mentioned above, it is reported that the gradient-based approach provides much more accurate results [84].

One of the well-known gradient-based approaches is based on averaging squared gradient, which was proposed by Kass and Witkin [85]. They proposed a simple and efficient idea, which is to double the gradient angles. The average squared gradient process compensates for the noise present in the block so that a much more accurate estimation of the local ridge orientation can be conducted. Furthermore, with the aim of obtaining a better degree of robustness in the estimation of the local ridge orientation, the fingerprint orientation certainty level approach was suggested by Lim, Jiang and Yau [86], which estimates the reliability for the local ridge orientation.

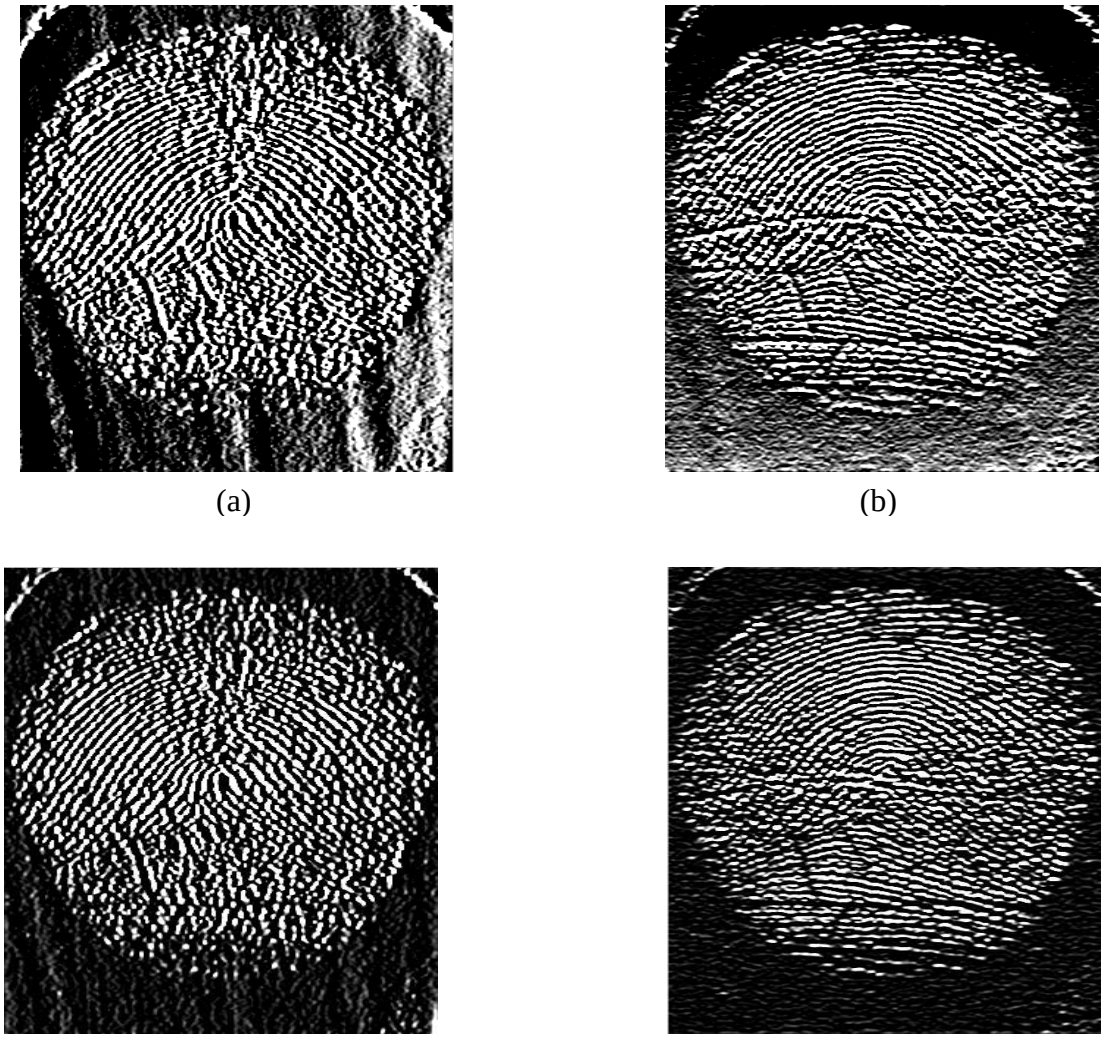
We propose a new gradient-based algorithm that is related to the averaging squared gradient method [85] and the orientation certainty level approach [86]. The detailed steps of the proposed method are described as follows, which consists of three stages:

A: First-Stage : Obtain gradient vectors.

1) Compute the $g_x(i,j)$ and $g_y(i,j)$ components of the gradient at each pixel (i, j) for original image $I(i,j)$, which are shown in Figure 3.8 (a) and (b).

2) Compute the gradients $g_{v\_v}(i,j)$ and $g_{v\_h}(i,j)$ at each pixel (i, j) for the gradient vector $g_x(i,j)$, and gradients $g_{h\_v}(i,j)$ and $g_{h\_h}(i,j)$ for gradient

image $g_y(i,j)$. The gradient images $g_{v\_v}(i,j)$ and $g_{h\_h}(i,j)$ are used at the following stages, and example results are illustrated in Figures 3.8 (c) and (d).



(a) (b)

(c) (d)

Figure 3.8: (a) The gradient image $g_x(i,j)$, (b) the gradient image $g_y(i,j)$,(c) the gradient image $g_{v\_v}(i,j)$, (d) the gradient image $g_{h\_h}(i,j)$.

B: Second-Stage : Estimate local ridge orientation for gradient images $g_{v\_v}(i,j)$ and $g_{h\_h}(i,j)$ respectively.

In this stage, the local ridge orientation is estimated based on a classic gradient-based method [4] and then noise is removed using Hong's method [64].

1) Compute the gradient images $\mathrm{Gx(i,j)}$ and $\mathrm{Gy(i,j)}$ for gradient images $g_{v\_v}(i,j)$ and $g_{h\_h}(i,j)$ respectively, using the Gaussian operator.

2) Divide gradient images $\mathrm{Gx(i,j)}$ and $\mathrm{Gy(i,j)}$ into blocks of size $\mathrm{W} \times \mathrm{W}$. In this case, W = 8 as suggested by [87].

3) Calculate the average squared gradient $[\mathrm{Vx(i,j)}, \mathrm{Vy(i,j)}]$ using equations 3.3.2.1 and 3.3.2.2:

$$\mathrm{Vx(i,j)} = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2 * \mathrm{Gx(i,j)} * \mathrm{Gy(i,j)} \qquad (3.3.2.1)$$

$$\mathrm{Vy(i,j)} = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} \mathrm{Gx(i,j)}^2 - \mathrm{Gy(i,j)}^2 \qquad (3.3.2.2)$$

4) Compute the local ridge orientation, which is perpendicular to the gradient direction, as shown in equation 3.3.2.3.

$$\theta(\mathrm{i,j}) = \frac{1}{2} * \tan^{-1}\left(\frac{\mathrm{Vy(i,j)}}{\mathrm{Vx(i,j)}}\right) + \frac{\pi}{2} \qquad (3.3.2.3)$$

5) In order to remove noise, the orientation image needs to be converted into a continuous vector field, φ_x and φ_y, as defined in equations 3.3.2.4 and 3.3.2.5, and then they are smoothed them using the Gaussian low–pass filter $W(u,v)$,as shown in equations 3.3.2.6 and 3.3.2.7.

$$\varphi_x(i,j) = \cos\big(2\theta(i,j)\big) \quad (3.3.2.4)$$

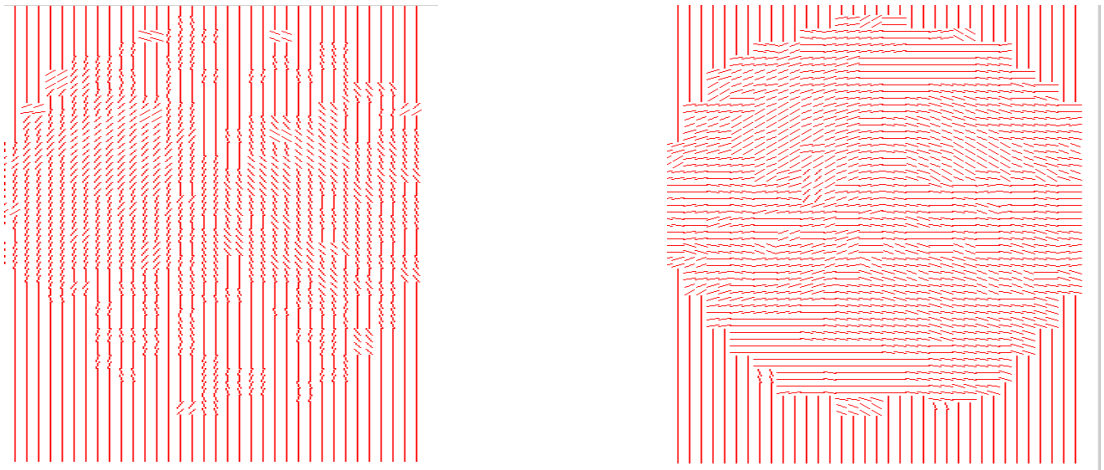
$$\varphi_y(i,j) = \sin\big(2\theta(i,j)\big) \quad (3.3.2.5)$$

$$\varphi_x'(i,j) = \sum_{u=-W_{\varphi}/2}^{W_{\varphi}/2} \sum_{v=-W_{\varphi}/2}^{W_{\varphi}/2} W(u,v)\,\varphi_x(i-uw, j-vw) \quad (3.3.2.6)$$

$$\varphi_y'(i,j) = \sum_{u=-W_{\varphi}/2}^{W_{\varphi}/2} \sum_{v=-W_{\varphi}/2}^{W_{\varphi}/2} W(u,v)\,\varphi_y(i-uw, j-vw) \quad (3.3.2.7)$$

6) Compute the original local ridge orientation at $\theta(i,j)$ using equation 3.3.2.8. Example results of the orientation for gradient images $g_{v\_v}(i,j)$ and $g_{h\_h}(i,j)$ are illustrated respectively in Figures 3.9 (a) and (b).

$$\theta(i,j) = \frac{1}{2} * \tan^{-1}\left(\frac{\varphi_x'(i,j)}{\varphi_y'(i,j)}\right) \quad (3.3.2.8)$$



(a) (b)

Figure 3.9: (a) The local ridge orientation of gradient image $g_{v\_v}(i,j)$; (b) the local ridge orientation of gradient image $g_{h\_h}(i,j)$.

C: Third-Stage : Estimate the local ridge orientation for the segmented image $G(i,j)$ (the segmented image $G(i,j)$ is obtained from Section 3.3.1 of this chapter, and an example is shown in Figure 3.9 (a)):

1) Divide gradient images $g_x(i,j)$,$g_y(i,j)$, $g_{v\_v}(i,j)$ and $g_{h\_h}(i,j)$, which were obtained in first stage, into blocks of size W × W. In this case, W = 8, which is the same as second-stage in Section 3.3.2.

2) Compute the mean values M_x and M_y for gradient images $g_{v\_v}(i,j)$ and $g_{h\_h}(i,j)$ using equations 3.3.2.9 and 3.3.2.10 respectively.

$$M_x = \frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}} g_{v\_v}(i,j) \qquad (3.3.2.9)$$

$$M_y = \frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}} g_{h\_h}(i,j) \qquad (3.3.2.10)$$

3) Calculate the standard deviation value $std_x$and std_y using equations 3.3.2.11 and 3.3.2.12.

$$std_x = \sqrt{\frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}}(g_{v\_v}(i,j) - M_x)^2} \qquad (3.3.2.11)$$

$$std_y = \sqrt{\frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}}(g_{h\_h}(i,j) - M_y)^2} \qquad (3.3.2.12)$$

4) The covariance matrices $g_x(i,j)$ and $g_y(i,j)$ of the gradient vector for a block image of size W × W are given 3.3.2.13 and 3.3.2.14.

$$Cg_x(i,j) = \frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}}\left\{\begin{bmatrix} g_{v\_v} \\ g_{v\_h}\end{bmatrix}\begin{bmatrix} g_{v\_v} & g_{v\_h}\end{bmatrix}\right\} = \begin{bmatrix} a_{gv} & c_{gv} \\ c_{gv} & b_{gv}\end{bmatrix}$$

(3.3.2.13)

$$Cg_y(i,j) = \frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}}\left\{\begin{bmatrix} g_{h\_v} \\ g_{h\_h} \end{bmatrix}\begin{bmatrix} g_{h\_v} & g_{h\_h} \end{bmatrix}\right\} = \begin{bmatrix} a_{gh} & c_{gh} \\ c_{gh} & b_{gh} \end{bmatrix}$$

(3.3.2.14)

5) According to the above expressions, the covariance matrixes were obtained, and then eigenvalues λ are found by equations 3.3.2.15 and 3.3.2.16.

$$\begin{cases} \lambda_{g_v(\max)} = \dfrac{(a_{gv}+b_{gv})+\sqrt{(a_{gv}-b_{gv})^2+4(c_{gv})^2}}{2} \\ \lambda_{g_v(\min)} = \dfrac{(a_{gv}+b_{gv})-\sqrt{(a_{gv}-b_{gv})^2+4(c_{gv})^2}}{2} \end{cases} \quad (3.3.2.15)$$

$$\begin{cases} \lambda_{g_h(\max)} = \dfrac{(a_{gh}+b_{gh})+\sqrt{(a_{gh}-b_{gh})^2+4(c_{gh})^2}}{2} \\ \lambda_{g_h(\min)} = \dfrac{(a_{gh}+b_{gh})-\sqrt{(a_{gh}-b_{gh})^2+4(c_{gh})^2}}{2} \end{cases} \quad (3.3.2.16)$$

6) Compute the orientation certainty level in each block for the gradient images $g_x(i,j)$ and $g_y(i,j)$, respectively using equations 3.3.2.17 and 3.3.2.18.

$$ocl_{gv} = 1 - \lambda_{g_v(\min)}/\lambda_{g_v(\max)} \quad (3.3.2.17)$$

$$ocl_{gh} = 1 - \lambda_{g_h(\min)}/\lambda_{g_h(\max)} \quad (3.3.2.18)$$

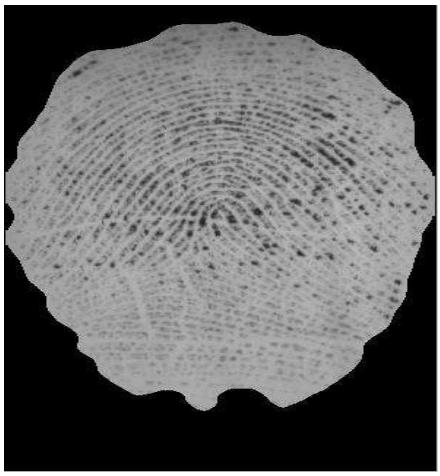
7) Convert orientation matrix values of gradient images $g_x(i,j)$ and $g_y(i,j)$ from radians to angle in degrees, θ_x and θ_y respectively.

8) Estimation of the local ridge orientation, θ_o, for the original image using the methods in the stage 2, and $g_{v\_v}(i,j)$ and $g_{h\_h}(i,j)$ are determined as the components of gradients, which are obtained from stage 1.

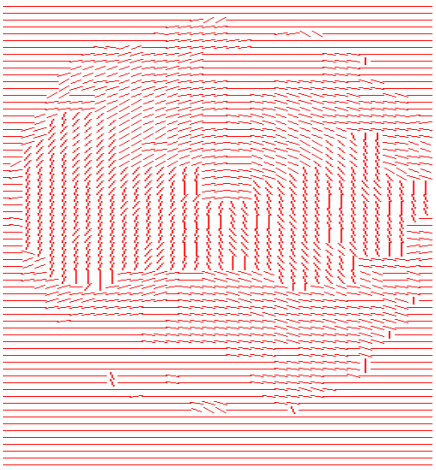
9) Estimate the local ridge orientation for the segmented image $G(i,j)$. Divide ROI image, θ_x and θ_y into blocks. And then calculate the average value $\overline{ROI}, \overline{\theta_x}$ and $\overline{\theta_y}$ for ROI, θ_x and θ_y in each block. In order to remove noise in the local ridge orientation, θ_o, it is calculated by equation 3.3.2.19 and an example result is shown in Figure 3.10 (b).

$$\overline{\theta_o} = \begin{cases} \overline{\theta_x}, & if\ \overline{ROI} \neq 0, |\theta_x - \theta_y| \leq 15\ and\ ocl_{gv} \geq ocl_{gh} \\ \overline{\theta_y}, & if\ \overline{ROI} \neq 0, |\theta_x - \theta_y| \leq 15\ and\ ocl_{gv} \leq ocl_{gh} \\ \overline{\theta_x}, if\ \overline{ROI} \neq 0, |\theta_x - \theta_y| > 15, ocl_{gv} \geq ocl_{gh}\ and\ std_x > std_y \\ \overline{\theta_y}, if\ \overline{ROI} \neq 0, |\theta_x - \theta_y| > 15, ocl_{gv} \leq ocl_{gh}\ and\ std_x < std_y \\ 0, & if\ \overline{ROI} = 0 \\ \bar{\theta}_o, & else \end{cases}$$

(3.3.2.19)



(a)



(b)

Figure 3.10: (a) The segmented image $G(i,j)$; (b) the local ridge orientation for the segmented image$G(i,j)$.

3.3.3 Estimation of local ridge frequency

Local ridge frequency is an essential parameter for the proposed fingerprint image enhancement algorithm, because it is another fundamental property of a fingerprint image. Assuming that a local region exists where no minutiae and singular points are included, a sinusoidal-shaped wave of ridges and valleys can be formed perpendicularly to the local ridge orientation of that region [64]. It is defined as:

"The local ridge frequency (or density) f_{xy} at point [x,y] is the inverse of the number of ridges per unit length along a hypothetical segment centered at [x,y] and orthogonal to the local ridge orientation θ_{xy}. A frequency image F, analogous to the orientation image D, can be defined if the frequency is estimated at discrete positions and arranged into a matrix."[4]

Although the estimation of local ridge frequency is very important for fingerprint image enhancement, in practice, it is difficult to evaluate due to the following factors:

1) for the same finger, different image resolution may result in changes in the local ridge frequency;
2) Even with the same finger, poor fingerprint image quality may distort estimations;
3) The different regions of the same fingerprint image may have different local ridge frequency;
4) The local ridge frequencies of various fingers varies;
5) High curvature (e.g. singular points) affects the accuracy of the frequency estimation algorithm [4], [88].

Many examples of local ridge frequency estimation methods have been published in recent years to address these factors. Among these are the following;

- Kovacs-Vajna, Rovattii, and Frazzoni [89] proposed fingerprint ridge distance computation methodologies, which consist of a two-step procedure. In the first step, geometric and spectral methods are both adopted to estimate local ridge distance, and then the diffusion equation is employed to complete the incomplete ridge distance map that is generated by the geometric and spectral methods.

- Yin, Tian, and Yang [88] computed the local ridge frequency based on a spectral analysis method and statistical method. First, they estimated local ridge distances using a statistical method, and then if this block image cannot be accurately estimated by the statistical method, the spectral analysis method is applied.

- Maio and Maltoni [90] employed the partial derivatives to estimate the sinusoidal signals and then adopted a two-dimensional model in order to approximate the ridge-line patterns.

We propose a local ridge frequency estimation method which is related to the algorithms described in [89], [88], [90]. However, unlike other fingerprint frequency estimation algorithms, we propose the idea to obtain the pre-processed fingerprint image before we use a classic algorithm for estimation of local ridge frequency. The detailed steps of the proposed method are described as follows, which consists of two stages.

A: First-Stage : Obtain pre-processed image

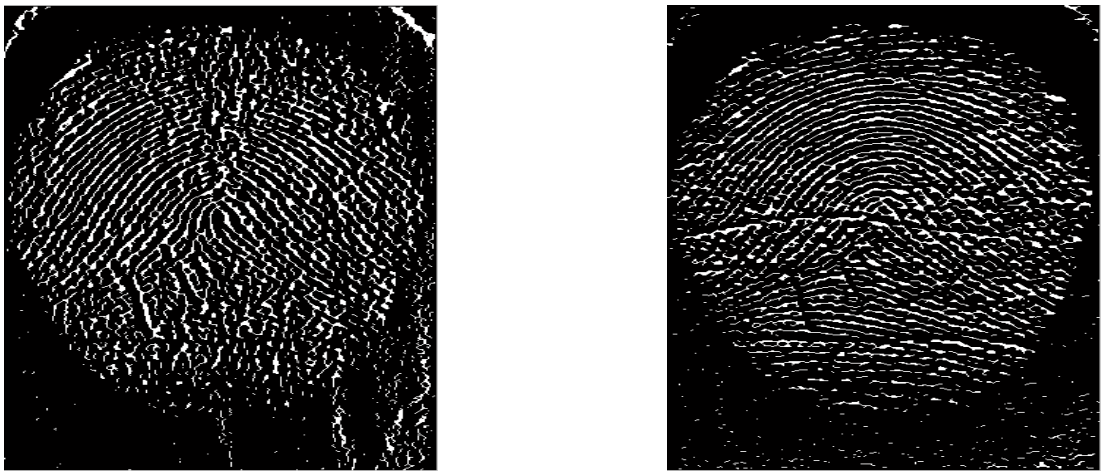
The aim of this stage is to generate a pre-processed image, which includes less noise and better clarity of ridges and valleys structures from the input fingerprint image so as to obtain much more accurate estimation of the fingerprint frequency value at the next stage.

1) Compute the gradients $g_x(i,j)$ and $g_y(i,j)$ at each pixel (i, j) for the segmented image $G(i,j)$.

2) Obtain binary images $g_v(i,j)$ and $g_h(i,j)$ using equations 3.3.3.1 and 3.3.3.2, and then apply a morphological operation to these two binary images, which thins objects to lines. Example results are shown in Figures 3.11(a) and (b).

$$g_v(i,j) = g_x(i,j) > 0 \quad (3.3.3.1)$$

$$g_h(i,j) = g_y(i,j) > 0 \quad (3.3.3.2)$$



(a) (b)

Figure 3.11: (a): The binary image $g_v(i,j)$; (b): the binary image $g_h(i,j)$.

3) Divide gradient images $g_x(i,j)$, $g_y(i,j)$ and ROI image, which was obtained from the step of segmentation, into blocks of size W × W. In this case, W = 8, which is as same as second-stage in Section 3.3.2.

4) Compute the mean values M_x and M_y for gradient images $g_x(i,j)$ and $g_y(i,j)$ using equations 3.3.3.3 and 3.3.3.4 respectively.

$$M_x = \frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}} g_x(i,j) \quad (3.3.3.3)$$

$$M_y = \frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}} g_y(i,j) \quad (3.3.3.4)$$

5) Calculate the standard deviation values std_x and std_y using equations 3.3.3.5 and 3.3.3.6.

$$std_x = \sqrt{\frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}}(g_x(i,j) - M_x)^2} \quad (3.3.3.5)$$

$$std_y = \sqrt{\frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}}(g_y(i,j) - M_y)^2} \quad (3.3.3.6)$$

6) Create two binary masks, mask1 and mask2, which are defined by equations 3.3.3.7 and 3.3.3.8.

$$mask1 = \begin{cases} 1, if\ \overline{ROI} \neq 0\ and\ std_x \geq std_y \\ 0, \quad else \end{cases} \quad (3.3.3.7)$$

$$mask2 = \begin{cases} 1, if\ \overline{ROI} \neq 0\ and\ std_y \geq std_x \\ 0, \quad else \end{cases} \quad (3.3.3.8)$$

7) Morphological operations are used to fill holes in the two binary masks separately, and then eliminate small areas in them.

8) Generate the binary image $I(i,j)$ by equation 3.3.3.9, and then inverse the binary image $I(i,j)$ to obtain binary image $I_2(i,j)$. Example results of binary images $I(i,j)$ and $I_2(i,j)$ are shown in Figures 3.12 (a) and (b).

$$I(i,j) = mask1 \times g_v + mask2 \times g_h \quad (3.3.3.9)$$

9) Generate the pre-processed image $O(i,j)$ by equation 3.3.3.10, which is illustrated in Figure 3.12 (c).

$$O(i,j) = I(i,j) \times G(i,j) + I_2(i,j) \times 255 \qquad (3.3.3.10)$$

Figure 3.12: (a) The binary image $I(i,j)$; (b) the binary image $I_2(i,j)$; (c) the pre-processed image $O(i,j)$.

B. Second-Stage: Estimate fingerprint ridges frequency.

1) Convert orientation matrix value from radians to angle in degrees, which is obtained from the orientation field estimation algorithm.

2) Divide the pre-processed image $O(i,j)$ (see Figure 3.12(c)) into blocks of size W $\times W_2$. In our case, $W = 16$ and $W_2 = 32$ as suggested by [64]. And then, these blocks are rotated by the average of angle degrees so as to bring them into vertical alignment, and generate an output image $O_2(i,j)$, which is large enough to contain the entire rotated image. Example results are shown in Figure 3.13 (a) and (b).

(a) (b)

Figure 3.13: (a) The block of the pre-processed image $O(i,j)$; (b) the block image $O_2(i,j)$, which is rotated from Figure 3.13 (a) by the average of angle degrees so as to bring it into vertical alignment.

3) A column sum of each block is computed and then vector *P* is obtained.

4) The variation of P determines the number of fingerprint ridges in sequence. Local ridge distance is defined as the distance between two consecutive peaks of valleys or ridges. In this case, the local maximum points are determined as fingerprint ridges, and local minimum points as valleys.

5) In order to find peaks and obtain their locations L, The function FINDPEAKS of MATLAB is used, which returns a vector with the local peaks of the input data. A local peak is considered that it is either larger than its two neighbouring data or equal to Inf. After that, the distance between two consecutive peaks is computed by equation 3.3.3.11. In this case, select a threshold value empirically. In order to reduce the noise and compute a reliable frequency value, if peak distance Ds is smaller than the chosen threshold, this peak is ignored. Figure 3.14 shows an example of the result.

$$\text{Ds} = \sum_{i=1}^{p-1}(L_{i+1} - L_i) \qquad (3.3.3.11)$$

In above expression, L is location of peak in the x-axis; p is the number of the peaks in the sequence.

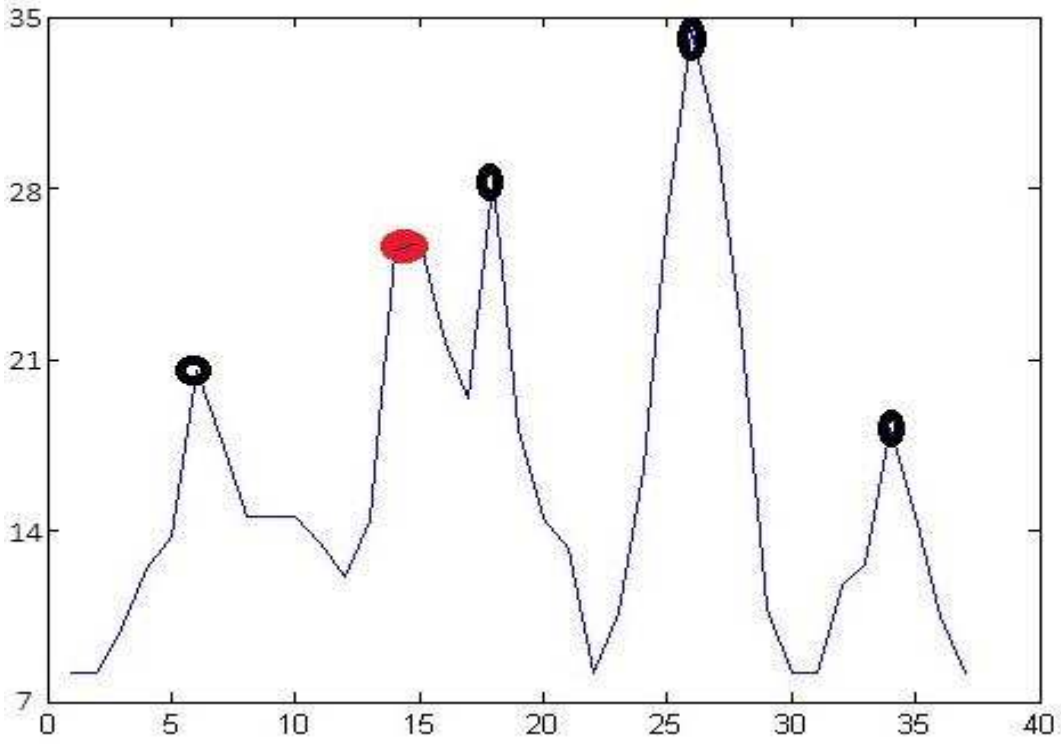


Figure 3.14: Modified waveform of ridges distance. The black circles show the maximum point of fingerprint ridges, and the red circle show the noise occurring in fingerprint image, which is ignored.

6) The local ridge frequency f is determined as the inverse of the average distance Ds using equation 3.3.3.12.

$$f = \frac{1}{\sum_{i=1}^{r} Ds_i / r} \qquad (3.3.3.12)$$

In above expression, Ds is peak distance between two consecutive peaks. r is the number of Ds in the sequence.

3.3.4 Gabor filter

The Gabor filter technique is an effective method to enhance a fingerprint image, which is proposed by Hong, Wan, and Jain [64], [4]. This technique takes account of contextual information, both the local ridge frequency and local ridge orientation, estimated from the local region to derive a suitable filter for that region. Therefore, this approach provides an efficient and effective way to remove noise and preserve the valid fingerprint information. The even-symmetric two-dimensional Gabor filter is defined mathematically as follows:

1) Create the Gabor filter using by formula presented in equations 3.3.4.1 to 3.3.4.3 [66]:

$$g(x, y: \theta, f) = \exp\left\{-\frac{1}{2\left[\frac{x_\theta{}^2}{\sigma_x^2}+\frac{y_\theta{}^2}{\sigma_y^2}\right]}\right\}\cos(2\pi f x_\theta) \tag{3.3.4.1}$$

$$x_\theta = x\cos\theta + y\sin\theta. \tag{3.3.4.2}$$

$$y_\theta = -x\sin\theta + y\cos\theta \tag{3.3.4.3}$$

In the above expressions, θ is the local ridge orientation, f is the local ridge frequency, and $\sigma_x$and $\sigma_y$are the standard deviations of the Gaussian envelope along the x- and y-axes, respectively. The modulation transfer function (MTF) of the Gabor filter can be represented as shown in equations 3.3.4.4 to 3.3.4.8.

$$H(u, v: \theta, f) = 2\pi\sigma_x\sigma_y exp\left\{-\frac{1}{2}\left[\frac{(u_\theta-u_o)^2}{\sigma_u^2}+\frac{(v_\theta-v_o)^2}{\sigma_v^2}\right]\right\} + 2\pi\sigma_x\sigma_y exp\left\{-\frac{1}{2}\left[\frac{(u_\theta+u_o)^2}{\sigma_u^2}+\frac{(v_\theta+v_o)^2}{\sigma_v^2}\right]\right\}. \tag{3.3.4.4}$$

$$u_\theta = u\,cos\theta + v\,sin\theta, \tag{3.3.4.5}$$

$$v_\theta = -u\,sin\theta + v\,cos\theta \tag{3.3.4.6}$$

$$u_o = \frac{2\pi\,cos\theta}{f}, \tag{3.3.4.7}$$

$$v_o = \frac{2\pi\,sin\theta}{f}, \tag{3.3.4.8}$$

In the above expressions, $\sigma_u = 1/2\pi\sigma_x$ and $\sigma_v = 1/2\pi\sigma_y$.

In order to utilize the Gabor filter for fingerprint image enhancement, the parameters $(\theta, f, \sigma_x, \sigma_y)$, which are used to create the Gabor filters, should be specified. The frequency characteristic of the filter, f, is completely determined by the local ridge frequency and the orientation is determined by the local ridge orientation, both of which are described in previous sections of this chapter (3.3.2 and 3.3.3). Depending on the selected values of σ_x and σ_y, the enhancement algorithm involves a trade-off between the extent of noise removal and the possible generation of spurious features. The selection of large values would remove more noise from the local region and, at the same time, results in more erroneous features being created. On the contrary, a selection of small values would generate fewer spurious features while less noise would be removed in the local region. In our case, the values of σ_x and σ_y were changed by variation of the frequency value, which is set as $\sigma = \frac{1}{f} \times 0.5$ (as suggested by [64]). To make the enhancement faster, instead of computing the best-suited contextual filter for each pixel, a set of filters are generated and stored corresponding to these distinct frequencies and orientations as follows:

1) In order to reduce the computational effort, round the array of frequencies to the nearest 0.1 and then generate and store an array of these distinct frequencies.

2) Convert orientation matrix values of θ from radians to angle in degrees O, and generate and store an array of these distinct degrees, which is computed by round $O/\text{angleIncrement}$ to nearest integers. In this case, the angle increment is set to 6^o.

3) Store the Gabor filters, which are rotated by degrees and the block sizes are determined by the frequency value. Figure 3.15 shows some examples of Gabor filters with different degrees.

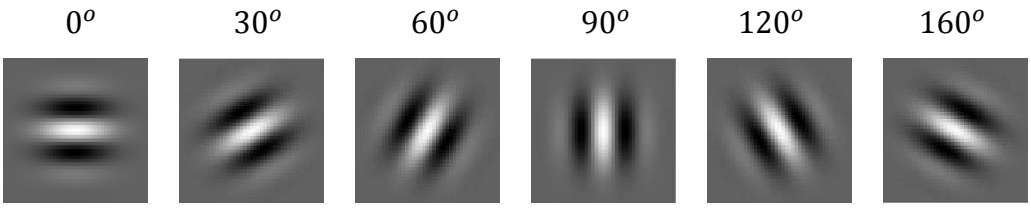
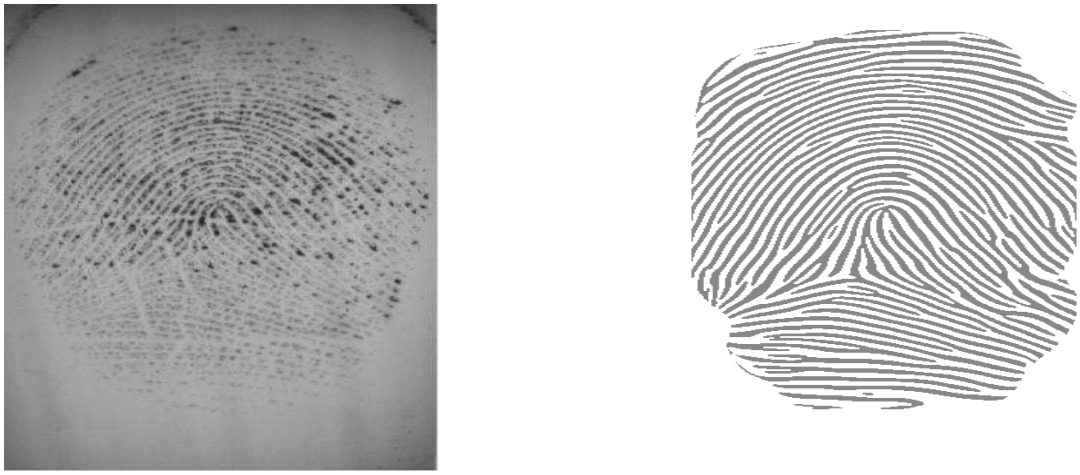


Figure 3.15: Gabor Filters of different orientation value.

4) Enhance the original image using the Gabor filters, a result which is illustrated in Figure 3.16 (b).



(a) (b)

Figure 3.16: (a) The original image; (b) the enhanced image.

3.4 Experiments

3.4.1 Database

In order to evaluate the performance of the proposed fingerprint image enhancement algorithm, three different databases from the overall FVC 2004 database are used in our experiments.

In these databases, a total of 90 people were asked to donate images of their fingerprint, and they were randomly divided into three different databases designated FVC2004 DB1_A, FVC2004 DB2_A, and FVC2004 DB3_A. And for each database, a number of 800 images were captured with an optical sensor (DB1_A and DB2_A) or a swiping thermal sensor (DB3_A). Each individual was required to donate four impressions of two fingers (index and middle finger) of both hands, and this is done in three separate sessions. The technical description of the FVC2004 database was provided in the Section 2.1 of Chapter 2. Since the fingerprints in the FVC 2004 database are collected under different conditions, the fingerprint image samples vary in quality (illustrated in Figure 3.17).

(a) (b) (c)

Figure 3.17: (a) A good quality fingerprint; (b) a medium quality fingerprint degraded by ridge breaks; (c) a poor quality fingerprint including a lot of noise.

3.4.2 Performance evaluation of fingerprint image enhancement algorithm

The purpose of this evaluation is to examine the effect of the proposed fingerprint image enhancement algorithm for use in a fingerprint recognition system. The performance indicator Equal Error Rate (EER), is suggested here. Equal error rate is widely accepted to represent the system's performance independent of threshold selection, and is the point where the corresponding the False Match Rate (FMR) and the False Non Match Rate (FNMR) have an equal value [68]. In practice, most fingerprint recognition systems intentionally decrease the FMR of the fingerprint recognition system so as to achieve a higher level of security. However, there is a trade-off between the FMR and FNMR which means that the decrease in FMR will result in the increase in the FNMR, and therefore the fingerprint recognition system may falsely reject acceptance of someone who should be accepted. In consequence, it is helpful to evaluate the FNMR of the fingerprint recognition system when it is operating at 1%, 0.1%, and 0% of FMR which are named as FMR 100, FMR 1000, and Zero FMR points, where the last is the lowest FNMR obtained when no false matching occurs [69]. In order to make a fair comparison of a fingerprint recognition system's performance on different database, the same parameter values are used for all the databases involved in this study. The protocols for all the databases are described as follows:

- **The protocol for the FVC2004 databases [48][70]**

  FNMR: there are 8 fingerprint images for each finger. Each fingerprint image of this finger is matched against the other 7 fingerprint images of the same finger. A total number of genuine matching is 5600 in each database of FVC 2004 databases. Figure 3.18 illustrates an example of FNMR matching results. Since the database contains 100 fingers in total, in Figure 3.18 they are numbered as 1 to 100 so as to distinguish them from other fingers. Figure 3.18 consist of several numbers of tables. Each child-table records the verification score for all pairs of fingerprint images collected from the same finger in the database. The header in top left corner of the table specified the numbered

finger in the database. Both raw and column header indicates the identical number of the fingerprint images included in the database for that particular numbered finger as specified in the top left corner of the table. The matching score of '1000' indicates that two fingerprint images are identical to each other which mean that the same image is used both as template fingerprint and as testing fingerprint. Moreover, a higher matching score reflects higher similarity between the template fingerprint and testing fingerprint, and vice versa. In the end, a verification score of '0' implies a non-match.

$$FNMR = \frac{Number\ of\ rejectd\ genuine\ claims}{Total\ number\ of\ genuine\ accesses} \times 100\% \qquad (4.4.2.1)$$

FMR: there are 100 fingers in each database. The first fingerprint of each finger is compared against the first fingerprint of all the remaining fingers (i.e. 99 matching is performed for each finger) in the database. A total of imposter matching is 9,900 in each database of FVC 2004 databases. Figure 3.19 illustrates an example of FMR matching results. For Figure 3.19, the raw and column header of the table indicates identification number of fingers contains in the database. A diagonal line in the table indicates the particular matching between the specified two fingers is not conducted. A matching score of '0' means a non-match, while a non-zero matching score indicates that two different fingers are falsely matched and have a matching score as specified by the cell.

$$FMR = \frac{Number\ of\ accepted\ imposter\ claims}{Total\ number\ of\ imposter\ accesses} \times 100\% \qquad (4.4.2.2)$$

EER: the equal error rate is one of the most popular performance indicator widely used by the fingerprint research community. It is calculated where the FRR and FAR are equal. If the equal error rate (EER) of the proposed algorithm is less than other's algorithm, this will demonstrate that the proposed algorithm can improve the performance of the fingerprint recognition system.

1- ()	1	2	3	4	5	6	7	8
1	1000	200	584	383	465	680	785	671
2	200	1000	210	188	225	389	477	354
3	584	210	1000	732	504	725	827	600
4	383	188	732	1000	353	584	624	389
5	465	225	504	353	1000	576	479	441
6	680	389	725	584	576	1000	906	819
7	785	477	827	624	479	906	1000	770
8	671	354	600	389	441	819	770	1000

2- ()	1	2	3	4	5	6	7	8
1	1000	0	812	201	710	819	794	152
2	0	1000	0	0	0	0	0	0
3	812	0	1000	246	795	707	653	299
4	201	0	246	1000	165	129	218	0
5	710	0	795	165	1000	638	678	183
6	819	0	707	129	638	1000	660	135
7	794	0	653	218	678	660	1000	171
8	152	0	299	0	183	135	171	1000

3- ()	1	2	3	4	5	6	7	8
1	1000	503	548	89	605	539	494	0
2	503	1000	554	107	705	584	629	0
3	548	554	1000	147	959	792	896	0
4	89	107	147	1000	182	233	204	0
5	605	705	959	182	1000	755	630	0
6	539	584	792	233	755	1000	669	0
7	494	629	896	204	630	669	1000	0
8	0	0	0	0	0	0	0	1000

4- ()	1	2	3	4	5	6	7	8
1	1000	480	654	168	500	557	426	146
2	480	1000	876	524	546	723	689	404
3	654	876	1000	540	804	783	795	365
4	168	524	540	1000	279	564	330	75
5	500	546	804	279	1000	753	995	149
6	557	723	783	564	753	1000	753	192
7	426	689	795	330	995	753	1000	159
8	146	404	365	75	149	192	159	1000

5- ()	1	2	3	4	5	6	7	8
1	1000	639	201	450	257	237	522	320
2	639	1000	140	662	348	179	422	305
3	201	140	1000	92	99	75	159	63
4	450	662	92	1000	516	78	336	237
5	257	348	99	516	1000	36	329	153
6	237	179	75	78	36	1000	312	63
7	522	422	159	336	329	312	1000	342
8	320	305	63	237	153	63	342	1000

48- ()	1	2	3	4	5	6	7	8
1	1000	380	816	302	998	656	339	344
2	380	1000	467	443	360	497	204	75
3	816	467	1000	669	821	803	215	198
4	302	443	669	1000	410	518	120	42
5	998	360	821	410	1000	719	177	389
6	656	497	803	518	719	1000	248	144
7	339	204	215	120	177	248	1000	182
8	344	75	198	42	389	144	182	1000

49- ()	1	2	3	4	5	6	7	8
1	1000	203	372	389	96	371	0	413
2	203	1000	656	609	183	704	69	420
3	372	656	1000	707	227	750	**50**	648
4	389	609	707	1000	179	578	**50**	581
5	96	183	227	179	1000	608	123	134
6	371	704	750	578	608	1000	252	602
7	0	69	**50**	**50**	123	252	1000	74
8	413	420	648	581	134	602	74	1000

50- ()	1	2	3	4	5	6	7	8
1	1000	372	528	701	735	918	305	354
2	372	1000	126	216	218	249	0	78
3	528	126	1000	596	425	558	149	165
4	701	216	596	1000	552	627	116	122
5	735	218	425	552	1000	635	177	494
6	918	249	558	627	635	1000	174	461
7	305	0	149	116	177	174	1000	180
8	354	78	165	122	494	461	180	1000

51- ()	1	2	3	4	5	6	7	8
1	1000	377	795	47	711	515	582	0
2	377	1000	299	170	353	435	305	0
3	795	299	1000	102	959	927	873	0
4	47	170	102	1000	122	144	74	0
5	711	353	959	122	1000	750	624	0
6	515	435	927	144	750	1000	485	0
7	582	305	873	74	624	485	1000	0
8	0	0	0	0	0	0	0	1000

52- ()	1	2	3	4	5	6	7	8
1	1000	443	981	416	248	729	678	**59**
2	443	1000	515	747	480	698	599	**51**
3	981	515	1000	539	384	701	857	**57**
4	416	747	539	1000	512	794	641	29
5	248	480	384	512	1000	611	516	24
6	729	698	701	794	611	1000	720	**53**
7	678	599	857	641	516	720	1000	**59**
8	**59**	**51**	**57**	29	24	**53**	**59**	1000

53- ()	1	2	3	4	5	6	7	8
1	1000	642	468	405	872	392	642	0
2	642	1000	162	335	473	182	467	0
3	468	162	1000	452	692	120	284	0
4	405	335	452	1000	728	390	443	0
5	872	473	692	728	1000	540	509	0
6	392	182	120	390	540	1000	369	0
7	642	467	284	443	509	369	1000	0
8	0	0	0	0	0	0	0	1000

54- ()	1	2	3	4	5	6	7	8
1	1000	210	81	**54**	117	102	45	363
2	210	1000	369	426	624	527	24	155
3	81	369	1000	642	477	167	0	77
4	**54**	426	642	1000	371	315	26	74
5	117	624	477	371	1000	515	0	86
6	102	527	167	315	515	1000	0	78
7	45	24	0	26	0	0	1000	62
8	363	155	77	74	86	78	62	1000

55- ()	1	2	3	4	5	6	7	8
1	1000	360	563	176	126	206	330	188
2	360	1000	888	455	441	636	588	**59**
3	563	888	1000	593	389	723	548	78
4	176	455	593	1000	405	416	459	**48**
5	126	441	389	405	1000	518	533	29
6	206	636	723	416	518	1000	582	72
7	330	588	548	459	533	582	1000	75
8	188	**59**	78	**48**	29	72	75	1000

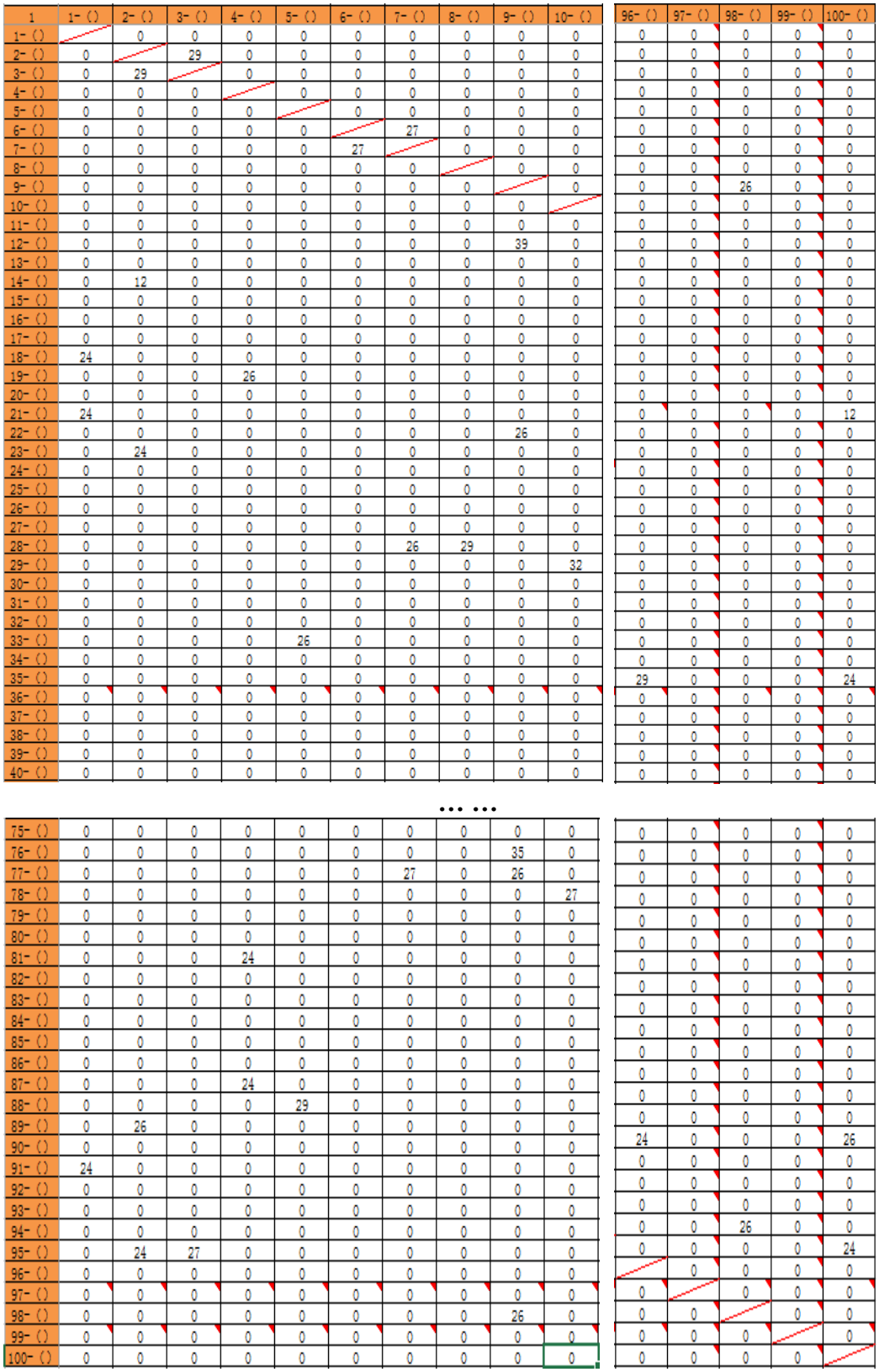
… …

98- ()	1	2	3	4	5	6	7	8
1	1000	669	1121	173	639	507	437	36
2	669	1000	669	354	653	567	626	135
3	1121	669	1000	356	818	711	557	71
4	173	354	356	1000	369	464	192	**54**
5	639	653	818	369	1000	1023	582	77
6	507	567	711	464	1023	1000	545	75
7	437	626	557	192	582	545	1000	95
8	36	135	71	**54**	77	75	95	1000

99- ()	1	2	3	4	5	6	7	8
1	1000	0	0	0	0	0	0	0
2	0	1000	0	0	0	0	0	0
3	0	0	1000	0	0	0	0	0
4	0	0	0	1000	0	0	0	0
5	0	0	0	0	1000	0	0	0
6	0	0	0	0	0	1000	0	0
7	0	0	0	0	0	0	1000	0
8	0	0	0	0	0	0	0	1000

100- ()	1	2	3	4	5	6	7	8
1	1000	0	159	29	68	98	105	126
2	0	1000	0	0	0	0	0	0
3	159	0	1000	69	158	210	144	375
4	29	0	69	1000	44	47	45	63
5	68	0	158	44	1000	183	132	164
6	98	0	210	47	183	1000	125	146
7	105	0	144	45	132	125	1000	257
8	126	0	375	63	164	146	257	1000

Figure 3.18: An example of matching results of FNMR using FVC 2004_DB2_A.



1	1- ()	2- ()	3- ()	4- ()	5- ()	6- ()	7- ()	8- ()	9- ()	10- ()	96- ()	97- ()	98- ()	99- ()	100- ()
1- ()		0	0	0	0	0	0	0	0	0	0	0	0	0	0
2- ()	0		29	0	0	0	0	0	0	0	0	0	0	0	0
3- ()	0	29		0	0	0	0	0	0	0	0	0	0	0	0
4- ()	0	0	0		0	0	0	0	0	0	0	0	0	0	0
5- ()	0	0	0	0		0	0	0	0	0	0	0	0	0	0
6- ()	0	0	0	0	0		27	0	0	0	0	0	0	0	0
7- ()	0	0	0	0	0	27		0	0	0	0	0	0	0	0
8- ()	0	0	0	0	0	0	0		0	0	0	0	0	0	0
9- ()	0	0	0	0	0	0	0	0		0	0	0	26	0	0
10- ()	0	0	0	0	0	0	0	0	0		0	0	0	0	0
11- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12- ()	0	0	0	0	0	0	0	0	39	0	0	0	0	0	0
13- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14- ()	0	12	0	0	0	0	0	0	0	0	0	0	0	0	0
15- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18- ()	24	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19- ()	0	0	0	26	0	0	0	0	0	0	0	0	0	0	0
20- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21- ()	24	0	0	0	0	0	0	0	0	0	0	0	0	0	12
22- ()	0	0	0	0	0	0	0	0	26	0	0	0	0	0	0
23- ()	0	24	0	0	0	0	0	0	0	0	0	0	0	0	0
24- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28- ()	0	0	0	0	0	0	26	29	0	0	0	0	0	0	0
29- ()	0	0	0	0	0	0	0	0	0	32	0	0	0	0	0
30- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33- ()	0	0	0	0	26	0	0	0	0	0	0	0	0	0	0
34- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35- ()	0	0	0	0	0	0	0	0	0	0	29	0	0	0	24
36- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
37- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
... ...															
75- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
76- ()	0	0	0	0	0	0	0	0	35	0	0	0	0	0	0
77- ()	0	0	0	0	0	0	27	0	26	0	0	0	0	0	0
78- ()	0	0	0	0	0	0	0	0	0	27	0	0	0	0	0
79- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
80- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
81- ()	0	0	0	24	0	0	0	0	0	0	0	0	0	0	0
82- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
83- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
84- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
85- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
86- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
87- ()	0	0	0	24	0	0	0	0	0	0	0	0	0	0	0
88- ()	0	0	0	0	29	0	0	0	0	0	0	0	0	0	0
89- ()	0	26	0	0	0	0	0	0	0	0	24	0	0	0	26
90- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
91- ()	24	0	0	0	0	0	0	0	0	0	0	0	0	0	0
92- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
93- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
94- ()	0	0	0	0	0	0	0	0	0	0	0	0	26	0	0
95- ()	0	24	27	0	0	0	0	0	0	0	0	0	0	0	24
96- ()	0	0	0	0	0	0	0	0	0	0		0	0	0	0
97- ()	0	0	0	0	0	0	0	0	0	0	0		0	0	0
98- ()	0	0	0	0	0	0	0	0	26	0	0	0		0	0
99- ()	0	0	0	0	0	0	0	0	0	0	0	0	0		0
100- ()	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

Figure 3.19: An example of matching results of FMR using FVC 2004_DB2_A.

3.4.3 Experimental results and analysis

- **Experiment procedure**

In this experiment, we have carried out an evaluation of the proposed fingerprint image enhancement algorithm on samples taken from the FVC2004 DB1_A database, FVC2004 DB2_A database, and FVC2004 DB2_A database [48]. This procedure includes two sessions. In the first session, each original fingerprint image in the database is matched against the other original fingerprint images in the database by two kinds of software, which are the NIST Biometric Image Software (NBIS) [120] and Neurotechnology fingerprint recognition algorithm demo software (VeriFinger6.5) [54]. In the second session, the proposed fingerprint image enhancement algorithm is first applied to each fingerprint image in the database, and then a verification procedure is conducted using the enhanced fingerprint images. Besides that, comparison studies with other relative fingerprint improvement methods [68], [69] will also be introduced. The detailed steps of the used software are explained as follows:

1. NIST Biometric Image Software (NBIS)

1) The fingerprint images of the FVC 2004 database are converted to RAW formatted image by the conversion program XnConvert [121].
2) The obtained RAW formatted images are converted to WSQ formatted image by the image compression program CWSQ, which is one of utilities in the NBIS.
3) The MINDTCT program extracts the minutiae in the WSQ formatted images in order to record the XY coordinates of ridge ending and bifurcations of the input fingerprint image.
4) The BOZORTH3 program is a fingerprint matching algorithm, which calculates matching score by using the minutiae files from the MINDTCT program.

2. Neurotechnology fingerprint recognition algorithm demo software (VeriFinger6.5): this algorithm uses minutiae-based matching to extracts minutiae from the fingerprints, which is the most popular matching technique in current use, and also a filtration algorithm is built in to remove noise so as to ensure a reliable feature can be extracted from even poor quality fingerprint images. The advantages of this software is that it provides reliable results, has a fast matching speed, and includes great quality determination and feature generalization algorithms, which is to ensure that only the best quality fingerprint image will be stored into database when the fingerprint is enrolled [122]. The detailed steps of the fingerprint verification process for VeriFinger 6.5 demo software are described as follows:

1) Select Verify from the menu of operation modes (See Figure 3.20).
2) Select Open file... to open two fingerprint images to verify. If this operation is successful, the match score will be shown in the bottom-left window (See Figure 3.20). Algorithm parameter can be changed by choosing Tools->Options.

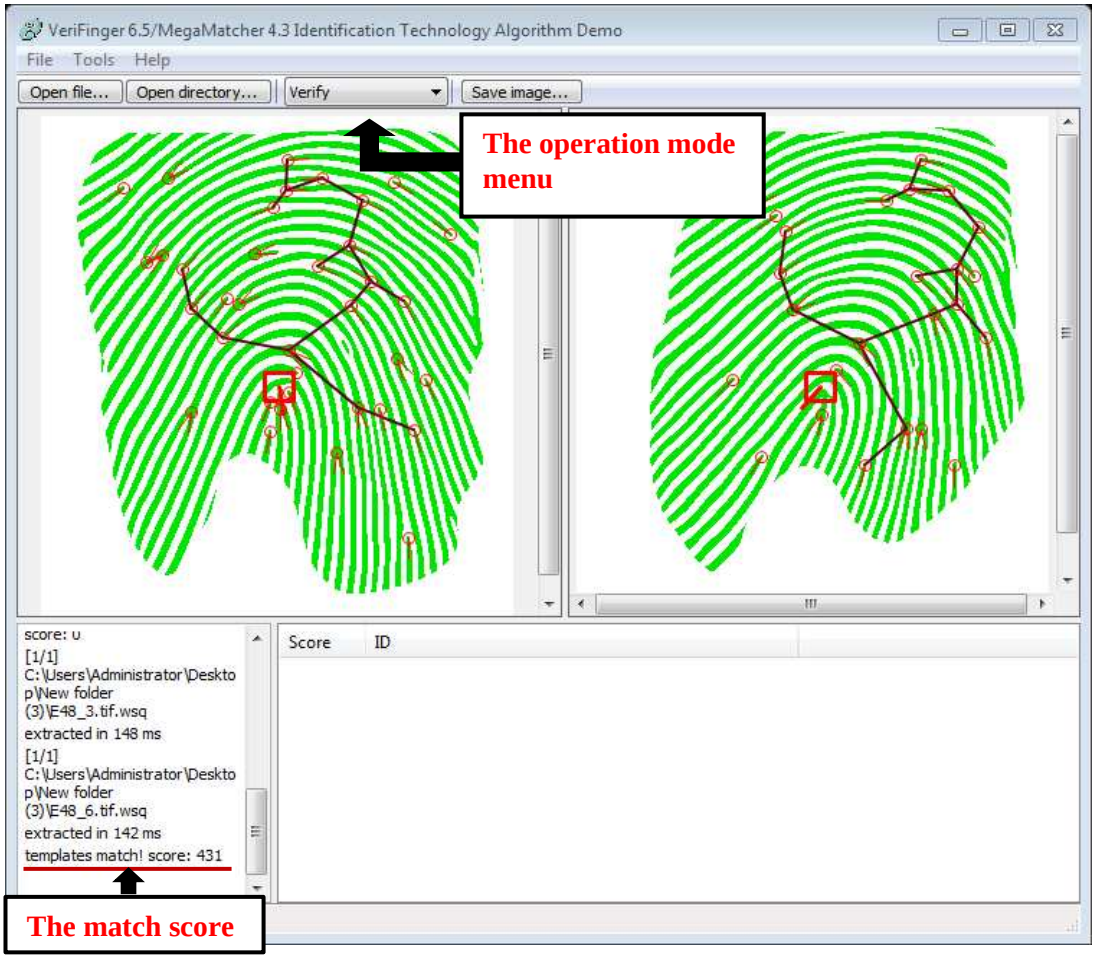


Figure 3.20: Illustration of the VeriFinger 6.5 Algorithm Demo Software to verify the fingerprint images.

Before presenting the experimental results obtained, in order to aid clarity, all of the above processing steps for comparison with evaluation of this fingerprint image enhancement algorithm are illustrated in Figure 3.21

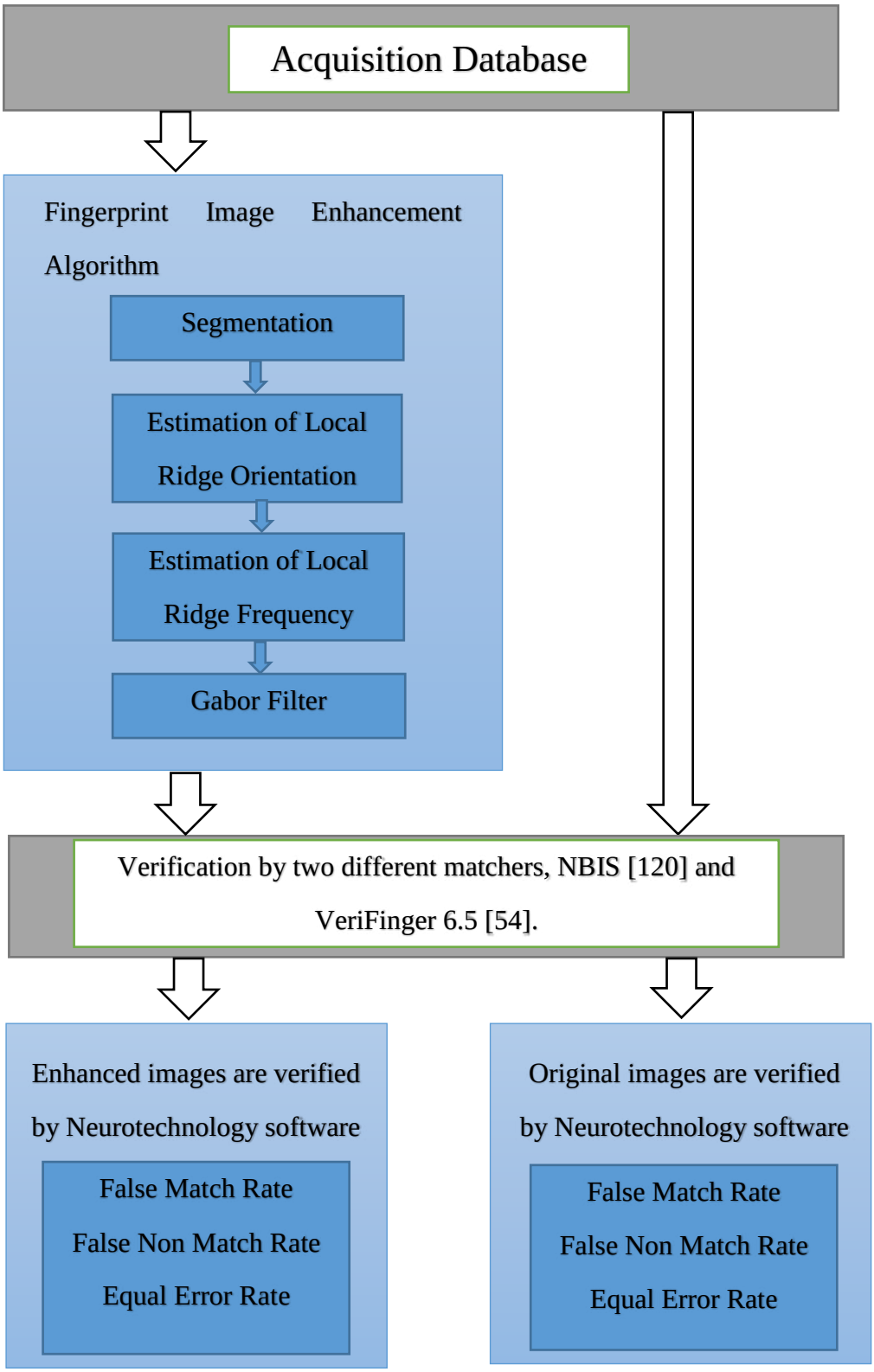


Figure 3.21: Processing steps for the evaluation of Fingerprint image enhancement algorithm.

- **Experimental Results**

	NBIS	NBIS + Bartunek [68]	NBIS + Fronthaler [69]	NBIS + Proposed
FVC2004 DB1_A				
EER	13.7%	9.6%	12%	8.09%
FMR 100	26.8%	18.9%		14.5%
FMR 1000	35.3%	26.4%		20.25%
Zero FMR	48.7%	30.9%		29.04%
FVC2004 DB2_A				
EER	10.8%	5.9%	8.2%	4.91%
FMR 100	19.9%	10.5%		8.11%
FMR 1000	26.6%	17.5%		13.98%
Zero FMR	31.0 %	22.9%		20.27%
FVC2004 DB3_A				
EER	6.6%	6.2%	5%	3.67%
FMR 100	15.1%	12.8%		6.18%
FMR 1000	29.7%	19.6%		11.93%
Zero FMR	39.8%	24.5%		15.23%

Table 3.1: Comparison of experimental results using FVC2004 databases based on NBIS matcher.

In Table 3.1, we have tabulated the comparative results using NBIS matcher [120] on the original and enhanced images. In this Table, all fingerprint images of the FVC 2004 databases were enhanced with three different enhancement methods: our new proposed method, Bartunek's method [68], and Fronthaler's method [69]. As shown in the Table, we can observe that the enhanced images using our proposed method achieves lower error rates (including EER, FMR 100, FMR 1000 and Zero FMR) than other methods. Studying Table 3.1 reveals that the enhanced images using our proposed method lead to decreased error rates of the NBIS matcher across three

FVC2004 databases, for which the error rates dropped by over 45%. And compared with other methods, the results indicate that the performance of NBIS matcher with our proposed method outperforms the other methods. The experimental results from Fronthaler's method only provided EER results, and the other error rates (FMR 100, FMR 1000, and Zero FMR) were not given. It is also reflected in the experimental result that our appoach has the most significant imrpovement on DB3_A.To sum up, we can conclude that the proposed algorithm can improve the accuracy of fingerprint verification and also is suitable for different databases.

	EER	**FMR 100**	**FMR 1000**	**Zero FMR**
FVC2004 DB1_A				
VeriFinger 6.5	3.91%	7.11%	12.43%	17.96%
VeriFinger 6.5 + Proposed	2.23%	3.14%	6.96%	12.05%
FVC2004 DB2_A				
VeriFinger 6.5	3.62%	6.04%	8.75%	13.79%
VeriFinger 6.5 + Proposed	2.75%	3.96%	5.43%	6.57%
FVC2004 DB3_A				
VeriFinger 6.5	4.21%	7.43%	12.64%	14.32%
VeriFinger 6.5 + Proposed	1.86%	2.66%	4.93%	6.82%

Table 3.2: Comparison of experimental results using FVC2004 databases based on VeriFinger 6.5 matcher

In Table 3.2, we have tabulated the comparative results using the commercial matchers, VeriFinger 6.5, on the original and enhanced images. In this Table, all fingerprint images of the FVC 2004 databases were enhanced by the proposed method were operated on VeriFinger 6.5 matcher. Studying Table 3.2 reveals that the enhanced images using our proposed method can efficiently decrease error rates of the VeriFinger 6.5 matcher, for which the error rates (EER, FMR 100, FMR 1000 and Zero FMR) dropped by over 40%.

It should be noted that the matcher VeriFinger 6.5 has a built in enhancement step which cannot be turned off, so that the results for the original images are obtained on matching images which were also enhanced.

As are shown in Table 3.1 and Table 3.2, all the performance indicators of the proposed algorithm based on two different matchers can achieve higher accuracy than other methods. Therefore, we can conclude that the proposed algorithm can efficiently enhance the quality of fingerprint images so as to improve the performance of the fingerprint-based recognition system.

Although comparison of error rates is one of the most essential aspects for evaluating the performance of the proposed fingerprint image enhancement algorithm in fingerprint recognition systems, another important aspect which needs to be considered is the execution time for the proposed image enhancement algorithm, because more complex algorithms may achieve higher accuracy at the cost of more computation time from the system, which obviously reduces the usability of a fingerprint recognition system. Therefore, this is worth further investigation to evaluate this area in the future. However, informal testing suggests that the proposed algorithm would have a similar execution time to the Bartunek's and Fronthaler's algorithm.

3.5 Chapter conclusions

In this chapter, a new fingerprint image enhancement algorithm has been presented which efficiently removes noise and improves the clarity of ridge and valley structures of the input fingerprint image.

Initially, all relevant information and background about the fingerprint image enhancement in general is presented, and we also point out why the use of a fingerprint image enhancement algorithm is very important for the overall fingerprint recognition system. After that, some related reported work about a range of fingerprint image enhancement algorithms has been discussed.

Subsequently, the proposed new fingerprint enhancement algorithm has been described, which includes four steps: fingerprint image segmentation, local ridge orientation, local ridge frequency and Gabor filter. For each step, all relevant background and related research have been introduced. And also the functioning of the algorithm corresponding to each step has been explained in detail. Especially, two essential parameters, local ridge orientation and frequency have been estimated by new and novel methods.

Finally, the FVC 2004 databases were used in our experiments in order to examine and evaluate the proposed fingerprint enhancement algorithm including FVC2004 DB1_A, FVC2004 DB2_A, and FVC2004 DB3_A [48], where all the databases contain fingerprint images of varying quality. A comparative study evaluating the range of selected enhancement methods [68], [69], and the new algorithm proposed in our work has also been presented. According to the experimental results obtained, the proposed algorithm is found to effectively and efficiently improve the verification accuracy obtained for the fingerprint databases tested, and is therefore shown to be suitable for different databases.

The next Chapter will present a new fingerprint image quality evaluation method, which can analyse a fingerprint image in relation to five different aspects, specifically

valid area, dry finger, wet finger, worn ridge and position deflection to determine the particular factors which generated the poor quality image. This proposed method will be tested using publicly available databases, and comparative studies with other relative algorithms will also be introduced in the next chapter.

Chapter 4

Fingerprint image quality assessment

This chapter will present a new fingerprint image quality evaluation algorithm for improving the fingerprint system performance. The input fingerprint image will be analysed from five aspects including the detection of valid area (defined as foreground of fingerprint image), dry finger, wet finger, worn ridge and position deflection to determine the particular factors, which generated the poor quality image. Section 5.1 will introduce some background about the effect of fingerprint image quality in an automatic fingerprint recognition system in general. Section 5.2 will survey existing reported research about fingerprint image quality evaluation algorithms. Section 5.3 will describe in detail a proposed new algorithm, which includes four separate sub-components: the detection of valid area, dry or wet finger, worn ridge and position deflection. Finally, section 5.4 is the brief conclusion of this chapter.

4.1 Introduction

One of the challenging issues in fingerprint-based identity authentication is that performance relies heavily on the quality of the enrolled fingerprint images, because without a careful consideration of data quality, biometric system designers and evaluators will struggle to make significant improvement. Good quality images have easily distinguishable patterns and features, and vice versa, poor quality images result in spurious or missing features, and so fingerprint image quality evaluation is important for a fingerprint recognition system [2], [91]. In this chapter, we will introduce a new algorithm for fingerprint image quality evaluation in fingerprint biometric, which look into issues around the effect of fingerprint image quality, which generated the poor quality data.

According to a biometric sample quality draft standard from ISO/IEC [92] [93] [94], biometric sample quality can be evaluated from three different aspects. Specifically, the standard states:

1) Character, which related with the quality attributable to inherent features of the subject.
2) Fidelity, which is the degree of similarity between a captured biometric sample and its source.
3) Utility, which indicates the performance of a sample in the biometric system and its influence over the performance of the biometric system with respect to sample quality.

It is generally accepted that the utility is most importantly mirrored by a quality metric, so that images assigned higher quality will necessarily lead to better identification of individuals. Thus, it is clear that quality of fingerprint should be predictive of recognition performance [1] [2].

The characteristics of an ideally scanned fingerprint image should satisfy three broad criteria: it should contain the core and delta points, have clear and distinct ridges and

valleys, and cover as much of the sensor area as possible for the valid area of fingerprint image [2], [95]. However, in practice, a fingerprint image is often far from this ideal because of skin condition or imperfect acquisition. Table 4.1 lists a number of factors affecting the quality of fingerprint images [61].

Category		**Factor**
Population demographic		Age, Ethic origin, Gender, Occupation.
Application		Time elapsed between enrolment and verification (time ageing), User familiarity, User motivation.
User	Physiology	Amputation, Fingernail (finger positioning), Fingerprint condition (cracked or damp, dry).
	Behaviour	Swimming (shrivelling of fingers), Sweatiness, Stress, Pose, Positioning (offset, rotation).
	Appearance	Ring, False nail.
	Interface	Feedback users receive.
Environmental influence		Light level, Weather (temperature, humidity), Dirt.
Sensor & hardware		Smears, Residual print, Camera quality, Sensor type.

Table 4.1: Factors affecting fingerprint image quality (Taken from [61]).

Unfortunately, many of these factors cannot be controlled or avoided. For example: compared with males, female subjects tend to have worse fingerprint image quality, because females present higher ridge density (defined as the number of ridges within a unit of space) [96] [97]. It is generally accepted that there are eight types of fingerprint image defect which commonly occur when a fingerprint image is collected [95]. An analysis of the available studies shows that there are the following:

- Type 1: The fingerprint image is dark as a result of applying excessive pressure or wet finger on the sensor (Figure 4.1 a).

- Type 2: The fingerprint image is light as a result of applying insignificant pressure or dry finger on the sensor (Figure 4.1 b).
- Type 3: Valid area of fingerprint image is too small because finger placement is out of alignment (Figure 4.1 c).
- Type 4: The fingerprint image is blurred because of finger movement during image capture (Figure 4.1 d).
- Type 5: Degraded or worn ridge is detected from the fingerprint image because of finger with wrinkle, scars, dirty or poor skin condition applied on the sensor (Figure 4.1 e).
- Type 6: No area of interest from fingerprint image is found as a result of applying incorrect area of finger on the sensor (Figure 4.1 f).
- Type 7: An acceptable fingerprint image is captured, but verification fails.
- Type 8: No fingerprint image is captured, because the finger was hastily moved away from the sensor.

Figure 4.1: Examples of defective fingerprint images (a) type 1; (b) type 2; (c) type 3; (d) type 4; (e) type 5; (f) type 6.

Obviously, type 7, 8 of fingerprint image defect cannot be evaluated using the proposed fingerprint image quality evaluation algorithm, for the following reasons:

- Type 7 fingerprint image defect occurs when a user successfully enrols the fingerprint, but the system fails to verify due to a systematic defect.

- Type 8 image defect occurs when no fingerprint image is captured. Without a fingerprint image, the proposed algorithm obviously cannot be applied.

In this work, the aim of our proposed fingerprint assessment algorithm is to analyse the existing detailed regulations, discussing the influence on fingerprint image quality from valid area, dryness, wetness, damaged ridge, and position deflection which means type 1, 2, 3, 4, 5, 6 of fingerprint image defect can be measured.

4.2 Related research

Many papers in the literature have introduced different methods to evaluate the fingerprint image quality. In general, the existing fingerprint quality evaluation methods can be divided into two categories: 1) methods based on local features; 2) methods based on global features [93], [4]. Table 4.2 lists a summary of existing local and global fingerprint quality approaches.

Methods Based on Local Features of Image	
Classification	**Approaches**
Local directional strength	Orientation certainty level [86], [97], [98]
	Gabor features [99]
	Evaluation of directional area and non-directional area [100]
	Spatial Coherence [101]
Ridge valley clarity	Ridge frequency, ridge thickness, ridge to valley thickness [86], [102], [103]
	Contrast, curvature and flow map [64]
	Pixel intensity, local clarity [102], [103]
Orientation consistency	Continuity of the direction field [102]
	Overlapping regions of the distributions [97]
Methods Based on Global Features of Image	
Ridge flow	Sum of local ridge orientation change [86]
	Average of all the local average absolute different in orientation angles [102]
Minutiae and foreground map	Neural network [2]

Table 4.2: A summary of existing local and global fingerprint quality approaches.

4.2.1 Methods based on local features of image

For fingerprint quality evaluation methods based on local features, a fingerprint image should be divided into non-overlapped blocks, and features estimated from each block [4], [93]. A local measure of quality is generated when blocks are categorised into groups of different quality. The local measure of the quality evaluation can be a representation of the percentage of categorized "high" or "low" blocks, or a fusion of both [93]. Some previous related studies are described as follows:

- Lim et al. [86] presented two different approaches for evaluating fingerprint quality based on local features. One is to calculate orientation certainty level, which is to define the orientation strength (described as "how strong the energy along the ridge-valley orientation" [86], [97]) of a certain block. The ratio of the eigen-values of the gradient vector is used to estimate the local ridge orientation certainty. Another approach is to compare the ridges and valleys, which is an essential analysis for an inaccuracy check for preventing strong orientation strength received from the fingerprint image of the previous user. For optical sensors, they only scan the surface of finger's skin and do not detect the deep skin layer. Thus, some marks or traces from the previous user may be left on the sensor, resulting in subsequent fingerprints possibly become very noisy. There are several methods for this analysis, including ridge frequency value, ridge-to-valley thickness ratio and ridge thickness.

- Shen et al. [99] proposed the use of the Gabor filter to estimate the fingerprint image quality. The Gabor filter also depends on the ridge orientation strength to evaluate the fingerprint image quality, and it is based on a local analysis. It should be noted that ridge frequency value and orientation must be calculated before using the Gabor filter, because they are the important characteristics of the Gabor filter. After acquiring the Gabor feature, its standard can be calculated to segment the fingerprint image into two areas: foreground and background of the image. Furthermore, the quality region value is calculated from the foreground of the image, which is classified into two groups: 'good'

and ‘poor’. If the quality region value is larger than the threshold, this block is considered as a ‘good’ block; otherwise it is categorised as a ‘poor’ quality block. Finally, the ratio of the number of good blocks to the summation of all foreground blocks is used to define the quality of a fingerprint image.

- Chen et al. [102] introduced an approach to classify the ridge area and valley area, and then calculating the area failing to verify ridge or valley as an overlapping region. Finally, the overlapped area is calculated which demonstrates the clarity between the ridge and valley, because in general, the good quality fingerprint should have a well-defined ridge and valley with a very small overlapped area between them.

4.2.2 Methods based on global features of image

Global quality estimation methods analyse the image in a universal mode and compute a single quality value for the whole image [93], [4]. Some past efforts in the investigation of fingerprint image quality are illustrated as follows:

- Lim et al. [86] presented a global quality evaluation method based on the general characteristics of a fingerprint image. Continuity is one fingerprint attribute, which can be observed by the orientation change along each horizontal row and each vertical column of the image block. If there are smooth changes, it means there is the valid fingerprint; otherwise, there is a noisy fingerprint image. Another property of a fingerprint image is uniformity, which is demonstrated by clear ridges and valleys. The ratio for ridge thickness to valley thickness for each image block is calculated, and the standard deviation indicates the quality of fingerprint.

- Chen et al. [102] introduced a method to analyse the global orientation flow, which is another indicator to describe the quality of a fingerprint. In general, the flow of the ridge direction changes gradually with the exception of the area of a delta or core point. In this work, the average absolute difference is

calculated in orientation angles for determining the orientation flow of the fingerprint.

In the present study, a new proposed fingerprint quality evaluation method will be introduced, which analyses the quality of a fingerprint at a local level and at a global level. Also, four different quality scores will be calculated which will indicate the impact of fingerprint quality with respect to valid area, dryness, wetness, worn ridge and position deflection. Figure 4.2 shows the flowchart of the proposed method.

Figure 4.2: The flowchart of the proposed fingerprint quality evaluation method.

4.3 Technical approach and experimental results

4.3.1 Quality score 1

4.3.1.1 Methodology of valid area

The "valid area" is the one of the most importants aspect to evaluate when determining the quality of a fingerprint image, which is defined as the ratio of the foreground area of fingerprint image to the area of fingerprint sensor. In general, most automatic fingerprint identification systems are based on minutiae matching [4]. Therefore, when the valid area is too small, it will result in less minutiae on the fingerprint image and thus critically decrease the performance of the overall fingerprint identification system. The detailed steps for the method to determine the valid area are described as follows:

1) Calculate region of interest (ROI) for distinguishing the foreground area from the background area, which is described in the Section 3.3.1 of Chapter 3.

2) Calculate the valid area of the fingerprint image using equation 4.3.1.1. The range of QS_1 value is between 0 and 1. The idea is that if the QS_1 value is larger than a threshold, then the quality for valid area of this image is acceptable; otherwise, while for QS_1 value is less than threshold, then the quality for valid area of the selected image is unacceptable, which we would expect to have a significant likelihood of resulting in a false match in an automatic fingerprint identification system.

$$QS_1 = \frac{S_{Foreground}}{S_{ImageSensor}} \tag{4.3.1.1}$$

In the above expressions, the $S_{Foreground}$ is the foreground area of the input fingerprint image. The $S_{ImageSensor}$ is the fingerprint sensor area.

4.3.1.2 Classification of quality score for valid area

In order to determine the threshold of classification of two different groups, a good quality image group and a bad quality image group, we selected 25 unmatched images from the FVC2004 DB1A database [48] as the unmatched group, which are analysed by human visual inspection to show that the valid area is one aspect to cause unmatched results, and also chose another 25 matched images with a high match score from the same database as the match group. In this case, the matched scores were generated using VeriFinger 6.5 software by Neurotechnology [54]. If a fingerprint image can be matched, this software will give a result with match score; otherwise, the result of match score is marked as 0. Most of fingerprint images in this database can be matched, thus the number of 25 unmatched images is the maximum we can collect for the unmatched group. We set a threshold T to split all the match scores in this database into two classes: high match score class and low match score class, which is

also described by equation 4.3.1.2 and 4.3.1.3.

$$T = u + \frac{\sigma}{2} \tag{4.3.1.2}$$

$$\begin{cases} high\ matched\ class, & if\ quality\ score\ \geq T \\ low\ matched\ class, & otherwise \end{cases} \tag{4.3.1.3}$$

In the above expression, the u is the mean value of match scores for all fingerprint images. The σ is the standard deviation. In order to better separate these two groups, we chose 25 images from the high matched class, which is the same number as for the unmatched group.

In Figure 4.3, we can observe that a threshold T 0.24 can be used to distinguish the matched group from the non-matched group. Thus, we can define that when QS_1 is lower than this threshold, the valid area of the selected image is unacceptable.

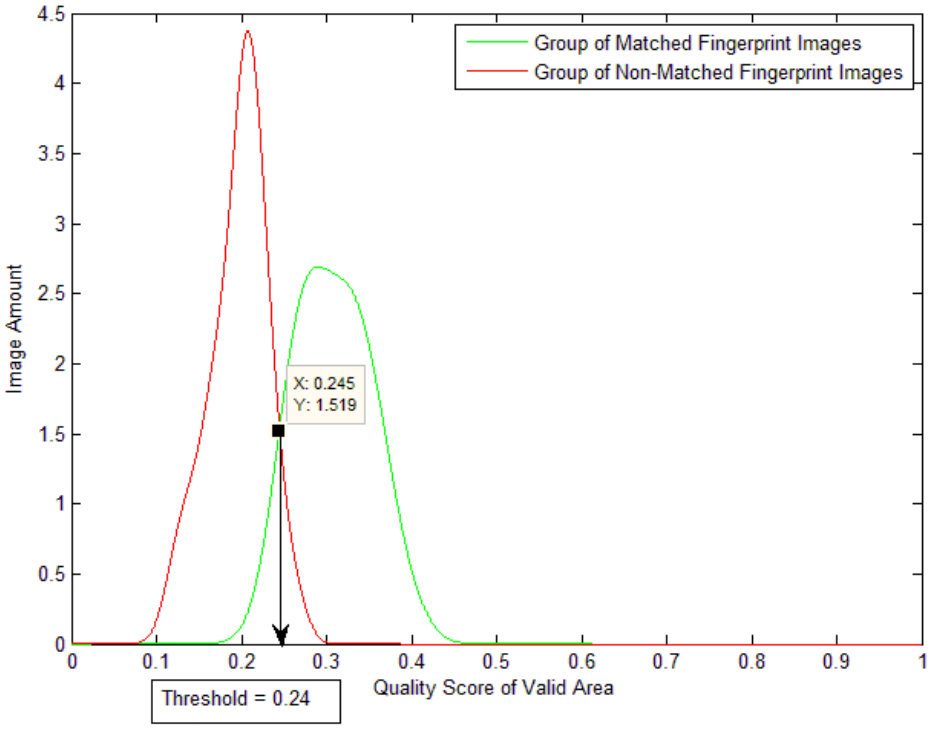


Figure 4.3: Quality Score of Valid Area distributions of Non-matched Images Group and Matched Images Group.

4.3.2 Quality score 2

4.3.2.1 Methodology of Influence of fingerprint image quality from dry or wet fingers.

Wet or dry finger is a serious factor affecting the performance of an automatic fingerprint identification system, because it will result in fingerprint impressions with blotchy or patchy appearance, respectively. Generally, a dry fingerprint creates faint ridges in the image and a wet fingerprint has thick and dark ridges. A fingerprint image probably exhibits all or part of these areas, including faint ridges, thick ridges and equally spaced ridge – valleys [103]. Figure 4.4 shows an example of a fingerprint image with a range of different regions.

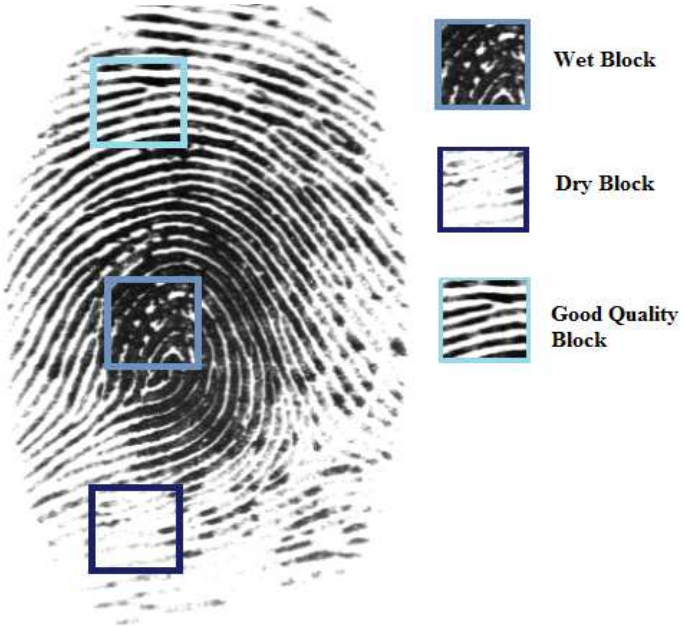


Figure 4.4: Three different types in a fingerprint image: wet, dry and good quality block

Hence, in order to estimate factors which have an impact on fingerprint quality correctly, a new proposed method will be introduced, which is developed, evolved and synthesised from other reported approaches and consists of two stages. For the first stage, the orientation certainty level is computed, which is one of most important

feature to determine whether the quality of the fingerprint image is good or bad, that is based on an algorithm proposed by Lim et al [86]. Regarding the second stage, further analysis will be carried out to distinguish a good fingerprint block from a bad block, and then the bad quality area can be divided into two groups, wet poor quality block and dry poor quality block, which is estimated by methods based on the block's mean intensity and standard deviation. After that, the proportion of wet area against dry area will indicate the fingerprint with a wet or dry condition. The detailed steps for this algorithm are described as follows:

A: First-Stage : Estimate orientation certainty level based on local features of image.

1) Compute the segmented image $G(i,j)$ using the first step of the proposed fingerprint image enhancement algorithm, which is described in the Section 3.3.1 of Chapter 3.

2) Compute the $g_x(i,j)$ and $g_y(i,j)$ components of the gradient at each pixel (i, j) for the segmented image $G(i,j)$.

3) Compute the gradients $g_{v\_v}(i,j)$ and $g_{v\_h}(i,j)$ at each pixel (i, j) for the gradient vector $g_x(i,j)$, and gradients $g_{h\_v}(i,j)$ and $g_{h\_h}(i,j)$ for gradient image $g_y(i,j)$.

4) The covariance matrices $Cg_x(i,j)$ and $Cg_y(i,j)$ of the gradient vector for a block image of size W × W are given by equations 4.3.2.1 and 4.3.2.2. In this case, W = 32 as suggested by [86], [97], [98].

$$Cg_x(i,j) = \frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}}\left\{\begin{bmatrix} g_{v\_v} \\ g_{v\_h}\end{bmatrix}\begin{bmatrix} g_{v\_v} & g_{v\_h}\end{bmatrix}\right\} = \begin{bmatrix} a_{gv} & c_{gv} \\ c_{gv} & b_{gv}\end{bmatrix} \quad (4.3.2.1)$$

$$Cg_y(i,j) = \frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}}\left\{\begin{bmatrix} g_{h\_v} \\ g_{h\_h} \end{bmatrix}\begin{bmatrix} g_{h\_v} & g_{h\_h} \end{bmatrix}\right\} = \begin{bmatrix} a_{gh} & c_{gh} \\ c_{gh} & b_{gh} \end{bmatrix}$$

(4.3.2.2)

5) According to the above expressions, the covariance matrices were obtained, and then the eigenvalues λ are found by equations 4.3.2.3 and 4.3.2.4.

$$\begin{cases} \lambda_{g_v(\max)} = \frac{(a_{gv}+b_{gv})+\sqrt{(a_{gv}-b_{gv})^2+4(c_{gv})^2}}{2} \\ \lambda_{g_v(\min)} = \frac{(a_{gv}+b_{gv})-\sqrt{(a_{gv}-b_{gv})^2+4(c_{gv})^2}}{2} \end{cases} \quad (4.3.2.3)$$

$$\begin{cases} \lambda_{g_h(\max)} = \frac{(a_{gh}+b_{gh})+\sqrt{(a_{gh}-b_{gh})^2+4(c_{gh})^2}}{2} \\ \lambda_{g_h(\min)} = \frac{(a_{gh}+b_{gh})-\sqrt{(a_{gh}-b_{gh})^2+4(c_{gh})^2}}{2} \end{cases} \quad (4.3.2.4)$$

6) Compute the orientation certainty level in each block for the gradient images $g_x(i,j)$ and $g_y(i,j)$, respectively using equations 4.3.2.5 and 4.3.2.6. After that, generate an orientation certainty level matrix ocl, using equation 4.3.2.7.

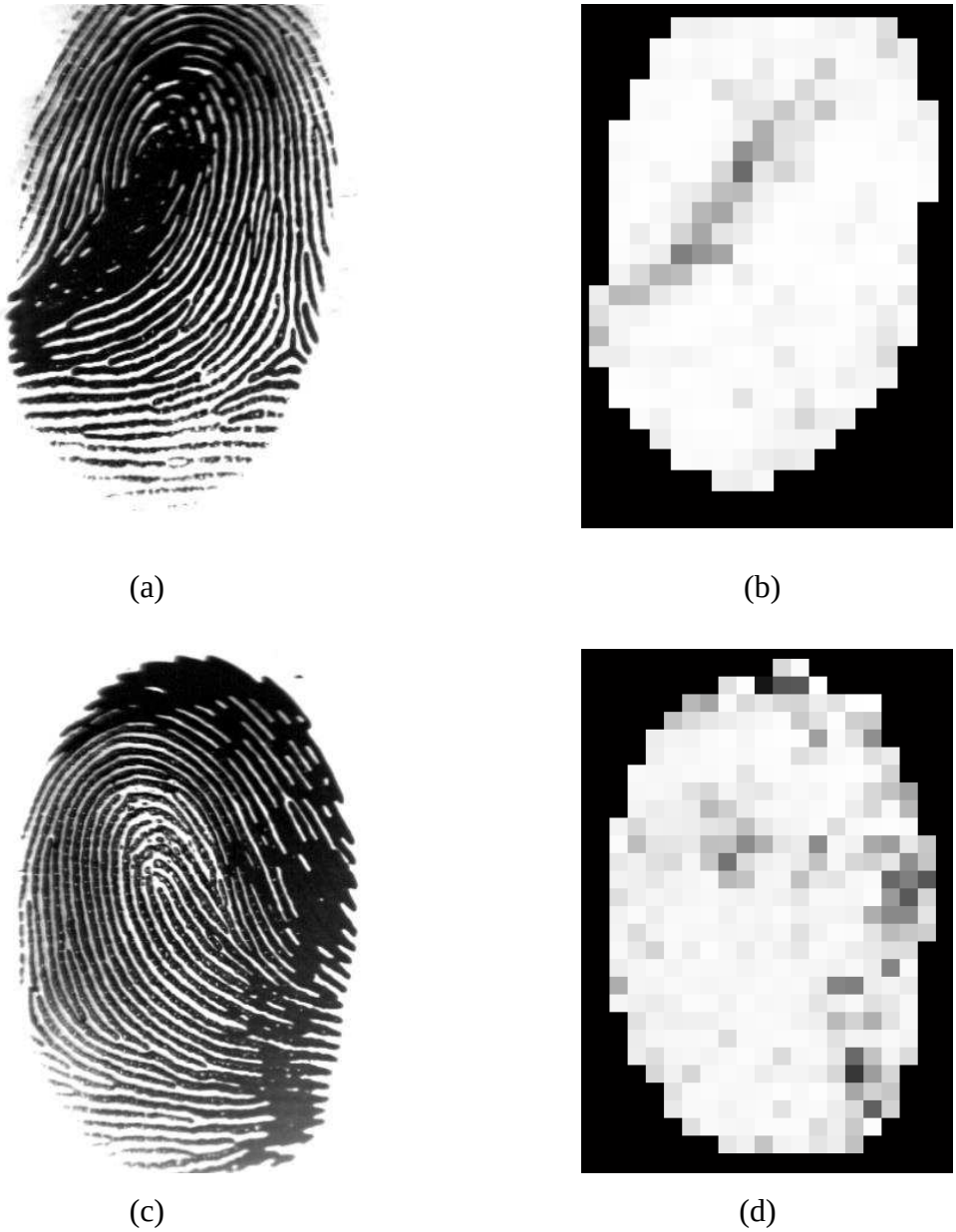
$$ocl_{gv} = 1 - \lambda_{g_v(\min)}/\lambda_{g_v(\max)} \quad (4.3.2.5)$$

$$ocl_{gh} = 1 - \lambda_{g_h(\min)}/\lambda_{g_h(\max)} \quad (4.3.2.6)$$

$$ocl = \begin{cases} ocl_{gh}, & ocl_{gv} \le ocl_{gh} \\ ocl_{gv}, & ocl_{gv} \ge ocl_{gh} \end{cases} \quad (4.3.2.7)$$

In the above expression, the ocl range is from 0 to 1, which defines the orientation strength of a certain block and therefore is a good method to determine fingerprint image quality. For a high certainty block, ridges and valleys are very clear with small changes of orientation and, as the value is

higher. On the contrary, the lower value means the ridges and valleys shows discontinuities in orientation. However, this method has some limitations. For example, if the fingerprint image quality is low with wet finger skin condition, the value of orientation certainty level (OCL) is high. Figure 4.5 shows illustrations of OCL value of fingerprint images.



(a) (b)

(c) (d)

Figure 4.5: (a) (c) A Original fingerprint image, (b) (d) the orientation certainty level values of the selected image. (Light: good quality block; Dark: bad quality block)

In Figure 4.5, we can observe that the OCL approach can correctly measure the quality for the selected fingerprint image (a), but as for the selected image (c), this method does not show an ideal result. In this case, the second stage of the algorithm will further examine the fingerprint image, and its detailed steps are described below.

B: Second-Stage : Determine the quality of the fingerprint image, and measure image defect from a wet or dry finger.

1) Divide the segmented image $G(i,j)$ into non-overlapping blocks with size W × W. In our case, W=32 and is the same as the first-stage of this Section.

2) Compute the mean values M_I for the segmented image $G(i,j)$ using equation 4.3.2.8.

$$M_I = \frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}} G(i,j) \qquad (4.3.2.8)$$

3) Calculate the average of the standard deviation value std_I using equation 4.3.2.9.

$$std_I = \sqrt{\frac{1}{W^2}\sum_{i=-W/2}^{\frac{W}{2}}\sum_{j=-W/2}^{\frac{W}{2}}(G(i,j) - M_I)^2} \qquad (4.3.2.9)$$

4) Calculate the average value $\overline{std_I}$ for std_I, and then evaluate the quality of fingerprint image using equation 4.3.2.10.

$$\begin{cases} good\ quality\ block, & if\ ocl \geq T\ and\ std_I \geq \overline{std_I} \\ bad\ quality\ block, & otherwise \end{cases} \qquad (4.3.2.10)$$

In the above expression, threshold T is the optimal level value to grade blocks into two groups. in this case, T = 0.96, which is determined by statistical results as shown in Figure 4.6.

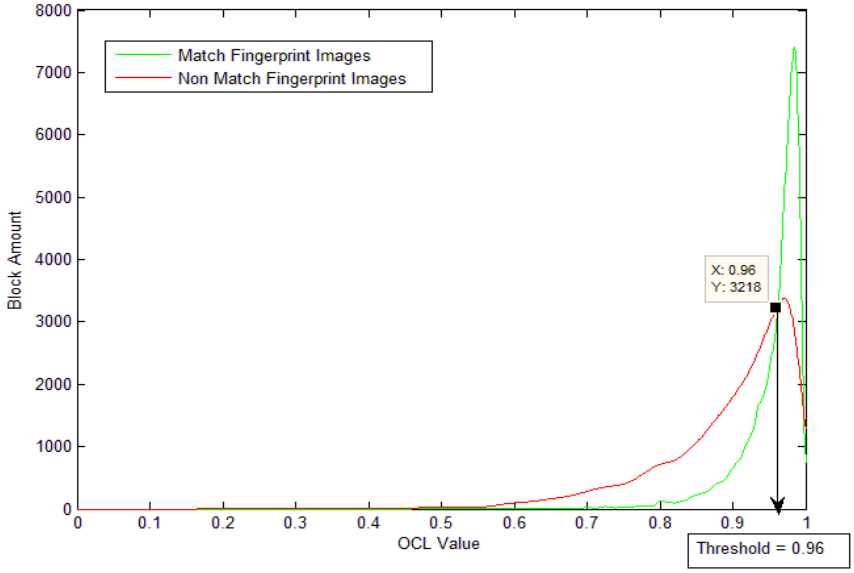


Figure 4.6: Distributions of OCL values of the match fingerprint images and non-match images.

5) Quality score is defined as the ratio of the number of good blocks to the summation of all foreground blocks of the fingerprint image, which is found by equation 4.3.2.11. If the quality score is lower than the chosen threshold, the quality of this fingerprint image would be estimated from aspects of wetness or dryness. Setting up the threshold value and experimental results demonstrating separating dry fingerprint images from wet images will be explained later in this Chapter.

$$QS_2 = {block_{(goodness)}}\Big/{block_{(foreground)}} \qquad (4.3.2.11)$$

6) Calculate the average value $\overline{M_I}$ for M_I. If M_I is greater than $\overline{M_I}$ and this block is categorised as a bad quality block, this block is considered as a wet block; otherwise, if M_I is smaller than $\overline{M_I}$ and this block is also classified as bad quality block, it is a dry block.

7) Characterize whether it is a wet or dry fingerprint according to the ratio of numbers of wet poor quality blocks to dry poor quality blocks, which is shown in equation 4.3.2.12. If the value is greater than 1, this image is a wet fingerprint; in other respects, while the value is less than 1, it is a dry fingerprint. Figure 4.7 illustrate some examples of fingerprints with wet and dry considitions.

$$Q_{wd} = {sum(block_{wet)}}/{sum(block_{dry)}} \quad (4.3.2.12)$$

(a) $Q_{wd} = 1.5462$ (b) $Q_{wd} = 0.7624$

Figure 4.7: Quality score on different type of fingerprint image; (a) wet fingerprint image; (b) dry fingerprint image.

4.3.2.2 Classification of quality score based on clarity of ridge-valley texture.

The goal of the experiment described here is to decide a threshold for separating the good quality images group from the poor quality images group, which is similar to the experiment described in section 4.3.1.2 of this chapter. We selected 25 unmatched images from FVC2004 DB1_A database [48] as the unmatched group, and these images were observed to have lower contrast of ridge-valley texture and this is one of

aspects resulting in unmatched result. Another group designated the matched group is formed by 25 matched images with a high match score. The experimental result is shown in Figure 4.8.

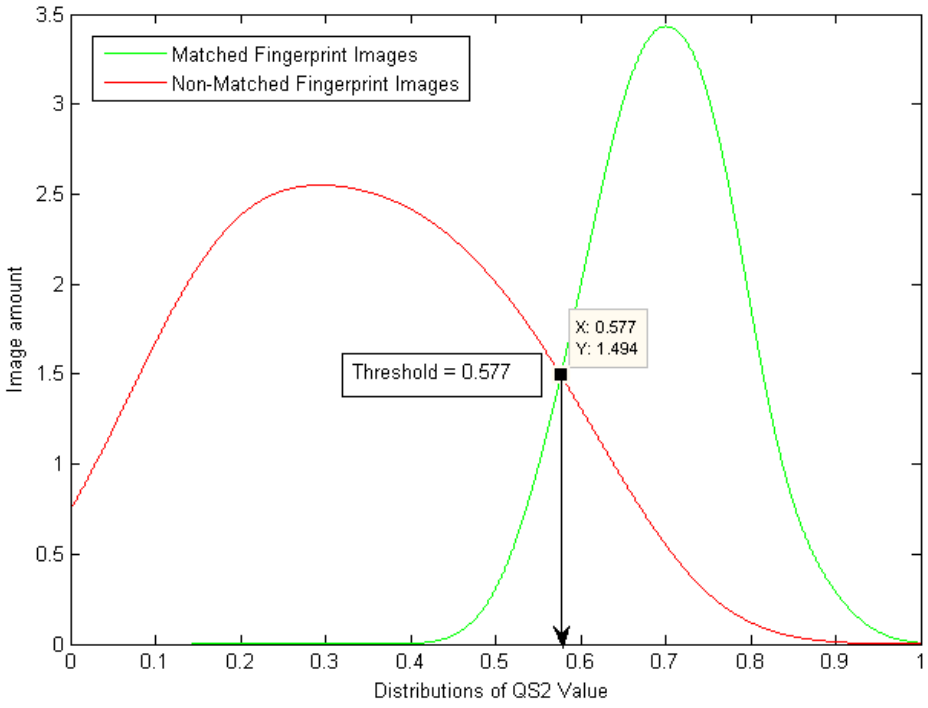


Figure 4.8: Distributions of QS_2 value between Matched Fingerprint Images and Non-Matched Fingerprint Images.

In Figure 4.8, we can observe that the threshold 0.577 is an optimal classification value to separate these two groups. Therefore, we can conclude that while QS_2 is lower than this threshold, the selected image has poor clarity of ridge-valley pattern. And then, this image will be further analysed using equation 4.3.2.12 to determine whether the image is from a wet or dry fingerprint.

4.3.3 Quality score 3

4.3.3.1 Methodology of influence of fingerprint image quality from worn ridge

Worn ridges are another aspect which has an impact on fingerprint image quality, which is caused for various reasons [104], [4] (e.g., dirt/cut/damaged finger, previous fingerprint impression on the sensor surface). In this work, the orientation flow will be analysed, which represents the flow of the ridge direction changes, to examine whether the fingerprint image possesses a valid global orientation structure. The Local Orientation Quality (OCL)approach will be applied, which is also suggested by Lim et al [86]. The detailed steps for this algorithm are described as follows:

1) Calculate the local ridge orientation θ_o for the segmented image $G(i,j)$ using the method of fingerprint image enhancement in the Section 3.3.2 of Chapter 3.

2) In order to compute the average absolute different $LOQ(i,j)$ in the targeted block θ_t , its eight neighboring blocks are used, which is defined by equation 3.3.3.1.

$$LOQ(i,j) = \frac{\sum_{m=-1}^{1}\sum_{n=-1}^{1}|\,\theta_t(i,j) - \theta_t(i-m,j-n)|}{8} \qquad (3.3.3.1)$$

3) When orientation changes smoothly, then the $LOQ(i,j)$ value is less than the chosen threshold. In this case, 8 degrees of tolerance angle are suggested by Lim [86]. Therefore, the local orientation quality score $LOQS$ is defined by equation 4.3.3.2.

$$LOQS = \begin{cases} 0, LOQ(i,j) \le 8^o \\ \frac{LOQ(i,j)-8^o}{90^o-8^o}, LOQ(i,j) > 8^o \end{cases} \qquad (4.3.3.2)$$

4) Calculate the average of all $LOQS$ values for analysing the overall orientation flow of the selected image. The Global Orientation Quality Score QS_3 can be computed by equation 4.3.3.3. If QS_3 value is larger than a threshold, the selected image is determined as a poor quality image with worn ridges;

otherwise, the factor of worn ridge is not a reason to cause the quality decrease of the selected image.

$$QS_3 = E\big(LOQS(i,j)\big) \qquad (4.3.3.3)$$

4.3.3.2 Classification of quality score based on clarity of ridge-valley texture

Similar to previous experiments described in sections 4.3.1.2 and 4.3.2.2 of this Chapter, the target of this experiment is to find the appropriate threshold value, which can best be used to separate the unmatched group from the matched group. In this case, 25 images were collected in each group, where the assignment to each group is based on an estimation of the orientation flow by human visual inspection. The experimental results are shown in Figure 4.9.

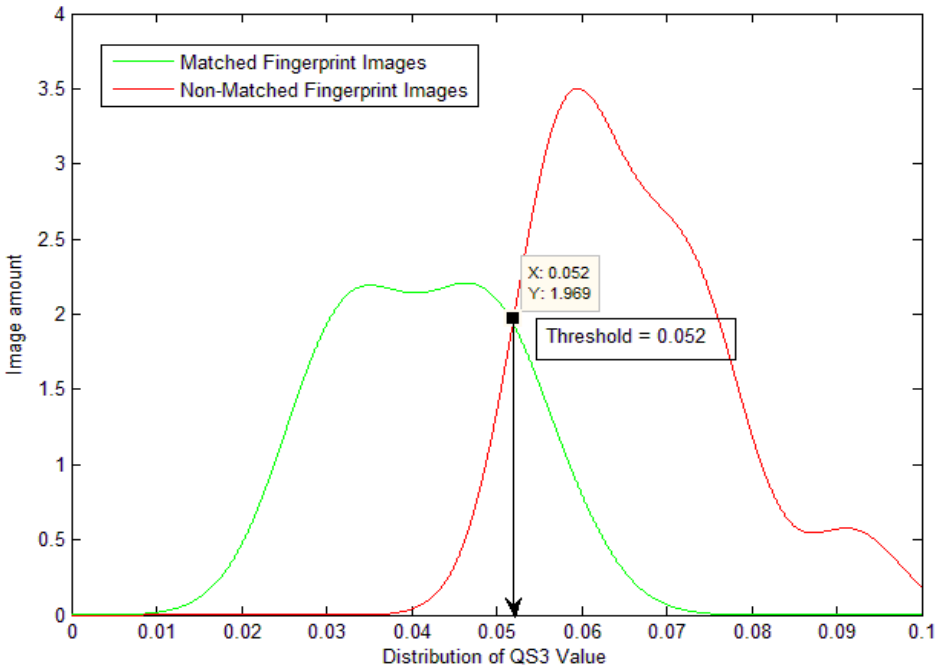


Figure 4.9: Distributions of QS_3 value between Matched Fingerprint Images and Non-Matched Fingerprint Images.

From Figure 4.9, we can observe that the threshold 0.052 can optimally separate these

two groups, namely the matched fingerprint images and the non-matched fingerprint images. Hence, we can conclude that if the value for a selected fingerprint image is larger than this threshold, this image will be considered to show a worn ridge, which is one of the aspects representing an image defect.

4.3.4 Quality score 4

4.3.4.1 Methodology of position deflection

For a score 4 (see Figure 4.2), the position deflection algorithm is the one aspect relevant to the evaluation of sample fingerprint quality, which is the offset about the core point of the fingerprint relative to the geometric centre of the fingerprint sensor. An ideal fingerprint image should contain the print's core and delta points [105]. Unfortunately, in practice, the core point is often not included in the fingerprint image, because the finger's placement is significantly out of alignment for correct capture of a full image. Therefore, in order to ensure the accuracy of this algorithm, a primary requirement is to build a reliable fingerprint core detection algorithm.

There are many approaches proposed in the literature for singular point detection, and most operate on the local ridge orientation.

- The Poincaré index method is the most popular method to detect a singular point, which was proposed by Kawagoe and Tojo [106]. The fingerprint orientation image is evaluated firstly with the smoothing process of ridge direction. After that, the Poincaré index method extracts singular points, core and delta, based on the sum of the orientation changes between the adjacent blocks. However, this method is very sensitive to the fingerprint orientation image, resulting in many false detections, especially in a noisy/low quality fingerprint image.

- Tomohiko Ohtsuka et al [107] proposed a singular candidate method using candidate analysis with an extended relational graph. With the purpose of increasing the success rate of singular detection, both the local and global

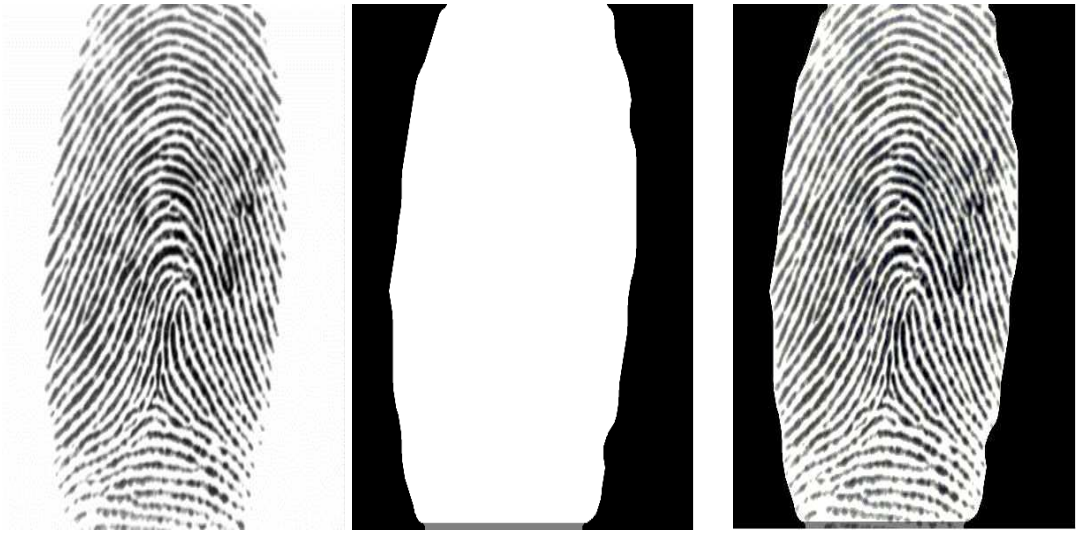
features are employed to detect the local ridge orientation. In order to estimate the local features of ridge direction with high tolerance to local image noise, different types of candidate models are introduced. In addition, extended relational analysis method is used to obtain the global features of the local ridge orientation. However, in a case with the limitation that the selected fingerprint image is notably degraded, this method can fail in locating the singular points.

For the studies to be described later, the proposed singular detection algorithm is a most important step for the position deflection method, which aims to achieve more reliable detection of singular points when the fingerprint image has poor quality. The steps for this algorithm are described below in greater detail, which consist of four stages.

A: First-Stage: Fingerprint image segmentation

In order to avoid the detection of false singularities, fingerprint image segmentation is one of the significant steps of the singular detection approach, which is used to obtain a region of interest (ROI) from a fingerprint image.

To obtain a reliable segmented fingerprint image, the proposed fingerprint image segmentation method is applied, which is based on the gray level range method [99] and the traditional technique, mean and variance based method [2], and the detail of this method is noted in Section 3.3.1 of Chapter 3. Figure 4.10 shows an example of the process of this method.

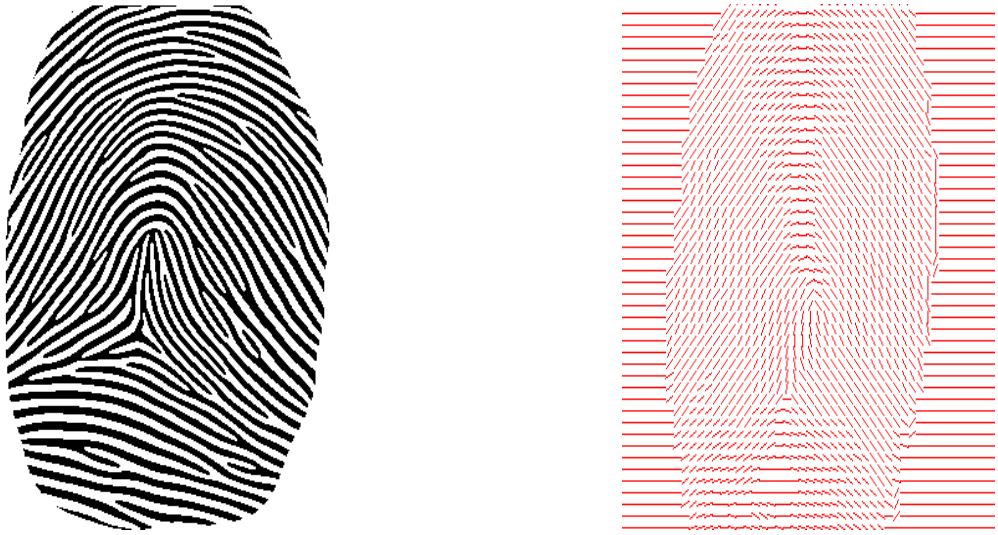


(a) (b) (c)

Figure 4.10: (a) Original image; (b) ROI image; (c) the segmented image

B: Second-Stage: Fingerprint ridge orientation estimation

Unlike other fingerprint orientation estimation algorithms, we proposed the idea to obtain the enhanced fingerprint image before we use a classic algorithm of estimation of the local ridge orientation. In this case, the enhanced image is obtained firstly, which is described in detail in Chpater 3. Subsequently, the proposed fingerprint orientation evaluation method as described in Section 3.3.2 of Chapter 3 will be used to estimate the local ridge orientation for this selected enhanced image. Figure 4.11 is shown examples of the local ridge orientation for a selected enhanced fingerprint image.



(a) (b)

Figure 4.11: (a) The enhanced image; (b) the local ridge orientation of the selected enhanced image.

C: Third-Stage: Fingerprint core points detection.

1) Divide the local ridge fingerprint orientation into four parts, and produce the image $C_{(i,j)}$. Based on the different fingerprint orientation evaluation method, the range of fingerprint orientation value θ, is different. In this case, θ can assume values -2/π to 2/π. If the range of θ is between 0 to$\frac{\pi}{4}$, it is designated part A; for the range of θ is between $\frac{\pi}{4}$ to$\frac{\pi}{2}$, it is part B; while for the range of θ is between $-\frac{\pi}{2}$ to$-\frac{\pi}{4}$, it is part C; Finally, when the range of θ is between $-\frac{\pi}{4}$ to 0, it is assigned to part D.

2) In order to reduce the noise in the image $C_{(i,j)}$, several operations are applied as follows: firstly, transform each part of the image $C_{(i,j)}$ into a binary image. After that, the morphological operations [108], dilation and erosion, are used to eliminate the holes, and the morphological close operation is used to return

the closed image. Finally, fill the holes in the binary image, and generate the image $C_{2(i,j)}$, which is shown in Figure 4.12.

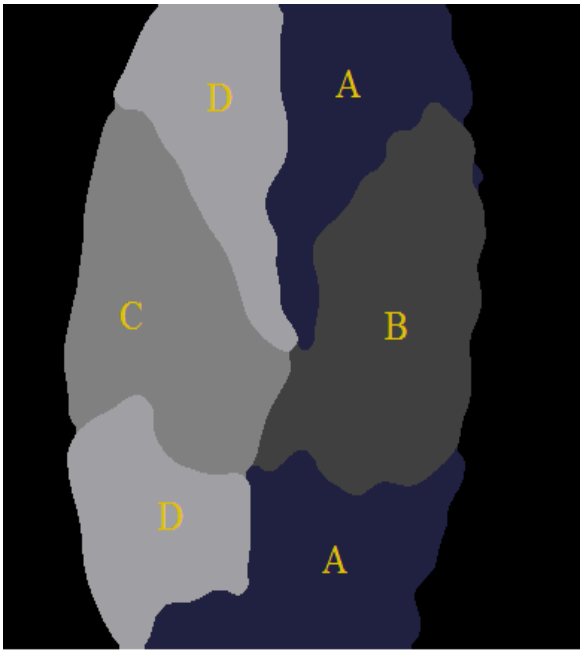


Figure 4.12: Partition of Orientation Image

3) Overview the core and delta points. According to the observed direction difference around each part of the image $C_{2(i,j)}$, we can determine that when the direction is a clockwise rotation, it is the core point. On the contrary, when the direction is a counter clockwise rotation, it is a delta candidate. Figure 4.13 illustrates an example of singularities points. In this thesis, the delta detection algorithm will not be introduced, because its algorithm is similar to the core point detection algorithm, and the delta points are not used for the position deflection method.

4) Generate the new orientation image θ_2 using equation 4.3.4.1.

$$\theta_2(i,j) = \begin{cases} \frac{\pi}{4}, & if\ \theta(i,j) \in Part\ A \\ \frac{\pi}{2}, & if\ \theta(i,j) \in Part\ B \\ \frac{3}{4}\pi, & if\ \theta(i,j) \in Part\ C \\ \pi, & if\ \theta(i,j) \in Part\ D \end{cases} \quad (4.3.4.1)$$

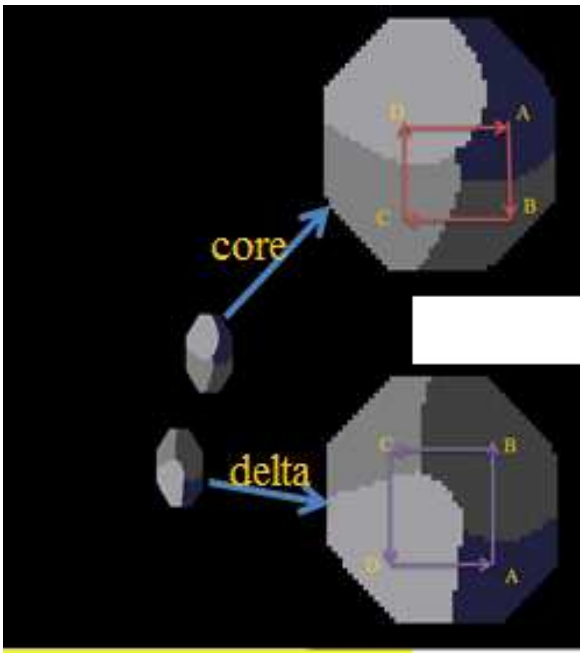
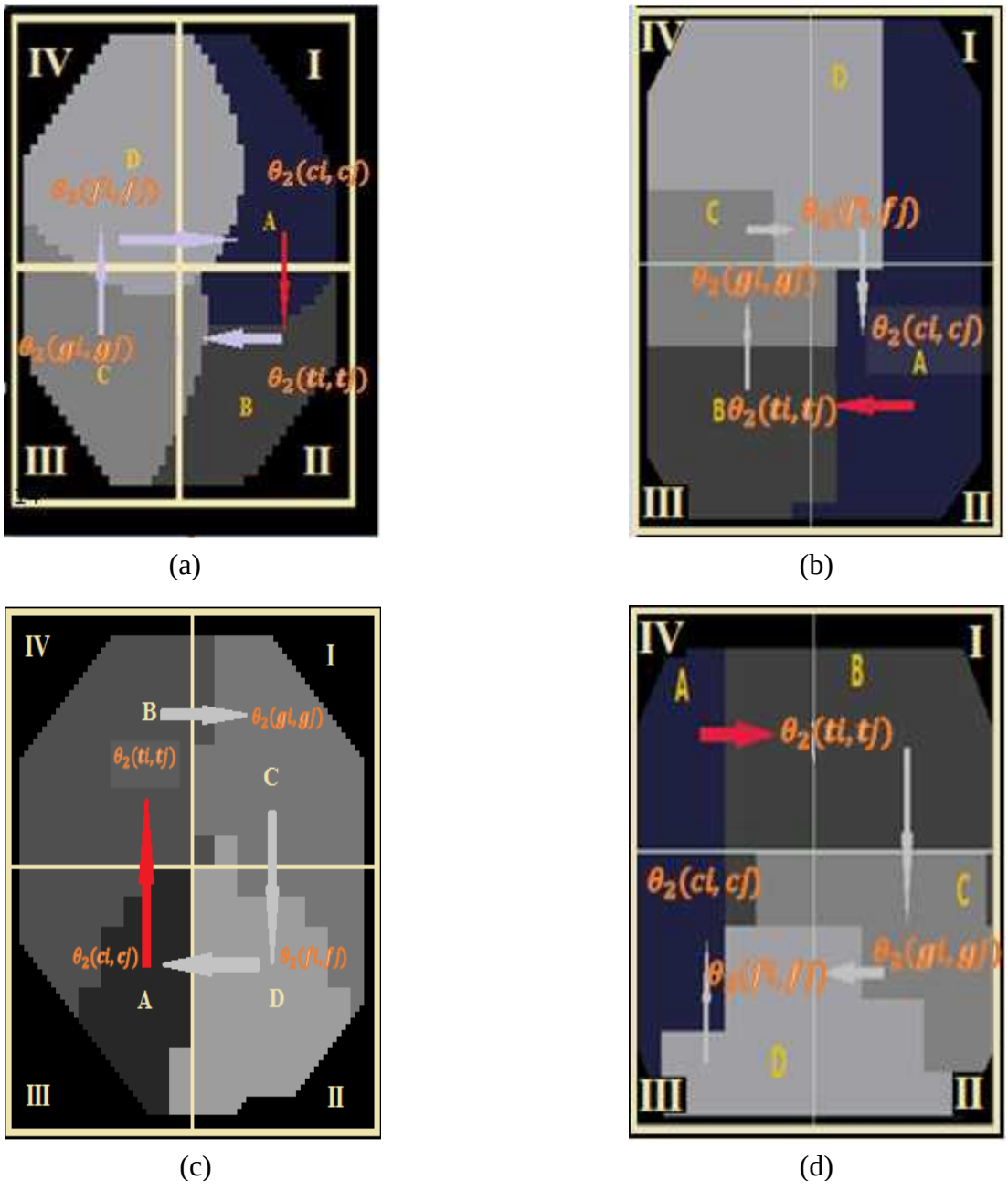


Figure 4.13: Singular points detection.

5) Detect the core points. Divide the image $C_{2(i,j)}$ into four parts, A, B, C, D. The start of the core point could appear in any one part of the image, which means this area is equal to π/4. Therefore, in order to detect the core points exactly, we have to observe the start of direction change at each part of image, which is illustrated in Figure 4.14.



(a) (b)

(c) (d)

Figure 4.14: Flow orientation change when the core point starts at different part of image.

6) The following steps illustrate an example for calculating the core point when the start point A of the core point is in the area I (see Figure 4.14 (a)).

i. Find the point $\theta_2(ti, tj)$ using equation 4.3.4.2, which is the boundary between A and B.

$$\begin{cases} ti = i + 1; \\ tj = j; \end{cases} \qquad if \begin{cases} \theta_2(\mathrm{i,j}) = \frac{\pi}{4} \\ \theta_2(\mathrm{i+1,j}) = \frac{\pi}{2} \\ \theta_2(i-1, j) \neq \pi/2 \end{cases} \tag{4.3.4.2}$$

ii. Pan left from the point$\theta_2(ti, tj)$ within the range of h as shown in equation 4.3.4.3, in order to find the point $\theta_2(gi, gj)$ which is the boundary between B and C.

$$\begin{cases} gi = ti; \\ gj = tj - h; \end{cases} \qquad if \begin{cases} \theta_2(\mathrm{ti, tj - h}) = \frac{3\times\pi}{4} \\ \theta_2(\mathrm{ti, tj - h}) \neq \pi \\ \theta_2(ti, tj - h) \neq \pi/4 \end{cases} \tag{4.3.4.3}$$

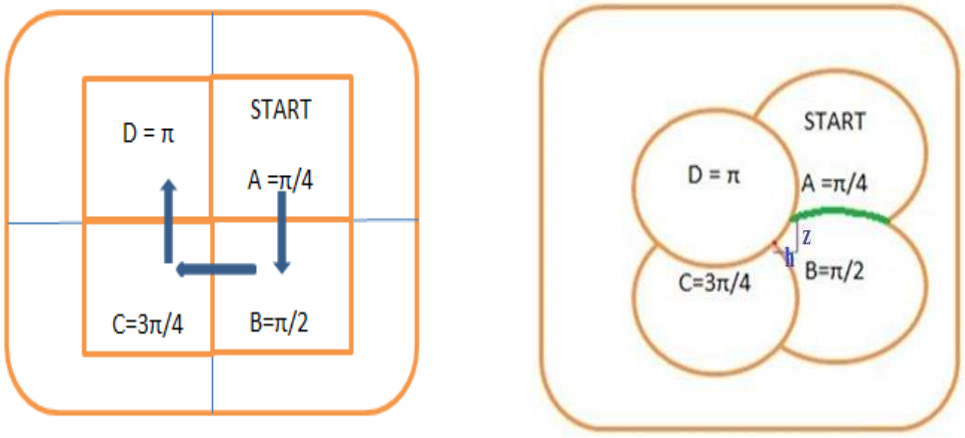
iii. Pan up from the point $\theta_2(gi, gj)$ within the range of h to find the core point $\theta_2(fi, fj)$ using equation 4.3.4.4.

$$\begin{cases} fi = ti; \\ fj = tj - h; \end{cases} \qquad if \begin{cases} \theta_2(\mathrm{gi - h, gj}) = \pi \\ \theta_2(\mathrm{gi - h, gj}) \neq \pi/2 \\ \theta_2(gi, gj - h) \neq \pi/4 \end{cases} \tag{4.3.4.4}$$

iv. For most fingerprint images, the core point cannot be detected using the above method, because the orientations change not along the rectangle. In this case, instead of equation 4.3.4.3 and 4.3.4.4, we set a parameter z to detect the core point more reliably using Equation 4.3.4.5 and 4.3.4.6. An example is illustrated in Figure 4.15.

$$\begin{cases} gi2 = ti; \\ gj2 = tj - h; \end{cases} \qquad if \begin{cases} \theta_2(\mathrm{ti + z, tj - h}) = \frac{3\times\pi}{4} \\ \theta_2(\mathrm{ti + z, tj - h}) \neq \pi \\ \theta_2(ti + z, tj - h) \neq \pi/4 \end{cases} \tag{4.3.4.5}$$

$$\begin{cases} fi2 = ti; \\ fj2 = tj - h; \end{cases} if \begin{cases} \theta_2(\mathrm{gi2 - h, gj2 - z}) = \pi \\ \theta_2(\mathrm{gi2 - h, gj2 - z}) \neq \frac{\pi}{2} \\ \theta_2(gi2 - h, gj2 - z) \neq \frac{\pi}{4} \end{cases} \quad (4.3.4.6)$$



(a) (b)

Figure 4.15: Ridge direction change when the core point starts at part A. (a) image orientation change along with rectangle; (b) orientation change not along the rectangle.

D: Fourth-Stage: Calculate the position deflection

The position deflection is the offset about the core point relative to the geometric centre of the fingerprint image. If it is so deflected, the offset was too large, that the image might be incomplete, and then a signal could be given to the user to move the finger severely leftward or rightward, and then it could be scanned again. The detailed steps are as shown below:

1) Calculate the centroid of the fingerprint sensor, X_h andY_v

$$X_h = \frac{W}{2}$$

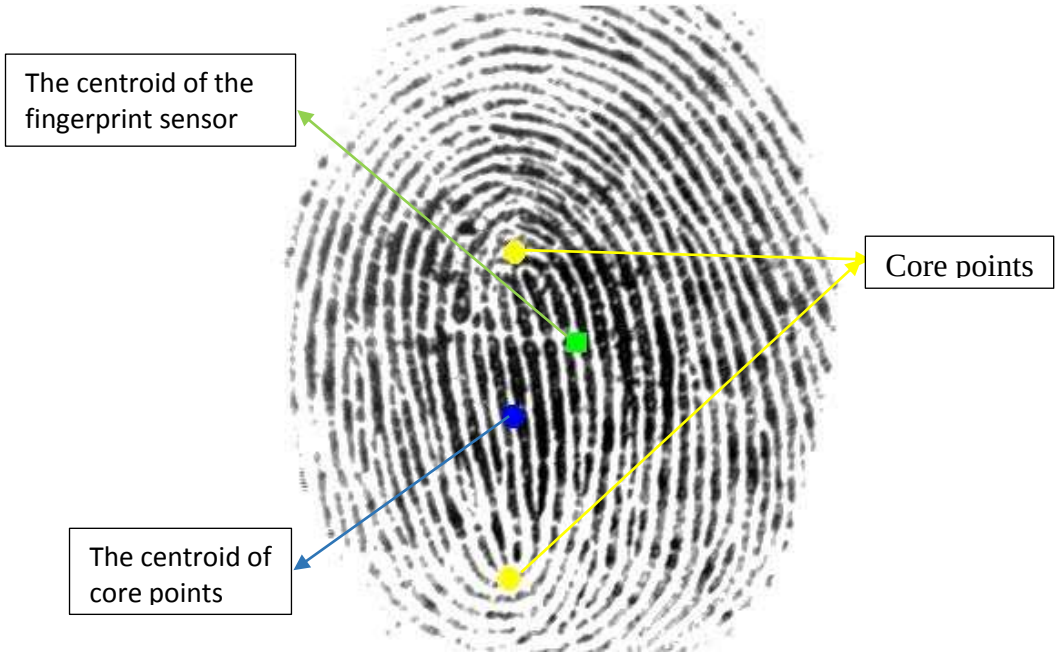
$$Y_v = \frac{H}{2} \quad (4.3.4.7)$$

In the above expression, the W means the width of fingerprint sensor surface; the H means the length of fingerprint sensor surface.

2) The coordinates of core points, f_j and f_i , of the input fingerprint image are calculated by the equation 4.3.4.3. If the image only includes one core print, if X_C is larger than $\mathrm{X_h}$, this fingerprint deflects severely rightward, while vice versa, this fingerprint deflects severely leftward. If Y_C is larger than $\mathrm{Y_v}$, this fingerprint deflects downward. In the opposite case, it deflects upward. If the image contains more than one core prints, the centroid of cores points have to compute for the position deflection calculation, which is defined by equation 4.3.4.8. Figure 4.16 shows examples of position deflection calculation.

$$\begin{cases} X_C = f_j, Y_C = f_i, & if\ the\ image\ only\ includes\ one\ core\ point \\ X_C = E(f_j), Y_C = E(f_i), & if\ the\ image\ have\ more\ than\ one\ core\ points \end{cases} \quad (4.3.4.8)$$

(a)



(b)

Figure 4.16: Examples of position deflection: (a) one core points in the input image; (b) the image contains more than one core points. (Green square: the centroid point of the fingerprint sensor; blue circle: the centroid of the core points; yellow circle: core points of the input fingerprint images).

4.3.4.2 Experimental result for detection of core points

We verified the proposed singular detection algorithm using the FVC2002 DB1_A database [47], which one of most popular fingerprint image databases in current use. This database contains 800 images of 100 fingers, and all fingerprints were captured with an optical sensor Touch View II manufactured by Identix. The size of the fingerprint image is 388 × 374 pixels with a resolution of 500 DPI. Fingerprints were collected under different condition, therefore many of fingerprint images are damaged by local image noise including creases, scars, smudges, dryness, dampness and so on.

Table 4.3 summarizes the experimental results for fingerprint singularity detection for the proposed algorithm and other relative fingerprint singularity detection algorithms.

The judgements (made by the experiment) of accepted core point and false core point were used for indicating the performance of the proposed algorithm.

	Accepted Core Point		**False Core Point**	
	Number	Accuracy %	Number	Error %
Poincare Index Method [4]	696	87.0	104	13.0
Extended Relational Graph Method [109]	629	78.6	171	21.4
Singular Candidate Method [107]	734	91.7	66	8.3
Proposed Method	769	96.1	31	3.9

Table 4.3: Summary of experimental results for fingerprint singular detection

According to Table 4.3, we can see that compared with other methods, the proposed approach can achieve the highest accuracy, showing a considerable improvement on the next best performing method. However, the singularity detection method based on the local ridge orientation has one limitation, that this kind of algorithm fails in locating the core point of fingerprints with an arch structure (see chapter 1) because the local ridge orientation of the arch-type fingerprint do not change as fast as other types of fingerprint image. Although the proposed method largely overcomes this limitation, some arch-type fingerprints still cannot be correctly detected in terms of their singular points. This is the principal reason why the proposed method cannot achieve perfect accuracy.

4.4 Chapter conclusions

In this chapter, we have defined a new fingerprint image quality evaluation algorithm, which can analyse fingerprint image defects from the point of view of five aspects including valid area, wet finger, dry finger, worn ridge and position deflection.

Initially, relevant information and background about the fingerprint image quality generally is introduced, which point out the reasons why this algorithm is very valuable for the overall fingerprint recognition process. And we have also introduced various related studies about estimation of fingerprint image quality.

Subsequently, the proposed fingerprint quality evaluation method has been described, which includes four isolated sub-methods for analysing the quality of fingerprint from different aspects. As for methods of valid area, dry or wet finger and worn ridge, the detailed steps are defined, and experimental results for determining the threshold value to separate good quality image from poor quality image has been also presented. For the method of position deflection, a range of fingerprint singularity detection algorithms reported in the literature, and also a proposed new algorithm for fingerprint singularity detection have been described in detail. According to the experimental results obtained, the proposed algorithm is shown to be more reliable.

The next chapter will present some detailed relevant information and background material about user feedback effects in overall fingerprint biometric system in general. In order to design better interaction between a fingerprint system and its user, this fingerprint feedback contains three different strategies for investigating the effect of different type of feedback, and how this might improve performance overall.

Chapter 5

Human-biometric-sensor interaction evaluation

This chapter will present a feedback unit for improving the usability of a fingerprint-based person recognition system. In this work, three different mechanisms will be introduced, which present different interfaces for interaction between the user and the biometric sensor to improve the effectiveness of the data acquisition process. Section 5.1 will introduce some background about the effect of usability of biometric systems. Section 5.2 will survey existing reported research about approaches for the design of software agents on the biometric system. Section 5.3 will describe in detail the feedback system unit, which includes the design of three different feedback mechanisms. Section 5.4 will show some experimental results on online collection databases in order to investigate whether the proposed feedback unit is able to improve the performance of the biometric system or not, and will compare the different mechanisms to seek the best strategy for the biometric system. Finally, section 5.5 provides a brief conclusion of this chapter.

5.1 Introduction

To date, in the fingerprint biometrics technology area, much research has been reported which deals with data processing in order to improve system performance. However, much less attention has been focused on improving the usability of biometric systems, which also is one of aspects which is known to highly affect the performance of biometric systems. Therefore, in this chapter, an "intelligent" feedback unit will be introduced and described for improving the usability of a fingerprint-based recognition system for the identification of individuals, which guides a user via a characterizing interface to interact with the biometric sensor correctly so as to improve the effectiveness of the data collection process.

According to the International Organization for Standardization (IOS) [110], the usability of a system can be described in terms of the following goals:

- Effectiveness: effectiveness is one of the most important characteristics in the biometric system, which is that users should be able to accomplish the desired tasks with ease.
- Efficiency: another characteristic of the biometric system is efficiency, which measures how well users can finish desired tasks with minimum expense of time and effort.
- Satisfaction: satisfaction describes the extent to which users feel pleased about their interaction with the biometric system.

Based on this concept, National Institute of Standards and Technology (NIST) provided a user-centred design process for the development of a biometric system, with an emphasis on improving ease of use, reducing system complexity, enhancing system performance, and increasing user satisfaction [111]. Four main components of the user-centred design process are illustrated in Figure 5.1. In addition, another popular approach for improving the usability of biometric systems is suggested by Kukula [112], which combines various methodologies, namely ergonomics [113], usability [114], and biometrics [115] known as the Human-Biometric Sensor

Interaction (HBSI) approach. Figure 5.2 shows the HBSI model, which demonstrates how to evaluate the overall performance of a biometric system from three aspects including biometrics (sample quality and system performance), ergonomics (physical and cognitive), and usability (efficiency, effectiveness, and satisfaction) [112].

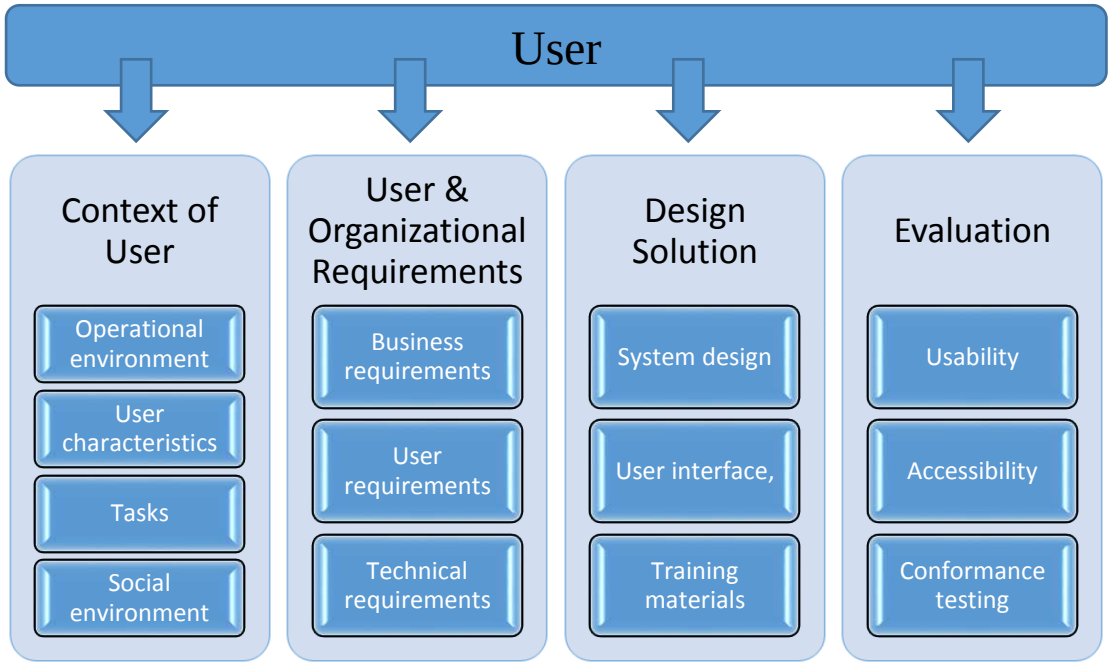


Figure 5.1: Biometric User-Centred Design Process (Taken from [111]).

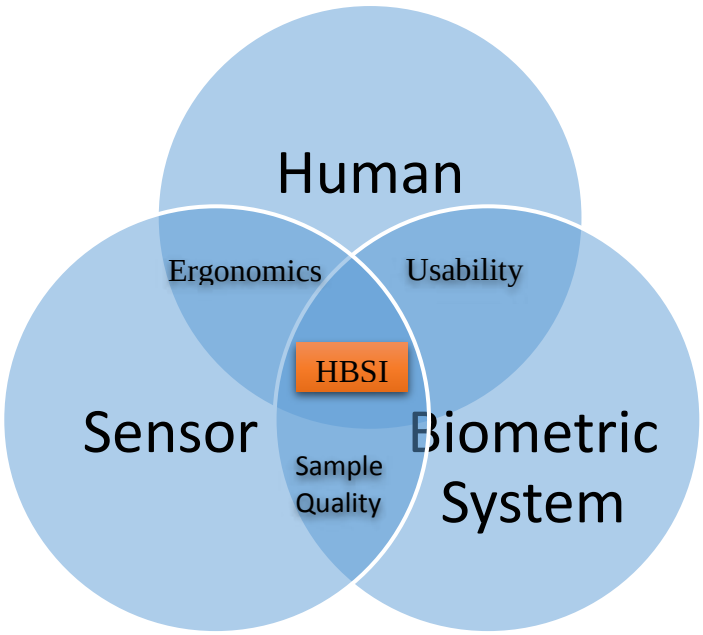


Figure 5.2: HBSI conceptual model (Taken from [112]).

According to the above concept, we can conclude that the benefit of usability can be summarized as following [111]:

- Improvement of the system performance.
- Efficiency of obtaining acceptable biometric data.
- Reduction of assistance requests from system staff.
- Saving the expense of extensive training and support.
- Increase in user acceptance.

As for the fingerprint-based recognition system, the improvement of usability is exceedingly necessary, because the quality of the fingerprint image critically impacts on the performance of the system, and a large percentage of incorrect interactions made by the user with the fingerprint sensor will result in the acquisition of a set of poor quality fingerprint images. Thus, the design of a friendly interface to assist the user to interact with the fingerprint sensor is a very important issue which justifies the potentially significant effort required to achieve this.

In the work to be reported here, our approach complements the above two general methods, and in particular focuses on the fingerprint quality factors and an appropriate interaction feedback mechanism to improve the usability of the fingerprint-based biometric system.

5.2 Related research

Prior reported work on improving the performance of a biometric system via a feedback mechanism is rather limited. In this area, few relevant papers in the literature can be found which have introduced different strategies for improving the interaction between the system and its user. Some examples include:

- R. Wong et al [116] proposed an interactive quality-driven feedback mechanism to improve the usability of the biometric system. The purpose of this mechanism is to improve the quality of biometric samples during the data acquisition process. If the quality of the biometric sample is evaluated as high quality, this biometric data is passed to next module for the feature extraction; otherwise, if the sample is considered as poor quality, this sample is evaluated by a quality analysis process to identify the factors that may degrade the system performance. After that, the analytical results are reported to the user in order to request the acquisition of a new biometric sample. The process of this mechanism continues until the timeout or when a biometric sample of acceptable quality is collected.

- N.J. Mavity et al [117] introduces a new concept of interface "utility" for optimizing the performance of biometric systems. In this work, the agent's utility relates to two important attributes, security level and quality, which represents an indicator to determine whether the user needs assistance or not. Normally, an agent is defined as "anything that can be viewed as perceiving its environment through sensors and acting upon that environment though effectors" [118]. However, in this case, it is described as an approach which combines biometrics and the use of software agents. In this system, four

different behaviour "bands" have been suggested. If the utility score is lower than 0.25, the level 1 behaviour band is activated, which is the lowest performance band. For this level, the system attempts to provide very detailed assistance to the user. If the utility score is below average (rate is between 0.251 and 0.5), the level 2 behaviour band is activated. A similar procedure is carried out as same as for level 1, where the quality of a biometric sample is analysed to investigate which factors degrade the performance of the system, and then provide very detailed assistance to the user. If the utility score is higher than average (rate is between 0.51 and 0.75), the level 3 behaviour band is activated, which means the selected sample obtains an acceptable verification score, and the system does not need to provide any assistance unless clearly requested for enrolling the new biometric sample. The level 4 behaviour band is activated when the utility value is higher than 0.75. For this level, the system does not need to provide any help because the selected sample produces a good verification.

As noted in Chapter 1, in order to obtain an acceptable fingerprint image to improve the performance of the fingerprint recognition system, three different units are added in the traditional fingerprint system including fingerprint image enhancement, fingerprint image quality evaluation and a feedback interface. Figure 5.3 shows the proposed fingerprint recognition system flowchart. In our work, a feedback interface based on three different possible mechanisms will be introduced. The aim of our work is to seek which mechanism can best improve the performance of the fingerprint image. A development of the proposed interface is to guide a user to interact with the biometric system correctly in order to improve the effectiveness of the data collection process.

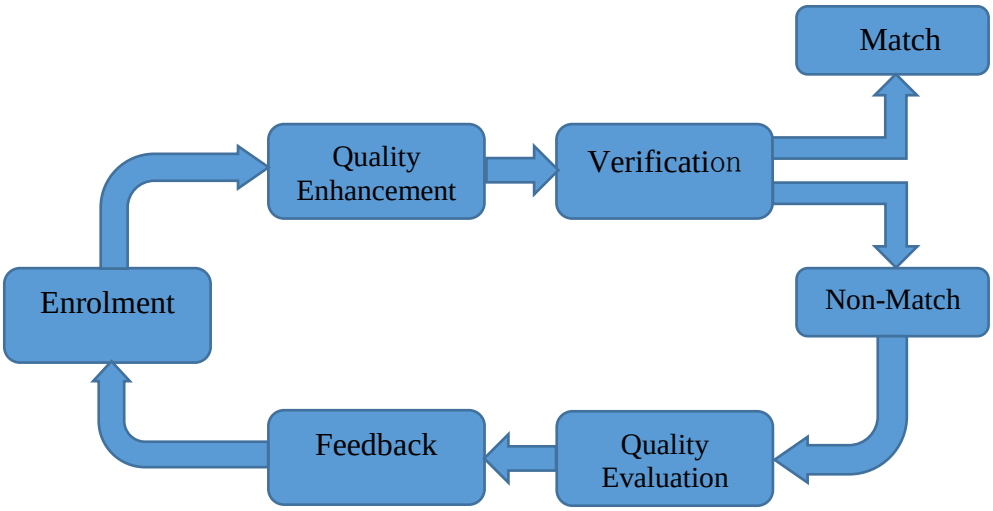


Figure 5.3: Flowchart of Proposed Fingerprint Biometric System.

5.3 Feedback unit design

The feedback unit is responsible for managing the interaction between the user and the biometric sensor. For the purpose of investigating which kind of feedback can achieve the best performance, three different feedback mechanisms are introduced and the participants in an evaluation experiment are divided into three different groups to donate their fingerprint using these three different mechanism. The designs of the three different feedback mechanisms are described below in greater detail.

- Mechanism 1: the first kind of feedback is only to show the previous captured fingerprint image to user, which is illustrated in Figure 5.4. In this case, if the user is achieving poor verification scores, this mechanism will actively attempt to improve the system's performance by showing the user's an image of the last failed sample. Thus, the user will be prompted to justify his/her behaviour at the next operation.

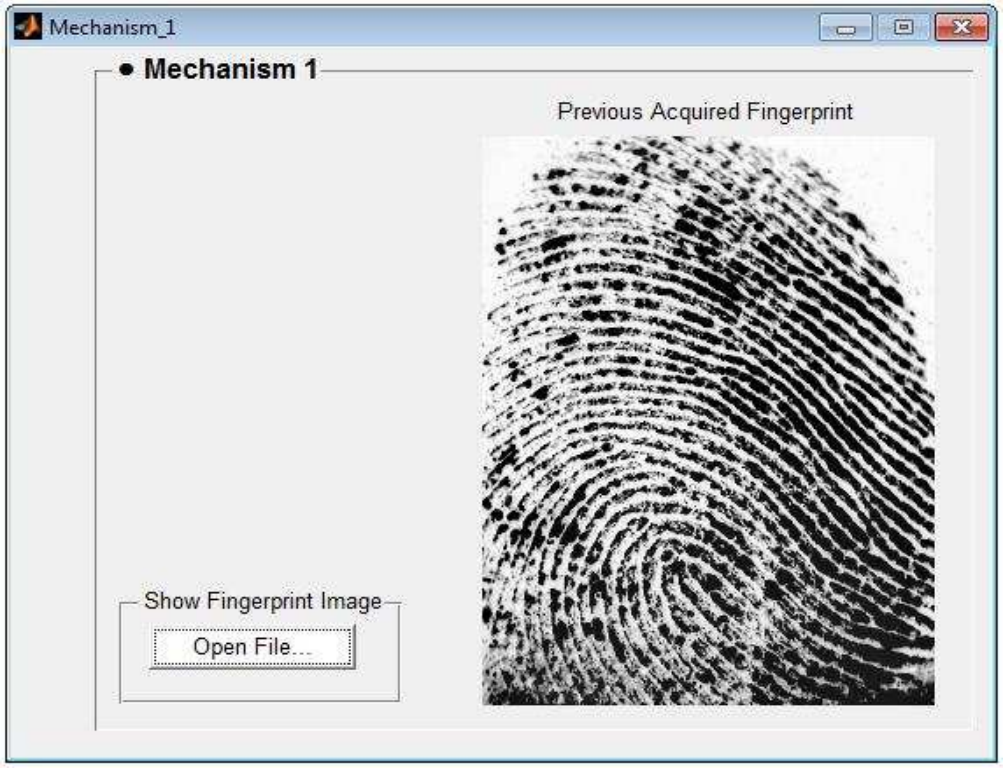


Figure 5.4: An example of the first kind of mechanism of feedback unit.

- Mechanism 2: the second possible mechanism is to send some possible solutions to the user, which modify some of the faults directly related to the poor score. As with mechanism 1, this mechanism is activated when the user cannot produce a fingerprint image of sufficient quality. In this case, the proposed fingerprint image quality evaluation method is embedded into this mechanism, which is to analyse the influence on fingerprint image quality from valid area, dryness or wetness finger, position deflection and worn ridges (as discussed in Chapter 4), and then to send a specific and detailed analytical report to the user illustrating the required action for promoting better interaction with the biometric sensor at the next fingerprint image enrolment operation. An example of this mechanism is illustrated in Figure 5.5, and a detailed analytical report is listed in Table 5.1.

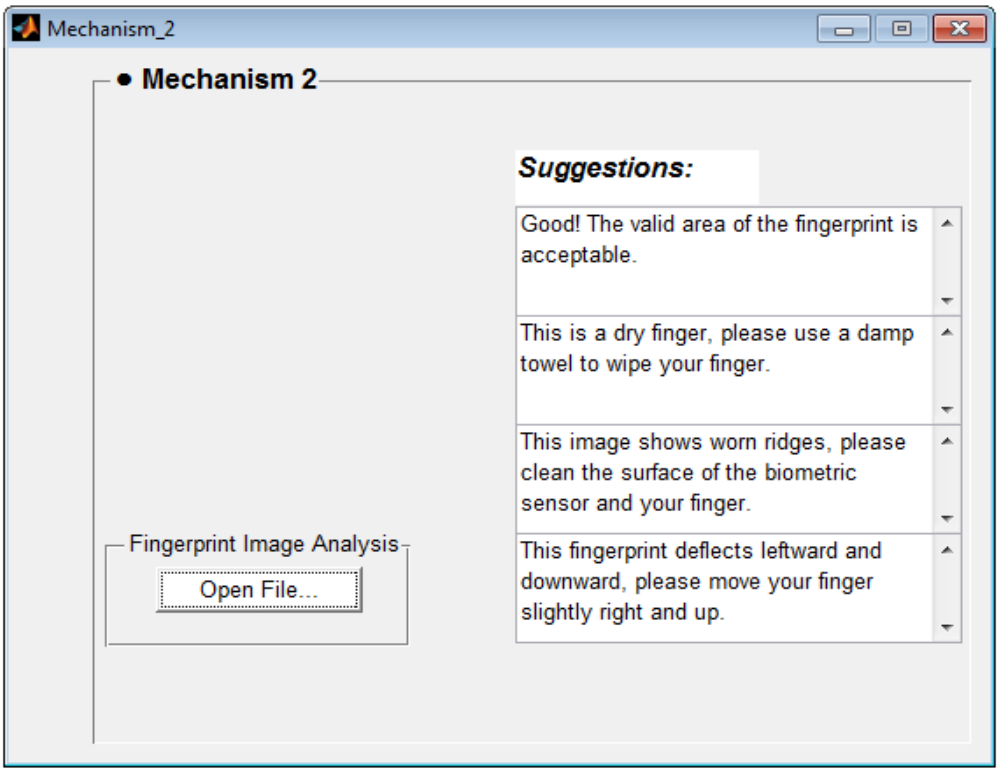


Figure 5.5: An example of the second kind of mechanism of feedback unit.

Factors affecting fingerprint image quality	Identified the image defect	Suggestions
Valid area	Unacceptable valid area	The valid area of the input image is unacceptable, please cover as much of the sensor area.
	Acceptable valid area	Good! The valid area of the fingerprint is acceptable.
Finger skin condition	Dry Finger	This is a dry finger, please use a damp towel to wipe your finger.
	Wet Finger	This is a wet finger, please use a dry towel or tissue to wipe your finger.
	Acceptable skin condition	Good! The condition of the input finger is acceptable.
Image degradation	Worn ridges	This image shows worn ridges, please clean the surface of the biometric sensor and your finger.
	Acceptable image condition	Good! This is not damaged finger.
Position deflection	Always show core points and centroid point of fingerprint sensor on the fingerprint image.	The guidance is always given to user, such as this fingerprint deflects rightward/leftward/upward/downward, please move your finger slightly left/right/down/up.

Table 5.1: A summary of an analytical report.

- Mechanism 3: the third kind of fingerprint feedback mechanism is to combine the characteristics of the first and second fingerprint feedback mechanisms that not only shows the previous acquired fingerprint image but also provides the analytical results to use, which is illustrated in Figure 5.6. For this mechanism, users receive very detailed feedback in the event of the fingerprint image

cannot be correctly verified. Specifically, the detailed analytical report will be sent to the user, which identified image defects leading to the failure, and at the same time, the user's previous enrolled fingerprint image will also be shown. Moreover, in order to assist the user to interact with the biometric sensor more efficiently, the core points of the input fingerprint and the centroid of fingerprint sensor will be marked in the fingerprint image.

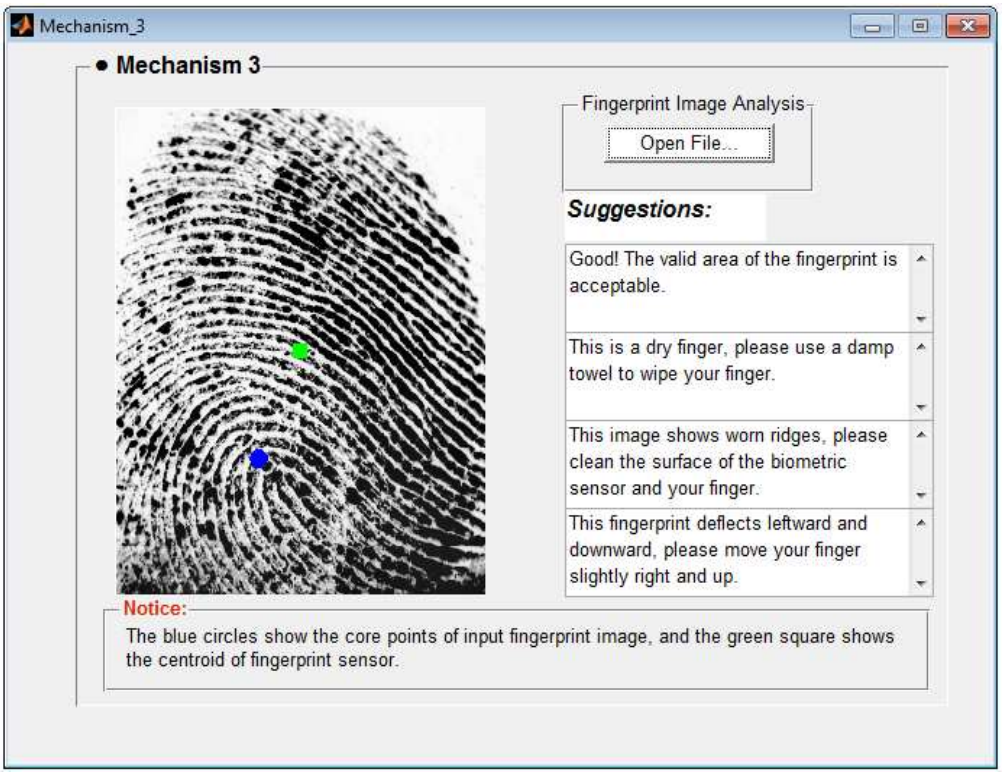


Figure 5.6: An example of the third kind of mechanism of feedback unit.

5.4 Experimental investigation

5.4.1 Fingerprint online database description

As noted in Chapter 2, a total of 240 different fingers from 30 volunteers enrolled in the fingerprint online database, which were randomly partitioned into three groups. Each group was associated with a "sub-database" and therefore with a different

fingerprint feedback mechanism. For each database, two images of 4 fingers (thumb, index, middle finger and ring finger) of the two hands of each volunteer were taken and this was done in two sessions. In order to evaluate the effect of feedback mechanisms in practice, all participants enrolled their fingerprint without any effort to control image quality, and the fingerprint sensor was also not cleaned. Thus, the fingerprint images samples of this database vary considerably in quality. Figure 5.7 shows some examples of different quality of fingerprint images in this database.

(a) (b) (c)

Figure 5.7: (a) A good quality fingerprint; (b) a medium quality fingerprint degraded by ridge breaks; (c) a poor quality fingerprint degraded by ridge breaks and a wet skin condition.

5.4.1.1 Test procedure

At the first session, the individual was requested to donate the fingerprint firstly without any guidance (in impression 1), and then this enrolled fingerprint was analysed by the one of fingerprint feedback mechanisms. After that the user was guided to enrol the fingerprint again by using the analytical results provided (in impression 2). During the second session, the procedure of fingerprint images enrolment was the same as the first session. At the first, the participant was asked to donate the fingerprint in

impression 3, and then the feedback mechanism was activated to send the feedback to the user to encourage better interaction with the biometric sensor again in impression 4. Table 5.2 lists detailed information about the fingerprint database description.

Database	Sensor	Image Size	Feedback Mechanism	Session 1 Numbers	Session2 Numbers	Total Numbers
DS1	SecuGen Hamster IV	258*336 pixels	1	160	160	320
DS2	SecuGen Hamster IV	258*336 pixels	2	160	160	320
DS3	SecuGen Hamster IV	258*336 pixels	3	160	160	320

Table 5.2: Fingerprint Database Description

5.4.2 Performance evaluation of fingerprint feedback unit

The purpose of this evaluation is to estimate the influence of the fingerprint feedback unit for use in a fingerprint recognition system. Four performance indicators are suggested here, which are FMR 100, FMR1000, Zero FMR and Equal error rate (EER). EER is the computation of the error rate at which the False Non Match Rate (FNMR) and the False Match Rate (FMR) have an equal value, which is a very common performance indicator used in biometric system evaluation. In addition, the measurement of FMR 100 and FMR 1000 are the value of FNMR when FMR is equal to 1% and 0.1 %, respectively. Also, Zero FMR is obtained as the lowest FNMR as a result of which no False Matches occur [31].

- **The protocol for the online database**

  FNMR: For each finger, 4 fingerprint images were collected. In order to evaluate the influence of the feedback unit for the fingerprint recognition system, these four impressions are divided into two classes. The impression 1

and 3 are classified into the class 1, which are the first captured fingerprint of each session and obtained without any feedback assistance. And the class 2 includes the impressions 2 and 4, which are the second captured fingerprint of each session and collected when the detailed feedback is provided. Each pair of impressions are verified using VeriFinger 6.5, marketed by the manufacturer Neurotechnology [54]. For each database, the total of genuine matches for each class is 80. Figure 5.8 illustrated the procedure for the FNMR calculation.

$$FNMR = \frac{Number\ of\ rejectd\ genuine\ claims}{Total\ number\ of\ genuine\ accesses} \times 100\% \qquad (6.4.2.1)$$

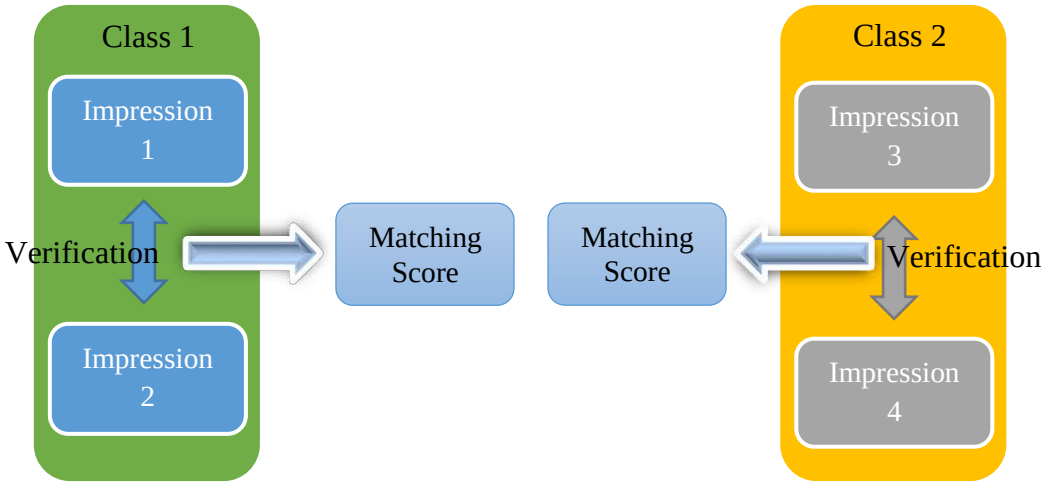


Figure 5.8: The procedure for the performance evaluation of FNMR.

FMR: in the same way as for the protocol for FNMR, four impressions of each finger are classified into two classes. And then the first sample of each class is matched against the first sample of the same class from the remaining persons with the same finger in same database. For each database, the total number of imposter matchings for each class is 720.

$$FAR = \frac{Number\ of\ accepted\ imposter\ claims}{Total\ number\ of\ imposter\ accesses} \times 100\% \qquad (6.4.2.2)$$

EER: the equal error rate is employed as a performance indicator, which is calculated where the FRR and FAR are equal. If the equal error rate (EER) of the second class is less than for the first class, this will demonstrate that the feedback unit can improve the performance of the fingerprint recognition system. The detailed experimental results will be described and discussed in next section.

5.4.3 Experimental results and analysis

Mechanism 1	Class 1	Class 2	Improvement
FMR 100	30%	18.75%	11.25%
FMR 1000	31.25%	20%	11.25%
Zero FMR	33.75%	23.75%	10%
EER	17.5%	11.875%	5.625%

Table 5.3: Experimental results for the first mechanism.

In Table 5.3, we have tabulated the comparative results for the collection of fingerprint images with/without the first feedback mechanism. As for the class 1, two fingerprint impressions were collected without guidance, and then the collected fingerprints were verified by the VeriFinger 6.5 software [54]. For the class 2, these two fingerprint images were enrolled with the feedback interface active. Using the first feedback mechanism, the previous fingerprint image is displayed (taken from the class 1), and the user will judge by himself how best to interact with the biometric sensor for the new sample acquisition. As shown in this table, one can observe that the accuracy for the class 2 is higher than for the class 1. Studying Table 5.3 reveals that the enrolment of fingerprint images with the first feedback mechanism is able to improve the performance of the fingerprint-based recognition system.

Mechanism 2	Class 1	Class2	Improvement
FMR 100	23.75%	18.75%	5%
FMR 1000	25%	20%	5%
Zero FMR	26.25%	22.5%	3.75%
EER	13.6%	11.1%	2.5%

Table 5.4: Experimental results for the second mechanism.

In Table 5.4, the experimental results are obtained by means of a comparison between the collections of fingerprint images with/without the second feedback mechanism. Using the same process as for the previous experiment, the class 1 includes two impressions, which were collected without any feedback, and the fingerprint images in the class 2 were captured with the second feedback mechanism active. In this mechanism, the fingerprint image quality algorithm is integrated into the feedback interface, which means the previous fingerprint image was analysed by the fingerprint quality algorithm first, seeking to identify the factors that can significantly affect the system performance, and the analytical reports were provided to the user in order to guide the user to interact with the biometric sensor correctly. As shown in Table 5.4, we can see that the accuracy of the class 2 is slightly higher than the class 1, which reveals the second feedback mechanism also can increase the performance of the fingerprint-based recognition system.

Mechanism 3	Class 1	Class 2	Improvement
FMR 100	22.5%	5%	17.5%
FMR 1000	26.25%	6.25%	20%
Zero FMR	31.25%	7.5%	23.75%
EER	14.27%	5.52%	8.75%

Table 5.5: Experimental results for the third mechanism.

Table 5.5 shows the comparative results of the collection of the fingerprint image with/without the third feedback mechanism. In the case of this configuration, the

characteristics of the first and second mechanisms are combined, which means the fingerprint image quality evaluation algorithm (described in Chapter 4) is integrated along with the demonstration of the fingerprint image in the feedback interface. Therefore, the user is guided by this very detailed information to interact with the biometric sensor including the provision of the previous fingerprint image and analytical results (estimated by the fingerprint image quality algorithm). From Table 5.5, we can observe that the matching performance based on the third feedback mechanism is higher than the others, and this indicates that this mechanism efficiently enhances the performance of the fingerprint-based recognition system.

As are shown in Table 5.3, Table 5.4 and Table 5.5, all the performance indicators of the third feedback mechanism are notably higher than when the other mechanisms are used, while the second feedback mechanism obtained the smallest degree of improvement. During the process of the collection of fingerprint images based on the second feedback mechanism, visual observation of the process suggested that the user does not appear always to find it easy to understand the analytical results without the provision of the fingerprint image. For example, if the analytical result shows the enrolled fingerprint image deflects upward, the user often moved the finger severely, which results in a situation where the finger is out of alignment. And in the process of data collection based on the first feedback mechanism, we observed that if the user has no experience with the fingerprint recognition system, it is not helpful for the demonstration of the previous fingerprint image, because the user does not know exactly what problems occurred with the previous of fingerprint image. Therefore, the third feedback mechanism is a good method to rectify these problems, the user can clearly understand the factors causing the effect on the fingerprint image quality by the analytical results, and the demonstration of a previous fingerprint image is also a good indicator to guide the user to interact with the biometric sensor correctly. Overall, we can conclude that the feedback interface based on the design of the third mechanism is generally better as a means of improving the performance of the fingerprint-based recognition system than the others.

Although comparison of accuracy for the different feedback mechanisms is one aspect of an evaluation of the performance of fingerprint recognition systems, carrying out an experiment about the measurement of the execution time for the different feedback mechanisms is another important aspect, because more information feedback will generally needs more analysis from the user, which in turn can result in a slower interaction. In other words, performance in terms of accuracy may go up, but throughput will go down. There is thus a trade-off to be considered. This broader evaluation is an area which will benefit from further investigation in the future.

5.5 Chapter conclusions

In this chapter, a feedback interface has been introduced as a means for improving the usability of the fingerprint-based recognition system. In this work, this feedback interface is based on three different feedback mechanisms to investigate which mechanism can best improve the performance (in terms of recognition accuracy) of the fingerprint system.

Initially, the importance of the improvement of the usability for the fingerprint recognition system is pointed out. And then some existing reported research about the methods for the design of the feedback interface has also been introduced.

Subsequently, the design of the feedback interface based on the three different mechanisms have been proposed, which described the detailed information about the characteristics of each mechanism. The first interaction mechanism displays previous fingerprint images directly to the user, and then each user makes their own judgement about how best to interact (in terms, for example, of best finger placement on the sensor) with the biometric sensor for a new sample acquisition. Regarding the second mechanism, the fingerprint image quality evaluation algorithm is now integrated in the feedback interface. The previous fingerprint image is analysed by the fingerprint image quality evaluation algorithm to seek the factors which impact the performance of the fingerprint recognition system, and the analytical results are fed back to the user to

guide the next interaction with the biometric sensor. As for the third mechanism, the first and the second mechanisms are combined in the feedback interface. In this mechanism, the user receives very detailed information including the previous the fingerprint image and the analytical results to interact with the biometric sensor for the collection of the new data.

Finally, in order to evaluate the effect of the feedback interface for the fingerprint recognition system, an online fingerprint collection database is used here. In this database, each finger includes four impressions, and they are separated into two classes. For the class 1, all fingerprint images were collected without any feedback suggestion. For the class 2, the fingerprint image was enrolled with different mechanisms. The comparison of experimental results based on the different mechanisms has been presented. According to the results, we can observe that all mechanisms can improve the performance of the fingerprint recognition system, but the feedback interface based on the third mechanism achieve the highest accuracy than others.

The next chapter is the final chapter of this thesis, which will includes two aspects: firstly, we will summarize all the studies accomplished. Furthermore, we will provide some guidance for the improvement of fingerprint-based recognition systems in the future.

Chapter 6

Final remarks

This chapter will present a final overview of the work which has been reported in this thesis, addressing some of the important problems associated with practical fingerprint recognition systems, reviewing the work carried out to overcome these limitations, and taking a brief look into the future. Section 7.1 summarizes the main studies and experiments carried out in this study and stresses the most important contributions and findings of our study. Section 7.2 provides some guidance for further possible research directions in the future. Section 7.3 will summarize and draw the reported study to a conclusion.

6.1 Summary of work done and contributions

In this study, some of the fundamental factors have been identified relating to the performance of an automatic fingerprint biometric system, and investigated the relevant issues from a coarse level to a finer level. This study has composed a thorough empirical analysis of the influence of the quality of the fingerprint image in a fingerprint biometric system and described the interrelationship between the quality of a fingerprint image and other primary components of a fingerprint biometric system, such as the feature extraction operation and the matching process. Furthermore, with the purpose of improvement of the performance of an automatic fingerprint biometric system, three components/enhancements have been introduced which can be added into the traditional fingerprint biometric system in our proposed system, which are a fingerprint enhancement algorithm, a fingerprint image quality evaluation and a feedback unit, the purpose of which is to assist the user in interacting with the fingerprint sensor in a better and more accurate way, using analytical information collected during the interaction process for this purpose.

Firstly, the overall background to biometrics have been introduced in general, the history and development of fingerprint biometrics and automatic fingerprint recognition systems in particular, and then the most important components have been described in a practical fingerprint recognition system, which included the general structure of a fingerprint biometric system and some background about current state-of-the-art techniques, in order to provide us with a thorough understanding of the structure and techniques involved in designing an automatic fingerprint recognition system. Subsequently, some essential limitations of an automatic fingerprint biometric system have been identified relating to poor quality fingerprint images and their effects on the performance of a fingerprint biometric system. After that, a number of factors were summarized which can degrade the quality of a fingerprint image. Furthermore, different categories of degradations affecting the quality of a fingerprint image were generalized and what problems they might create in the processing units after sample

capture in the overall processing chain (e.g. in the feature extraction stage and the matching stage).

Hence, in order to improve the overall performance of an automatic fingerprint biometric system, two different solutions have been introduced in this thesis to overcome these issues in order to obtain a more acceptable quality of fingerprint image, allowing improved performance.

The first solution to overcome the limitation bought about by poor quality fingerprint images is addressed with a new fingerprint image enhancement algorithm. This algorithm efficiently removes noise in the image and improves the overall clarity of the ridges and valleys structures in the input fingerprint images. An advantage of this algorithm is that it will not generate any spurious features while ensuring the accuracy and reliability of extraction of distinct characteristics of a fingerprint image.

Initially, relevant information and general background of the fingerprint image enhancement process was presented, and then further described a range of state-of-the-art fingerprint image enhancement algorithms which have a particular bearing on the development of our proposed algorithm. And then, the proposed fingerprint enhancement algorithm based on Gabor filtering was introduced, which consists of 4 sequential steps: fingerprint image segmentation, local ridge orientation estimation, local ridge frequency estimation, and the application of Gabor filtering to enhance the quality of the fingerprint images. In order to deliver a clear understanding of the proposed algorithm, a general background and related research for each of the steps of our algorithm were provided, and also described in detail the key functionality of these processing steps.

Beyond that, the proposed fingerprint enhancement algorithm was examined and evaluated using three different databases, specifically the FVC2004 DB1_A database, the FVC2004 DB2_A database, and the FVC2004 DB3_A database [26]. With the purpose of producing a better evaluation of the performance, reliability and robustness

of the proposed algorithm, those databases were selected because they represent scenarios where the fingerprint images were collected with varying quality, while different types of fingerprint sensors were utilized, including an optical sensor and a thermal sweeping sensor. Finally, the proposed algorithm was compared with a range of other selected enhancement methods. According to the experimental results obtained, the proposed algorithm was found to effective and efficient improve the verification accuracy for the fingerprint databases tested, and this proposed algorithm is therefore shown to be potentially suitable for other databases compiled using various fingerprint sensors including an optical sensor and a thermal sweeping sensor.

The second solution is to help the user of a fingerprint-based biometric system to donate a fingerprint sample with an increased probability of acceptable quality via a feedback unit, which evaluates the quality of the initially captured fingerprint images and delivers appropriate feedback to the user when the input fingerprint fails to match the targeted template stored within the system. In this thesis, the design of the feedback interface have been explained based on three different possible mechanisms, and a comprehensive comparison of these three mechanisms have been made in terms of the accuracy of the fingerprint recognition system as a result of adopting the feedback.

The first feedback interaction mechanism only displays to the user an image of the last failed sample directly, and allows the user to understand, analyse and improve his/her behaviour during interaction (e.g. placing the finger in the centre of the sensor, moisturising a dry finger, pressing harder on the platen) with the sensor so as to obtain an improved and acceptable quality of the fingerprint image. In the second feedback mechanism, a fingerprint image quality evaluation algorithm is embedded to analyse the quality of the previously acquired fingerprint image to identify the factors which may impact on the performance of the fingerprint recognition system, and then the analytical result is provided to the user to guide the next interaction with the fingerprint sensor. The third feedback mechanism combines the key properties of the first and second mechanisms in its design. The user is provided with the most completed knowledge about the fingerprint images including a display of the previously acquired

fingerprint image and the detailed analytical report, which identifies the image defects leading to the failure in order to assist the user in interacting with the fingerprint sensor in a further verification attempt. Furthermore, in order to evaluate the influence of the feedback unit for the fingerprint recognition system, design and collect a dedicated in-house online fingerprint collection database was required. In this database, 30 people volunteered to take part in the online data collection. This consisted of two sessions with at least one week of time lapse between them. In order to examine whether the proposed feedback unit can help improve the overall performance of an automatic fingerprint recognition system or not, two classes of data were designed to be collected. One represents fingerprint images which were collected without the intervention of the feedback unit, while the other represents fingerprint which images were collected with the aid of feedback unit. According to the experimental results, we have observed that all three feedback mechanisms can improve the performance of the automatic fingerprint recognition system to some extent, while the third feedback mechanism delivers the best improvement and yields the highest performances in terms of recognition accuracy.

Finally, a new fingerprint image quality evaluation algorithm was introduced, which can analyse fingerprint image defects from the point of view of five aspects including valid area, wet finger, dry finger, worn ridge and position deflection to determine the particular factors which generated the poor quality image. In this thesis, some general background and a discussion of the influence of the quality of a fingerprint image in an automatic fingerprint recognition system was introduced, and also the state-of-the-art overview of fingerprint image quality evaluation algorithms was presented. The proposed algorithm consists of four separate components: the detection of a valid area, whether we are dealing with a dry or wet finger, whether worn ridges are present, and the issue of position deflection. As for methods concerning the questions about valid area, dry or wet finger and worn ridge, the detailed steps were defined, and experimental results for determining the threshold value to separate good quality image from poor quality image have been also presented. With regard to the methods for dealing with position deflection, a range of state-of-the-art fingerprint singular

point detection algorithms have been reviewed, and a novel algorithm was proposed. The proposed fingerprint singular point detection algorithm is examined using the FVC2002 DB1_A database and, according to the analytical results obtained from the experiment, the proposed algorithm has been shown to be more reliable.

All in all, the main contributions of this project can be sorted into three parts:

- A novel fingerprint quality enhancement algorithm with new approaches of fingerprint image segmentation algorithm, local ridge orientation calculation, and local ridge frequency estimation. According to the experimental result, the enhanced images using the proposed algorithm lead to decreased error rates of both the NBIS matcher and VeriFinger 6.5 matcher, for which the error rates dropped by over 45% and 40% respectively.

- A novel quality estimation algorithm which analyse the fingerprint image from five distinct and important aspect, including valid area, dry/wet finger, worn ridge, and position deflection, among which a novel position deflection estimation algorithm which utilize a new reliable and robust method to detect fingerprint singular points is also proposed. The proposed novel fingerprint singular point detection method can detect core points with a detection accuracy of 96.1%, which is 4.4% higher than the next best algorithm.

- A feedback unit which provides the user with appropriate guidance through analyse the captured fingerprint image. Furthermore, a novel online fingerprint database is created to evaluate the proposed feedback unit

6.2 Future work

The research presented in this thesis has aimed to explore some significant limitations of an automatic fingerprint recognition system relating to the occurrence of poor quality fingerprint image effects in a fingerprint recognition system, and also to

propose some different possible solutions to overcome this issue. Some possible new research ideas based on quality issues about a fingerprint recognition system have emerged from the presented contributions in thesis, which are as follows:

Considering a fingerprint image enhancement algorithm, there are still some challenging problems to be investigated. For instance, this algorithm was evaluated only using the fingerprint databases for which the fingerprint images were collected using two different types of fingerprint sensors including an optical sensor and a thermal sweeping sensor. However, as for fingerprint images collected from other fingerprint sensors (e.g. ultrasound sensor, capacitive sensor, pressure sensor) or latent fingerprint images, the proposed fingerprint image algorithm requires further investigation to determine whether it will be able to improve the quality of the particular fingerprint image or not. It is obvious and clear that there is also a need for various fingerprint databases for which it is necessary to ask individuals to enrol their fingerprint images by means of different types of fingerprint sensors, and also a need to collect latent fingerprints on a variety of surfaces. This will need a long-term research effort and is part of a general problem about the lack of appropriate databases which is almost universally acknowledged by researchers in the fingerprint biometrics field.

Considering a feedback unit, which embedded a fingerprint image quality evaluation algorithm, this is a new approach for improving the usability of a fingerprint-based person recognition system. In this case, the tested online fingerprint databases were collected specifically for this study, and all in-house, with the result that only one fingerprint sensor was provided and an only limited number of fingerprint images were enrolled in these databases. Thus, the factors which have an influence on fingerprint image quality have been analysed based on this limited data, which implies that the algorithm has been investigated thoroughly only for matching the data specific to this test, and the experimental results obtained in the study cannot fully guarantee the robustness and reliability of such a feedback unit more generally. Although the study reported here provides important insights into how to guide a user via a interface to

interact with the biometric sensor correctly so as to improve the effectiveness of the data collection process, it is necessary to enlarge the online fingerprint databases to further and more comprehensively evaluate the performance of the feedback unit. Another important aspect which needs to be considered when designing a feedback unit is the execution time for the different feedback mechanisms. The provision of more information feedback to the user will generally result in the user spending more time to analyse this information, which obviously in turn can result in a slower interaction, and therefore may not be suitable for all application scenarios. This broader evaluation is an area which will benefit from further investigation in the future.

6.3 Chapter conclusions

This chapter has presented a summary of the research studies performed and the significant contributions of the study relating to the problem of obtaining an acceptable quality of fingerprint image, as well as providing some interesting finding to encourage further research to be developed in related research areas.

Initially, the work documented in this thesis explored the research problems with respect to fingerprint quality issues in fingerprint recognition systems, indicating how they are related and the impact which they may eventually have. Furthermore, in view of the interesting findings and contributions reported, some research areas have been briefly discussed which will encourage further directions in which to develop our research area in the future.

Reference

[1] Tabassi, Elham, C. Wilson, and C. Watson. "NIST fingerprint image quality." NIST Res. Rep. NISTIR7151 (2004): 34-36.

[2] Tabassi, Elham, and Charles L. Wilson. "A novel approach to fingerprint image quality." Image Processing, 2005. ICIP 2005. IEEE International Conference on. Vol. 2. IEEE, 2005.

[3] Jain, Anil, Patrick Flynn, and Arun A. Ross, eds. Handbook of biometrics. Springer Science & Business Media, 2007: 1-3.

[4] Maltoni, Davide, et al. Handbook of fingerprint recognition. Springer Science & Business Media, 2009.

[5] Radhika, K. S., and S. Gopika. "Online and Offline Signature Verification: A Combined Approach." Procedia Computer Science 46 (2015): 1593-1600.

[6] Zhao, Wenyi, et al. "Face recognition: A literature survey." ACM computing surveys (CSUR) 35.4 (2003): 399-458.

[7] Chen, Hong, and Anil K. Jain. "Dental biometrics: Alignment and matching of dental radiographs." Pattern Analysis and Machine Intelligence, IEEE Transactions on 27.8 (2005): 1319-1326.

[8] Delac, Kresimir, and Mislav Grgic. "A survey of biometric recognition methods." Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium. IEEE, 2004.

[9] Jain, Anil K., Arun Ross, and Salil Prabhakar. "An introduction to biometric recognition." Circuits and Systems for Video Technology, IEEE Transactions on 14.1 (2004): 4-20.

[10] Canuto, Anne MP, Fernando Pintro, and Michael C. Fairhurst. "An effective template protection method for face and voice cancellable identification."International Journal of Hybrid Intelligent Systems 11.3 (2014): 157-166.

[11] M. C. Fairhurst. “Biometrics and Universal Access,” in The Universal Access Handbook, CRC Press, 2009: 13–1 13–12.

[12] Suykens, Johan AK, and Joos Vandewalle. "Least squares support vector machine classifiers." Neural processing letters 9.3 (1999): 293-300.

[13] Haykin, Simon, and Neural Network. "A comprehensive foundation." Neural Networks 2.2004 (2004).

[14] Rabiner, Lawrence R., and Biing-Hwang Juang. "An introduction to hidden Markov models." ASSP Magazine, IEEE 3.1 (1986): 4-16.

[15] Rish, Irina. "An empirical study of the naive Bayes classifier." IJCAI 2001 workshop on empirical methods in artificial intelligence. Vol. 3. No. 22. IBM New York, 2001.

[16] Redner, Richard A., and Homer F. Walker. "Mixture densities, maximum likelihood and the EM algorithm." SIAM review 26.2 (1984): 195-239.

[17] Jain, Anil K., Arun Ross, and Umut Uludag. "Biometric template security: Challenges and solutions." Signal Processing Conference, 2005 13th European. IEEE, 2005.

[18] Rattani, Ajita, et al. "Template update methods in adaptive biometric systems: a critical review." Advances in Biometrics. Springer Berlin Heidelberg, 2009. 847-856.

[19] Y. Chen, "Law system seen in sale contracts from Dunhuang," Dunhuang research, vol. 66, no. 4, 2000.

[20] Grew, Nehemiah. "The Description and Use of the Pores in the Skin of the Hands and Feet, by the Learned and Ingenious Nehemiah Grew, MD Fellow of the College of Physicians and of the Royal Society." Philosophical Transactions 14.155-166 (1984): 566-567.

[21] Lambourne, Gerald. The fingerprint story. Harrap, 1984.

[22] Lee, Henry C., Robert Ramotowski, and R. E. Gaensslen, eds. Advances in fingerprint technology. CRC press, 2001: 21-23

[23] Hueske, Edward E. Firearms and Fingerprints. Infobase Publishing, 2008: 48-50.

[24] Holder, Eric Himpton, Laurie O. Robinson, and John H. Laub. The fingerprint sourcebook. US Department. of Justice, Office of Justice Programs, National Institute of Justice, 2011.

[25] Samsung, "Samsung Digital Door Lock," 2015. [Online]. Available: http://www.samsungdigitallife.com/.

[26] Clockrite, "FINGERPRINT CLOCKING SYSTEM," 2015. [Online]. Available: http://www.clockrite.co.uk/.

[27] Apple, “Apple Web Site,” 2015. [Online]. Available: www.apple.com.

[28] Transfarm, “Fingerprint and Palmprint Pads,” 2015. [Online]. Available: http://www.transfarm.pl/technika-kryminalistyczna/produkty-sirchie/daktyloskopowanie/poduszki-tusze-i-walki.html.

[29] Ashwini, Barbadekar, Ladhav Shivaji Digambarrao, and S. P. Patil. "Performance analysis of finger print sensors." Mechanical and Electronics Engineering (ICMEE), 2010 2nd International Conference on. Vol. 1. IEEE, 2010.

[30] Xie, Shan Juan, et al. "Fingerprint quality analysis and estimation for fingerprint matching." State of the art in Biometrics. Intech, Vienna. ISBN(2011): 978-953.

[31] Cappelli, Raffaele, et al. "Performance evaluation of fingerprint verification systems." Pattern Analysis and Machine Intelligence, IEEE Transactions on28.1 (2006): 3-18.

[32] Lee, Chulhan, Sanghoon Lee, and Jaihie Kim. "A study of touchless fingerprint recognition system." Structural, Syntactic, and Statistical Pattern Recognition. Springer Berlin Heidelberg, 2006. 358-365.

[33] Hiew, Bee Yan, Andrew BJ Teoh, and Ying-Han Pang. "Touch-less fingerprint recognition system." Automatic Identification Advanced Technologies, 2007 IEEE Workshop on. IEEE, 2007.

[34] “Optical fingerprint sensor,” 2015. [Online]. Available: http://www.aliexpress.com/store/product/DHL-fast-shipping-U-are-U4000B-optical-sensor-fingerprint-scanner-USB-free-shipping/912913_1502855894.html.

[35] “Ultrasound fingerprint sensor,” 2015. [Online]. Available: http://www.digitaltrends.com/mobile/sonavation-ultrasound-fingerprint-sensor-in-depth/#/2.

[36] “Capacitive sensor,” 2015. [Online]. Available: http://www.bromba.com/tdeikon2e.htm.

[37] “Thermal sensor,” 2015. [Online]. Available: http://www.neurotechnology.com/fingerprint-scanner-atmel-fingerchip.html.

[38] “Pressure sensor,” 2015. [Online]. Available: http://www.bromba.com/musbm01e.htm.

[39] Cappelli, Raffaele, Matteo Ferrara, and Davide Maltoni. "On the operational quality of fingerprint scanners." Information Forensics and Security, IEEE Transactions on 3.2 (2008): 192-202.

[40] J. Schneider, C. Richardson, and F. Kiefer, “On the correlation of image size to system accuracy in automatic fingerprint identification systems,” Audio-and Video-Based, 2003.

[41] G. Marcialis and F. Roli, “Fingerprint verification by fusion of optical and capacitive sensors,” Pattern Recognition Letters, 2004.

[42] Moenssens, Andre A. Fingerprint techniques. London: Chilton Book Company, 1971.

[43] Greenberg, Shlomo, et al. "Fingerprint image enhancement using filtering techniques." Pattern Recognition, 2000. Proceedings. 15th International Conference on. Vol. 3. IEEE, 2000.

[44] Kumar, L. Ravi, et al. "Fingerprint minutia match using bifurcation technique." S Sai Kumar et al, International Journal of Computer Science & Communication Networks 2.4 (2012): 478-486.

[45] Lee, Sanghoon, et al. "Fingerprint-quality index using gradient components."Information Forensics and Security, IEEE Transactions on 3.4 (2008): 792-800.

[46] Maio, Dario, et al. "FVC2000: Fingerprint verification competition." Pattern Analysis and Machine Intelligence, IEEE Transactions on 24.3 (2002): 402-412.

[47] Maio, Dario, et al. "FVC2002: Second fingerprint verification competition."Pattern recognition, 2002. Proceedings. 16th international conference on. Vol. 3. IEEE, 2002.

[48] Maio, Dario, et al. "Fvc2004: Third fingerprint verification competition."Biometric Authentication. Springer Berlin Heidelberg, 2004. 1-7.

[49] Cappelli, Raffaele, et al. "Fingerprint verification competition 2006."Biometric Technology Today 15.7 (2007): 7-9.

[50] “FVC2004 unveils worst-case scenario results,” Biometric Technology Today, vol. 12, no. 6. 2004: 2-4.

[51] Cybarcode Inc., “Identix Touch View II,” 2015. [Online]. Available: http://cybarcode.com/identix/data_collection_terminals/stationary/fingerprint/tv2-555.

[52] Antonelli, Athos, et al. "Fake finger detection by skin distortion analysis."Information Forensics and Security, IEEE Transactions on 1.3 (2006): 360-373.

[53] SecuGen, “Hamster IV,” 2015. [Online]. Available: http://www.secugen.com/products/ph4.htm.

[54] NeuroTechnology, “VeriFinger,” 2015. [Online]. Available: http://www.neurotechnology.com/free-fingerprint-verification-sdk.html.

[55] Bazen, Asker M., et al. "A correlation-based fingerprint verification system." (2000).

[56] Liang, Xuefeng, and Tetsuo Asano. "Fingerprint matching using minutia polygons." Pattern Recognition, 2006. ICPR 2006. 18th International Conference on. Vol. 1. IEEE, 2006.

[57] Prabhakar, Salil, et al. "Minutia verification and classification for fingerprint matching." Pattern Recognition, 2000. Proceedings. 15th International Conference on. Vol. 1. IEEE, 2000.

[58] Li, Jiang, et al. "Integrating minutiae based fingerprint matching with local mutual information." Pattern Recognition, 2008. ICPR 2008. 19th International Conference on. IEEE, 2008.

[59] Marana, Aparecido Nilceu, and Anil K. Jain. "Ridge-based fingerprint matching using hough transform." Computer Graphics and Image Processing, 2005. SIBGRAPI 2005. 18th Brazilian Symposium on. IEEE, 2005.

[60] Greenberg, Shlomo, et al. "Fingerprint image enhancement using filtering techniques." Pattern Recognition, 2000. Proceedings. 15th International Conference on. Vol. 3. IEEE, 2000.

[61] Joun, Sungwook, et al. "An experimental study on measuring image quality of infant fingerprints." Knowledge-Based Intelligent Information and Engineering Systems. Springer Berlin Heidelberg, 2003.

[62] Hong, Lin, and Anil Jain. "Fingerprint enhancement." Automatic Fingerprint Recognition Systems. Springer New York, 2004. 127-143.

[63] Khalefa, Mustafa Salah, Zaid Amin Abduljabar, and Huda Ameer Zeki. "Fingerprint Image Enhancement By Develop Mehtre Technique." Advanced Computing: An International Journal (ACIJ) 2.6 (2011): 171-182.

[64] Hong, Lin, Yifei Wan, and Anil Jain. "Fingerprint image enhancement: algorithm and performance evaluation." Pattern Analysis and Machine Intelligence, IEEE Transactions on 20.8 (1998): 777-789.

[65] Hsieh, Ching-Tang, Eugene Lai, and You-Chuang Wang. "An effective algorithm for fingerprint image enhancement based on wavelet transform."Pattern Recognition 36.2 (2003): 303-312.

[66] Sherlock, Barry G., D. M. Monro, and K. Millard. "Fingerprint enhancement by directional Fourier filtering." Vision, Image and Signal Processing, IEE Proceedings-. Vol. 141. No. 2. IET, 1994.

[67] Zhang, Hong, and Xinsheng Wang. "A new fingerprint enhancement algorithm." Broadband Network and Multimedia Technology (IC-BNMT), 2010 3rd IEEE International Conference on. IEEE, 2010.

[68] Bartunek, Josef Strom, et al. "Adaptive fingerprint image enhancement with emphasis on preprocessing of data." Image Processing, IEEE Transactions on 22.2 (2013): 644-656.

[69] Fronthaler, Hartwig, Klaus Kollreider, and Josef Bigun. "Local features for enhancement and minutiae extraction in fingerprints." image processing, IEEE Transactions on 17.3 (2008): 354-363.

[70] “FVC2004,” 2004. [Online]. Available: http://bias.csr.unibo.it/fvc2004/.

[71] Bazen, Asker M., and Sabih H. Gerez. "Segmentation of fingerprint images."Proc. Workshop on Circuits Systems and Signal Processing (ProRISC 2001). Vol. 276280. 2001.

[72] Soille, Pierre. Morphological image analysis: principles and applications. Springer Science & Business Media, 2013: 1-8.

[73] Akram, M. Usman, et al. "Improved fingerprint image segmentation using new modified gradient based technique." Electrical and Computer Engineering, 2008. CCECE 2008. Canadian Conference on. IEEE, 2008.

[74] Akram, M. Usman, et al. "Fingerprint Image Segmentation Based on Boundary Values." VISAPP (1). 2008.

[75] Rao, A. Ravishankar, and Ramesh C. Jain. "Computerized flow field analysis: Oriented texture fields." IEEE Transactions on Pattern Analysis & Machine Intelligence 7 (1992): 693-709.

[76] Bazen, Asker M., and Sabih H. Gerez. "Systematic methods for the computation of the directional fields and singular points of fingerprints."Pattern Analysis and Machine Intelligence, IEEE Transactions on 24.7 (2002): 905-919.

[77] Maio, Dario, and Davide Maltoni. "Direct gray-scale minutiae detection in fingerprints." Pattern Analysis and Machine Intelligence, IEEE Transactions on 19.1 (1997): 27-40.

[78] Sherlock, Barry G., and Donald M. Monro. "A model for interpreting fingerprint topology." Pattern recognition 26.7 (1993): 1047-1055.

[79] Vizcaya, Pedro R., and Lester A. Gerhardt. "A nonlinear orientation model for global description of fingerprints." Pattern Recognition 29.7 (1996): 1221-1231.

[80] Gu, Jinwei, Jie Zhou, and David Zhang. "A combination model for orientation field of fingerprints." Pattern Recognition 37.3 (2004): 543-553.

[81] Li, Jun, Wei-Yun Yau, and Han Wang. "Constrained nonlinear models of fingerprint orientations with prediction." Pattern Recognition 39.1 (2006): 102-114.

[82] Wang, Yi, Jiankun Hu, and Damien Phillips. "A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing." Pattern Analysis and Machine Intelligence, IEEE Transactions on 29.4 (2007): 573-585.

[83] Tao, Xunqiang, et al. "Estimation of fingerprint orientation field by weighted 2D Fourier expansion model." Pattern Recognition (ICPR), 2010 20th International Conference on. IEEE, 2010.

[84] Wang, Yi, Jiankun Hu, and Fengling Han. "Enhanced gradient-based algorithm for the estimation of fingerprint orientation fields." Applied Mathematics and Computation 185.2 (2007): 823-833.

[85] Kass, Michael, and Andrew Witkin. "Analyzing oriented patterns." Computer vision, graphics, and image processing 37.3 (1987): 362-385.

[86] Lim, Eyung, Xudong Jiang, and WeiYun Yau. "Fingerprint quality and validity analysis." Image Processing. 2002. Proceedings. 2002 International Conference on. Vol. 1. IEEE, 2002.

[87] Van, Thien Hoang, and Hoang Thai Le. "Adaptive noisy fingerprint enhancement based on orientation consistency." Knowledge and Systems Engineering, 2009. KSE'09. International Conference on. IEEE, 2009.

[88] Yin, Yilong, Jie Tian, and Xiukun Yang. "Ridge distance estimation in fingerprint images: algorithm and performance evaluation." EURASIP Journal on Advances in Signal Processing 2004.4 (2004): 1-8.

[89] Kovacs-Vajna, Zs M., Riccardo Rovatti, and Mirko Frazzoni. "Fingerprint ridge distance computation methodologies." Pattern Recognition 33.1 (2000): 69-80.

[90] Maio, Dario, and Davide Maltoni. "Ridge-line density estimation in digital images." icpr. IEEE, 1998.

[91] Xie, Shan Juan, et al. "An optimal orientation certainty level approach for fingerprint quality estimation." Intelligent Information Technology Application, 2008. IITA'08. Second International Symposium on. Vol. 3. IEEE, 2008.

[92] InterNational Committee for Information Technology Standards, "Biometrie Sample Quality Standard Draft (Revision 4)", document number M1/06-0003, February 7, 2005.

[93] Alonso-Fernandez, Fernando, et al. "A comparative study of fingerprint image-quality estimation methods." Information Forensics and Security, IEEE Transactions on 2.4 (2007): 734-743.

[94] Jin, Changlong, et al. "Comparative assessment of fingerprint sample quality measures based on minutiae-based matching performance." Electronic Commerce and Security, 2009. ISECS'09. Second International Symposium on. Vol. 1. IEEE, 2009.

[95] Fairhurst, M. C., and C. McIntosh. "Assessing image characteristics for user feedback in biometric fingerprint identity verification tasks." (2005): 135-140.

[96] Marasco, Emanuela, Luca Lugini, and Bojan Cukic. "Exploiting quality and texture features to estimate age and gender from fingerprints." SPIE Defense+ Security. International Society for Optics and Photonics, 2014.

[97] Wang, Lidong, and Cheryl Ann Alexander. "Fingerprint Patterns and the Analysis of Gender Differences in the Patterns Based on the U Test."International Transaction of Electrical and Computer Engineers System 2.3 (2014): 88-92.

[98] Wu, Jun, et al. "A new approach for classification of fingerprint image quality." Cognitive Informatics, 2008. ICCI 2008. 7th IEEE International Conference on. IEEE, 2008.

[99] Xie, Shan Juan, et al. "Rule-based fingerprint quality estimation system using the optimal orientation certainty level approach." Biomedical Engineering and Informatics, 2009. BMEI'09. 2nd International Conference on. IEEE, 2009.

[100] Shen, LinLin, Alex Kot, and Waimun Koo. "Quality measures of fingerprint images." Audio-and Video-based Biometric Person Authentication. Springer Berlin Heidelberg, 2001.

[101] Bolle, Rudolf Maarten, Sharathchandra Umapatirao Pankanti, and Yi-Sheng Yao. "System and method for determining the quality of fingerprint images." U.S. Patent No. 5,963,656. 5 Oct. 1999.

[102] Chen, Yi, Sarat C. Dass, and Anil K. Jain. "Fingerprint quality indices for predicting authentication performance." Audio-and Video-Based Biometric Person Authentication. Springer Berlin Heidelberg, 2005.

[103] Chen, Tai Pang, Xudong Jiang, and Wei Yun Yau. "Fingerprint image quality analysis." Image Processing, 2004. ICIP'04. 2004 International Conference on. Vol. 2. IEEE, 2004.

[104] Awasthi, Abhishek, Krithika Venkataramani, and Avani Nandini. "Image quality quantification for fingerprints using quality-impairment assessment."Applications of Computer Vision (WACV), 2013 IEEE Workshop on. IEEE, 2013.

[105] Alonso-Fernandez, Bigun, et al., “Fingerprint Recognition,” in Guide to Biometric Reference Systems and Performance Evaluation, Springer, 2009: 51–88.
[106] Zhao, Yulan, Chunfeng Jiang, and Wei Xu. "Research and application of fingerprint image quality estimation." Information Engineering and Computer Science, 2009. ICIECS 2009. International Conference on. IEEE, 2009.
[107] Kawagoe, Masahiro, and Akio Tojo. "Fingerprint pattern classification."Pattern Recognition 17.3 (1984): 295-303.
[108] Ohtsuka, Tomohiko, et al. "Reliable detection of core and delta in fingerprints by using singular candidate method." Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on. IEEE, 2008.
[109] Efford, Nick. Digital image processing: a practical introduction using java (with CD-ROM). Addison-Wesley Longman Publishing Co., Inc., 2000.
[110] Ohtsuka, Tomohiko, and Takeshi Takahashi. "A new detection approach for the fingerprint core location using extended relation graph." IEICE transactions on information and systems 88.10 (2005): 2308-2312.
[111] ISO, SFSEN. "13407: 1999." Human-centred design processes for interactive systems.
[112] Theofanos, M., B. Stanton, and C. A. Wolfson. "Usability & biometrics: Ensuring successful biometric systems." National Institute of Standards and Technology (NIST) (2008): 23.
[113] Kukula, Eric P., Mathias J. Sutton, and Stephen J. Elliott. "The human–biometric-sensor interaction evaluation method: biometric performance and usability measurements." Instrumentation and Measurement, IEEE Transactions on 59.4 (2010): 784-791.
[114] Bhattacharya, Amit, Nancy Talbott, and Laurel Kincl. "Occupational Ergonomics: Principles and Applications." Patty's Toxicology.
[115] ISO, SFSEN. "9241-11. 1998." Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)–Part II Guidance on Usability.
[116] Mansfield, A. J. "Information technology: biometric performance testing and reporting-part 1: principles and framework." ISO/IEC (2006): 19795-1.

[117] Wong, Rita, et al. "Interactive quality-driven feedback for biometric systems." Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on. IEEE, 2010.

[118] Mavity, N. J., F. Deravi, and M. C. Fairhurst. "Adaptive User Agents for Intelligent Biometric Applications." Applications and Science in Soft Computing. Springer Berlin Heidelberg, 2004. 323-330.

[119] Russell, Stuart, Peter Norvig, and Artificial Intelligence. "A modern approach." Artificial Intelligence. Prentice-Hall, Egnlewood Cliffs 25 (1995): 27.

[120] National Institute of Standards and Technology, "NIST Biometric Image Software," 2011. [Online]. Available: http://www.nist.gov/itl/iad/ig/nbis.cfm.

[121] XnSoft, "XnConvert," [Online]. Available: http://www.xnview.com/en/xnconvert/.

[122] NeuroTechnology, "VeriFinger SDK Fingerprint identification for PC and Web solutions," 2010. [Online]. Available: http://www.neurotechnology.com/verifinger.html.