MULTI-STAGE ENHANCEMENT SCHEME FOR LOW QUALITY FINGERPRINT IMAGES

by

RAMAKRISHNA VIGHNA VENKATA LANKA

Presented to the Faculty of the Graduate School of

The University of Texas at Arlington in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

THE UNIVERSITY OF TEXAS AT ARLINGTON

May 2016

Acknowledgements

I would like to express my sincere gratitude to my advisor, Dr. K. R. Rao at the University of Texas at Arlington, for his excellent guidance, care, patience, and unwavering support whenever I ran into a trouble spot or had a question about my research or writing. I would like to thank him for allowing me to research on a topic of my interest. His persistence and attention to detail are qualities that I have always admired and have brought out the best of my efforts.

I would also like to thank Dr. Kambiz Alavi and Dr. Howard Russell for participating in my thesis committee. Without their passionate participation and input, the thesis defense could not have been successfully conducted. I am also grateful to the staff at the University of Texas at Arlington, for their enduring support during my graduate study and making me feel comfortable in a new country away from home.

Finally, I must express my very profound gratitude to my parents, my sister, my girlfriend and my friends for providing me with unceasing encouragement and support throughout my years of study and research, and writing this thesis. This accomplishment would not have been possible without them.

April 19, 2016

Abstract

MULTI-STAGE ENHANCEMENT SCHEME FOR

LOW QUALITY FINGERPRINT IMAGES

Ramakrishna Vighna Venkata Lanka, MS

The University of Texas at Arlington, 2016

Supervising Professor: K.R. Rao

Security and authentication go hand in hand in today's internet age. The population growth and increase in web-based services have posed a substantial risk of identity theft and fraud. The need for reliable authentication to protect one's belongings has become essential. The goal of such an authentication system is to recognize a person by validating his/her identity.

The traditional identity management systems which validate on the basis of knowledge and tokens such as passwords and identity cards are susceptible to theft and duplication. Hence these systems cannot suffice for reliable identity management. Biometrics on the other hand validate an individual on the basis of his personal traits such as face, retina, voice and fingerprint. Since the biometric traits cannot be duplicated, the biometric system has grown to become a popular identity management system.

The fingerprint biometric has proved to be the most viable option as one's fingerprint does not change with age, the ridge pattern on each finger is unique even between identical twins and the fingerprint matching process is relatively inexpensive compared to other forms of biometrics. Fingerprint recognition is predominantly feature-based and the features used have a physical interpretation. A feature-based method, as the name suggests, extracts explicit features from the image under consideration and

encodes these features into a feature set, which is subsequently used for matching. The process of fingerprint matching comes with its drawbacks. As the fingerprint is captured as an image, it is almost certain to be corrupted by noise. The quality of the acquired fingerprint image is affected by complex input factors like shape of the sensor and ridge distortion from a moist or dry finger. The quality of the image has a significant impact on the matching performance. Hence optimal de-noising of the acquired image is crucial.

Various image enhancement schemes are investigated and a two stage combination of spatial and frequency domain enhancement scheme is studied and enhanced as part of this research. The spatial domain enhancement aims to reconstruct broken ridges by image smoothening and the frequency domain enhancement aims to eliminate noise by using a directional bandpass filter which estimates the orientation and frequency of the ridges in the fingerprint.

The scheme is implemented using MATLAB. Different fingerprint quality metrics such as visual inspection, performance time, true minutiae ratio (TMR) and false minutiae ratio (FMR) are measured for the proposed scheme and state of the art schemes over the standard fingerprint print databases. Conclusions are drawn based on the results. The conclusions discuss about how much the scheme was able to enhance the fingerprint image compared to the current scheme.

Table of Contents

List of Illustrations

List of Tables

Chapter 1

Introduction

1.1. Personal identity management

Humans associate personal attributes with an individual to uniquely identify themselves. The typical attributes such as face, voice and other contextual attributes such as clothing are used to recognize each person. Each person has a set of attributes or characteristics that define his/her personal identity. A number of crucial societal applications like international border crossing, electronic commerce, and welfare disbursement are based on personal identity [1].

Authenticating the identity of the individual has never been more important in this age of identity theft, phishing and hacking. The exponential growth of population and migration of people has posed a large challenge to the effective and efficient functioning of the crucial societal applications. Also, the proliferation of web-based services (e.g., online banking) and the deployment of decentralized customer service centers (e.g., credit cards) have led to the risk of identity theft. Rising magnitude of identity theft and heightened concerns about national security have reinforced the need for reliable identity management systems. As a result, the answer to the question "Who are you?" has taken on a new dimension [2]. The solution to this is the implementation of a sophisticated identity management system that can efficiently record, maintain, and obliterate personal identities of individuals. An Identity management system plays a key role in fighting identity fraud and is essential to establishing the trust necessary in a number of applications. Examples of such applications include regulating international border crossings, restricting physical access to important facilities like nuclear plants or airports, controlling logical access to shared resources and information, performing remote financial transactions, or distributing social welfare benefits [1].

An identity management system has a fundamental task which is to establish the association between an individual and his/her personal identity. One must be able to determine a person's identity or verify the identity claim of an individual whenever required. This process is known as person recognition. A person can be recognized based on the following three basic methods: (a) what he/she knows, (b) what he/she possesses extrinsically, and (c) who he/she is intrinsically.

The first method relies on the fact that the individual has exclusive knowledge of some secret information (e.g., password, personal identification number, or cryptographic key), the second method assumes that the person has exclusive possession of an extrinsic token (e.g., identification card, driver's license, passport, physical key, or personal device such as a mobile phone). Examples of the first and second methods are shown in figure 1-1 [1].

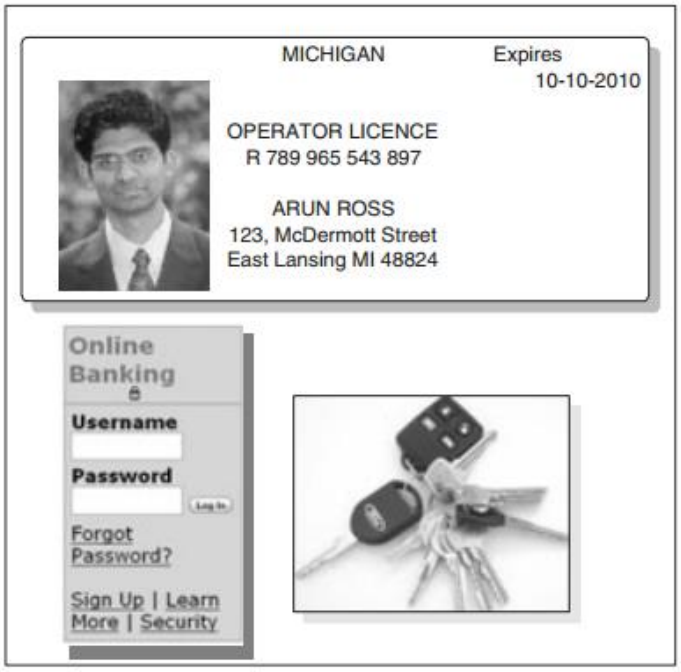


Figure 1-1 Traditional schemes to validate individuals [1]

The third method establishes the person's identity based on his/her inherent physical or behavioral traits and is known as biometric recognition. Formally, biometric recognition can be defined as the science of establishing the identity of an individual based on the physical and/or behavioral characteristics of the person either in a fully automated or a semi-automated manner. Examples of the third method are shown in figure 1-2 [1].

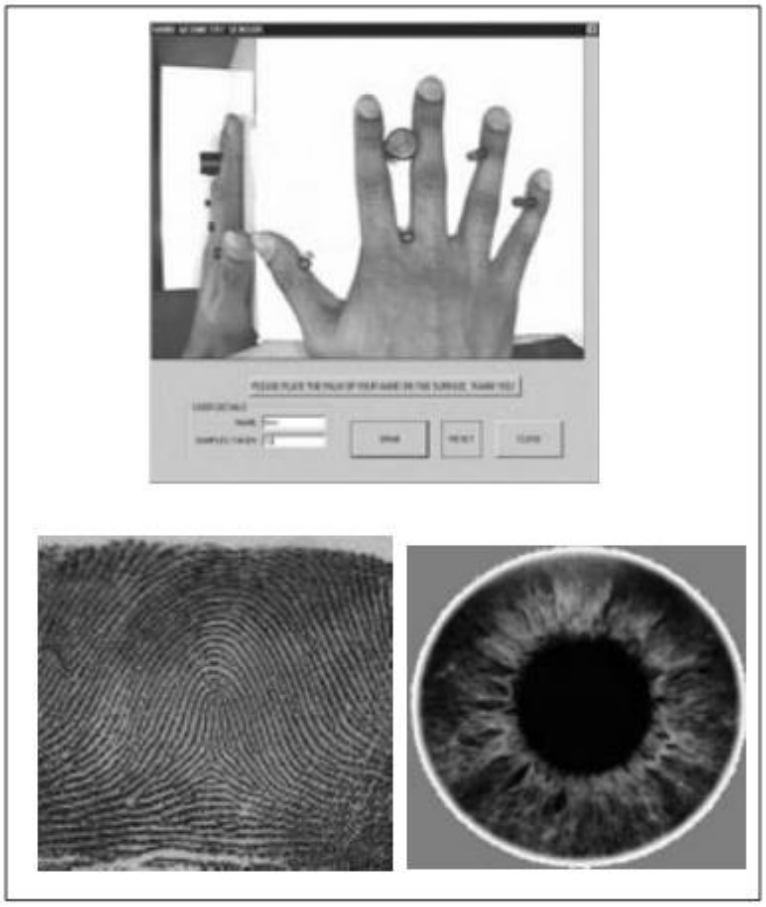


Figure 1-2 Biometrics to validate individuals [1]

1.2. Need for biometrics

Knowledge-based and token-based person recognitions rely on surrogate representations of identity such as passwords or identity cards. Most enterprises still use these traditional methods like a password or a passphrase which the user knows or like a key or a card which the user has. These traditional security solutions can easily be forgotten, lost or stolen [3]. Moreover, they cannot provide vital identity management functions like non-repudiation and detecting multiple enrollments by the same person under different identities. For example, individuals can easily deny using a service by claiming that their password had been stolen or guessed. Individuals can also conceal their true identity by presenting forged or duplicate identification documents. In addition, traditional mechanisms like passwords and tokens do not provide strong evidence for post-event person recognition, such as suspect identification at a crime scene. Therefore, it is becoming increasingly apparent that knowledge-based and token-based mechanisms alone are not sufficient for reliable identity management [6]. Biometric recognition, or simply biometrics, offers a natural and more reliable solution to the problem of person recognition. Since the biometric identifiers are inherent to an individual, it is more difficult to manipulate, share, or forget these traits. Hence, biometric traits constitute a strong and reasonably permanent link between a person and his identity [1].

Biometric identification has a faint whiff of the future about it, though what that future looks like depends entirely on your perspective. It could be a dystopian world, often seen in movies, novels, and comic books where Big Brother haunts the heroes, monitoring them through iris scans or facial recognition. Or it could be a sleek and polished future, where speaking an authorization code grants you control of a vehicle or glancing at a camera opens a locked door with a hushed hiss. Any person who presents his/her biometric identifier to a biometric system for the purpose of being recognized can

be called a user of the system [6]. Since biometric systems require the user to be present at the time of authentication, they can also deter users from making false repudiation claims. Moreover, only biometrics can establish whether a certain individual is already known to the identity management system, although the individual might deny it. This is especially critical in applications such as welfare disbursement, where an impostor may attempt to claim multiple benefits (i.e., double dipping). Due to these reasons, biometric recognition is being increasingly adopted in a number of government and civilian identity management applications either to replace or to complement existing knowledge-based and token-based mechanisms [1].

1.3. Biometric Systems

The term ‘biometrics’ is derived from the Greek words bio (life) and metric (to measure). In recent years, “Biometrics” has become the characteristic which is defined as a measurable biological and behavioral trait that can be used to recognize a person uniquely. Biometric systems have been researched and tested for several years, but widespread public use has only begun recently due to the need for individual recognition and content protection [5].

Biometric systems measure physical or behavioral characteristics information of an individual to determine or verify his identity. These characteristics are referred to by different terms such as traits, indicators, identifiers, or modalities. The several traits include fingerprints, face, iris, retina, voice, signature, gait, or the Deoxyribonucleic acid (DNA). There are two phases to the working of a biometric system, namely, enrollment and recognition [1].

Enrollment phase is where the biometric data is acquired from the individual and stored in a database along with the person’s identity. During the recognition phase, the

validation is done by acquiring the biometric data from the individual and compared with the stored data from the enrollment process. The biometric system consists of 4 basis components, which are sensor, feature extractor, database and matcher. The biometric system block representation is shown in figure 1-3 [1].

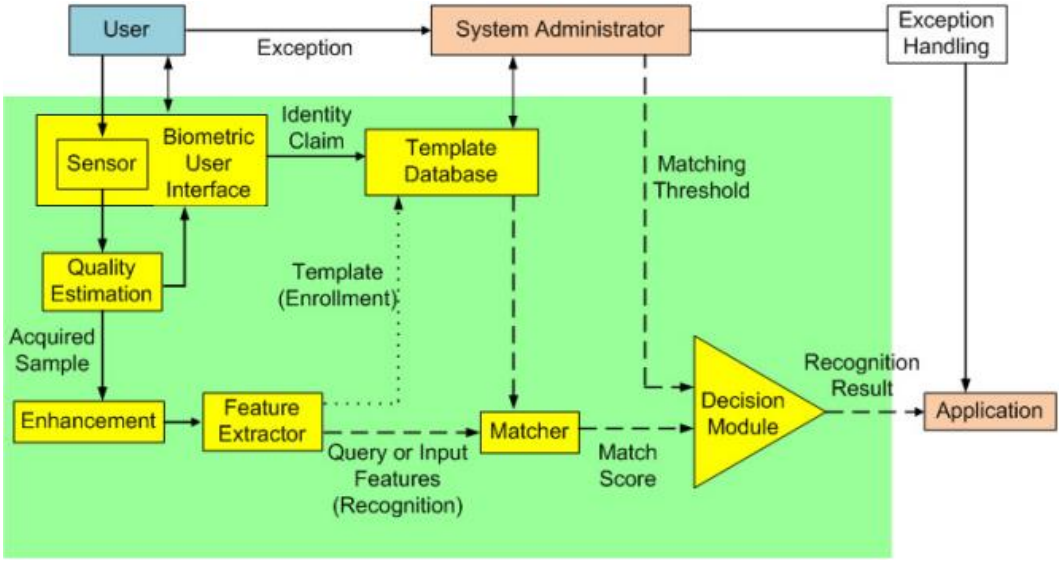


Figure 1-3 Block diagram of a biometric system [1]

1.3.1 Sensor module

A suitable user interface incorporating the biometric sensor or reader is needed to measure or record the raw biometric data of the user. For example, an optical fingerprint sensor may be used to image the friction ridge pattern at the tip of the finger. The design of a good user (or human-machine) interface is critical for the successful implementation of a biometric system. An intuitive, ergonomic, and easy to use interface may facilitate rapid user habituation and enable the acquisition of good quality biometric samples from the user [8].

1.3.2 Feature extraction module

Usually, the raw biometric data from the sensor is subjected to pre-processing operations before features are extracted from it. The three commonly used pre-processing steps are (a) quality assessment, (b) segmentation, and (c) enhancement. First, the quality of the acquired biometric samples needs to be assessed to determine its suitability for further processing. If the raw data is not of sufficient quality, there are two options. One can either attempt to re-acquire the data from the user or trigger an exception (failure alarm) alerting the system administrator to activate suitable alternate procedures (typically involving some form of manual intervention by the system operator). The next pre-processing step is known as segmentation, where the goal is to separate the required biometric data from the background noise. Detecting a face in a cluttered image is a good example of segmentation. Finally, the segmented biometric data is subjected to a signal quality enhancement algorithm in order to improve its quality and further reduce the noise. In the case of image data, enhancement algorithms [10] [11] like smoothing or histogram equalization may be applied to minimize the noise introduced by the camera or illumination variations. In some cases, these pre-processing steps may be inseparable from the actual feature extraction step [8].

1.3.3 Database

The biometric system database acts as the repository of biometric information. During the enrollment process, the feature set extracted from the raw biometric sample (i.e., the template) is stored in the database along with some personal identity information (such as name, Personal Identification Number (PIN), address, etc.) characterizing the user. One of the key decisions in the design of a biometric system is whether to use a centralized database or a decentralized one. Storing all the templates in a central database may be beneficial from a system security perspective, because the data can be

secured through physical isolation and by having strict access control mechanisms. On the other hand, compromise of a central database would have far greater implications than the compromise of one of the sites in the decentralized database. This is because malicious individuals (corrupt administrators or hackers) can abuse the biometric information stored in the database to compromise the privacy of innocent users [8].

1.3.4 Matching

The purpose of a biometric matcher is to compare the query features against the stored templates to generate match scores. The match score is a measure of the similarity between the template and the query. Hence, a larger match score indicates greater similarity between the template and the query. If a matcher measures the dissimilarity (instead of the similarity) between the two feature sets, the score is referred to as a distance score. A smaller distance score indicates greater similarity. In a fingerprint-based biometric system, the number of matching minutiae between the input and the template feature sets can be considered as the degree of similarity (match score). The match score may also be moderated based on the quality of the presented biometric data. The matcher module also encapsulates a decision making module, in which the match scores are used to either validate a claimed identity or provide a ranking of the enrolled identities in order to identify an individual.

1.3.5 Types of Biometrics characteristics

Face recognition analyzes facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. This technique has attracted considerable interest, although many people do not completely understand its capabilities. Some vendors have made extravagant claims - which are very difficult, if not impossible, to substantiate in practice - for facial recognition devices. Because facial scanning needs an extra peripheral not customarily included with basic personal

computers (PC), it is more of a niche market for network authentication. However, the casino industry has capitalized on this technology to create a facial database of scam artists for quick detection by security personnel [7].

Fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching minutiae; others use straight pattern-matching devices; and still others are a bit more unique, including things like moiré fringe patterns and ultrasonic. Some verification approaches can detect when a live finger is presented; some cannot. A greater variety of fingerprint devices is available than for any other biometric. As the prices of these devices and processing costs fall, using fingerprints for user verification is gaining acceptance - despite the common - criminal stigma. Fingerprint verification may be a good choice for in-house systems, where you can give users adequate explanation and training, and where the system operates in a controlled environment. It is not surprising that the workstation access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices [7].

Iris based biometric [7], on the other hand, involves analyzing features found in the colored ring of tissue that surrounds the pupil. Iris scanning, undoubtedly the less intrusive of the eye-related biometrics, uses a fairly conventional camera element and requires no close contact between the user and the reader. In addition, it has the potential for higher than average template-matching performance. Iris biometrics work with glasses in place and is one of the few devices that can work well in identification mode. Ease of use and system integration have not traditionally been strong points with iris scanning devices, but one can expect improvements in these areas as new products emerge [7].

Voice authentication is not based on voice recognition but on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics has the most potential for growth, because it requires no new hardware — most PCs already contain a microphone. However, poor quality and ambient noise can affect verification. In addition, the enrollment procedure has often been more complicated than with other biometrics, leading to the perception that voice verification is not user friendly. Therefore, voice authentication software needs improvement. One day, voice may become an additive technology to finger-scan technology. Because many people see finger scanning as a higher authentication form, voice biometrics will most likely be relegated to replacing or enhancing PINs, passwords, or account names [7].

1.4. Thesis Outline

Chapter 2 describes the fingerprint biometric, the important features in a fingerprint and fingerprint matching system. Chapter 3 explains the need for image enhancement of fingerprint images in a fingerprint biometric system and the various image enhancement techniques. Also chapter 3 explains the various state of the art and novel fingerprint image enhancement algorithms. Chapter 4 describes the enhancement algorithm developed in this thesis. Chapter 5 shows the thesis enhancement results discussing about how well the proposed algorithms performed. Chapter 6 sums up the conclusions that can be drawn from the results and also discusses the future areas of research in the same direction.

Chapter 2

The Fingerprint biometric

2.1. Introduction

Finger-scan technology is the most widely deployed biometric technology, with a number of different vendors offering a wide range of solutions [5]. The fingerprint biometric provides a high level of recognition accuracy. The growing market of low-cost small-size acquisition devices, allowing its use in a broad range of applications, e.g., electronic commerce, physical access, PC logon, etc., and the easy to use devices with non-complex user-system interaction are remarkable strengths of fingerprint recognition [8].

There are 2 types of skin on the body. Smooth skin with hair and oil glands as shown in figure 2-1 and skin which does not contain any hair or oil glands. The later type of skin is the type of skin which is present on the fingertip and is called fingerprint. Fingerprint is the pattern of intervening ridges and valleys on the tip of a finger as shown in figure 2-2. These fingerprints offer potential individuality which means that no two persons have the same fingerprint. The wide spread use of the fingerprints for personal identification began only in the 20^{th} century. Originally, the fingerprints were acquired by rolling an inked fingertip on a paper, but today advanced sensor technology has paved way to the design of solid-state sensors which are compact and low-cost. These sensors can rapidly image the finger to generate a digital representations of the finger which can be used for biometric analysis [1]. With the use of these sensors, Automated Fingerprint Identification Systems (AFIS) were developed to improve the efficiency and accuracy of fingerprint matching. Currently, almost every law enforcement agency worldwide relies on AFIS to match fingerprints. Growing concerns about homeland security and consumer fraud have prompted the use of fingerprint-based biometric systems in many non-forensic applications. In

fact, fingerprint-based biometric systems are so popular and successful that they have become synonymous with the notion of biometric recognition in the minds of the general public [1].

Figure 2-1 Smooth skin [1]

Figure 2-2 Friction ridge skin on the fingertips [1]

The pattern of ridges on each finger is claimed to be unique and immutable, enabling its use as a mark of identity. In fact, even identical twins can be differentiated based on their fingerprints. Superficial injuries such as cuts and bruises on the finger surface alter the pattern in the damaged region only temporarily. Indeed, the ridge structure has been observed to reappear after the injury heals [1].

2.2. How the fingerprint biometric works

Fingerprint recognition is predominantly feature-based and the features used have a physical interpretation. A feature-based method, as the name suggests, extracts explicit features from the image under consideration and encodes these features into a feature set, which is subsequently used for matching. Figure 2-3 shows a grayscale image of a fingerprint [1].

Figure 2-3 Grayscale fingerprint image [1]

For optimal feature extraction, the image is enhanced and thinned to be represented as s a ridge skeleton image in which each ridge is only one-pixel wide shown in figure 2-4.

Figure 2-4 Enhanced and thinned fingerprint image [1]

The locations where a ridge emerges, ends, splits, or merges with another ridge are termed as ridge characteristics or minutiae. In addition to its location, a minutia generally has two other properties: direction and type. The direction of a minutia is along the local ridge orientation. Figure 2-5 shows that there are two basic types of minutiae: ending (also called ‘termination’) and bifurcation [1].

Figure 2-5 Ridge ending and bifurcation [1]

A minutiae set, consisting of all the minutiae in a fingerprint, is an abstract representation of the ridge skeleton. Minutiae-based representations are extensively used in automated fingerprint recognition systems, primarily due to the following reasons: (a) minutiae capture much of the discriminative or individuality information in fingerprints, (b) minutiae-based representations are storage efficient, and (c) minutiae extraction is reasonably robust to various sources of degradation [1].

Once the thinned ridge image is available, the ridge pixels with three ridge pixel neighbors are identified as ridge bifurcations and those with only one ridge pixel neighbor are identified as ridge endings. The minutiae set is then matched with a template to compute the match score based on the corresponding minutiae points. Figure 2-6 shows the matching algorithm [1] [4].

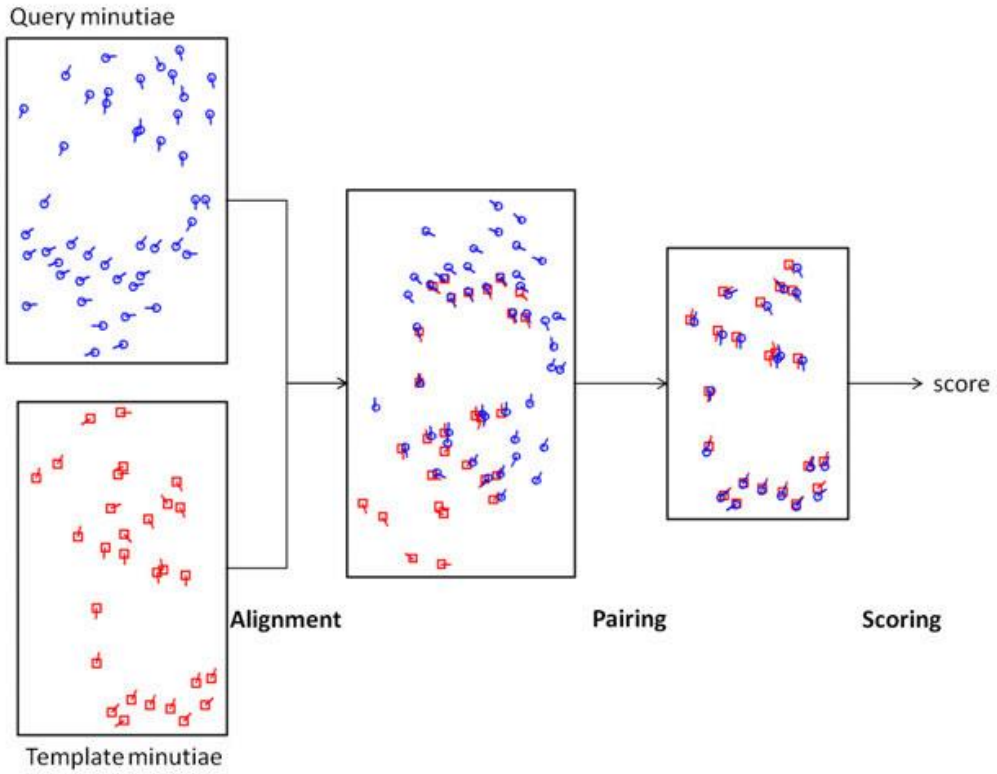


Figure 2-6 Minutiae matching process [1]

Computer vision matching algorithms [1] are used to match paired features. Figure 2-7 shows that a high score is generated when fingerprints match. Figure 2-8 shows that a very low score is generated when fingerprints do not match [5] [1].

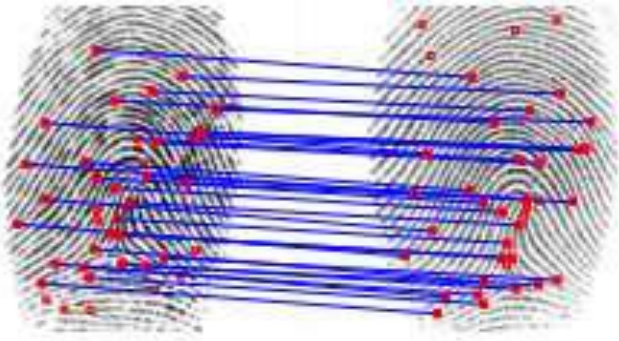


Figure 2-7 A genuine pair with maximum matched minutiae [1]

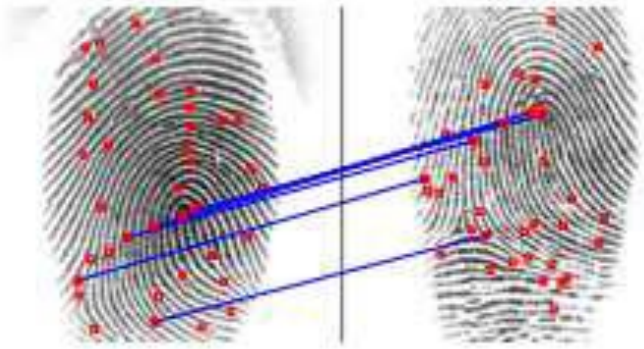


Figure 2-8 An imposter pair with very few matched minutiae [1]

Fingerprint recognition, whether done manually by a human expert or automatically by a machine, is predominantly feature-based (as opposed to image-based) and the features used have a physical interpretation. The terms feature-based and image-based are widely used in the computer vision literature to indicate the methods used for representing and matching images such as fingerprints. A feature-based method, as the name suggests, extracts explicit features from the image under

consideration and encodes these features into a feature set, which is subsequently used for matching. An image-based method, on the other hand, directly uses the image for matching without explicitly extracting any features from it [1].

First the different types of features that can be extracted from a fingerprint are introduced, followed by a description of the histology of friction ridge skin and its formation. Knowledge of these two topics is essential in understanding the uniqueness and permanence of friction ridge patterns, which are the two fundamental premises in fingerprint recognition [1].

2.2.1. The crucial features

The details in a fingerprint can be characterized at three different levels ranging from coarse to fine. Under ideal conditions, coarse level features can be derived from the finer levels of fingerprint representation.

2.2.1.1. Level 1 features

At the first level, a fingerprint is represented as a ridge orientation map as shown in figure 2-9. The orientation map records the local ridge orientation and the local ridge frequency at each location in the fingerprint. A fingerprint is often referred to as an oriented texture pattern since its global shape and structure can be defined by the orientation and frequency of its ridges. In Level 1 detail, only the ridge flow and ridge frequency are observed; the exact location and dimensional details of ridges are ignored. Thus, low-resolution image sensors capable of scanning 250 pixels per inch (ppi) can be used to observe the Level 1 details of a fingerprint [1].

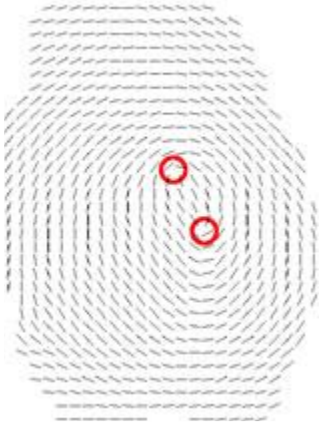


Figure 2-9 Level 1 orientation map [1]

The local ridge orientation at a pixel (x,y) represents the tangential direction of ridge lines passing through the pixel (x,y). Ridge orientation is defined in the range [0,π). Thus, the ridge orientation map can be viewed as a unit-length vector field whose direction is defined between 0 and π. Local ridge frequency at (x,y) is the average number of ridges per unit length along a line segment centered at (x,y) and normal to the local ridge orientation. Ridge frequency is the reciprocal of the ridge period. The ridge orientation at a pixel p is illustrated in Figure 2-10, which shows a portion of a fingerprint with ridges indicated as dark lines with the ridge orientation θ and ridge period 'ab' (reciprocal of ridge frequency) marked at a pixel p. Generally, the ridge orientation information is viewed as being more important than the ridge frequency information for fingerprint matching and classification purposes.

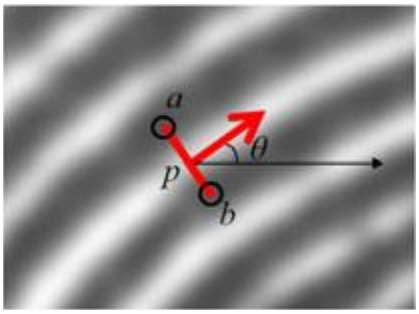


Figure 2-10 Ridge orientation estimation [1]

A ridge orientation map contains salient locations where the ridge orientations change abruptly. These salient locations are termed as singular points. There are two basic types of singular points - loop and delta. The two types are visually distinctive. A loop-type singularity, also called the core, refers to a local area where a set of ridges enters from one direction and exits in the same direction as shown in figure 2-11. A loop in a fingerprint can be used as a landmark point to align the fingerprint core. Generally, the core point corresponds to the north most loop-type singular point in a fingerprint; if a fingerprint does not contain any singular points, the core usually refers to the point of maximum ridge curvature. However, the term core itself is often used to indicate a loop-type singularity in practice. A delta-type singularity indicates a local area where three ridge systems appear to meet as shown in figure 2-12. The set of singular points in a fingerprint can be viewed as an abstract representation of the orientation map so that the orientation map can be roughly predicted based on the number and location of singular points. An even more abstract representation of the orientation map is the pattern type (often referred to as a fingerprint class), which can be deduced based on the number of loops and deltas, and the spatial relationship between them. Singularities in most fingerprints are observed to satisfy the following constraints: (a) the numbers of loops and deltas in a full print are the same; in other words, loops and delta appear in pairs; and (b) the total number of singular points are either 0, 2, or 4 [1].

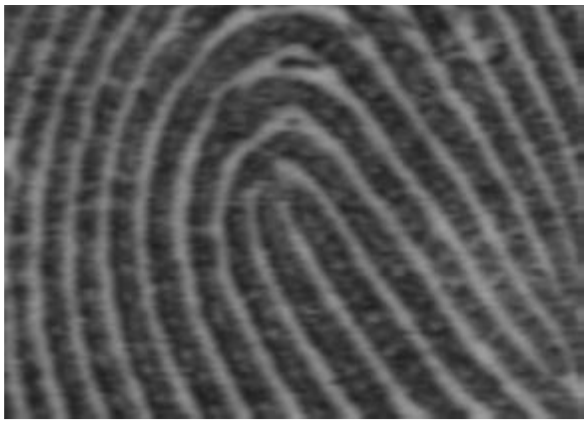


Figure 2-11 Loop singularity [1]

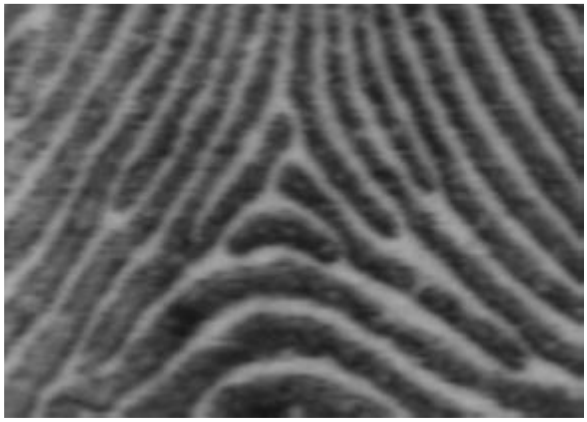


Figure 2-12 Delta singularity [1]

2.2.1.2. Level 2 features

In the second level, a fingerprint is represented as a ridge skeleton image in which each ridge is only one-pixel wide as seen in figure 2-4. At this level, the exact locations of the ridges are recorded, but the geometric and dimensional details of the ridges are ignored. The locations where a ridge emerges, ends, splits, or merges with another ridge are termed as ridge characteristics or minutiae. In addition to its location, a minutia generally has two other properties: direction and type. The direction of a minutia is along the local ridge orientation. There are two

basic types of minutiae: ending (also called ‘termination’) and bifurcation. Figure 2-13 shows the two basic types of minutiae. Thus, each minutia can be characterized by its (a) location in the image, (b) direction, and (c) type. Level 2 details of a fingerprint can be easily observed in images acquired at a resolution of 500 ppi. The number of minutiae found in a fingerprint varies a lot according to the acquisition method and other factors [1].

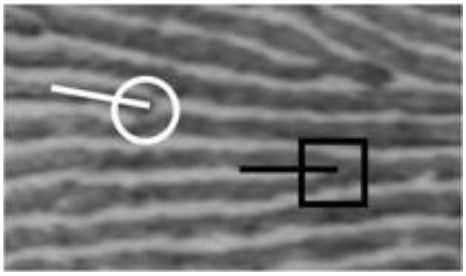


Figure 2-13 Ridge ending denoted by the white circle and ridge bifurcation denoted by the black square [1]

A minutiae set, consisting of all the minutiae in a fingerprint, is an abstract representation of the ridge skeleton in the sense that the minutiae set captures most of the discriminative information at Level 2, and ridge skeletons can be approximately derived from the minutiae information alone. Minutiae-based representations are extensively used in automated fingerprint recognition systems, primarily due to the following reasons: (a) minutiae capture much of the discriminative or individuality information in fingerprints, (b) minutiae-based representations are storage efficient, and (c) minutiae extraction is reasonably robust to various sources of degradation. The spatial distribution of minutiae in a fingerprint is an interesting topic of study that has gained increased attention due to the need for assessing the individuality of fingerprints using minutiae information alone [1].

2.2.1.3. Level 3 features

In the third level, a fingerprint is represented using both the inner holes (sweat pores) and outer contours (edges) of the ridges. So the ridges are no longer viewed as being simple, one-pixel

wide skeletal images. Rather, information embedded within the ridges are observed in detail. Incipient ridges and dots are also included at this level. Incipient ridges are immature ridges, which are thinner than mature ridges and contain no sweat pores. A dot is a very short ridge containing only a single ridge unit. With advances in fingerprint sensing technology, many large sensors are now equipped with 1000 ppi scanning capability that is needed to capture the Level 3 details in a fingerprint [1]. Figure 2-14 shows a fingerprint with level 3 features like ridge contours, pores and dots.

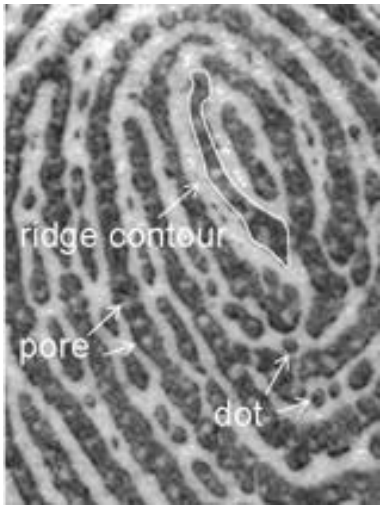


Figure 2-14 Level 3 features [1]

2.2.1.4. Additional features

Fingerprints often have other features such as creases, cuts, and scars. While these features are not inherent to fingerprint formation, they may become permanent depending on the severity of cuts and scars. However, since these features are not as universal as the three levels of features discussed earlier, their utility in fingerprint matching is limited. In fact, such abnormalities are often the source of matching errors [1].

2.2.2. The system

The main modules of a fingerprint biometric system are: a) fingerprint sensing, in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation; b) preprocessing, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction; c)feature extraction, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors; and d) matching, in which the feature vector of the input fingerprint is compared against one or more existing templates. The templates of approved users of the biometric system, also called clients, are usually stored in a database. Clients can claim an identity and their fingerprints can be checked against stored fingerprints [8]. Figure 2-15 shows the structure of a basic fingerprint biometric system.

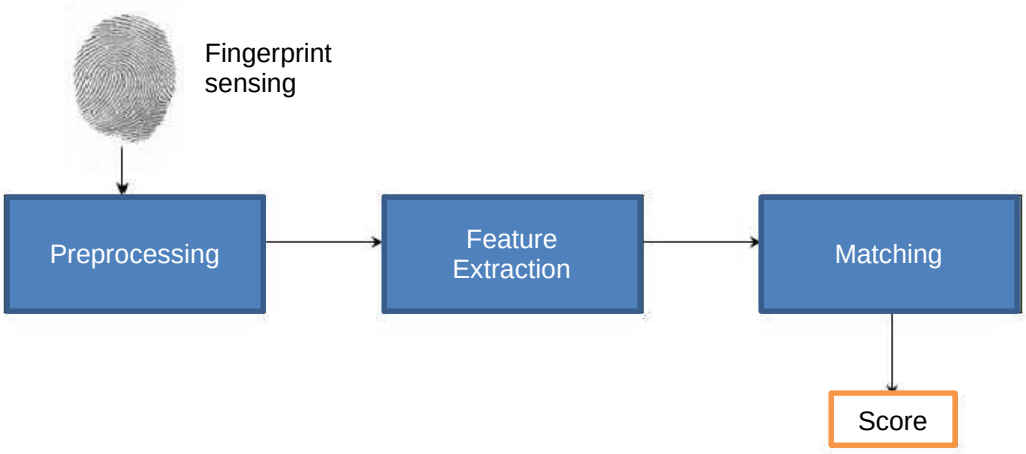


Figure 2-15 Basic fingerprint biometric system structure [4]

2.2.2.1. Fingerprint Sensing

The acquisition of fingerprint images [4] has been historically carried out by spreading the finger with ink and pressing it against a paper card. The paper card is then scanned, resulting in a digital representation. This process is known as off-line acquisition and is still used in law enforcement applications. Currently, it is possible to acquire fingerprint images by pressing the finger against the flat surface of an electronic fingerprint sensor. This process is known as online acquisition [8].

There are various types of fingerprint sensors. The most popular types are Solid-state sensors and Optical sensors. The solid-state sensors have found application in the latest smartphones and gadgets as they are compact and they do not have optical components. The solid-state sensor has a capacitive plate consisting of pixels which covert ridge-valley contact information into an electrical signal. Figure 2-16 shows the principle of a solid-state sensor.

The optical sensors are much more accurate but are not compact. Here, the finger touches a glass prism which is illuminated with diffused light, which is reflected at

the valleys and absorbed at the ridges. The reflected light is focused onto an image sensor which generates the fingerprint image. The image sensors used are charge-couple device (CCD) or complementary metal-oxide semiconductor (CMOS) image sensors. Figure 2-17 shows the principle of an optical sensor.

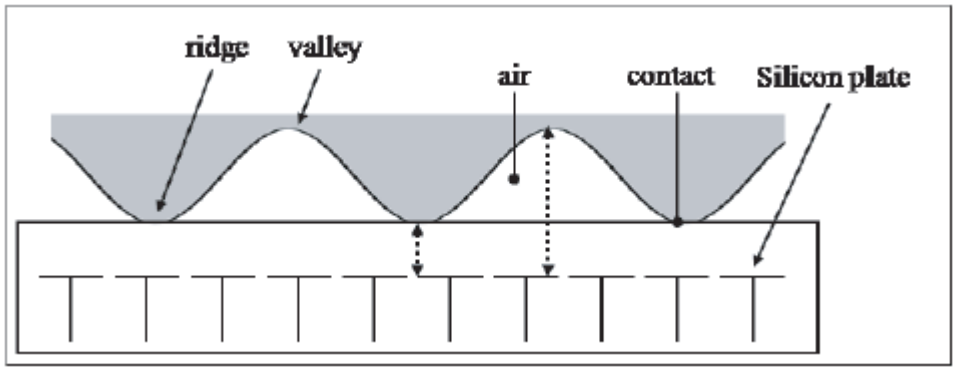


Figure 2-16 Solid-state sensor [8]

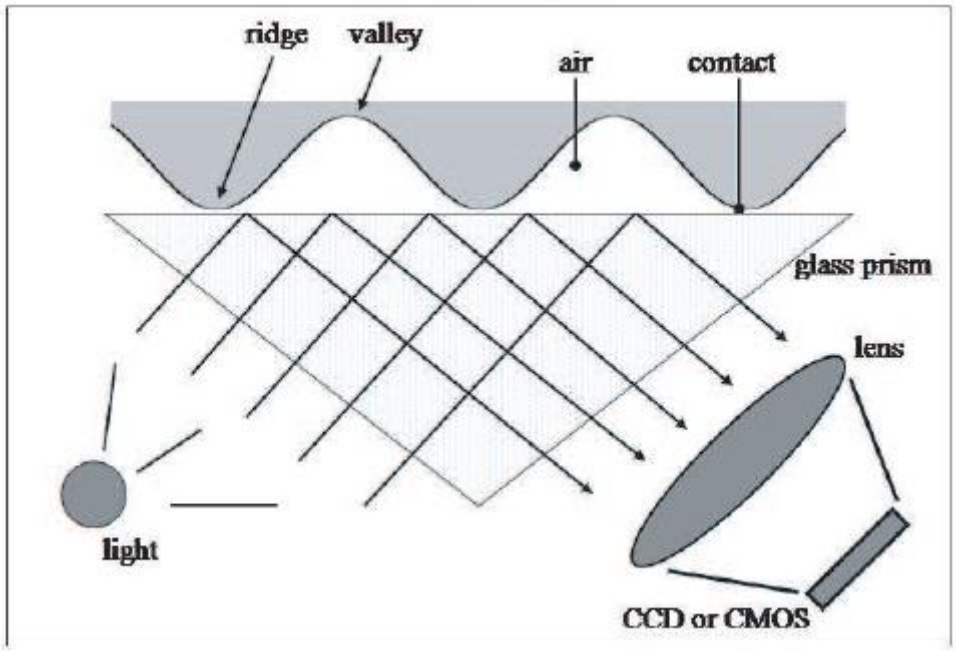


Figure 2-17 Optical sensor [8]

2.2.2.2. Preprocessing

The quality of the acquired fingerprint image has a significant impact on the performance of feature extraction and matching. Important factors that determine fingerprint quality include image resolution, finger area, and clarity of ridge pattern [8].

In most forensic and biometric applications, an image resolution of 500 pixels per inch (ppi) is necessary for successful processing and matching. At this resolution, the distance between adjacent ridges is approximately 9 pixels. Law enforcement agencies have now started scanning fingerprints at 1000 ppi in order to capture Level 3 features. In civilian applications, fingerprint sensors with resolution lower than 500 ppi are often used to reduce the cost of the sensor [1].

The captured finger area of a fingerprint image is also an important factor impacting image quality. The clarity of ridge pattern is another important determinant of quality. Both the finger skin and the sensor have a large impact on the ridge clarity. In a good quality fingerprint, ridges continuously flow and adjacent ridges are well separated. When the finger is moist, adjacent ridges may be joined; when it is dry, the ridges may have many breaks; and the inherent quality of some fingers is poor. Figure 2-18 shows low quality fingerprints. The feature extraction algorithms rely on the quality of the image to be able to extract the minutiae features faithfully. The preprocessing stage enhances the low quality images to provide the feature extraction algorithms a good quality fingerprint image.

Figure 2-18 Examples of low quality fingerprint images: (a) dry finger, (b) wet finger, and (c) finger with many creases [1].

2.2.2.3. Feature extraction

Once the fingerprint image has been preprocessed, a feature extraction step is performed. Most of the fingerprint recognition systems are based on minutiae matching, so that reliable minutiae extraction is needed. The preprocessed fingerprint image is converted into a binary image, which is then thinned using morphology. The thinning step reduces the ridge thickness to one pixel, allowing straightforward minutiae detection. Figures 2-19 and 2-20 show the feature extraction process [8] [1].

Figure 2-19 Fingerprint image thinning and minutiae extraction process [8]

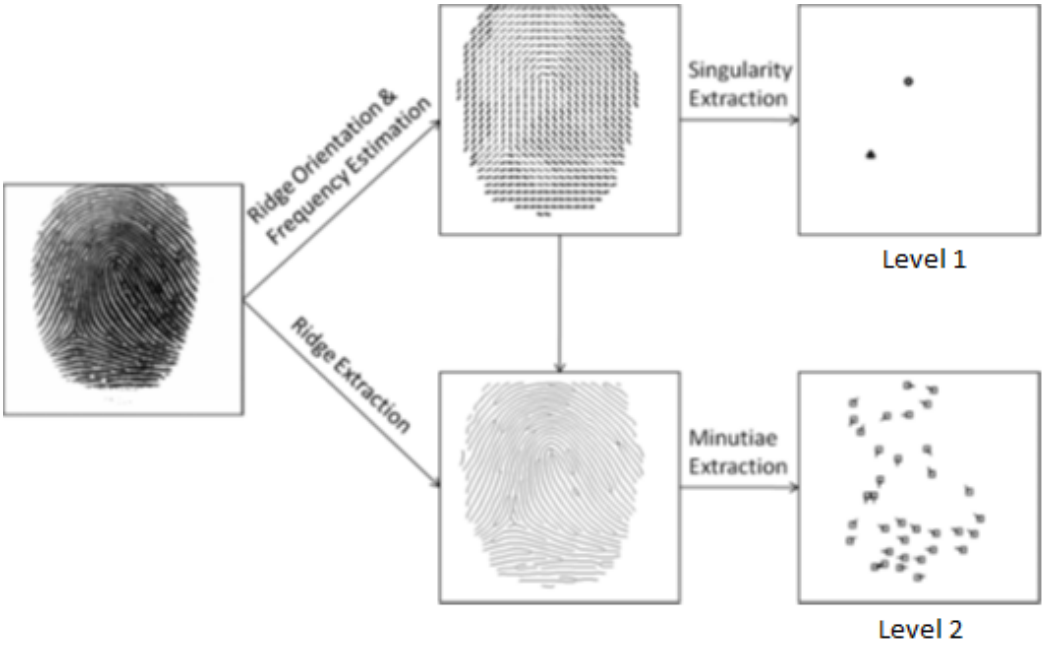


Figure 2-20 Schematic for the extraction of level 1 and level 2 features [1]

2.2.2.4. Fingerprint matching

In the matching step, features extracted from the input fingerprint are compared against those in a template, which represents a single user (retrieved from the system database based on the claimed identity). The result of such a procedure is either a degree of similarity (also called matching score) or an acceptance/rejection decision. There are fingerprint matching techniques that directly compare gray scale images (or sub-images) using correlation-based methods, so that the fingerprint template coincides with the gray scale image. However, most of the fingerprint matching algorithms use features that are extracted from the gray scale image [8].

Minutiae-based approaches are the most popular and widely used methods for fingerprint matching, since they are analogous with the way that forensic experts compare fingerprints [1]. A fingerprint is modeled as a set of minutiae, which are usually

represented by its spatial coordinates and the angle between the tangent to the ridge line at the minutiae position and the horizontal or vertical axis. The minutiae sets of the two fingerprints to be compared are first aligned, requiring displacement and rotation to be computed [1]. Figure 2-21 shows a successful match, whereas the figure 2-22 shows an unsuccessful match.

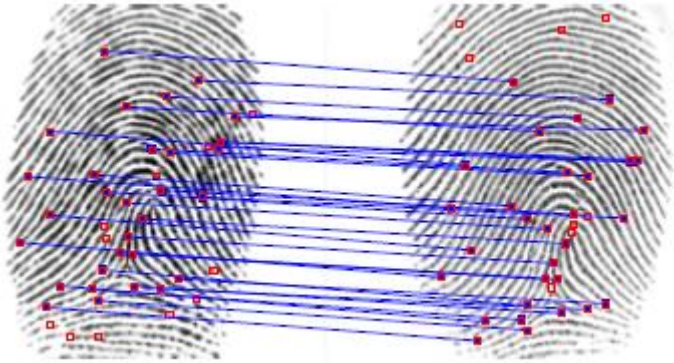


Figure 2-21 Successful match with a score = 614

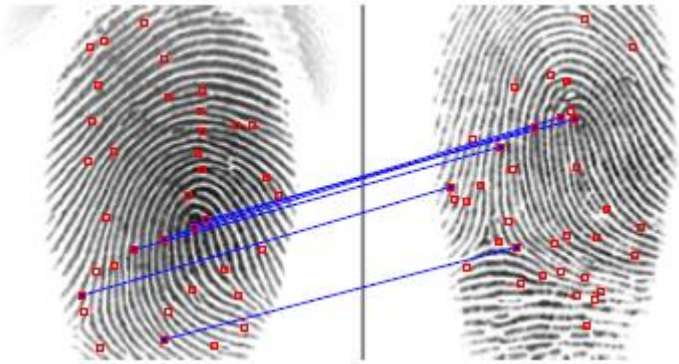


Figure 2-22 Unsuccessful match with a score = 7

2.3. Challenges

One of the open issues in fingerprint verification is the lack of robustness against image quality degradation [1]. The performance of a fingerprint recognition system is heavily affected by fingerprint image quality. Several factors determine the quality of a fingerprint image: skin conditions (e.g., dryness, wetness, dirtiness, temporary or permanent cuts and bruises), sensor conditions (e.g., dirtiness, noise, size), user cooperation, etc. Some of these factors cannot be avoided and some of them vary along time. Poor quality images result in spurious and missed features, thus degrading the performance of the overall system. Therefore, it is very important for a fingerprint recognition system to estimate the quality and validity of the captured fingerprint images. The degraded images can either reject or adjust some of the steps of the recognition system based on the estimated quality [1] [8].

Chapter 3

Fingerprint image enhancement

3.1 The need for fingerprint image enhancement

Automatic fingerprint matching depends on the comparison of the local ridge characteristics and their relationships to make a personal identification. A critical step in fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images, which is a difficult task. The performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In an ideal fingerprint image, ridges and valleys alternate and flow in a locally constant direction and minutiae are anomalies of ridges, i.e., ridge endings and ridge bifurcations. In such situations, the ridges can be easily detected and minutiae can be precisely located from the thinned ridges [13] [8]. Figure 3-1 shows a good quality fingerprint image scan.

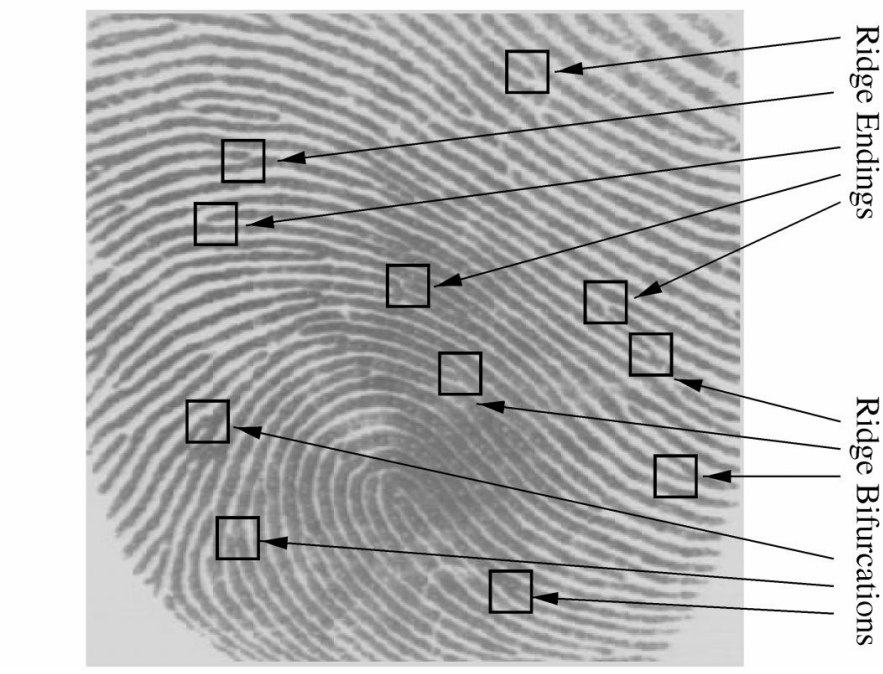


Figure 3-1 Good quality fingerprint scan [13]

In practice, due to variations in impression conditions, ridge configuration, skin conditions (aberrant formations of epidermal ridges of fingerprints, postnatal marks, occupational marks), acquisition devices, and non-cooperative attitude of subjects, etc., a significant percentage of acquired fingerprint images (approximately 10 percent according to experience) is of poor quality. The ridge structures in poor-quality fingerprint images are not always well-defined and, hence, they cannot be correctly detected. In order to ensure that the performance of the minutiae extraction algorithm will be robust with respect to the quality of input fingerprint images, an enhancement algorithm which can improve the clarity of the ridge structures is necessary. [13] [8].

Fingerprint enhancement can be conducted on either binary ridge images or gray-scale images. Binarization before enhancement will generate more spurious minutiae structures and lose some valuable original fingerprint information; it also poses more difficulties for later enhancement procedure, so it is an inherent limitation of this process. Different techniques [14] for gray-level fingerprint images enhancement have been proposed assuming that the local ridge frequency and orientation can be reliably estimated. The main reason for performing enhancement is to eradicate the noise in the fingerprint images, illuminate the parallel ridges and valleys, and protect their true configuration as shown in figure 3-2 [14].

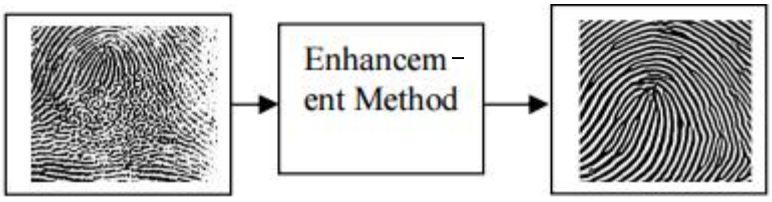


Figure 3-2 Fingerprint image enhancement process [14]

3.2 Image enhancement

There is no general theory of image enhancement. When an image is processed for visual interpretation, the viewer is the ultimate judge of how well a particular method works. Most of the quality checks have been used as a criterion, which determine image rejection, or a performance measurement of image enhancement algorithm. There have existed a variety of research activities along the stream of reducing noise and increasing the contrast between ridges and valleys in the gray-scale fingerprint images. Most popular among of them are spatial domain and frequency domain enhancement techniques [14] [11].

3.2.1 Spatial domain

Spatial domain refers to the image plane itself, and image processing methods in this category work on the principle of direct manipulation of pixels in an image. Spatial domain process can be denoted by the expression (1) [14] [11]:

$$g(x,y) = T[f(x,y)] \quad (1)$$

Where f(x,y) is the input image, g(x,y) is the output image and T is an operator defined over a neighborhood of the point (x,y).

3.2.2 Frequency domain

Frequency domain refers to the principle of modifying the Fourier transform of an image and then computing the inverse transform such as Discrete Fourier Transform (DFT) [20] to get back to input image. Thus given a digital image f (x,y), of size M x N, the basic filtering equation has the form (2) [14] [19] [8]:

$$g(x,y) = \tau^{-1}[H(u,v)F(u,v)] \quad (2)$$

Where τ^{-1} is the inverse discrete Fourier transform (IDFT), F (u,v) is the DFT of the input image f (x,y), H (u,v) is the filter function and g (x,y) is the filtered output image.

3.3 State of the art techniques

3.3.1 L. Hong et al. Orientation and frequency tuned Gabor filtering

The state of the art Parameter fingerprint enhancement technique is the method employed by L. Hong et al. [16], which is based on the convolution of the image with Gabor filters [19] tuned to the ridge orientation and ridge frequency. The main stages of this algorithm include normalization, ridge orientation estimation, ridge frequency estimation and filtering. Figure 3-3 shows the flowchart of the algorithm [13].

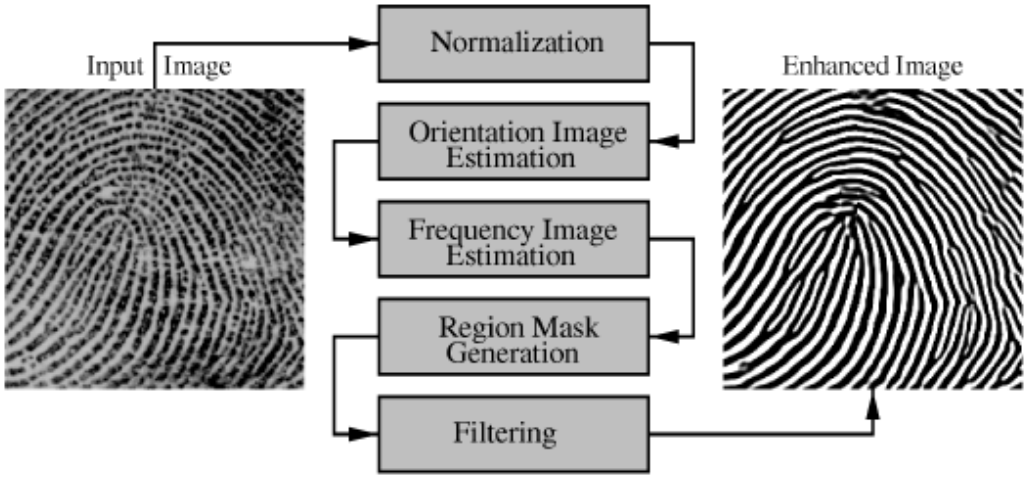


Figure 3-3 Flowchart of the L. Hong et al fingerprint enhancement algorithm [13]

3.3.1.1 Normalization

An input fingerprint image is normalized so that it has a pre specified mean and variance. Normalization is used to standardize the intensity values in an image by adjusting the range of grey-level values so that it lies within a desired range of values. Let I(i, j) represent the grey-level value at pixel (i, j), and G(i, j) represent the normalized grey level value at pixel (i, j). The normalized image is defined as:

$$G(i,j) = \begin{cases} M_0 + \sqrt{\frac{VAR_0\left(I(i,j)-M\right)^2}{VAR}} & \text{if } I(i,j) > M \\ M_0 - \sqrt{\frac{VAR_0\left(I(i,j)-M\right)^2}{VAR}} & \text{otherwise} \end{cases} \quad (3)$$

where M and VAR are the estimated mean and variance of I(i, j), and M_0 and VAR_0 are the desired mean and variance values, respectively. Normalization does not change the ridge structures in a fingerprint; it is performed to standardize the dynamic levels of variation in grey-level values, which facilitate the processing of subsequent image enhancement stages [13].

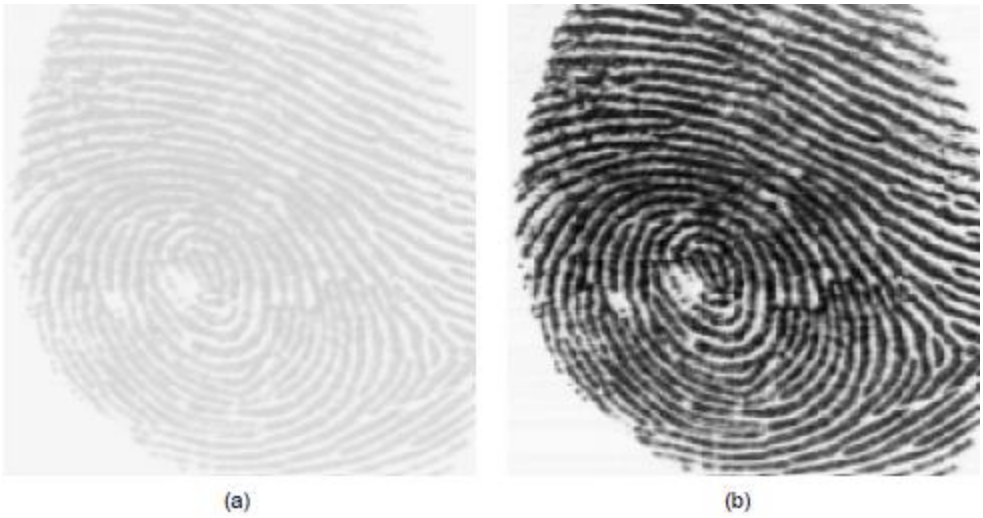


Figure 3-4 The result of normalization. (a) Input image. (b) Normalized image (M_0 =100, VAR_0 = 100). [13]

3.3.1.2 Orientation image estimation

The orientation image as shown in figure 3-5 represents an intrinsic property of the fingerprint images and defines invariant coordinates for ridges and valleys in a local neighborhood. By viewing a fingerprint image as an oriented texture, a least mean square

orientation estimation algorithm [13] has been developed. Given a normalized image, G, the main steps of the algorithm are as follows:

1) Divide G into blocks of size $w \times w$ (16 x 16).
2) Compute the gradients $\delta_x(i,j)$ and $\delta_y(i,j)$ at each pixel (i,j).
3) Estimate the local orientation of each block centered at pixel (i,j) by using the equations (5) (6) and (7):

$$V_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u,v)\partial_y(u,v) \tag{5}$$

$$V_y(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} \left(\partial_x^2(u,v)\partial_y^2(u,v)\right) \tag{6}$$

$$\theta(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{V_y(i,j)}{V_x(i,j)}\right) \tag{7}$$

where θ(i, j) is the least square estimate of the local ridge orientation at the block centered at pixel (i, j). Mathematically, it represents the direction that is orthogonal to the dominant direction of the Fourier spectrum of the w x w window. Due to the presence of noise, corrupted ridge and valley structures, minutiae, etc. in the input image, the estimated local ridge orientation, θ(i, j), may not always be correct. Since local ridge orientation varies slowly in a local neighborhood where no singular points appear, a low-pass filter can be used to modify the incorrect local ridge orientation [13].

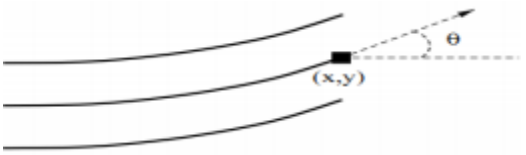


Figure 3-5 Orientation estimation at pixel (x,y) [13]

3.3.1.3 Ridge frequency image estimation

The gray levels along ridges and valleys can be modeled as a sinusoidal-shaped wave along a direction normal to the local ridge orientation as shown in figure 3-6. Therefore, local ridge frequency is another intrinsic property of a fingerprint image. Let G be the normalized image and O(i,j) be the orientation image, then the steps involved in local ridge frequency estimation are as follows [13]:

1) Divide G into blocks of size w x w (16 x 16).
2) For each block centered at pixel (i, j), compute an oriented window of size l x w (32 x 16) that is defined in the ridge coordinate system.
3) For each block centered at pixel (i, j), compute the x-signature, X[0], X[1],...X[l-1], of the ridges and valleys within the oriented window, where

$$\mathrm{X[k]} = \frac{1}{w}\sum_{d=0}^{w-1} \mathrm{G(u,v)}, \qquad \mathrm{k} = 0,1,\ldots\ldots,\mathrm{l}-1 \tag{8}$$

$$u = i + \left(d - \frac{w}{2}\right) cosO(i,j) + \left(k - \frac{l}{2}\right) sinO(i,j) \tag{9}$$

$$v = j + \left(d - \frac{w}{2}\right) sinO(i,j) + \left(\frac{l}{2} - k\right) cosO(i,j) \tag{10}$$

If no minutiae and singular points appear in the oriented window, the x-signature forms a discrete sinusoidal- shape wave, which has the same frequency as that of the ridges and valleys in the oriented window. Therefore, the frequency of ridges and valleys can be estimated from the x-signature. Let τ(i, j) be the average number of pixels between two consecutive peaks in the x-signature, then the frequency, Ω(i, j), is computed as: Ω(i, j) = τ^{-1}(i, j). If no consecutive

peaks can be detected from the x-signature, then the frequency is assigned a value of -1 to differentiate it from the valid frequency values.

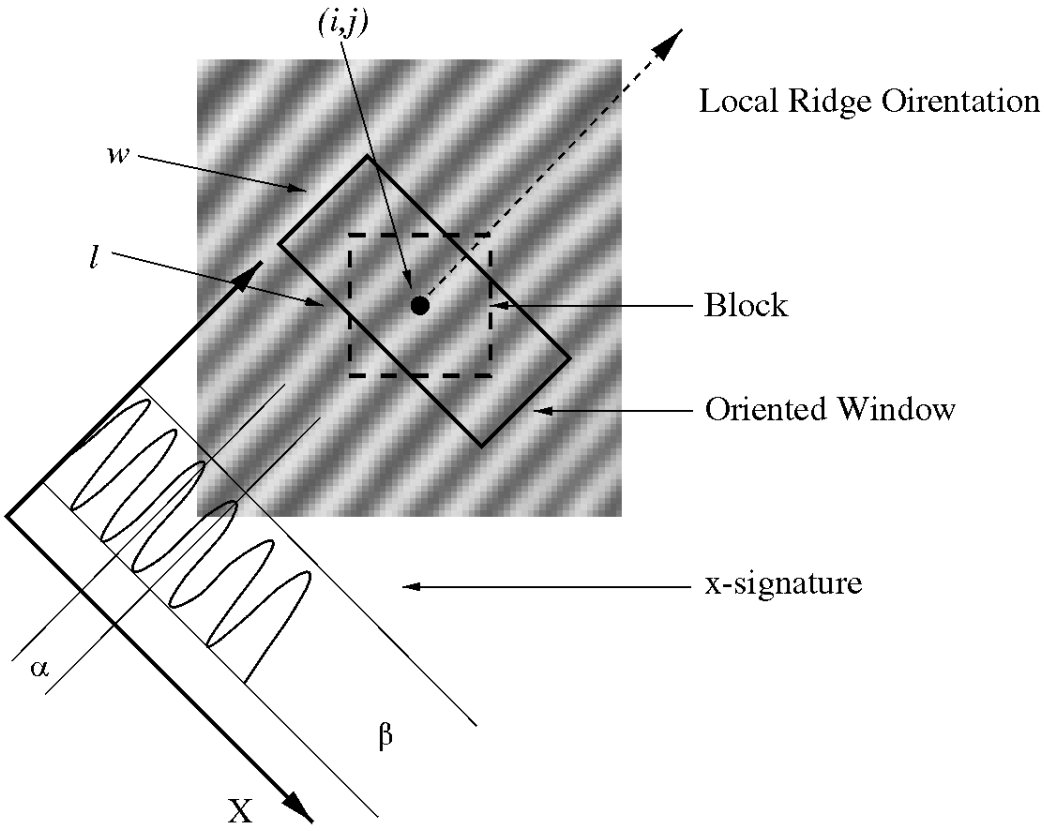


Figure 3-6 Oriented window method to estimate the ridge frequency [13]

3.3.1.4 Region mask generation

A pixel (or a block) in an input fingerprint image could be either in a recoverable region or an unrecoverable region. Classification of pixels into recoverable and unrecoverable categories can be performed based on the assessment of the shape of the wave formed by the local ridges and valleys. In this algorithm, three features are used to characterize the sinusoidal-shaped wave: amplitude (α), frequency (β), and variance (γ). Let X[1], X[2], ..., X[l] be the x-signature of a block centered at (i, j). The three features corresponding to pixel (block) (i, j) are computed as follows [13]:

1) α = (average height of the peaks - average depth of the valleys).

2) β = τ^{-1} (i, j), where τ (i, j) is the average number of pixels between two consecutive peaks.

3) γ = $\frac{1}{l}\sum_{i=0}^{l}\left(X[i]-\left(\frac{1}{l}\sum_{i=0}^{l}X[i]\right)\right)^2$

3.3.1.5 Filtering

The configurations of parallel ridges and valleys with well-defined frequency and orientation in a fingerprint image provide useful information which helps in removing undesired noise. The sinusoidal-shaped waves of ridges and valleys vary slowly in a local constant orientation. Therefore, a bandpass filter that is tuned to the corresponding frequency and orientation can efficiently remove the undesired noise and preserve the true ridge and valley structures. Gabor filters have both frequency-selective and orientation- selective properties. Therefore, it is appropriate to use Gabor filters as bandpass filters to remove the noise and preserve true ridge/valley structures [13] [19] [12].

The general form of a Gabor filter is represented as (10) [19]:

$$h(x,y:\phi,f)=exp\left\{-\frac{1}{2}\left[\frac{x_\phi^2}{\delta_x^2}+\frac{y_\phi^2}{\delta_y^2}\right]\right\}\cos(2\pi f x_\phi) \qquad (10)$$

where ϕ is the orientation of the Gabor filter, f is the frequency of a sinusoidal plane wave, and δ_x and δ_y are the space constants of the Gaussian envelope along x and y axes, respectively. The modulation transfer function (MTF) of the Gabor filter can be represented as (11) [13] [19].

$$H(u, v: \emptyset, f) =$$

$$2\pi\delta_x\delta_y exp\left\{-\frac{1}{2}\left[\frac{(u_\emptyset - u_0)^2}{\delta_u^2} + \frac{(v_\emptyset - v_0)^2}{\delta_v^2}\right]\right\} +$$

$$2\pi\delta_x\delta_y exp\left\{-\frac{1}{2}\left[\frac{(u_\emptyset + u_0)^2}{\delta_u^2} + \frac{(v_\emptyset + v_0)^2}{\delta_v^2}\right]\right\} \quad (11)$$

$$u_\emptyset = u\cos\emptyset + v\sin\emptyset \quad (12)$$

$$v_\emptyset = -u\cos\emptyset + v\sin\emptyset \quad (13)$$

$$u_0 = \frac{2\pi\cos\emptyset}{f} \quad (14)$$

Where $\delta_u = (1/2\pi)\delta_x$ and $\delta_v = (1/2\pi)\delta_y$.

In order to apply the Gabor filter to an image, the following three parameters must be specified:

1) Frequency of the sinusoidal plane wave, f.
2) Filter orientation, θ.
3) Standard deviations of the Gaussian envelope, δ_x and δ_y.

3.3.1.6 Implementation

In this algorithm, f is determined by the ridge frequency estimation step, θ is determined by the ridge orientation estimation step, and the δ_x and δ_y values are approximated based on empirical data. Let G be the normalized image, O be the orientation image, F be the frequency image, R be the recoverable mask, and w_g be the size of the Gabor filter. The enhanced image E is obtained by (15) [13]:

$$E(i,j) =$$

$$\begin{cases} 255 & if\ R(i,j) = 0 \\ \sum_{u=-{}^{w_g}/_2}^{{}^{w_g}/_2} \sum_{v=-{}^{w_g}/_2}^{{}^{w_g}/_2} h\big(u, v: O(i,j), F(i,j)\big) G(i-u, j-v) & otherwise \end{cases} \quad (15)$$

3.3.1.7 Results

Figure 3-7 is an image of the originally scanned fingerprint from the fingerprint scan sensor. Visually, the image is very hazy and the essential features required by the fingerprint system cannot be extracted from this image. Figure 3-8 is the resulting image which is enhanced by this algorithm. The ridge features much more prominent in the enhanced image.

Figure 3-7 Original scanned fingerprint [13]

Figure 3-8 Enhanced fingerprint image [13]

3.3.2 S. Chikkerur et al. Finger Fingerprint Image Enhancement Using STFT Analysis

Another state of the art fingerprint enhancement techniques is the method employed by Chikkerur et al [17], which is based Short Time Fourier Transform (STFT) analysis. STFT is a well-known technique in signal processing to analyze non-stationary signals. Here its application is extended to 2D fingerprint images. The algorithm simultaneously estimates all the intrinsic properties of the fingerprints such as the foreground region mask, local ridge orientation and local frequency orientation [17].

The technique is based on contextual filtering in the Fourier domain. The fingerprint image can be assumed as a system of oriented texture with non-stationary properties. Therefore, traditional Fourier analysis is not adequate to analyze the image completely. The properties of the image both in space and in frequency have to be resolved. The traditional one dimensional time-frequency analysis should be extended to two dimensional image signals to perform short (time/space)-frequency analysis [17].

The main steps of this algorithm are to compute the ridge orientation and ridge frequency images, define a region mask by computing an energy image to differentiate the fingerprint region from its background, compute the coherence image to adapt the angular bandwidth of the directional filter, and perform STFT enhancement to generate the final enhanced image. Figure 3-9 shows the flowchart of the algorithm [30].

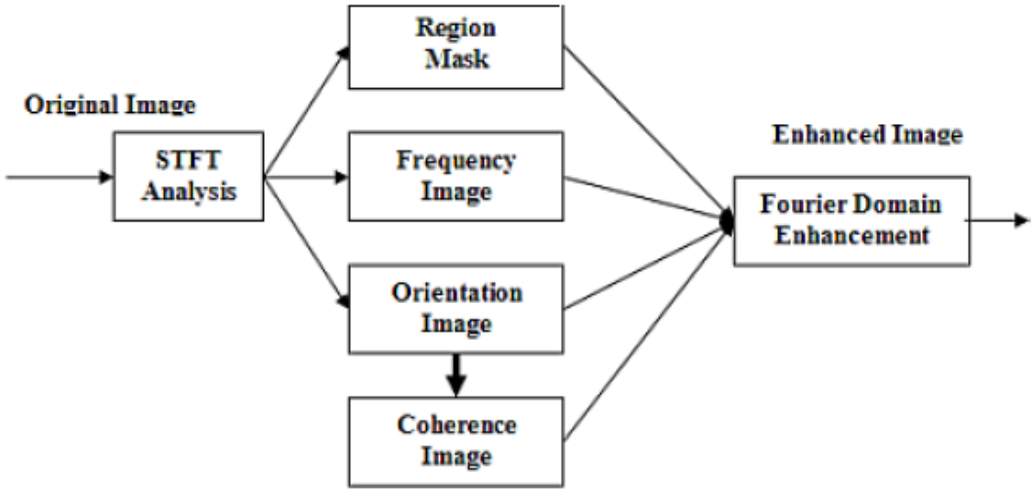


Figure 3-9 Flowchart of the STFT fingerprint enhancement algorithm [30]

3.3.2.1 Ridge orientation image

To compute the ridge orientation image, the orientation θ is assumed as a random variable that has the probability density function p(θ). The expected value of the orientation E{ θ } can then be obtained by performing a vector averaging according as (16) [17].

$$E\{\theta\} = \frac{1}{2} tan^{-1} \left\{ \frac{\int_{\theta} p(\theta) \sin(2\theta) d\theta}{\int_{\theta} p(\theta) \cos(2\theta) d\theta} \right\} \quad (16)$$

The terms sin(2θ) and cos(2θ) are used to resolve the orientation ambiguity between orientations ±180°. However, if there is a crease in the fingerprints that spans

several analysis frames, the orientation estimation will still be wrong. The estimate will also be inaccurate when the frame consists entirely of unrecoverable regions with poor ridge structure or poor ridge contrast. In such instances, the ridge orientation can be estimated by considering the orientation of its immediate neighborhood. The resulting orientation image O(x,y) is further smoothened using vector averaging. Considering W(x,y) as a Gaussian smoothing kernel, the smoothened image O'(x,y) is obtained using (17) [17].

$$O'(x,y) = \frac{1}{2} tan^{-1} \left\{ \frac{\sin\big(2O(x,y)\big) * W(x,y)}{\cos\big(2O(x,y)\big) * W(x,y)} \right\} \quad (17)$$

3.3.2.2 Ridge frequency image

The average ridge frequency is estimated in a manner similar to the ridge orientation. Assume the ridge frequency r to be a random variable with the probability density function p(r) [17]. The expected value of the ridge frequency is given by $E\{r\} = \int_r p(r) r dr$.

The frequency map so obtained is smoothened by process of isotropic diffusion. Simple smoothening cannot be applied since the ridge frequency is not defined in the background regions. Consider the Gaussian smoothing kernel W(u,v), indicator variable I(u,v) to ensure only valid ridge frequencies are considered and frequency image F(u,v), the smoothened is obtained by the equation (18) [17].

$$F'(x,y) = \frac{\sum_{u=x-1}^{x+1} \sum_{v=y-1}^{y+1} F(u,v) W(u,v) I(u,v)}{\sum_{v=y-1}^{y+1} W(u,v) I(u,v)} \quad (18)$$

3.3.2.3 Region mask

The fingerprint image may be easily segmented based on the observation that the surface wave model does not hold in regions where ridges do not exist. In the areas

of background and noisy regions, there is very little energy content in the Fourier spectrum. An energy image E(x,y) can be defined, where each value indicates the energy content of the corresponding block. The fingerprint region may be differentiated from the background by thresholding the energy image. Given the frequency image F, the ridge orientation θ and ridge frequency r, the energy image E can be generated by (19) [17].

$$E(x,y) = \log\left\{\int_r \int_\theta |F(r,\theta)|^2\right\} \tag{19}$$

Enhancement is especially problematic in regions of high curvature close to the core and deltas that have more than one dominant direction. Excessively narrow angular bandwidth causes spurious artifacts and ridge discontinuities in the reconstructed image. A coherence measure ensures robust singular point detection [17]. Consider the orientation of a block as θ(x,y) and the block size W x W, the coherence measure image C is given by the equation (20)

$$C(x_0,y_0) = \frac{\sum_{i=0}^{W} |\cos(\theta(x_0,y_0) - \theta(x_i,y_i))|}{W \times W} \tag{20}$$

The coherence is high when the orientation of the central block θ(x_0, y_0) is similar to each of its neighbors θ(x_i, y_i). In a fingerprint image, the coherence is expected to be low closer to regions of high curvature. Hence this coherence measure can be utilized to adapt the angular bandwidth of the directional filter [17].

3.3.2.4 Enhancement

The image is divided into overlapping windows. It is assumed that the image is stationary within this small window and can be modeled approximately as a surface wave. The Fourier spectrum of this small region is analyzed and probabilistic estimates of the ridge frequency and ridge orientation. In each window a filter is applied that is tuned

to the radial frequency and aligned with the dominant ridge direction. The filter itself is separable in angle and frequency and is given by the equation (21)

$$H(\rho,\theta) = H_\rho(\rho)H_\emptyset(\emptyset) \tag{21}$$

$$H_\rho(\rho) = \sqrt{\left[\frac{(\rho\rho_{BW})^{2n}}{(\rho\rho_{BW})^{2n} + (\rho^2 - \rho_0^2)^{2n}}\right]} \tag{22}$$

$$H_\emptyset(\emptyset) = \begin{cases} cos^2\left[\frac{\pi}{2}\frac{(\emptyset - \emptyset_c)}{\emptyset_{BW}}\right], & if|\emptyset| < \emptyset_{BW} \\ 0, & otherwise \end{cases} \tag{23}$$

Here $H_\rho(\rho)$ is a band-pass Butterworth filter with center defined by ρ_0 and bandwidth ρ_{BW}. ρ_0 is derived from the intrinsic orientation image while the bandwidth ρ_{BW} is chosen to be inversely proportional to the angular coherence measure. The angular filter $H_\Phi(\Phi)$ is a raised cosine filter in the angular domain with support φ_{BW} and center φ_c [17].

3.3.2.5 Results

Figure 3-10 shows the results of the STFT fingerprint enhancement algorithm. Figure3-10(a) is the original scanned fingerprint image. Figure3-10(b) is the ridge orientation image. Figure3-10(c) is the region mask energy image. Figure3-10(d) is the ridge frequency image. Figure3-10(e) is the angular coherence measure image and Figure3-10(f) is the final enhanced image [17].

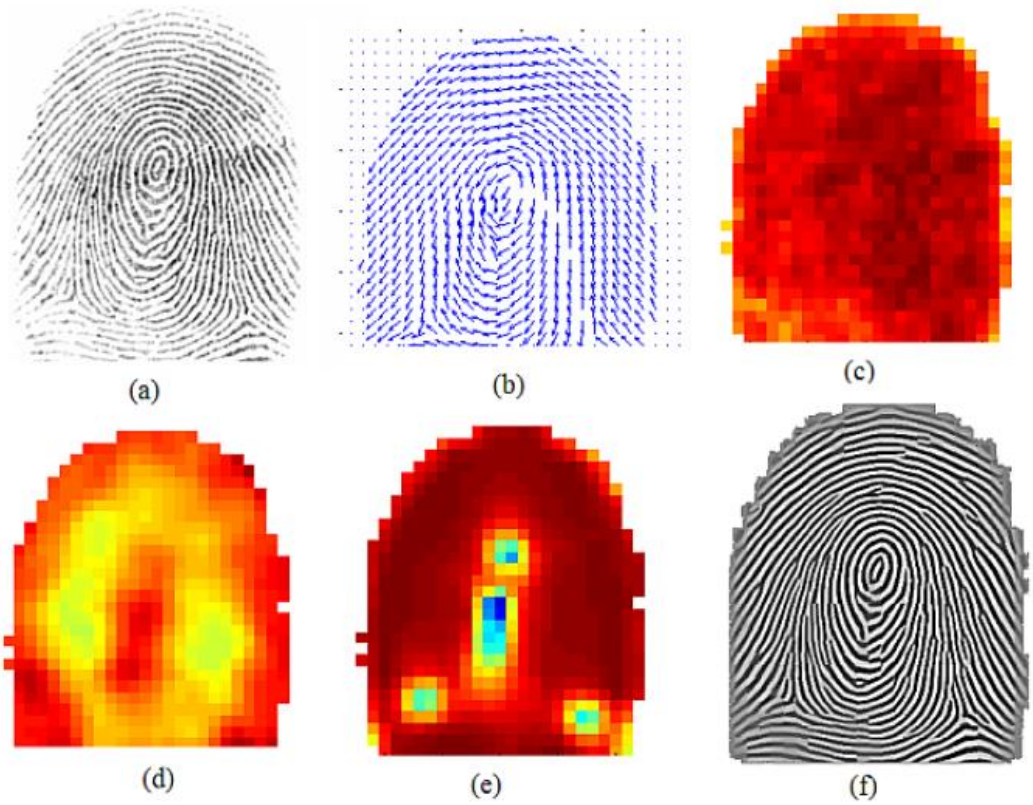


Figure 3-10 STFT enhancement results: (a) Original Image (b) Orientation Image (c) Energy Image (d) Ridge Frequency Image (e) Angular Coherence Image (f) Enhanced Image [17].

3.4 Related work done

An overview on the most popular approach to fingerprint enhancement was presented in section 3.3.1, which was proposed based on a directional Gabor filtering [19] kernel in spatial domain [13]. Chikkerur et al [17] proposed enhancing the fingerprint image using the STFT analysis in frequency domain. It acquires the block frequency through the STFT analysis and estimates the local ridge orientation too. The complex input contexts of the low-quality image, not all of the unrecoverable regions of the

fingerprint can be recovered clearly, as it is difficult to accurately estimate some parameters of the filters through a simple analysis presented in section 3.3.2. Thus, the algorithm needs to be improved to enhance the unrecoverable regions of low-quality images. A two-stage scheme to enhance the low-quality fingerprint image in both the spatial domain and the frequency domain based on the learning from the images [9] was developed in order to overcome the shortcomings of the existing algorithm [13] on the fairly poor fingerprint images with cracks and scars, dry skin, or poor ridges and valley contrast ridges. Figure 3-11 shows the flowchart for the new two-stage enhancement algorithm [9].

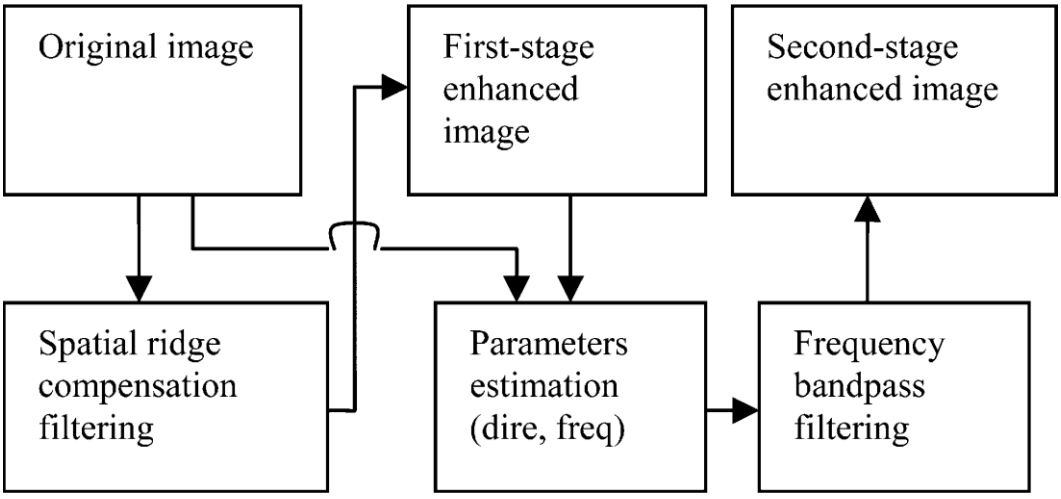


Figure 3-11 Flowchart of the two-stage enhancement algorithm [9]

The algorithm first enhances the images in the spatial domain with a spatial ridge compensation filter and, then, enhances the images in the frequency domain. The parameters (ridge direction and frequency) for the frequency bandpass filters are estimated from the original image and the first-stage enhanced image. The details are introduced as follows.

3.4.1 First-Stage Enhancement: Spatial Ridge-Compensation Filter

The first stage performs ridge compensation along the ridges in the spatial field. This step enhances the fingerprint's local ridges using the neighbor pixels in a small window with a weighted mask along the orientation of the local ridges. This enhances the gray-level values of ridges' pixels along local ridge orientation, while reducing the non-ridge pixels' gray-level values; thus, it is able to connect the broken bars and remove the smears in the fingerprint image [9].

The main idea of the first-stage enhancement scheme is to estimate unbiased local orientation and compensate the possible defects by using the local orientation. The scheme consists of three steps: local normalization, local orientation estimation, and local ridge-compensation filtering [9].

3.4.1.1 Local Normalization

This step is used to reduce the local variations and standardize the intensity distributions in order to consistently estimate the local orientation. The pixel wise operation does not change the clarity of the ridge and furrow structures but reduces the variations in gray-level values along ridges and furrows. For each pixel (i, j) in a subimage, which is acquired by dividing the fingerprint image into subimages first, the normalized image is defined as (23) [9]:

$$norimg(i,j) = M_0 + coeff * (img(i,j) - M) \quad (23)$$

$$coeff = \frac{V_0}{V} \quad (24)$$

Here, img(i, j) is the gray-level value of the fingerprint image in pixel (i, j), norimg(i, j) is the normalizing value in pixel (i, j), and coeff is the amplificatory multiple of the normalized image. M is the mean of the subimage, and V is the variance of the subimage. M_0 and V_0 are the desired mean and variance values, respectively [9].

3.4.1.2 Local Orientation Estimation

This step determines the dominant direction of the ridges in different parts of the fingerprint image. The gradient method is used for orientation estimation and an orientation smoothing method with a Gaussian window to correct the estimation. For a number of non-overlapping blocks with the size of W × W, a single orientation is assigned corresponding to the most probable or dominant orientation of the block. For each pixel in a block, a simple gradient operator, such as the Sobel mask [11], is applied to obtain the horizontal gradient value G_x (u, v) and vertical gradient value G_y (u, v). The block horizontal and vertical gradients, i.e., G_{xx} and G_{xy}, are obtained by adding up all the pixel gradients of the corresponding direction. Then, the block orientation O(x, y) is determined using the block horizontal and vertical gradients [9].

$$G_{xy} = \sum_{u=i-(\frac{w}{2})}^{i+(\frac{w}{2})} \sum_{v=j-(\frac{w}{2})}^{j+(\frac{w}{2})} 2G_x(u,v)G_y(u,v) \tag{25}$$

$$G_{xx} = \sum_{u=i-(\frac{w}{2})}^{i+(\frac{w}{2})} \sum_{v=j-(\frac{w}{2})}^{j+(\frac{w}{2})} G_x^2(u,v)G_y^2(u,v) \tag{26}$$

$$O(x,y) = \frac{1}{2}\tan^{-1}(\frac{G_{xy}}{G_{xx}}) \tag{27}$$

3.4.1.3 Local Ridge-Compensation Filter

With the estimated orientation values in place, the final step compensates the ridge artifacts using a local ridge-compensation filter with a rotated rectangular window to match the local orientation. For each pixel (i, j) in the normalized image, the computing formula for the ridge-compensation filter is defined as (28) [9]:

$$fltimg(i,j) = \frac{(\sum_{m=-(w-1)/2}^{(w-1)/2} \sum_{n=-(h-1)/2}^{(h-1)/2} norimg(i',j'))}{(((w-1)\times\beta+\alpha)\times h)} \quad (28)$$

$$i' = i + m\cos\big(O(i,j)\big) + n\sin\big(O(i,j)\big) \quad (29)$$

$$j' = j - m\sin\big(O(i,j)\big) + n\cos\big(O(i,j)\big) \quad (30)$$

Where fltimg(i, j) denotes the ridge-compensation filtered image, norimg(i, j) is the local normalized image, O(i, j) is the local ridge orientation image, and (i', j') is the pixel coordinate in the new axes with an affine transform to match the local ridge orientation. w and h are the width and height of the enhanced windows, respectively. m and n are the integer numbers and determined by w and h. α and β are the constant values that are adaptive to the contrast of the ridges, and they are experimentally determined. Unlike the smoothing operation, the compensation filter uses weighted constant values to control the contrast parameters. Figure 3-12 shows the w x h window along the local block orientation [9].

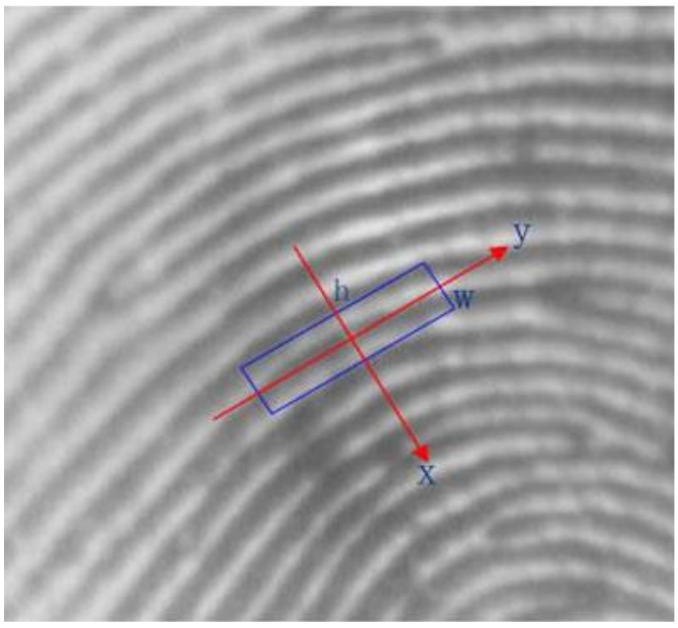


Figure 3-12 Window along the local ridge orientation [9]

3.4.2 Second-Stage Enhancement: Frequency Bandpass Filter

The result of the first spatial filter increases the ridge contrast in the direction perpendicular to the ridges, this processing may blur the image as well. Thus, a second-stage enhancement with a tuned bandpass filter is proposed to enhance the fingerprint image serially. The frequency bandpass filters used are separable in the radial and angular domains, respectively. The parameters of the bandpass filter are learnt from both the original image and the enhanced image [9].

Section 3.3.2.4 used the bandpass frequency filters for fingerprint image enhancement, and they have been proven to be effective for enhancement. However, these methods do have demerits, such as difficult parameters selection and non-effective filtering. To overcome these shortcomings, an improved scheme is proposed with an exponential bandpass filter. Using polar coordinates (ρ, φ) to express the filters as a separable function, the frequency bandpass filters H(ρ, φ) used are separable in the radial and the angular domains, that is explained in (31).

$$H(\rho,\theta) = H_\rho(\rho)H_\emptyset(\emptyset) \tag{31}$$

$$H_\rho(\rho) = \frac{1}{\sqrt{2\pi}\,\rho_{BW}} \exp\left(-\frac{(\rho-\rho_c)^2}{2\rho_{BW}}\right) \tag{32}$$

$$H_\emptyset(\emptyset) = \begin{cases} cos^2\left[\frac{\pi}{2}\frac{(\emptyset-\emptyset_c)}{\emptyset_{BW}}\right], & if|\emptyset| < \emptyset_{BW} \\ 0, & otherwise \end{cases} \tag{33}$$

The radial filter $H_\rho(\rho)$ is an exponential bandpass filter with the center frequency that is defined by ρ_c and bandwidth ρ_{BW}, where,

$$\rho_{BW} = \frac{C \times \rho_c - C}{\rho_c} \text{ ; C is a constant} \tag{34}$$

3.4.2.1 Local orientation estimation by learning

This step determines the dominant direction of the ridges in different parts of the fingerprint image by learning from the images. The orientation estimation is similar with Step 2 in the first-stage filtering. However, the new orientation θ(x, y) is corrected in the enhanced image after the first stage enhancement [9]. The formula for the computation of the new orientation θ(x, y) is as (35):

$$\theta(x,y) = \begin{cases} corr\_\theta(x,y), & if\ |corr_{\theta(x,y)} - orig\_\theta(x,y) < t \\ \dfrac{\sum_{(i,j)\epsilon W} corr_{\theta(x,y)}}{W \times W}, & else \end{cases} \quad (35)$$

where orig_θ(x, y) is the orientation of a pixel in the original image, $corr_\theta$(x, y) is the orientation of the corresponding pixel in the enhanced image, t is a threshold value, and W is the window size [9].

3.4.2.2 Local frequency estimation by learning

This step is used to estimate the inter-ridge separation in different regions of the fingerprint image. The local frequency is estimated by applying FFT to the blocks. The new frequency equals the average value of its neighbor if their difference is larger than a threshold value, or else it equals the frequency that is acquired from the enhanced image. The obtained frequency is also used to design the radial filter [9].

Similar to (20), a coherence image is computed to measure the coherence between the central block and its neighbors [9].

3.4.2.3 Frequency bandpass filtering

Image is divided into overlapping subimages, and the fast Fourier transform (FFT) of each subimage is obtained by removing the dc component. The radial filter $H_\rho(\rho)$ from (32) is applied followed by the angular filter $H_\varphi(\varphi)$ from (33). The block is now filtered in the frequency domain, i.e., $H(\rho, \varphi) = H_\rho(\rho) \times H_\varphi(\varphi)$ as in (31). The

Reconstructed image is obtained by taking the inverse fast Fourier transform (IFFT) of $H(\rho, \varphi)$ [9].

Figure 3-13 shows examples of the fingerprint image enhancement using the two stage fingerprint enhancement algorithm.

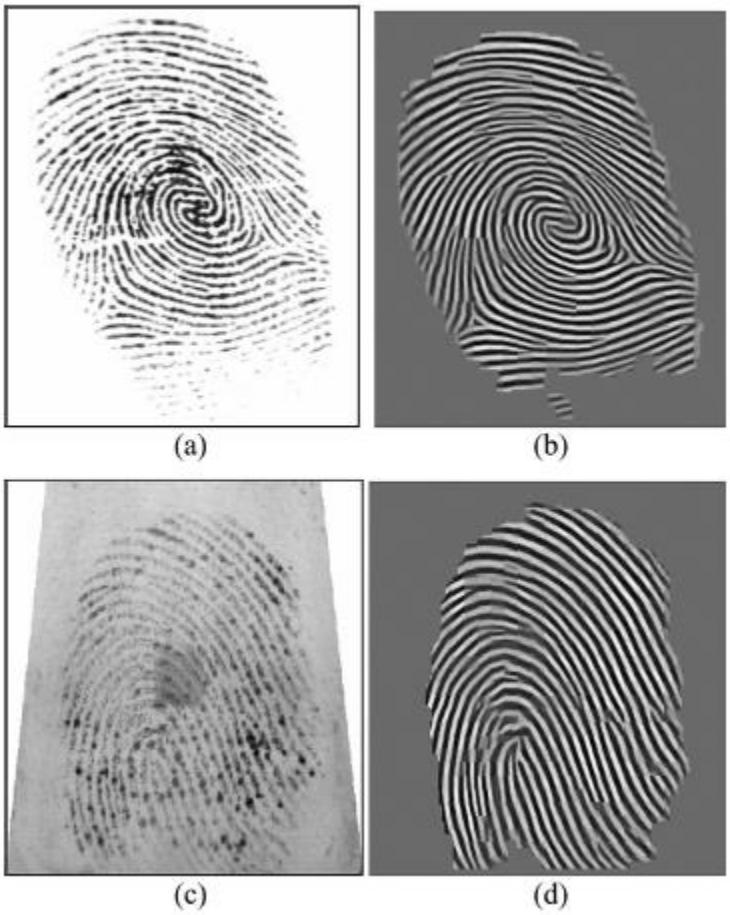


Figure 3-13 Results of the Two stage enhancement algorithm: (a),(c) are the original scanned images, and (b),(d) are the enhanced images [9]

Chapter 4

Enhancement using Laplacian image pyramids

4.1 Introduction

The goal of a fingerprint enhancement algorithm is to rectify the image degradation caused by source complexity and to restore the actual fingerprint pattern as best as possible. A noisy image will yield spurious information. As shown in chapter 3, there are several published studies on fingerprint image enhancement. Section 3.3.1 explains the algorithm proposed by Hong et al [13] which uses Gabor band-pass filters which are tuned to the ridge frequency and orientation to remove undesired noise while preserving the true ridge-valley structures. Here, all operations are performed in the spatial domain, whereas the contextual filtering is done in the Fourier domain. Either way, block-wise processing is used to obtain the enhancement result causing restoration discontinuities and blocking artifacts at block boundaries. Section 3.3.2 describes the STFT based block-wise fingerprint enhancement by Chikkerur et al [17], followed by contextual filtering using raised cosines. These methods are likely successful in easy and moderate degradation levels, but tend to result it discontinuities under bad conditions [31].

In section 3.4, a novel two stage fingerprint enhancement scheme is described and tested to be improve the state of the art algorithms described in section 3.3. But the algorithm tends to be rigid during the local normalization which smooths the image pixel wise based on its neighbor pixels. This type of smoothing degrades the image further in extremely bad conditions. As an alternative, the Laplacian image pyramid decomposition and reconstruction [32] is proposed to replace the 'Local Normalization and ridge compensation' process in the algorithm. Image pyramids or multi-resolution processing is especially known from image compression [32] and medical image processing [33], but has not been utilized much to enhance fingerprint images before. The Laplacian pyramid resembles bandpass filtering in the spatial domain. In this study,

the fingerprint images are decomposed using Laplacian pyramid decomposition (LPD) [32], since all the relevant information to be concentrated within a few frequency bands.

4.2 Laplacian Image Pyramids

The task for image pyramids in this study is to decompose images into multiple information scales which helps to accurately pronounce features of interest and attenuate noise. The first step in Laplacian pyramid coding is to low-pass filter the original image g_o to obtain image g_1, which is a 'reduced' version of g_o in a way that both resolution and sample density are decreased. In a similar way form g_2 as a reduced version of g_1, and so on. Filtering is performed by a procedure equivalent to convolution with one of a family of local, symmetric weighting functions. An important member of this family resembles the Gaussian probability distribution, so the sequence of images g_o, g_1, …, g_n is called the Gaussian pyramid. Figure 4-1 shows an example of a Gaussian pyramid where the dots represent the pixels in each pyramid image layer.

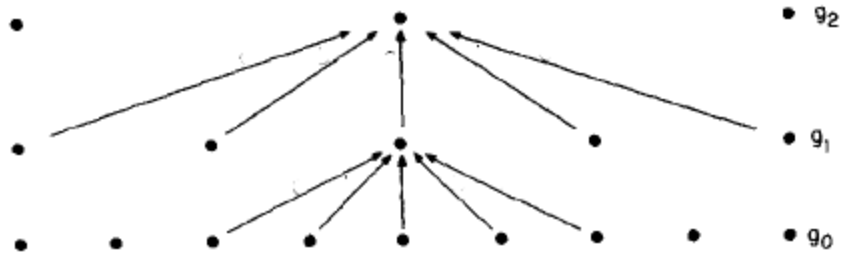


Figure 4-1 Example of a Gaussian pyramid [32]

The decomposition method in image pyramids is known as 'reduce' function [32]. Let 'g' be the original image with C columns and R rows and an equivalent weighting

function ‘h’ whose parameters (m,n) are integers ranging according to the size of the image. The reduced image g_l is obtained by the reduce function which is defined as (36)

$$g_l(i,j) = \sum_{m=-\frac{C}{2}}^{\frac{C}{2}} \sum_{n=-\frac{R}{2}}^{\frac{R}{2}} h_l(m,n) g_{l-1}(2i+m, 2j+n) \tag{36}$$

Here, l is the number of pyramid levels $0 < l < n$, and (i,j) are pixel values where $0 \leq i < C$ and $0 \leq j < R$ [32]. The equation (36) will be referred to as (37)

$$g_l = REDUCE(g_{l-1}) \tag{37}$$

The reconstruction method is known as ‘expand’ function [32]. This function is the reverse of reduce. Its effect is to expand an (M+1) x (N+1) array into a (2M+1) x (2N+1) array by interpolating new node values between given values. This will expand the array g_l of the Gaussian pyramid to yield an array $g_{l,n}$ which is the expanded image [32].

$$g_{l,n}(i,j) = \sum_{m=-\frac{C}{2}}^{\frac{C}{2}} \sum_{n=-\frac{R}{2}}^{\frac{R}{2}} h_l(m,n) g_{l,n-1}\left(\frac{i-m}{2}, \frac{j-n}{2}\right) \tag{38}$$

The equation (38) will be referred to as (39)

$$g_{l,n} = EXPAND(g_{l,n-1}) \tag{39}$$

Figure 4-2 shows the first six levels of the Gaussian pyramid for the “Lena” image. The original image, level 0, measures 257 by 257 pixels, and level 5 measures just 9 by 9 pixels [32].

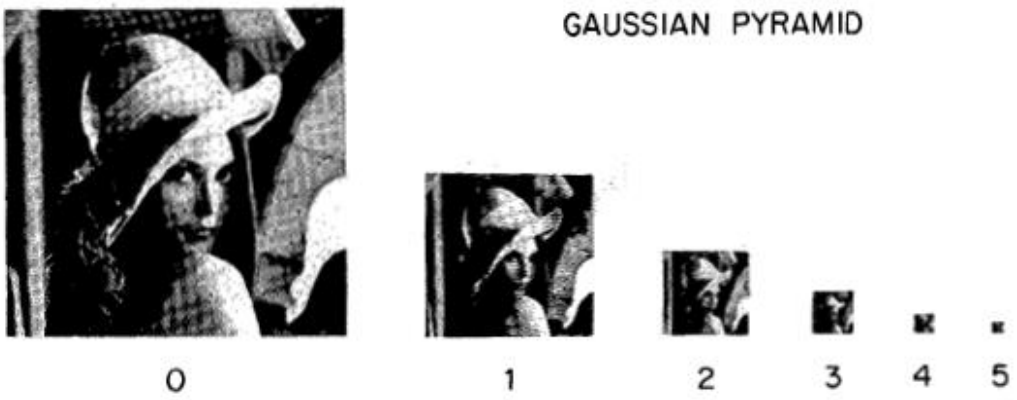


Figure 4-2 First six levels of the Gaussian pyramid for the “Lena” image [32].

To obtain the Laplacian pyramid representation, the error image which remains when an expanded g_1, is subtracted from g_o is encoded. This image becomes the bottom level of the Laplacian pyramid. The next level is generated by encoding g_1, in the same way. Hence the Laplacian pyramid representation can be defined as the sequence of error images L_0, L_1, ... L_N. Each is the difference between two levels of the Gaussian pyramid. Consider ‘l’ to the level of Laplacian sequence, where $0 \leq l < N$. The Laplacian representation image at l is given by (40) [32]:

$$L_l = g_l - EXPAND(g_{l+1}) \tag{40}$$

The reconstructed image can be obtained by expanding and summing all the levels of the Laplacian pyramid.

$$g_l = L_l + EXPAND(g_{l+1}) \tag{41}$$

Figure 4-3 shows the first four levels of the Gaussian pyramid on the top row and Laplacian pyramid in the bottom row for the “Lena” image. Here each Laplacian pyramid level is the difference between two levels of the Gaussian pyramid [32] and it can be seen that the Laplacian pyramid images pronounce the edges of the objects in the image, which are the vital features for a fingerprint image.

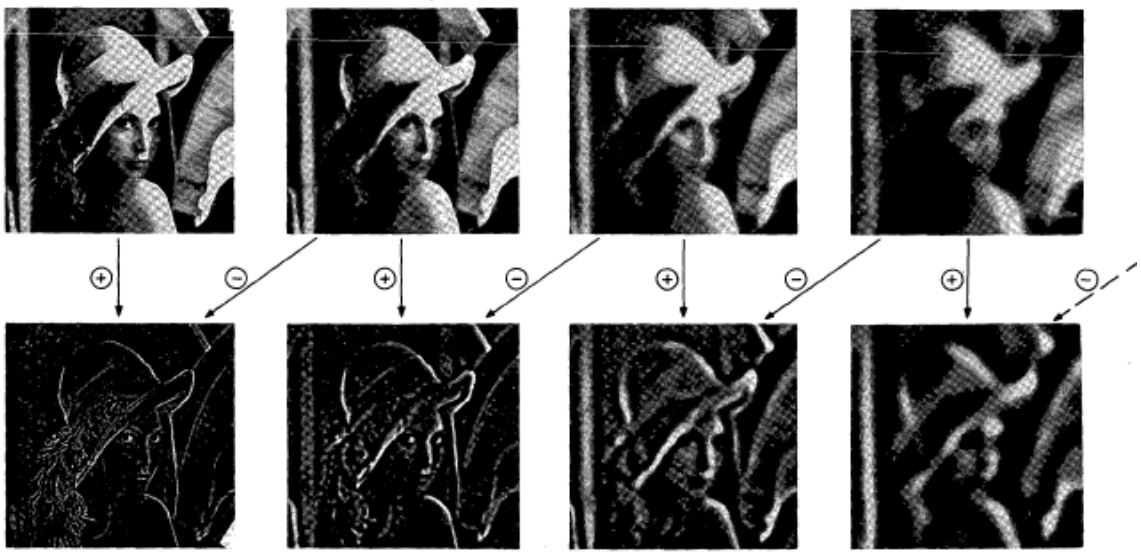


Figure 4-3 First four levels of the Laplacian pyramid for the “Lena” image [32].

4.3 Applying LPD to the two-stage enhancement scheme

The proposed enhancement to the novel two-stage enhancement scheme discussed in section 3.4 is to add a stage before the ‘First-Stage Enhancement’ which does the LPD process in the spatial domain so that the ridge features will be pronounced from the noise and it will yield an effective enhancement. Since the vital ridge features will be present in the 1st level of the Laplacian pyramid, the original image will be decomposed into 2 levels of Laplacian pyramids and each level will undergo the two-stage enhancement separately. The enhancement will now act as a 2 tier system, the enhancement of the Laplacian pyramid L_0 will majorly pronounce the pixels with ridge features, whereas the enhancement of the Laplacian pyramid L_1 will majorly attenuate noise as L_1 will mostly consist of unwanted pixel values. Laplace pyramid reconstruction (LPR) will be done to expand and sum the 2 tiers of enhanced Laplacian pyramid level images to obtain the final enhanced fingerprint image.

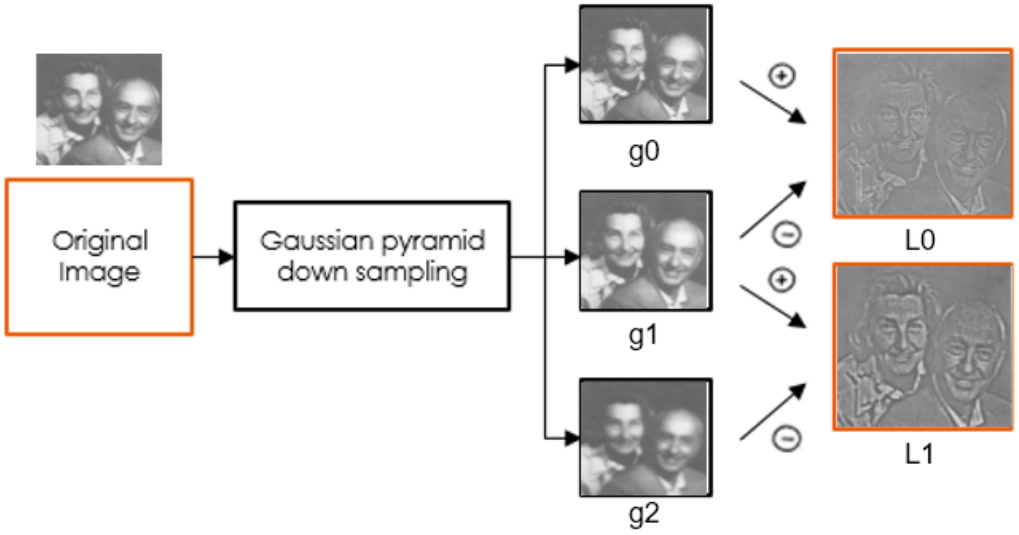


Figure 4-4 Proposed Laplacian decomposition flowchart

Figure 4-4 shows Laplacian decomposition flowchart and the figure 4-5 shows the flowchart of the proposed multi-stage fingerprint enhancement scheme.

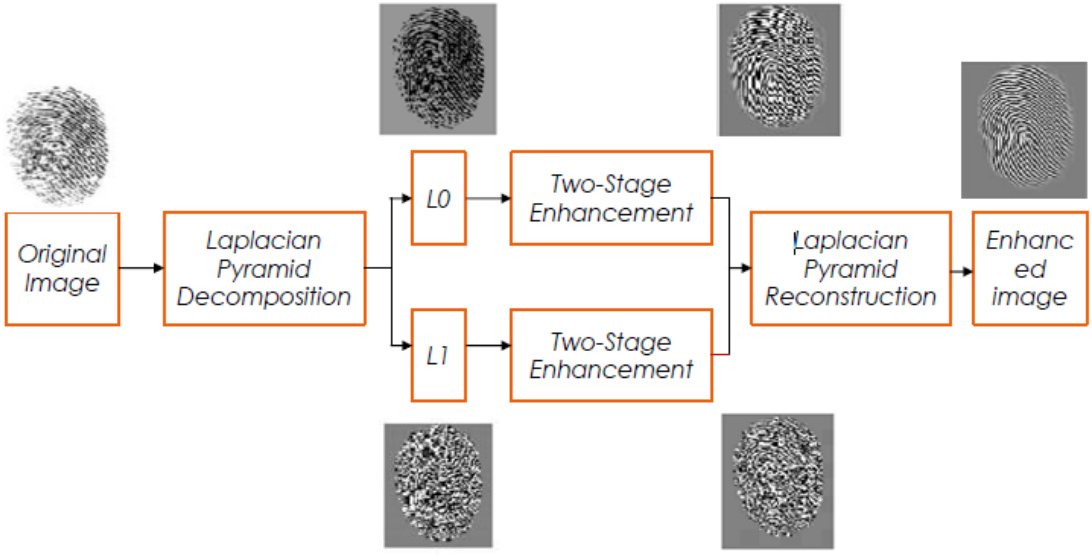


Figure 4-5 Proposed Multi-stage enhancement scheme

4.2. Summary

A novel multi-stage enhancement scheme has been proposed which by using LPD and LPR, gives better fidelity to the ridge-valley structure of the fingerprint images so as to better aid the feature extraction process in extracting as many features as possible. The approach can be summarized by assuming the original image as img(i,j). The Gaussian pyramid level images g_l required by the LPD are generated by equation (37). The LPD is performed to generate the Laplacian pyramid difference images L_l using equation (40). In order to reduce processing time, the LPD is restricted to 2 levels, however the enhancement will be much accurate as the LPD levels increase. Each L(i,j) can now be taken as input to equation (23) which begins the two-stage enhancement scheme [9]. The enhanced Laplacian image of each level L'(i,j) is obtained by taking IFFT of equation (31). Finally, the complete enhanced fingerprint image is generated by performing the LPR process on the sequence of L' images using the equation (41).

The enhanced images of the LPD based multi-stage enhancement scheme are compared with the enhanced images of the state of the art [16] scheme. The comparison is done using visual comparison, minutiae ratios and performance time. The test data set for this comparison is the set of databases from the standard FVC2004 database [18].

Chapter 5

Results

To compare the different enhancement methods, the Fingerprint Verification Competition database (FVC) [18] was chosen as the test data set of fingerprint images. Experiments were conducted on the FVC2004 databases. The enhancement was conducted using the state of the art directional Gabor filtering employed by Hong et al [16] and the novel two-stage scheme to enhance the low-quality fingerprint images proposed by Yang et al [9] with the proposed enhancement in this study.

5.1 Quality Metrics comparison

Different fingerprint quality metrics such as visual inspection, true minutiae ratio (TMR) and false minutiae ratio (FMR), and performance time are measured for the proposed scheme and state of the art schemes over the standard fingerprint print databases of FVC2004 [18].

5.2 Visual inspection

Figure 5-1 is an original scanned image of the DB1 105 fingerprint from the FVC2004 database. It does not have an extreme case of degradation but there are several points of ridge distortion. Figures 5-2 through 5-5 are enhanced images from the directional Gabor filtering [16], STFT based enhancement [17], two-stage enhancement scheme [9] and the proposed LPD based multi-stage scheme respectively.

From the figures 5-2 through 5-5, it is evident that all the enhancement methods are able to faithfully recover the ridge-valley structure. Blocking artifacts are visible in figures 5-2 and 5-3. Figure 5-5 has a sharper ridge-valley structure due to the LPD process aiding better enhancement of the features and attenuation of noise.

Figure 5-1 Original fingerprint FVC2004 DB1 105 [18]

Figure 5-2 Tuned Gabor filtering enhanced image.

Figure 5-3 Two-stage enhanced image

Figure 5-4 Proposed multi-stage scheme enhanced image

To compare with an extreme case with the state of the art STFT based enhancement, the image shown in figure 5-6 is taken which has a high percent of image degradation. Figure 5-7 is the enhanced image by the STFT based enhancement [17] and Figure 5-8 is the enhanced image by the proposed LDP based two-stage enhancement scheme. It is evident that the LDP based scheme made a better revering of the badly degraded feature area in the bad input image.

Figure 5-5 Bad quality FVC2004DB1 101 original fingerprint image [18]

Figure 5-6 STFT based enhancement of the bad image

Figure 5-7 Proposed LPD based two-stage scheme enhancement of the bad image

The figure 5-9 is a medium quality scanned fingerprint image with several ridge structure breaks and overall hazy image. The figures 5-10 and 5-11 are the level 1 and level 2 Laplacian pyramid decomposed [32] images respectively. Figures 5-12 and 5-13 are the two-stage scheme enhanced images of 5-10 and 5-11 figures respectively. Figure 5-14 is the state of the art [17] enhanced image where the distortion from the blocking artifacts are highlighted, this cases some false minutiae. Figure 5-15 is the image enhanced by the proposed LDP based multi-stage enhancement scheme.

Figure 5-8 FVC2004DB1 102 fingerprint input image [18]

Figure 5-9 Level 1 Laplacian pyramid image

Figure 5-10 Level 2 Laplacian pyramid image

Figure 5-11 Enhanced Level 1 Laplacian pyramid image

Figure 5-12 Enhanced Level 2 Laplacian pyramid image

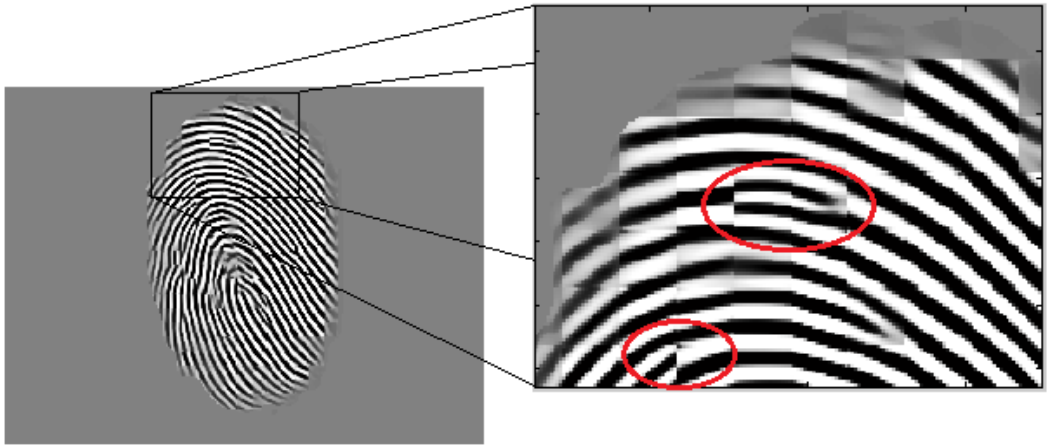


Figure 5-13 State of the art enhanced image with distortion highlighted

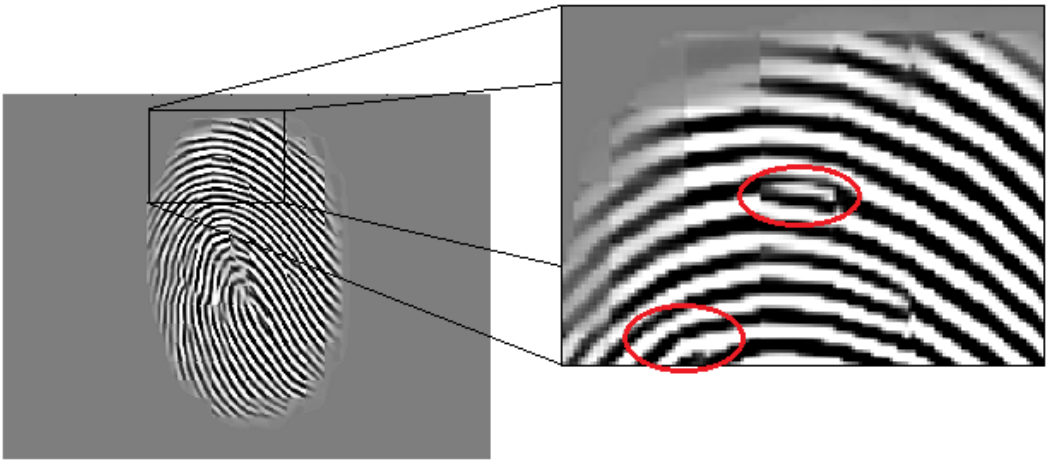


Figure 5-14 LPD based multi-stage enhanced less distortion highlighted

Figures 5-16 to 5-21 show the visual comparison of the state of the art tuned Gabor filtering enhancement [16] and the LPS based multi-stage enhancement scheme on fingerprint images from the standard fingerprint image database FVC2004 [18].

Figure 5-16 and 5-17 show FVC2004DB1 [18] fingerprint images 104 and 107 respectively. In figure 5-16 and 5-17, (a) shows the original fingerprint image, (b) shows the tuned Gabor filtered [16] image and (c) shows the LPD based multi-stage enhanced image.

Figure 5-15 (a) Original FVC2004DB1 104 fingerprint image (b) State of the art enhancement (c) Multi-stage enhancement

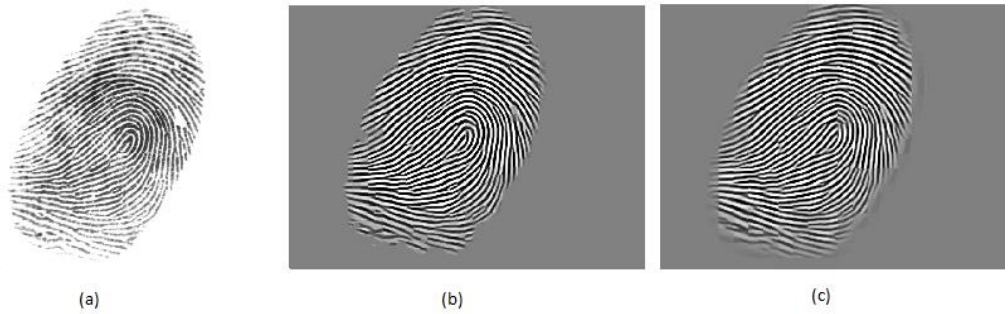


Figure 5-16 (a) Original FVC2004DB1 107 fingerprint image (b) State of the art enhancement (c) Multi-stage enhancement

Figure 5-18 and 5-19 show FVC2004DB2 [18] fingerprint images 101 and 104 respectively. In figure 5-18 and 5-19, (a) shows the original fingerprint image, (b) shows the tuned Gabor filtered [16] image and (c) shows the LPD based multi-stage enhanced image.

Figure 5-17 (a) Original FVC2004DB2 101 fingerprint image (b) State of the art enhancement (c) Multi-stage enhancement

Figure 5-18 (a) Original FVC2004DB2 104 fingerprint image (b) State of the art enhancement (c) Multi-stage enhancement

Figure 5-20 and 5-21 show FVC2004DB3 [18] fingerprint images 105 and 104 respectively. In figure 5-20 and 5-21, (a) shows the original fingerprint image, (b) shows the tuned Gabor filtered [16] image and (c) shows the LPD based multi-stage enhanced image.

Visual inspection of the results over the FVC2004 database [18] images show that the state of the art [16] and the LPD based multi-stage enhancement schemes have performed well to recover bad sections of the fingerprint images. However, the LPD based multi-stage scheme has done a better job of enhancing the ridge fidelity.

Figure 5-19 (a) Original FVC2004DB3 105 fingerprint image (b) State of the art enhancement (c) Multi-stage enhancement

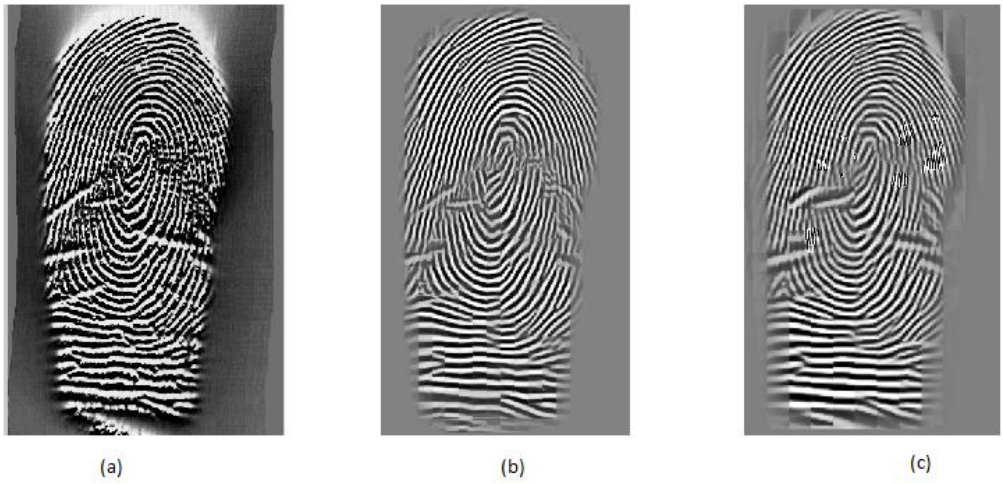


Figure 5-20 (a) Original FVC2004DB3 104 fingerprint image (b) State of the art enhancement (c) Multi-stage enhancement

Figure 5-22 shows the results of the post enhancement process of image binarization and thinning [1] to extract minutiae from the fingerprint images. Figure 5-22(a) shows the binarization and thinning [1] of the original non-enhanced FVC2004DB2 101 [18] image in which several spurious points can be seen. Figure 5-

22(b) shows the binarization and thinning [1] of the state of the art [16] FVC2004DB2 101 [18] image in which a few spurious points can still be seen. Figure 5-22(b) shows the binarization and thinning [1] of the LPD based multi-stage enhanced FVC2004DB2 101 [18] image in which very few spurious points can be seen and overall better ridge fidelity. Figure 5-23 shows the minutiae extracted from the thinned images seen in figure 5-22.

Figure 5-21 Thinning operation on (a) Original FVC2004DB2 101 fingerprint image (b) State of the art enhancement (c) Multi-stage enhancement

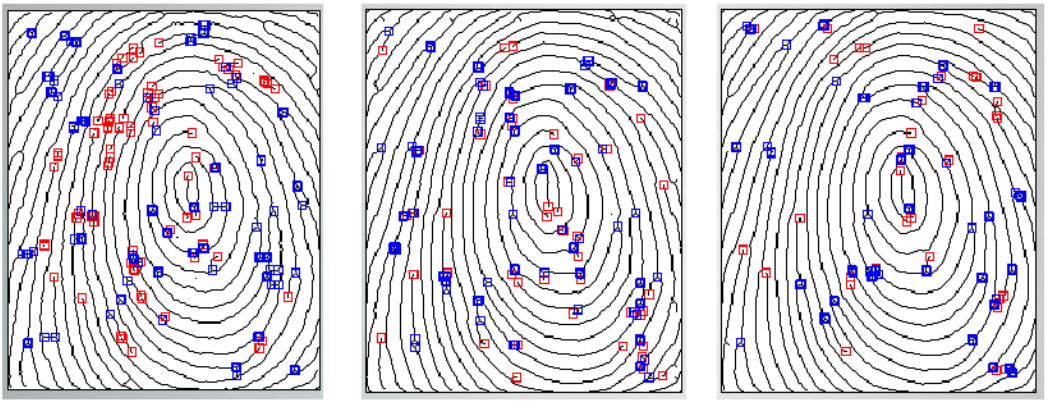


Figure 5-22 Minutiae extracted from the thinned (a) Original FVC2004DB2 101 fingerprint image (b) State of the art enhancement (c) Multi-stage enhancement

5.3 Minutiae ratio

The proposed LPD based multi-stage enhancement scheme will be implemented and compared to the state of the art fingerprint enhancement algorithm [16] in terms of the minutiae extracted. The following terms are defined for the purpose of comparing the algorithms [35]:

1) True minutia: a minutia point detected.

2) False minutia: a minutia that does not coincide with the true minutiae being a false minutia (Total minutiae – true minutiae).

These terms are further used to define true minutiae ratio (TMR) and false minutiae ratio (FMR) as the ratio of the number of true minutiae and false minutiae, divided by the number of total minutiae, respectively [35]. The TMR and FMR are expressed as percentages as shown in equations (42) and (43) respectively [9].

$$TMR\ \% = \frac{True\ minutiae\ x\ 100}{Total\ minutiae} \tag{42}$$

$$FMR\ \% = \frac{False\ minutiae\ x\ 100}{Total\ minutiae} \tag{43}$$

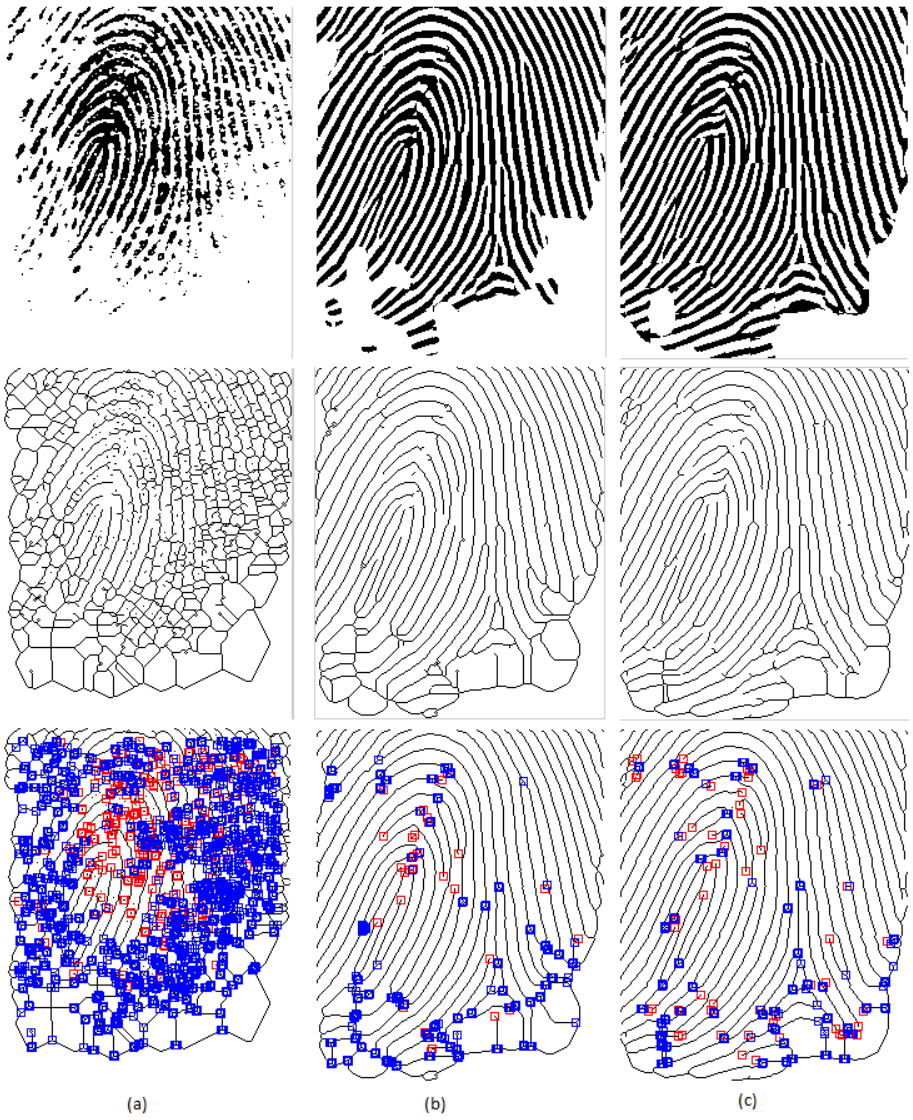


Figure 5-23 Minutiae extracted from (a) Original FVC2004DB1 104 fingerprint image (b) State of the art enhancement (c) Multi-stage enhancement

Table 5-1 Minutiae count for the FVC2004DB1 104 image (True minutiae = 129)

	FVC2004DB1 104 Original image	State of the art enhanced image	Multi-stage enhanced image
Minutiae count	1453	209	191

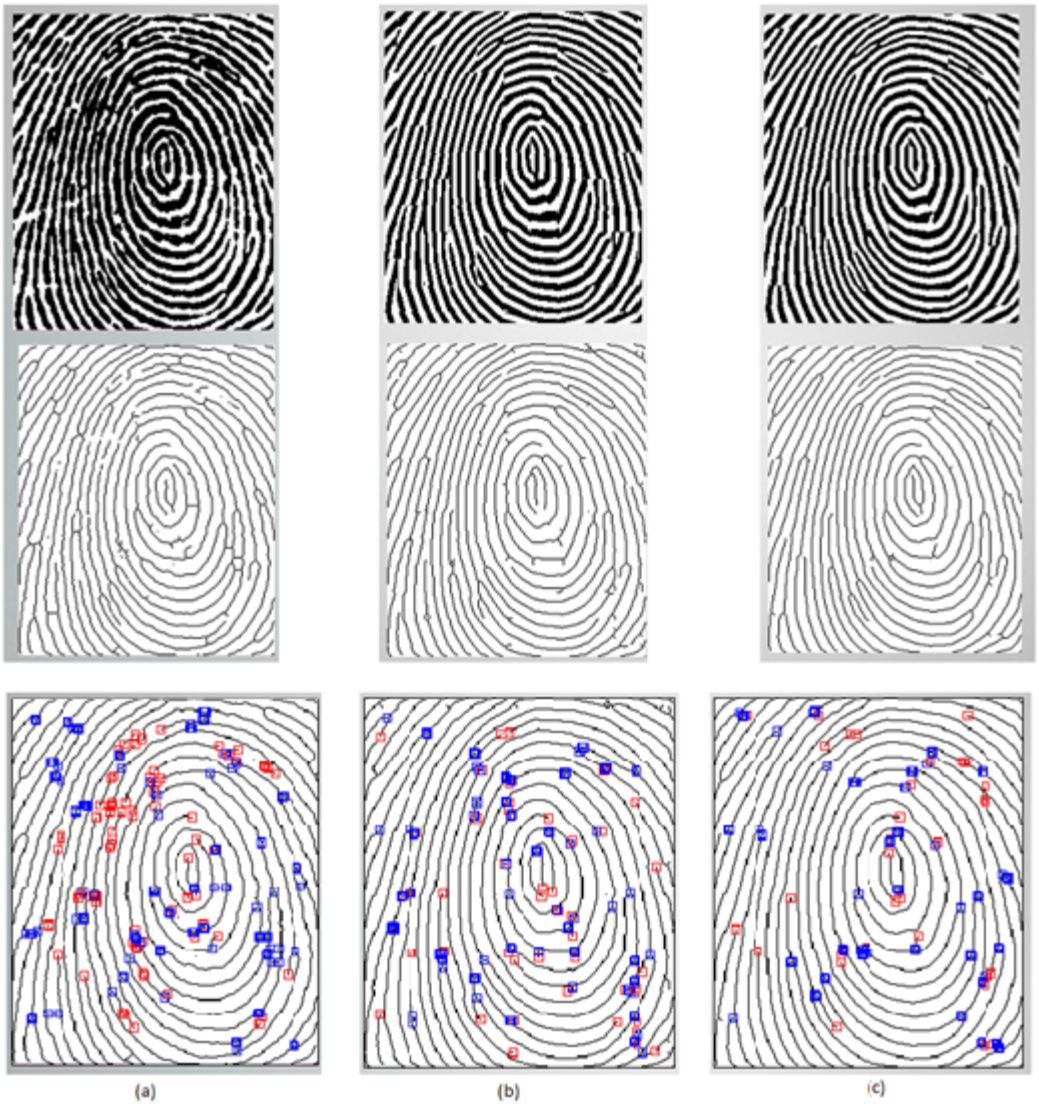


Figure 5-24 Minutiae extracted from (a) Original FVC2004DB2 101 fingerprint image (b) State of the art enhancement (c) Multi-stage enhancement

Table 5-2 Minutiae count for the FVC2004DB2 101 image (True minutiae = 106)

	FVC2004DB2 101 Original image	State of the art enhanced image	Multi-stage enhanced image
Minutiae count	371	134	126

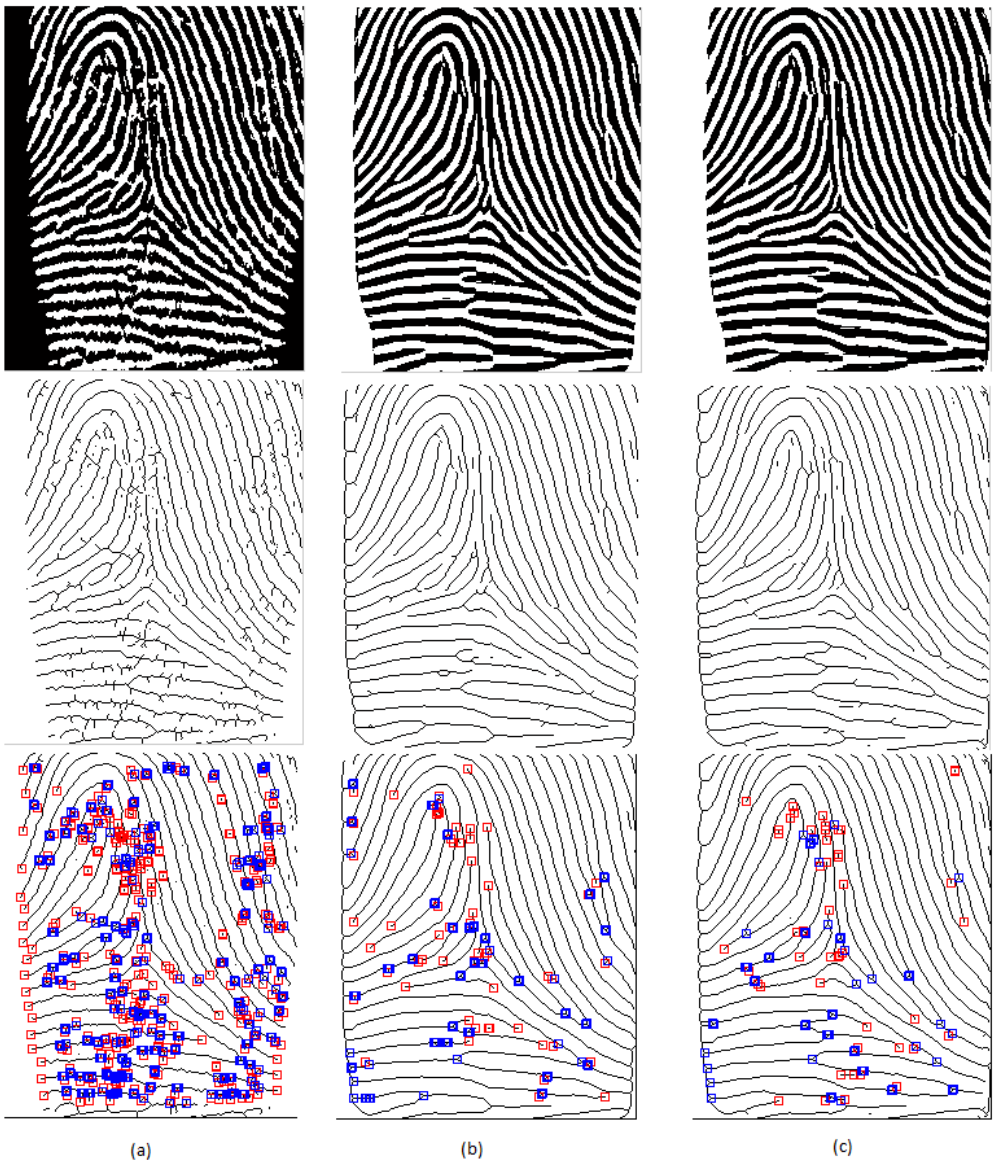


Figure 5-25 Minutiae extracted from (a) Original FVC2004DB3 105 fingerprint image (b) State of the art enhancement (c) Multi-stage enhancement

Table 5-3 Minutiae count for the FVC2004DB3 105 image (True minutiae = 112)

	FVC2004DB3 105 Original image	State of the art enhanced image	Multi-stage enhanced image
Minutiae count	283	132	124

Post binarization and thinning [1] process, the thinned image is used by computer vision algorithms [1] to extract minutiae from the fingerprint image as shown in figure 5-23. Figures 5-24, 5-25 and 5-26 show the minutiae extracted from images FVC2004DB1 104, FVC2004DB2 101 and FV2004DB3 105 respectively. (a), (b) and (c) Show the minutiae extraction from the original image, state of the art enhanced [16] image and LPD based multi-stage enhanced image respectively.

Tables 5-1, 5-2, 5-3 shows the extracted minutiae count from images FVC2004DB1 104, FVC2004DB2 101 and FV2004DB3 105 respectively. Table 5-4 shows the computed false minutiae count using. Table 5-5 is the tabulation of the TMR and FMR minutiae ratios, and ratio average using the equations (42) and (43). The tabulation shows that the TMR of non-enhanced images are very low for the low quality fingerprints and a high FMR of non-enhanced images is due to the several spurious features caused by the low quality. There is a 3-4% improvement in the LPD based multi-stage enhancement scheme compared to the state of the art enhancement [16]. The graphical chart shown in Table 5-7 is a graphical representation of the minutiae ratios.

Table 5-6 shows the performance time taken for reading the input image, enhancement and feature extraction. For the non-enhanced image the read input image is used for feature extraction. The time taken by the LPD based multi-stage enhancement is 2.5 times more than the time taken by the state of the art [16] scheme. This is also shown graphically in the table 5-8.

Table 5-4 Average false minutiae

	Original image	State of the art enhanced image	Multi-stage enhanced image
FVC2004 DB1	1324	80	62
FVC2004 DB2	265	28	20
FVC2004 DB3	185	34	26

Table 5-5 Tabulation of the compared minutiae ratio and average

Dataset	Original image		State of the art enhanced image		Multi-stage enhanced image	
	TMR	FMR	TMR	FMR	TMR	FMR
FVC2004 DB1	8.87	91.13	63.72	36.28	67.53	32.46
FVC2004 DB2	28.57	71.42	81.10	18.90	83.12	16.88
FVC2004 DB3	39.57	60.43	84.84	15.16	88.32	11.68
Average	25.67	74.32	76.55	23.44	79.65	20.34

Table 5-6 Performance time (seconds)

	Original image	State of the art enhanced image	Multi-stage enhanced image
FVC2004 DB1	0.9486	1.0789	2.9138
FVC2004 DB2	0.6637	0.9407	2.8239
FVC2004 DB3	0.7372	1.0124	2.8958
Average performance time	0.7831	1.010	2.8778

Table 5-7 Graphical chart of the average minutiae ratio

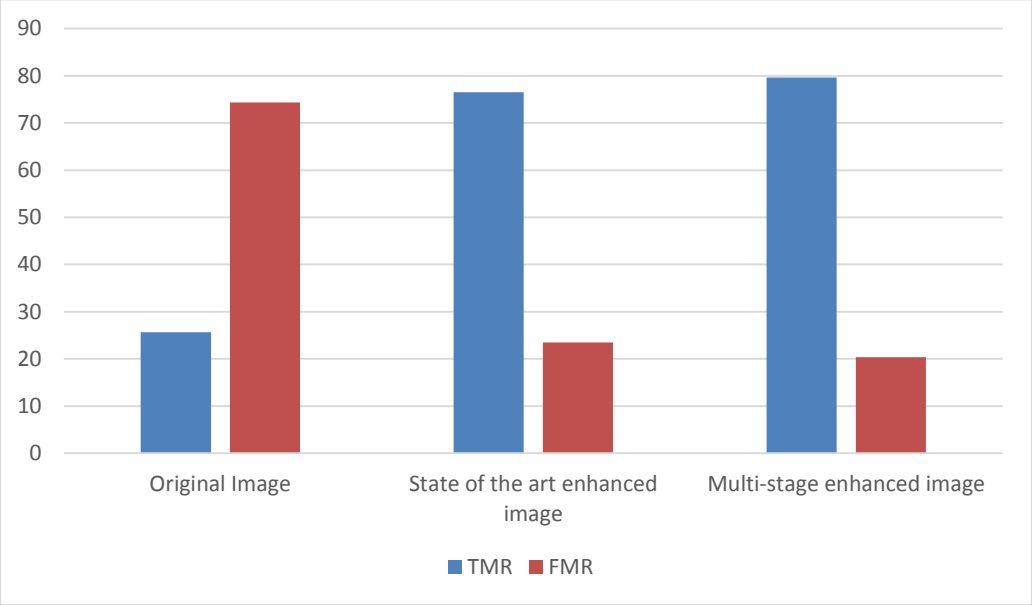
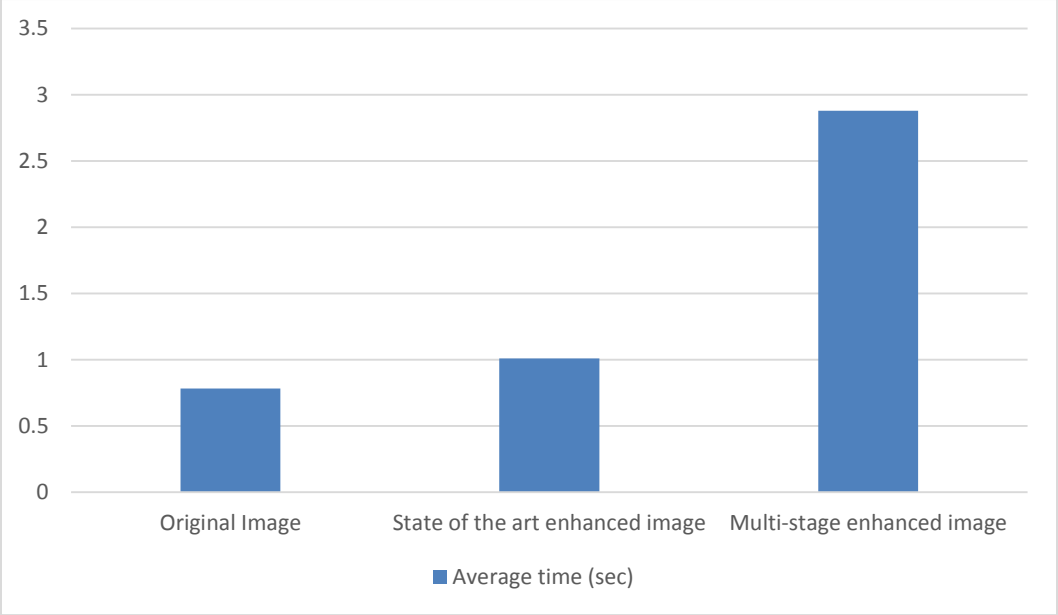


Table 5-8 Average performance time for enhancement and feature extraction



Chapter 6

Conclusions and Future Work

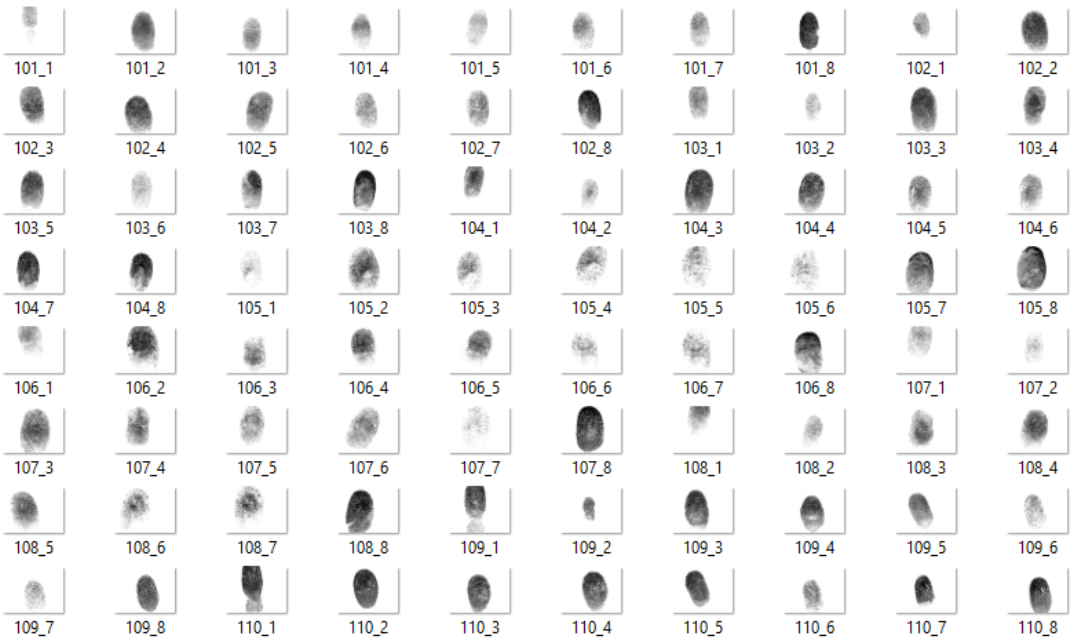
The objective of the thesis study is to enhance the two-stage enhancement scheme [9] in order to improve the fidelity of the gray scale image to enable better feature extraction process. The fingerprint biometric heavily relies on optimal image enhancement as it a feature based biometric system. With the advent of smaller sensors this need for a high fidelity fingerprint image enhancement algorithm has never been observed. It can be verified from the results in chapter 5 that the main purpose of any fingerprint enhancement algorithm being able to enhance a given fingerprint has been met and also bettered the state of the art techniques.

In the case of low quality fingerprint images, visually the enhanced images look much sharper and distinct, and also more unrecoverable sections are recovered compared to the state of the art algorithm discussed in chapter 3. The minutiae ratios, TMR and FMR show improvement in the features extracted from the images enhanced by the LPD based multi-stage scheme compared to the state of the art scheme [16], but due to the multi-tier and multi-stage approach the performance time has increased by 2.5 times which can be a vital penalty for a real time biometric system.

Future work in this scheme would be to optimize the bandpass filter to improve the second stage which is a filtering in the frequency domain, and also use an efficient multi-threaded programming language to better the processing time.

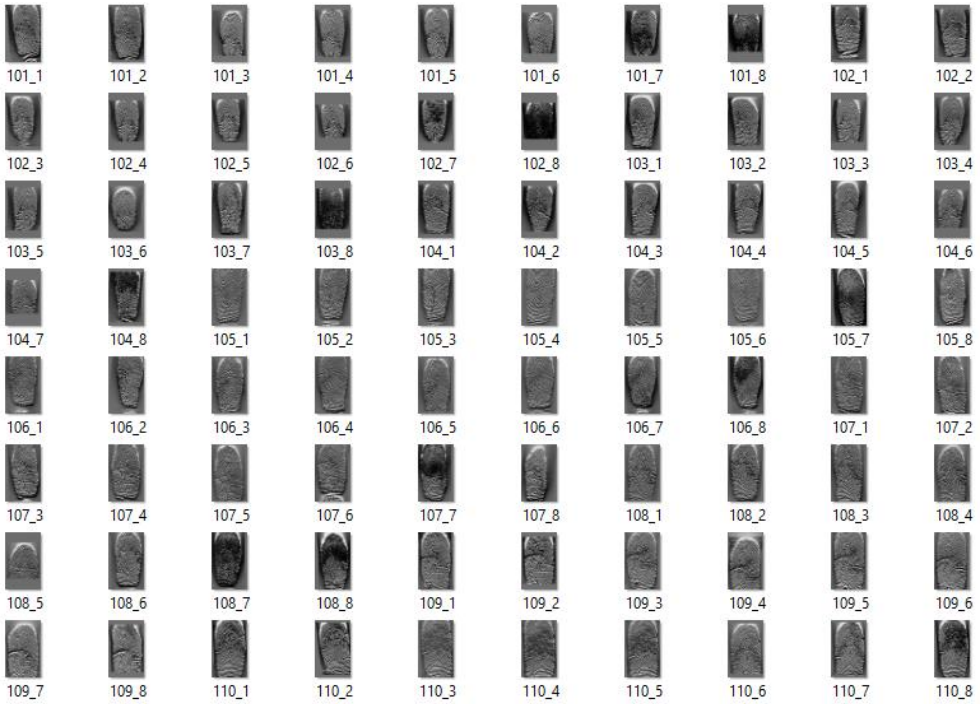
APPENDIX A

Test Sequences

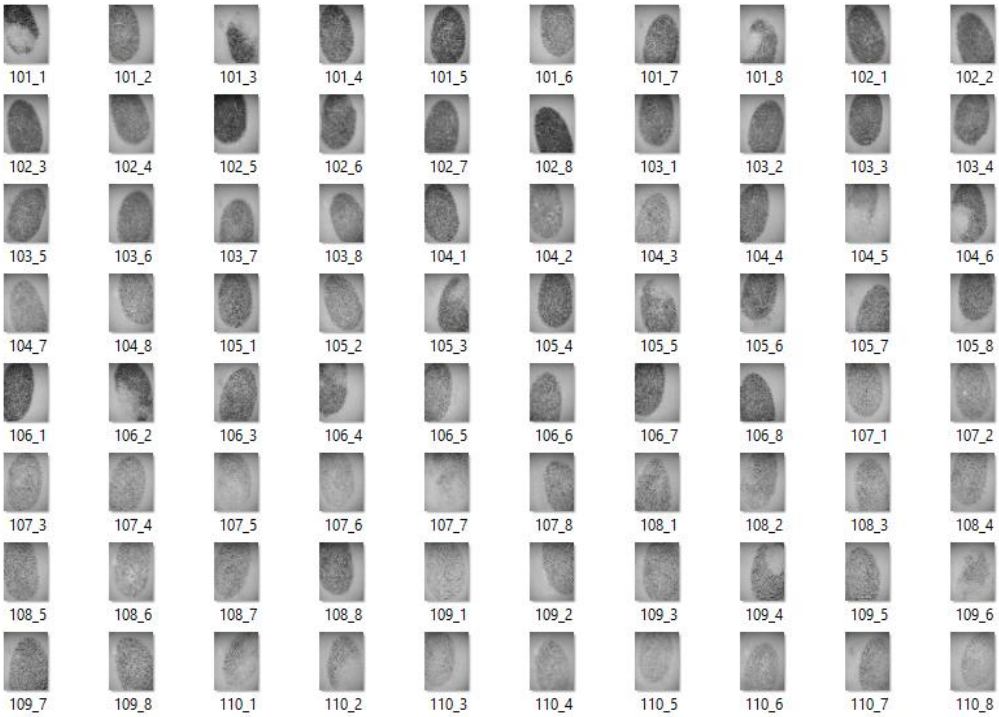


A 1: FVC2004 DB1_B

A 2: FVC2004 DB2_B



A 3: FVC2004 DB2_C



A 4:FVC2004 DB2_D

APPENDIX B

Test Condition

The code was developed and executed using the Mathworks MATLAB R2013a tool which uses a proprietary programming language and has support for image processing using its image processing toolbox [26].

The ‘fingerprint recognition v2.2’ software is used for true minutiae count [36] and the ‘Fingerprint minutiae extraction’ matlab code [37] to compute the total minutiae count and, ratios TMR and FMR.

All the work was done on a system with following configuration:

- Operating System: Windows 10 Home Edition
- Processor: Intel(R) Core(TM) i3-3120M CPU @ 2.50GHz 2.50GHz
- RAM: 8.00 GB
- System type: 64-bit Operating System, x64-based processor

APPENDIX C

Acronyms

AFIS - Automated Fingerprint Identification Systems

CCD - Charge-couple device

CMOS - Complementary metal-oxide semiconductor

DFT – Discrete Fourier transform

DMR - Dropped minutiae ratio

DNA - Deoxyribonucleic acid

EMR - Exchanged minutiae ratio

FFT - Fast Fourier transform

FMR - False minutiae ratio

FVC - Fingerprint verification completion

IFFT - Inverse fast Fourier transform

LMS - Least mean square

LPD - Laplacian pyramid decomposition

LPR - Laplacian pyramid reconstruction

MRTD - Machine readable travel document

MTF - Modulation transfer function

PC - Personal Computer

PIN - Personal Identification Number

PPI - Pixels per inch

STFT - Short-time Fourier transform

TMR - True minutiae ratio

UIDAI - Unique identification authority of India

US-VISIT - United States visitor and immigration status indicator technology

REFERENCES

[1] A. K. Jain, A. A. Ros, and K. NandaKumar, “Introduction to Biometrics”, Springer, 2011.

[2] S. C. Lee, “An Introduction to Identity Management”, SANS Institute, March 2003

[3] Article by V.Maty´aˇs and Z.R´ıha on ‘Biometric Authentication – Security and Usability’: http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf

[4] A. K. Jain, A. Ross, and S. Pankanti, “Biometrics: A tool for information security,” IEEE Trans. Info. Forensics Security, vol. 1, no. 2, pp. 125–143, June 2006.

[5] Article on the Overview of Biometrics: http://www.biometrics.gov/Documents/BioOverview.pdf

[6] Article on the future of Biometrics: http://www.pbs.org/wgbh/nova/next/tech/biometrics-and-the-future-of-identification/

[7] Article on types of Biometrics: http://www.tns.com/biometrics.asp

[8] D. Petrovska-Delacrétaz, G. Chollet, and B. Dorizzi, “Guide to Biometric Reference Systems and Performance Evaluation”, Springer-Verlag, 2009.

[9] J.Yang, N. Xiong, and A. V. Vasilakos, “Two-stage enhancement scheme for low-quality fingerprint images by learning from the images”, IEEE transactions on Human-Machine Systems, vol. 43, no. 2, pp. 235-248, Mar. 2013.

[10] A. K. Jain, “Fundamentals of Digital Image Processing”, Englewood Cliffs, NJ: Prentice Hall, 1989.

[11] R.C. Gonzalez and R.E. Woods, “Digital Image Processing”, 3rd edition, Prentice Hall, 2007.

[12] A. K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Trans. Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[13] L. Hong, Y. Wan, and A.K. Jain, “Fingerprint image enhancement: Algorithm and performance evaluation”. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 8, pp. 777–789, Aug. 1998.

[14] D.K. Misra, S.P. Tripathi and D. Misra, “A Review Report on Fingerprint Image Enhancement Techniques”. International Journal of Emerging Trends & Technology in Computer Science, vol. 2, no. 2, pp. 224-230, April 2013.

[15] S. Greenberg, M. Aladjem, D. Kogan, and I. Dimitrov, “Fingerprint image enhancement using filtering techniques”, ICPR, Vol. 3, pp. 326–329, Sep. 2000.

[16] L. Hong, A.K. Jain, S. Pankanti, and R. Bolle, “Fingerprint Enhancement,” Proc. First IEEE WACV, pp. 202-207, Sarasota, Fla.,1996.

[17] S. Chikkerur, A. N. Cartwright, and V. Govindaraju, “Fingerprint enhancement using STFT analysis”, IEEE Transactions on Pattern Recognition, vol. 40, no. 1, pp. 198–211, Jan. 2007.

[18] Fingerprint Verification Competition database: http://bias.csr.unibo.it/fvc2004/download.asp

[19] Article on Gabor filter: http://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/TRAPP1/filter.html

[20] K.R.Rao, D.N.Kim and J.J.Hwang, “Fast Fourier transform: Algorithms and applications”, Heidelberg, Germany: Springer 2010.

[21] MS thesis paper by S. Chakraborty on ‘Fingerprint enhancement by directional filtering’: http://www.uta.edu/faculty/krrao/dip/Courses/EE5359/Shreya_Paper_v6.pdf

[22] R.C. Gonzalez, R.E. Woods and S.L. Eddins, “Digital Image Processing Using MATLAB”, 2nd edition, McGraw Hill Education, 2010.

[23] Z. Shi and V. Govindaraju, “A chaincode based scheme for fingerprint feature extraction,” IEEE Transactions on Pattern Recognition, vol. 27, no. 5, pp. 462–468, Apr. 2006.

[24] K.G.Darpanis, “Gabor Filters”, York University, April 2007.

[25] O. Marques, “Practical Image and Video Processing Using MATLAB”, 1st Edition, Wiley-IEEE Press, 2011.

[26] Matlab: http://www.mathworks.com/downloads/

[27] Multimedia processing course website: http://www.uta.edu/faculty/krrao/dip/

[28] Visual studio: http://www.dreamspark.com

[29] D. Kumar and Y. Ryu, “A Brief Introduction of Biometrics and Fingerprint Payment Technology,” International Journal of Advanced Science and Technology, vol. 4, pp. 25–37, March 2009.

[30] P.K. Shimna and B. Neethu, “Fingerprint Image Enhancement Using STFT Analysis”, IOSR Journal of Electronics and Communication Engineering, vol. 10, Issue 2, pp. 61-68, Apr. 2015.

[31] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, “Handbook of fingerprint recognition”. Springer, 2003.

[32] P.J. Burt and E.H. Adelson, “The Laplacian Pyramid as a Compact Image Code”, IEEE Transactions on communications, vol. 31, no. 4, pp. 532-540, Apr. 1983

[33] H. F. D. Kunz, K. Eck, and T. Aach, "A Nonlinear Multi-Resolution Gradient-Adaptive Filter for Medical Images", In SPIE Medical Imaging, volume 5032, pages 732–742, May 2003.

[34] A. Jepson, “Notes on Image Pyramids to attenuate noise”: http://www.cs.toronto.edu/~jepson/csc320/notes/pyramids.pdf

[35] H. Fronthaler, K. Kollreider, and J. Bigun, “Local features for enhancement and minutiae extraction in fingerprints,” IEEE Trans. Image Process., vol. 17, no. 3, pp. 354–363, Mar. 2008.

[36] Fingerprint Recognition v2.2 software : http://www.codeproject.com/Articles/97590/A-Framework-in-C-for-Fingerprint-Verification

[37] Fingerprint minutiae extraction code by N.S. Athi: http://www.mathworks.com/matlabcentral/fileexchange/31926-fingerprint-minutiae-extraction/content/Fingerprint_Minutiae_Extraction/Minutuae_Extraction.m

BIOGRAPHICAL INFORMATION

Ramakrishna Lanka was born in Bangalore, Karnataka, India in 1989. He completed his bachelor of technology degree in electronics and communications engineering from Amrita school of engineering, Bangalore in the year 2011.

He worked as Senior Systems Engineer in Infosys Ltd, Bangalore, India from 2011 to 2014. In fall 2014, Ramakrishna enrolled at University of Texas at Arlington to pursue his Master of Science in Electrical Engineering.

Ramakrishna's focus areas are image processing and autonomous systems. He has also done several projects in image processing and robotics. With main focus in the area of image enhancement, he enrolled into MS-thesis study under the guidance of Dr. K.R. Rao. He also worked as an intern at UTA Research Institute during the summer 2015 semester and has been working at the Autonomous systems lab as a research assistant under Dr. F.L. Lewis.