ADDIS ABABA UNIVERSITY
ADDIS ABABA INSTITUTE OF TECHNOLOGY
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

Performance Analysis and Evaluation of Image Enhancement Techniques for Automatic Fingerprint Recognition System using Minutiae Extraction

By: Tesfay Haftu

Thesis Submitted to Addis Ababa Institute of Technology in Partial Fulfillment of the Requirements for the Degree of Master of Science in Electrical and Computer Engineering (Communication Engineering)

Advisor: Dr. -Ing. Dereje Hailemariam

Addis Ababa, Ethiopia

Oct 28, 2018

ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY

SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

Thesis Submitted to Addis Ababa Institute of Technology in Partial Fulfillment of the Requirements for the Degree of Master of Science in Electrical and Computer Engineering (Communication Engineering)

Performance Analysis and Evaluation of Image Enhancement Techniques for Automatic Fingerprint Recognition System using Minutiae Extraction

By: Tesfay Haftu

Approval by Board of Examiners

_____	_____	_____
Chairman Department of Graduate Committee	Signature	Date
Dr. -Ing. Dereje Hailemariam	_____	_____
Advisor	Signature	Date
_____	_____	_____
Internal Examiner	Signature	Date
_____	_____	_____
External Examiner	Signature	Date

DECLARATION

I the undersigned, declared that this MSc thesis is my original work, has not been presented for fulfillment of a degree in this or any other University and all sources and materials used for the thesis are duly acknowledged.

Tesfay Haftu _____

Name Signature

Addis Ababa _____

Place Date of Submission

This thesis work has been submitted for examination with my approval as a University Advisor.

Dr. -Ing. Dereje Hailemariam _____

Advisor's Name Signature

Acknowledgments

First of all, I am thankful for the Almighty God for the good health and well-being that has enabled me to complete this task. Next, I would like to express my deepest gratitude and special thanks to my advisor, Dr. –Ing. Dereje Hailemariam for his continuous support, patience, motivation and immense knowledge. His valuable suggestion and guidance put me on the right track to fulfill the requirement and without his help, it would not possible to present this thesis work. I am also very grateful to my family, colleagues, friends and those who supported me directly or indirectly in many ways for successful accomplishment of this thesis. Finally, I must also acknowledge Information Network Security Agency (INSA) for raising this research idea.

Abstract

The use of biometric recognition is increasing nowadays because the characteristics of biometrics are unique and immutable. Traditional identification methods like tokens and access cards are less reliable than the biometric identifiers because their passwords and personal identifications can be forgotten or stolen electronically. Fingerprint is one of the most widely accepted and reliable biometric personal identification method and is unique even for identical twins.

This thesis work mainly aims on the performance analysis of enhancement techniques used for reliable and high recognition rate automatic fingerprint recognition system (AFRS). The system is executed using the features that make every individual unique. The system accepts a gray scale low quality fingerprint image as an input, enhances the image using the combination of fast Fourier transform (FFT) and Gabor filter to level up its quality. Then features are extracted from a skeletonized binary image and then these features are used to identify who the person is.

The performance measurement metrices of the image enhancement techniques are the number of features detected, computational time, system error rates namely the false match rate (FMR), false non match rate (FNMR) and EER. The MATLAB simulation result shows that the combination of FFT cascaded with Gabor filter gives an accuracy of 95.5 % which is better than the FFT and Gabor filter applied independently.

Key Words: Biometric Recognition, Minutiae, Feature Extraction, Fingerprint, Gabor Filter

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Notations

AFAS	Automatic Fingerprint Authentication System
AFIS	Automatic Fingerprint Identification System
AFRS	Automatic Fingerprint Recognition System
ATM	Automatic Teller Machine
CDF	Cumulative Density Function
CN	Crossing Number
DFT	Discrete Fourier Transform
Dpi	Dots per inch
EER	Equal Error Rate
FAR	False Acceptance Ratio
FBI	Federal Bureau of Investigation
FFT	Fast Fourier Transform
FMR	False Match Rate
FNMR	False Non Match Rate
FRR	False Rejected Ratio
FVC	Fingerprint Verification Computation
GB	Giga Bytes
HE	Histogram Equalization
ID	Identification
IFFT	Inverse Fast Fourier Transform
JPEG	Joint Photographic Experts Group
PIN	Personal Identification Number
ROI	Region of Interest
TB	Tera Bytes

List of Notations

$F\{.\}$	Fourier Transform
$F^{-1}\{.\}$	Inverse Fourier Transform

Chapter 1

1.1. Introduction

Now a days, biometrics has become a potential authentication tool which can address the inherent weaknesses of the traditional knowledge-based (e.g., password) and possession based (e.g., key or token) recognition systems in terms of authenticating genuine individuals [1]. The uniqueness and permanence properties of biometric features such as ridge and valley structure on a fingerprint, geometry of hand, face structure, voice or iris structure have made it possible to replace the traditional knowledge and token based authentication system by more reliable, robust and effective biometric system [2]. Biometric recognition refers to the use of distinctive behavioral and anatomical characteristics for identification and verification of individuals. The use of biometric solution in recognition systems is thus increasing nowadays because they are difficult to be shared or misplaced due to their immutability and individuality properties [1, 3, 4].

The application areas of biometric recognition can be categorized into Authentication and Forensic investigations [5]. Authentication applications are those which require only the authorized persons to access the resources like information systems, National identification (ID) systems, driver registrations, documentations, military area etc. whereas the forensic applications include criminal investigations, terrorist identification, National security, and so on. Since the characteristic of biometric do not change with time, biometric identifiers are more reliable than traditional methods like tokens and access cards because passwords and personal identifications can be forgotten or stolen electronically [6].

Among all the biometrics, fingerprint is the most widely used and reliable personal identification method that is accepted by an individual as the acquisition of fingerprint image is unique, immutable and requires little hardware [1]. It is also easily accessible, recognition requires minimal effort, it does not capture information other than strictly necessary for the recognition process (such as race, health, etc.), and provides relatively good performance. Another reason for its popularity is its availability of relatively low price fingerprint sensors [6]. A fingerprint is the structural pattern of ridges and valleys on the surface of the fingertip. Each person even identical twins sharing the same deoxyribonucleic acid (DNA) has different fingerprint patterns with a permanent uniqueness [2]. Fingerprint recognition system can be implemented using image based

method or minutiae based method [7]. Minutiae's are the features that make for every individual unique. This thesis thus mainly focus on the second type of the algorithm due to its ability to provide high accuracy, high recognition rate and its independence of image scaling and translation that occurs during the acquisition of fingerprint image across the fingerprint scanner with some acceptable image rotation.

1.2. Literature Review

To enforce security and maintain a reliable recognition of any individual using biometric characteristics, a lot of researches have been done which most of them have mainly focused on the fingerprint based recognition system. Most of the automated fingerprint recognition systems (AFRS) depend on one of the two methods i.e. Image based methods and Minutiae based methods. Image-based approaches are directly applied onto the grayscale fingerprint image without preprocessing to extract the features and hence they can achieve high computational efficiency. However, image-based approaches do not have the ability to track with variations in position or translation, image rotation, image quality distortion and also they need more data storage [7]. The minutiae based fingerprint recognition system is the most commonly used method because the minutiae features can be extracted from a slightly rotated, distorted fingerprint image and extraction of these feature points does not require a high-resolution image [8]. Some of the reviewed related works on fingerprint recognition system are given as follows.

Marius Tico, Eero Immonen at el. [2001], worked on Fingerprint Recognition using Wavelet Features by detecting a core point as a reference point. Only two features namely the mean and the variance are extracted from the transformed low frequency image. These two features are not sufficiently enough to uniquely determine the individuals [7]. The paper finally states that, minutiae algorithm is the most prominent classes of fingerprint matching methods.

Ting Tang [2012], worked on Fingerprint Recognition using Wavelet Domain Features by detecting the core point as a reference by enhancing the image. An image is cropped around the detected reference core point and then a wavelet transform is applied to each blocks of the cropped image. From the transformed images, 1152 features are extracted to be used for matching and this algorithm takes more computational time in matching [9].

Pankaj Bhowmik, Kishore Bhowmik at el. [2012], worked on Fingerprint Image Enhancement and its Feature Extraction for Recognition [2]. This paper first acquires the fingerprint image and then next the combination of two image enhancement processes i.e. Discrete Fourier Transform (DFT) and Histogram equalization (HE) reconstructs the information of the low quality fingerprint image. The main steps are Image Acquisition, Image enhancement, Binarization, Thinning and Feature Extraction. This paper do not consider the region of interest (ROI) and hence image processing on the noisy background takes place which in turn results in computational inefficiency and extracting false features.

Kondreddi Gopi and J.T Pramod [2012], worked on Fingerprint Recognition using Gabor Filter and Frequency Domain Filtering [10]. This paper proposes to use a combination of fast Fourier transform (FFT) and Gabor filtering to carry out the image enhancement task. An algebraic sum of FFT enhanced and Gabor based enhanced images is made and the resulting image is binarized to get the final enhanced image. However, the orientation and frequency of the fingerprint image are estimated directly from the low quality image.

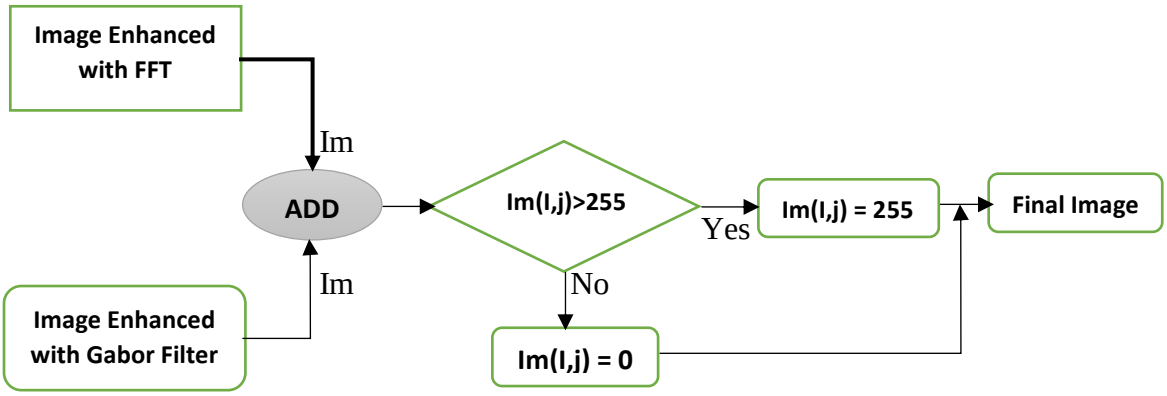


Figure 1.1. Block Diagram of Gabor with FFT Based Fingerprint Enhancement Method [10]

After the image is enhanced,

- ✓ Minutiae points are extracted from a skeletonized image
- ✓ Euclidian Distance is used for performance of recognition
- ✓ Needs post processing for false feature removal

The paper concludes that, "the overall recognition rate obtained from the proposed method is 95% which is much better compared to histogram method where the recognition rate is 64%".

Neeraj Bhargava, Ritu Bhargava at el. [2013], worked on Fingerprint Minutiae Matching using ROI [11]. This paper extracts the features namely the terminations and bifurcations by enhancing the image using HE and extracts the ROI to avoid processing and extraction of minutiae from the noisy part of the fingerprint image. However, HE has no the ability of connecting the discontinuous damaged ridges and it is not a powerful tool in removing artefacts. As a result, false removal algorithm is required to remove spurious minutiae and the matching performance is too much low.

Aliyu Tukur [2015], worked on Fingerprint Recognition and Matching using Matlab by extracting the feature points from sample fingerprint images and then performs matching based on the number of minutiae pairing among the two fingerprints in question. Edge detection is used to extract the ridges of the fingerprint. The features are extracted directly from the detected edges and a threshold of 90% is used during matching stage which results high false non match rate (FNMR). This method depends highly on the quality of the image and finally the paper recommends to enhance the low quality images to improve the matching performance [12].

Aneesha Karar, Amarjeet kaur at el. [2015], worked on Fingerprint Enhancement and feature extraction using minutiae extraction of ridge ending and bifurcation [8]. This paper states that minutiae representation is the most popular fingerprint representation method and the enhancement stage plays a very important role in image processing because it helps to improve the low contrast images. Local histogram equalization, wiener filtering, anisotropic filter which is based on the partial differential equation, binarization and thinning are used to enhance the image quality for better feature extraction and improve matching accuracy.

a) Enhanced image | b) Binary Image | c) Thinned Image | d) Extracted Features

Figure 1.2. Processed Fingerprint image and Extracted Features [8]

From the results of [8], (Figure 1.2(b and c)), the local HE, wiener filter and anisotropic filer have no ability to improve the image quality, have no ability of connecting damaged ridges, rather it

introduces many artefacts during thinning process, and hence the extracted features are so much denser than from the real feature of the original fingerprint (Figure 1.2d). This leads to post processing to remove false detected features which in turn leads to computational inefficiency, increased false match rate (FMR), high FNMR and high equal error rate (EER).

In general, Wavelet based fingerprint recognition procedures are quite sensitive to the variation in scaling and rotation. There is also loss of a significant amount of information during decomposition because the image data is decimated by four in every level of decomposition. High number of features are extracted which results in expensive computation in matching, features are statistical like mean and variance that they can't uniquely determine for an individual and these features varies with quality of the grayscale of the fingerprint image. Wavelet based needs a preprocessing for core detection as a reference point and all individuals may not have core, delta or both singular points and loss of information during cropping when the reference point is located around the border of the fingerprint image [7, 9].

Therefore, from the review, minutiae based recognition system is the most commonly used because it needs less data storage space, it is relatively less sensitive to scaling and rotation than of wavelet and image based recognition system, but its performance depends highly on the quality of the fingerprint image. In this thesis, the combination of FFT and Gabor filter where the parameters used to model Gabor filter are estimated from the FFT based enhanced image is the technique used to increase the image quality of the fingerprint.

1.3. Statement of the Problem

As the daily life activities of human being has become electronically connected and more mobile, representations of identity such as passwords and smart cards cannot be trusted to establish a person's identity. Cards can be lost or stolen and passwords or Personal Identification Number (PIN) can in most cases be guessed or shared. Manual fingerprint verification is also so tedious, time consuming, increased workloads and it is so expensive. Thus AFRS is a solution as it is a reliable personal identification method that is immutable and unique for each individual. The minutiae based method is an accurate method of feature extraction in AFRS, but it highly depends on the image quality of the fingerprint. HE, FFT and Gabor filter are the enhancement techniques used to level up a poor image quality. The main problem in applying Gabor filter is, the ridge orientation and frequencies of the fingerprint that are used to model the filter are estimated from the original low quality fingerprint images. Thus, false ridges that are oriented in unwanted direction at the damaged ridges are enhanced and introduce false features. This causes computation inefficient and lowers the performance and accuracy of the recognition system.

1.4. Objective of the thesis

This thesis is focused to achieve the following general and specific objectives.

1.4.1. General objective

The general objective of this thesis is performance analysis and evaluation of image enhancement techniques for fingerprint recognition system using minutiae extraction method.

1.4.2. Specific objectives

- ✓ To understand feature extraction techniques
- ✓ To evaluate different image enhancement techniques
- ✓ To estimate the ridge orientation and frequency from an FFT enhanced image
- ✓ To simulate fingerprint recognition algorithm on free test database
- ✓ To evaluate the implementation using free test databases

1.5. **Methodology**

The formal methodologies used to achieve the objectives of this thesis work are:

Literature review: includes reading books, articles, simulation tools and other resources related image enhancement techniques, feature extraction algorithm, classification and other related papers in detail.

System modeling and simulation: includes mathematical modeling of Gabor filter, feature extraction, fingerprint recognition algorithm and simulating the modeled algorithm, using MATLAB.

Performance comparison: this includes the performance comparison of image enhancement techniques on feature extraction and matching stages. It also includes evaluating the implementation using free test databases.

Result and conclusion: the results obtained from the implemented system is studied.

Recommendation: at the end a recommendation for the feature research work is given.

1.6. **Thesis Organization**

This thesis is organized into five chapters. The first Chapter deals about the proposal of implementation of AFRS, the second Chapter deals about the overview of biometric recognition and specifically fingerprint biometrics, features of fingerprint and some image processing to be applied on fingerprint image, Chapter three deals about the system model of fingerprint recognition system including the image enhancement, feature extraction and matching, the fourth Chapter deals about system analysis, simulation results and discussion found from Chapter three and finally Chapter five deals about the conclusion and recommendation.

Chapter 2

Theoretical Background of Biometric Recognition

2.1. Introduction

The word biometrics is derived from the Greek words bios meaning life and metron meaning measurement, and hence collectively, biometric identifiers means measurements taken from living human body [4]. Therefore, Biometric recognition (or simply biometrics) refers to the use of distinctive anatomical and behavioral characteristics, called biometric identifiers or traits for automatically recognizing individuals [3, 4, 13]. Recognition of persons on the basis of biometric features is an emerging phenomenon in our society. It has received an increasing attention in recent years due to the need for security in a wide range of applications, such as replacement of the PIN in banking and retail business, security of transactions across computer networks, high-security wireless access, tele voting, and admission to restricted areas [6].

Traditional systems that are used to verify a person's identity are based on the knowledge (secret code) or possession (ID card). However, as our daily life activities has become electronically connected and more mobile, surrogate representations of identity such as passwords (prevalent in electronic access control) and cards (prevalent in banking and government applications) cannot be trusted to establish a person's identity [6]. Codes, passwords or PIN, in most cases, can be guessed, forgotten or overhead, and ID cards can be lost or stolen, giving impostors the possibility to pass the identity. Further, passwords and cards can be easily shared and so they do not provide non-repudiation. Hence biometrics is becoming an essential component of effective person identification solutions that replaces cards, keys, and codes in order to decreases the possibility of fraud significantly because biometric identifiers are inseparable from a person's body which cannot be shared or misplaced, and they intrinsically represent the individual's identity [4].

All biometric identifiers are perhaps a combination of anatomical and behavioral characteristics and they should not be exclusively classified into either anatomical or behavioral characteristics. For example, fingerprints are anatomical in nature but the usage of the input device (e.g., how an individual presents a finger to the fingerprint scanner) depends on the person's behavior. Thus, the input to the recognition engine is a combination of anatomical and behavioral characteristics. A

number of questions related to a person's identity are asked every day in a variety of contexts such as, is this person authorized to enter the facility? Is this individual entitled to access privileged information? Is this person wanted for a crime? Has this person already received certain benefits? Is the given service being administered exclusively to the enrolled persons? Reliable answers to questions such as these are needed by business and government organizations. Because biometric identifiers can't be easily misplaced, forged, or shared, they are considered to be more reliable for person recognition than traditional token (ID cards) or knowledge-based (passwords or PIN) methods [4].

Many biometric features can be distinguished like fingerprint, iris, face, voice, hand geometry, retina, handwriting, gait, and more [3]. For several reasons, the fingerprint is considered one of the most practical biometric features. Fingerprints are easily accessible, recognition requires minimal effort on the part of the individual, it does not capture information other than strictly necessary for the recognition process (such as race, health, etc.), and provides relatively good performance. Another reason for its popularity is that its availability of relatively low price of fingerprint sensors. Fingerprint sensors can be built in personal computer (PC) keyboards, smart cards and these sensors can also be integrated easily in wireless hardware such as cell phones [6].

The objectives of biometric recognition are user convenience (e.g., money withdrawal at an automatic teller machine (ATM) machine without a ID card or PIN), better security (e.g., only authorized person can enter a facility), better accountability (e.g., difficult to deny having accessed confidential records), and higher efficiency (e.g., lower overhead than passwords). The tremendous success of fingerprint-based recognition technology in law enforcement applications, decreasing cost of fingerprint sensing devices, increasing availability of inexpensive computing power, and growing identity fraud/theft have all resulted in increasing the use of fingerprint-based person recognition in commercial, government, civilian and financial domains [4].

2.2. **Biometric System Overview**

Biometric systems are mechanisms that are used to identify a particular person using biological characteristics of the individual. The biometrics of the human body is the most reliable and secure, since they cannot be changed with time and cannot be stolen or forgotten as of the passwords. An important issue in designing a practical biometric system is to determine how an individual is

going to be recognized. Depending on the application context, a biometric system may be called either a verification system, identification system and/or classification system [6].

A verification system authenticates a person's identity by comparing the captured biometric characteristic with the previously captured (enrolled) biometric reference template that is pre-stored in the system. It conducts a one-to-one comparison to confirm whether the claim of identity by the individual is true or not. Such systems receive two inputs namely the claimed identity of the person requesting authentication (usually a username, ID number or smart card) and the live-scanned fingerprint of that person. The claimed identity is used to retrieve a reference fingerprint stored in a database and is matched (compared) against the currently offered fingerprint (the test fingerprint). A verification system either rejects or accepts the submitted claim of identity [12]. Verification is used to prevent multiple people from using the same identity.

An Identification systems receive only one input, namely the live-scanned query fingerprint image. An identification system recognizes an individual based on the live-scanned query fingerprint by searching from the entire previously enrolled template database for a match. It conducts one-to-many comparisons to establish if the individual is present in the database or not [12]. A person is identified if a matching fingerprint is found in the database. On the other hand, if no matching fingerprint is found in the database, the person is rejected [6].

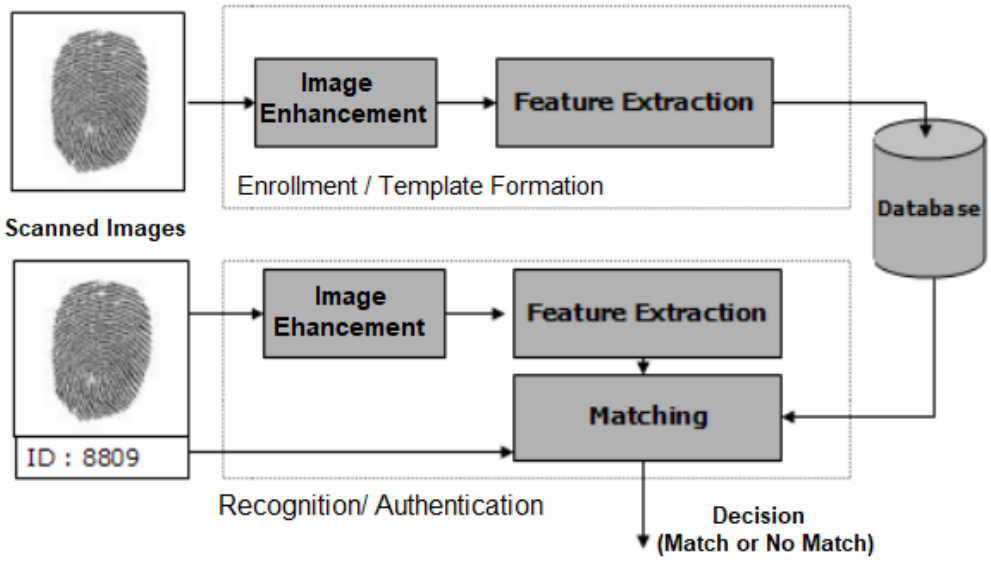


Figure 2.1. A typical Fingerprint identification/Verification Process [14]

Fingerprint classification system is used to determine which class (or group) the input fingerprint belongs to. These systems receive only a single fingerprint as input. A well-known set of categories is formed by the *Henry* classes, where fingerprints can be categorized based on their global pattern of ridges and valleys as a Whorl, left loop, right loop, tented arch and arch [2].

For both verification and identification systems, enrollment is an important step. Enrollment is the process of taking reference fingerprints of all individuals and storing these in the database for later comparison [6]. Any human anatomical or behavioral trait can be used as a biometric identifier to recognize a person as long as it satisfies the following requirements [4]:

1) ***Universality****:* Only very few people miss all the ten fingers. Most fingerprint recognition systems allow to enroll multiple fingers which avoids that an individual is no longer granted access after injury.
2) ***Uniqueness*****:** Any two persons should be sufficiently different in terms of their biometric traits. It is generally accepted that fingerprints are unique to an individual i.e. no two people have identical characteristics even in identical twins. However, there is a risk that fingerprints of two different individuals match if the fingerprint image is of insufficient quality. Therefore the False Acceptance Rate (FAR) and False Reject Rate (FRR) are highly dependent on the quality of the fingerprint image and/or reader.
3) ***Permanence*****:** The biometric characteristics should not vary with time. A person's face, for example, may change with age. However, fingerprints do not change with ageing. Injuries, such as fire wounds can damage a fingerprint but if multiple fingers are enrolled, the likelihood of an authorized individual being denied access is reduced.
4) ***Collectability*****:** The characteristics must be easily collectible and measurable. Biometric trait can be measured quantitatively. However, in a practical biometric system, there are a number of other issues that should be considered in selecting a trait, including:
   - ✓ *Performance:* The biometric can be measured in terms of recognition accuracy, speed, resource requirements, and robustness to operational and environmental factors. Generally, the method must deliver accurate results under varied environmental circumstances.
   - ✓ *Acceptability*: The extent to which individuals are willing to accept the biometric identifier in their daily lives. The general public must accept the sample collection routines. Fingerprints are easily accepted as soon as people reflect that they leave their fingerprints

everywhere and that no sensitive information, such as medical conditions, can be derived from fingerprints. Nonintrusive methods are more acceptable.

- ✓ *Circumvention*: The technology should be difficult to deceive. There are a number of concerns when using fingerprint recognition. Some of the cheapest devices can be fooled by a cut off finger or it can be even fooled by a fingerprint image that is printed on paper or transparency. Fingerprint sensors with liveness detection can resolve this issue since they are difficult to make fool.

In general, a practical biometric system should have acceptable recognition accuracy and speed with reasonable resource requirements, harmless to the individuals, accepted by the intended population, and sufficiently robust to various fraudulent methods.

2.3. **Benefits of Biometrics**

There are many benefits of using biometrics as an authentication tool over the knowledge based or token-based traditional tools. Access to personal computers, networks and applications, access to secured areas of a building, authorization at ATM and transaction in online banking are some common applications of knowledge-based authentication systems. Handheld tokens such as cards and key fobs are used mainly for building access but they have replaced with passwords in some high security applications. The generation of PIN using key generator for online banking is an example of this. However, passwords, PINs, tokens or cards have a number of weaknesses that may raise concern about their suitability in modern applications, especially high-security applications such as access to online financial accounts or medical data [6].

The authentication mechanism can be implemented by any of the followings or combination of these [15]

- ✓ Something you know such as passwords and PINs.
- ✓ Something you have such as smart cards, keys or tokens.
- ✓ Something you are, which refers to biometrics- the measurement of physical characteristics or personal traits.

The knowledge based system which is based on passwords and PINs is still most widely used authentication system but the shortcomings of the knowledge-based or token based authentication

can be overcome by the introduction of biometrics. Some of the benefits of biometrics are reduced fraud, increased security, increased convenience and efficiency, and increased accountability [4].

Increased Security*:* Biometrics can provide an enhanced level of security to the traditional authentication methods by allowing access only to authorized persons while restricting access or protect data from unauthorized ones. Although password is meant to be confidential, should be hard to guess and should not be written down, in practice, people can often forgot their passwords, sometimes share it with their friends and colleagues. Good passwords such as long passwords with numbers and symbols, are difficult to remember for most individuals and are rarely enforced. Many persons use obvious words or numbers to make passwords and PINs that can be easily guessed so unauthorized persons can break into account with little effort.

On the other hand, biometric data cannot be guessed or stolen in the same way as password or token. Biometric authentication can be used to allow individuals to access higher level of rights and privileges. Highly sensitive and critical information can be readily available on a biometrically protected network than on one protected by passwords. Therefore, a biometric system provides better security than of the knowledge based traditional tools.

Increased convenience and efficiency: As computer users are forced to manage a number of passwords, the likelihood of passwords being forgotten increases unless the user choose to use a universal password for every login, which in effect reduces the security. Therefore, for computer applications, where users can have access to multiple resources, biometric can simplify the authentication process by replacing multiple passwords and thus reduce the burden on both the user and the system administrator. In general, since biometrics are always attached with the person and so there is nothing to forget, it offers a greater user convenience (e.g., money withdrawal at an ATM machine without a card or PIN) than systems based on remembering multiple passwords. It also provides higher efficiency (e.g., lower overhead than computer password maintenance).

Increased accountability*:* The increased awareness of security in the enterprise and service industry has put a huge demand on auditing and reporting capabilities. Biometric system is difficult to deny having accessed confidential records. Therefore biometrics is a very useful tool to secure computers, facilities and offer a high degree of certainty as to what an individual has accessed in which computer at what time.

2.4. **Classification of Biometric Traits**

There are two main categories of biometric traits [4, 15]:

1. Physiological traits: show all static data of a person such as, fingerprints, iris pattern, and shape of the hand or the face image.
2. Behavioral traits: it refers to the actions taken by the person concerned, and then talks about his writings, audio track, and method of pounding the keyboard.

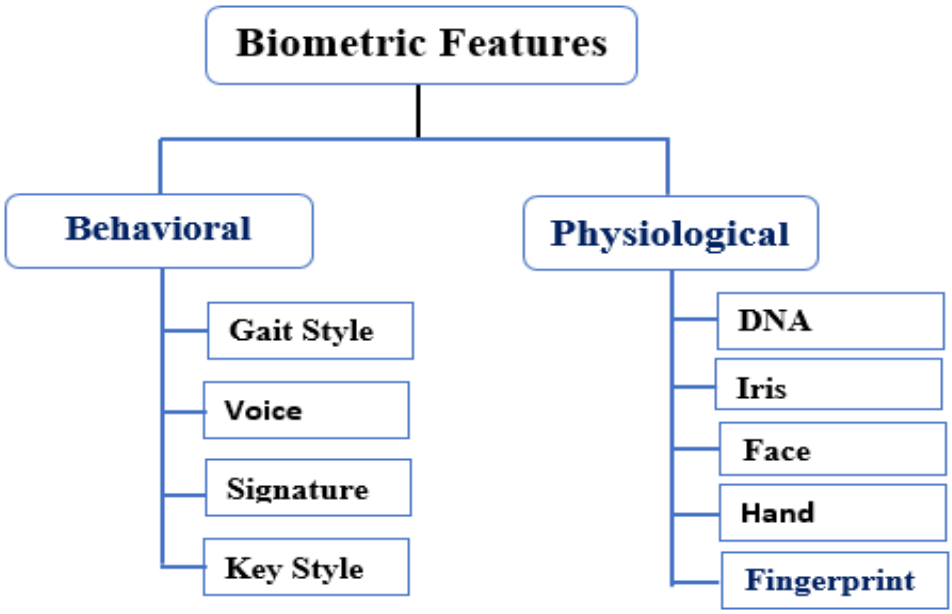


Figure 2.2. Biometric Features[15]

2.4.1. Behavioral Biometrics

Behavioral biometrics are leaned or evolved and temporal in nature, can be changed during the life time of an individual. These traits involve measuring the way in which an individual performs certain tasks. Behavioral biometrics include Gait, Speech, Signature, Handwriting etc. [16].

Gait Style: Gait-based recognition involves identifying a person's walking style. Although these systems are currently very limited, there is a significant amount of research being conducted in this area. Furthermore, studies have shown that gait changes over time and is also affected by clothes, footwear, walking surfaces, and other conditions [16].

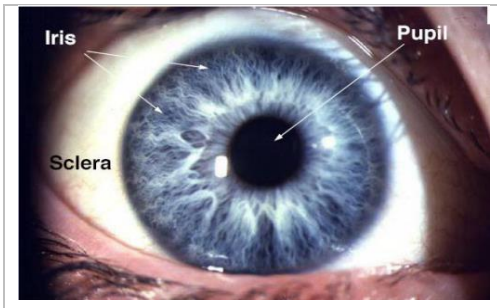
Voice: voice capture is unobtrusive and voice may be the only feasible biometric in applications requiring person recognition over a telephone. Voice is not expected to be sufficiently distinctive to permit identification of an individual from a large database of identities. Moreover, a voice signal available for recognition is typically degraded in quality by the microphone, communication channel, and digitizer characteristics. Voice is also affected by factors such as a person's health (e.g., cold), stress and emotional state. Besides, some people seem to be extraordinarily skilled in mimicking others voice [4].

Signature: the way a person signs his name is known to be a characteristic of that individual. Signatures have been acceptable in government, legal, and commercial transactions as a method of recognition for a long time. Signature is a behavioral biometric that changes over time and is influenced by physical and emotional conditions of the signatories. Signatures of some subjects vary a lot, even successive impressions of their signature are significantly different. Furthermore, professional forgers can reproduce signatures of others to fool the unskilled eye [4].

2.4.2. Physical Biometrics

Physical biometrics are the anatomical characteristics of an individual that are fixed through the lifetime and unique such as iris, face, hand geometry, DNA and fingerprint [15].

Iris of an eye: - visual texture of the human iris is determined by the chaotic morphogenetic processes during embryonic development and is believed to be distinctive for each person and each eye [4]. The features of iris are fixed and do not change over the life time of an individual and therefore does not require renewal scanning and updating the data stored in the security databases. Iris of an eye is one of the most accurate biometric features in humans and it is also difficult to manipulate it [17]. An iris image is typically captured using a noncontact imaging process. Capturing an iris image often involves cooperation from the person, both to register the image of iris in the central imaging area and to ensure that the iris is at a predetermined distance from the focal plane of the camera. [4].



a) Human eye

b) Iris scanner

Figure 2.3. Iris Pattern and Manipulations [16, 17]

***Face*: -** face is one of the most acceptable biometric traits and it is one of the most common methods of recognition that humans use in their daily visual interactions [4]. An individual can be identified by looking at him in the face by focusing on the dominant parts such as big ears, aquiline nose, mouth, head shape, etc. [17]. In addition, the method of acquiring face images is nonintrusive. It is very challenging to develop face recognition techniques that can tolerate the effects of aging, facial expression, variations in the imaging environment, and facial pose with respect to the camera [4].

Figure 2.4. Facial Recognition [16]

Hand Geometry: - human hand is also one of the most basic biometrics used for recognition of individuals in everyday life [16]. It is important to know that each individual possesses exclusively special hands because of their length, width, thickness and a particular curvatures [17]. A two-dimensional system can be implemented with a simple document scanner or digital camera, as these systems only measure the distances between various points on the hand. The geometry of the hand, however, is not a very distinctive quality to an individual. In addition, wearing jewelry or other items on the fingers may adversely affect the system's performance [16].

a) Hand Geometry Biometrics

b) Commercial three dimensional scanner

Figure 2.5. Hand Geometry and Scanner [16, 17]

Fingerprint

A fingerprint is one of from the physiological biometric solution used in recognition systems [18]. Each person has different patterns of fingerprints with the permanent uniqueness. Some of the fingerprint features are crossover, core, delta, island, sweat pores, ridge termination and bifurcation. Figure 2.6 shows an example of scanned fingerprint image with its features.

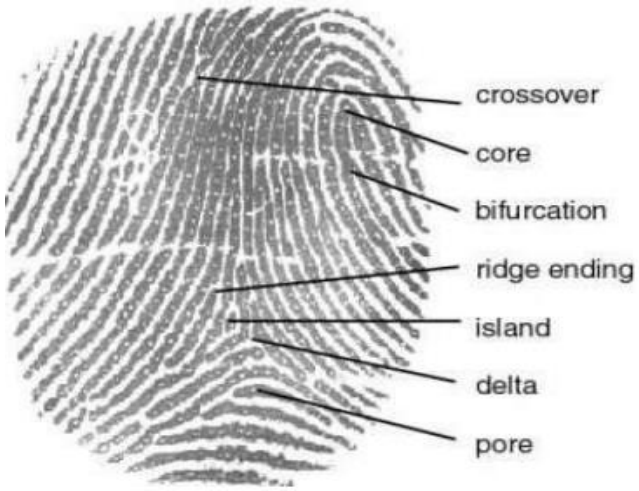


Figure 2.6. A typical fingerprint with its features[17]

The advantages and disadvantages of different behavioral and physical biometric traits are summarized in Table 2.1. From the table, it can be concluded that fingerprint is better than of the other biometrics because it is easy to use, most economical, needs small storage and gives high accuracy.

Table 2.1. Advantages and disadvantages of different biometric technologies [13]

Technology	***Advantages***	***Disadvantage***
Fingerprint	- Very high accuracy - Easy to use - Most economical & developed biometric technique - Small storage space required for the template to be stored - It is standardized	- It is intrusive for a person because it's related to criminal identification - It can make mistakes with the dryness or dirty of the finger's skin - Not appropriate for children, because the size of their fingerprint changes quickly
Facial recognition	- Non-intrusive or no contact is required - Commonly available sensors - Easy for humans to verify results	- Face can be obstructed by hair, glasses, hats, scarves etc. - Sensitive to changes in lighting, expression and pose - Faces change over time
Hand Geometry	- Easy to capture - High stable pattern over the adult lifespan - Usually used for verification of a claimed enrolment identity	- Requires some training to the user - Not sufficiently distinctive over large databases - Requires a large amount of physical space
Voice Recognition	- No contact is required - Has a public acceptance - Commonly available sensors - Cheap technology	- Difficult to control the sensor and channel variances - Not sufficiently distinctive over large database
Retina/Iris Recognition	- Very high accuracy - No way to replicate a retina - No need of liveness detection	- It is very intrusive i.e. it has the stigma of person's thinking that it is potentially harmful to the eye - Needs lot of memory Space - Complex and very expensive
Signature Recognition	- Non – intrusive - Little time of verification - Cheap technology	- Difficulty of enrolling and verifying in signature verification - Error rate: 1 in 50
DNA	- Very high accuracy - No way to replicate DNA	- Extremely intrusive - Very expensive

The biometric identifiers described in the above section are compared in Table 2.2.

Table 2.2. Comparison of commonly used biometric traits [4, 15]

Factors → / **Biometric Identifier** ↓	***Universality***	***Distinctiveness***	***Permanence***	***Collectability***	***Performance***	***Acceptability***	***Circumvention***	***Accuracy***	***Remarks***
Face	H	L	M	H	L	H	H	L	
Fingerprint	M	H	H	M	H	M	M	H	
Hand Geometry	M	M	M	H	M	M	M	L	H High
Hand/Finger Vein	M	M	M	M	M	M	L	M	M Medium
Iris	H	H	H	M	H	L	L	H	L Low
Signature	L	L	L	H	L	H	H	L	
Voice	M	L	L	M	L	H	H	L	
DNA	H	H	H	L	H	L	L	H	

Note from the Table 2.2 that fingerprint has a nice balance among all the desirable properties. Every human being possesses ten fingers (with the exception of hand-related disability). Fingerprints are very distinctive and permanent, even if they temporarily change slightly due to cuts and bruises on the skin, the fingerprint reappears after the finger heals *[4]*. Fingerprint is intrusive and it has a stigma of individual's thinking that it is highly associated with criminality because it is used by forensic divisions for criminal investigation for a long time. However, this is rapidly changing with high demand for automatic person recognition to fight identity fraud and security threats.

2.5. **Fingerprint Biometric**

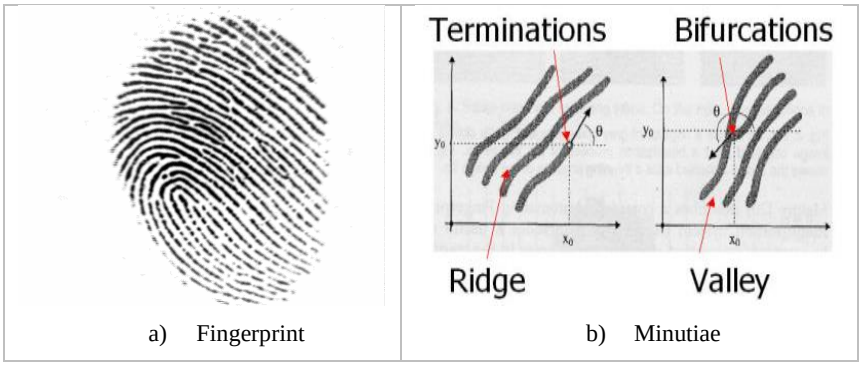
2.5.1. Introduction

Fingerprint is one of the physiological biometric characteristic used for personal recognition and forensic investigation purpose, which depends on the ridge lines, valley lines and the formations deployed on the surface of human skin at the fingertips [17] as shown in Figure 2.6.

2.5.2. Formation of Fingerprints

The formation of the structure of fingerprints depends on the initial conditions of the embryonic development (i.e. Fingerprints are fully formed at about seven months of the fetus development). Their ridge pattern is unchanged throughout the entire life time of an individual (immutability) except due to accidents such as bruises and cuts on the fingertips [4]. In addition, scientific studies of fingerprints shows that, no two fingerprints from different fingers have been found to have the same ridge pattern (uniqueness). The probability that two fingerprints that come from different fingers are alike is 1 in 1.9×10^{15} [2, 13]. Both the immutability and the uniqueness properties have determined the use of fingerprint matching as one of the most reliable and attractive techniques of people recognition [19].

A fingerprint is the pattern of ridges and valleys on surface of a fingertip with the permanent uniqueness where ridges are marked as dark lines while valleys as light areas between the ridges [20] as shown in Figure 2.7.



a) Fingerprint b) Minutiae

Figure 2.7. Fingerprint and Minutiae (Ridge, Valley, Termination and Bifurcation)[20]

A fingerprint is formed from an impression of the pattern of ridges on a fingerprint reader. Fingerprint readers utilize these lines and formations to scan fingerprint image and store in computerized systems [17].

2.5.3. Fingerprint Features

Extensive research has been done on fingerprints and two of the fundamental important conclusions that have risen from the researches are [16]:

- ✓ A person's fingerprint will not naturally change its structure about one year after birth and

- ✓ The fingerprints of individuals are unique. Even the fingerprints in twins are not the same. In practice two humans with the same fingerprint have never been found.

Fingerprint features are very important in recognition process and are generally categorized into three classes [16, 21] as shown in Figure 2.8.

1) Level 1 features mainly refer to the macro details of the ridge flow shape such as the ridge orientation field and features derived from it like singular points and pattern type.
2) Level 2 features refer to the ridge skeleton and features derived from it, such as ridge bifurcations and ridge endings and these features are discriminative enough for recognition.
3) Level 3 features include ridge contours, position, width, and shape of sweat pores and incipient ridges

The detail study of these features is presented in the following section.

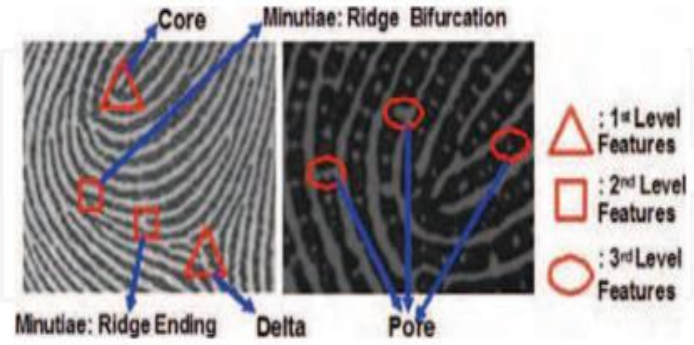


Figure 2.8. Three levels of fingerprint features [16]

2.5.4. Fingerprint Representation

There are mainly four different types of fingerprint representations that are used in fingerprint recognition systems and each one has its own advantages and drawbacks. These are image based representation, global feature representation, local feature representation and intra ridge detail feature representation [21].

2.5.5. Image-based representation

In an image based representation, the fingerprint image itself is stored in database to be used as a template. There is no need for a specific feature extracting algorithm, and the raw intensity pixel

values are directly used. This representation retains the most information about a fingerprint since fewer assumptions are made about the application. However, a fingerprint recognition system that uses the image-based representation requires tremendous storage space. For example, a 0.8mm × 1.0mm (400 ×500 pixels) fingerprint is obtained by a scanner at 500 dots per inch (dpi) with 8 bits gray-scale resolution. The resulting size of the fingerprint image is [16]

Image size = 400 x 500 x 8 = 1,600,000 bytes = 1.52 Mbytes

A system with large amount of fingerprint data may have difficulty of storing all the templates. For example, Federal Bureau of Investigation (FBI) has collected more than 200 million fingerprints since 1924 which require more than 250 Terabytes storage space [19]. Traditional compression techniques, such as Joint Photographic Experts Group (JPEG) [22] tend to lose the highest frequency details, which contain discriminating information and the blocking artifacts also affect the performance of AFRS. Although there is a compression method which can preserve the discriminating information without blocking artifacts while achieving a high compression ratio (around 20:1), it still requires about 20 Kbytes to store a compressed fingerprint image [19].

2.5.5.1. *Global Features Ridge Pattern*

A fingerprint is a pattern of alternating convex skin called ridges and concave skin called valleys with a spiral curve like line shape (Figure 2.10). There are two types of ridge flows namely the pseudo-parallel ridge flows and high-curvature ridge flows which are located around the core point and/or delta point(s). This representation relies on the ridge structure, global landmarks and ridge pattern characteristics. The commonly used global fingerprint features are Singular points [21].

Singular points – these features are a discontinuities in the orientation field of the fingerprint ridge flow. There are two main types of singular points that define the shape of a fingerprint. These are cores and deltas (also collectively known as macro-singularities). A core is the uppermost of the innermost curving ridge i.e. a point where a single ridge line turns through 180 degrees and a delta is the junction point where three ridge lines meet and form a triangle. These core and delta points characterize the overall shape of the fingerprint [21, 23]. It can be seen in Figure 2.9 where the cores and deltas are marked.

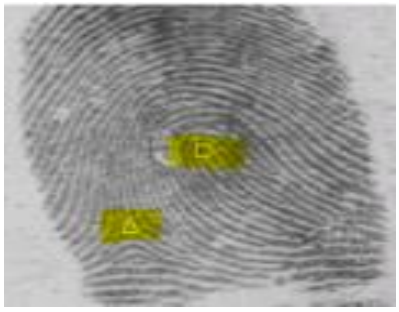


Figure 2.9. Sample fingerprints, with core and delta points [16]

Singular points (core and delta) and coarse ridge line shape are useful for fingerprint classification and indexing, but their distinctiveness is not sufficient for accurate matching. This representation is sensitive to the quality of the fingerprint images and the discriminative ability of this representation is limited due to the absence of singular points [24, 25]. When observing the patterns of a fingerprint form together created a classification of fingerprints into five classes [26]. These classes are, arch, tented arch, left loop, right loop and whorl. Arches can be easily identified through the lack of any delta or core points. Also, whorls can be easily identified through the presence of two core and two delta points. Differentiating the right loop, left loop and tented arch is slightly more difficult, as all three have one core and one delta point [25].

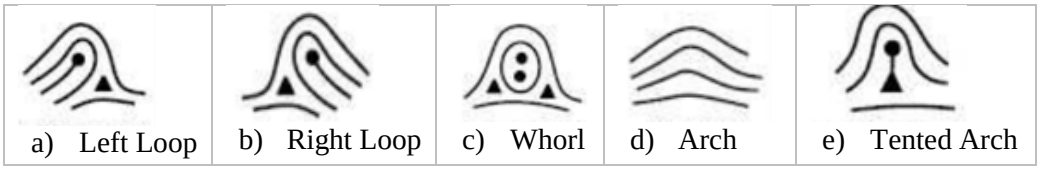


Figure 2.10. Global Fingerprint Ridge Flow Patterns [21]

External fingerprint shape, orientation image, and frequency image also belong to the set of features that can be detected at the global level [4, 21].

- **Ridge orientation** – is defined as the local direction of the ridge-valley structure. It is commonly utilized for classification, minutiae feature verification, image enhancement and filtering.
- **Ridge frequency** – is defined as the reciprocal of the inter ridge distance in the direction perpendicular to local ridge orientation and is extensively utilized for contextual filtering of fingerprint images.

2.5.5.2. *Local Ridge Detail Features*

Fingerprints are not only distinguished by pattern of ridges and valleys but also distinguished by some discontinuities of local ridge structure (i.e. abnormal points on the ridges and valleys) also referred to as minutiae. It includes minutiae location, type of minutiae and their orientation [27]. The minutiae orientation is defined as the direction of the underlying ridge at the minutiae location. Sir Francis Galton (1822-1922) was the first person who observed the structures and permanence of minutiae. Therefore, minutiae are also called Galton details. They are used by forensic experts to match two fingerprints. There are about 150 different types of local ridge characteristics called minutiae details categorized based on their configuration. These local ridge characteristics include islands, short ridges, enclosure, etc. and are not evenly distributed. Most of them depend heavily on the impression conditions and quality of the fingerprint image and are rarely observed in fingerprints [16, 24]**.** Some of the minutiae types are described in Figure 2.11.

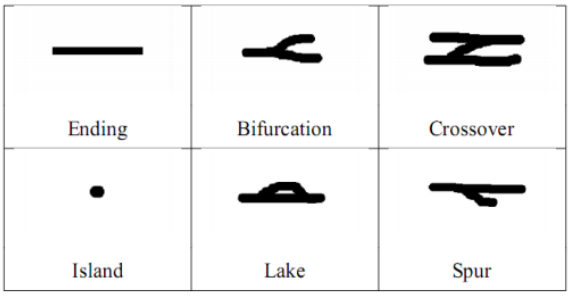
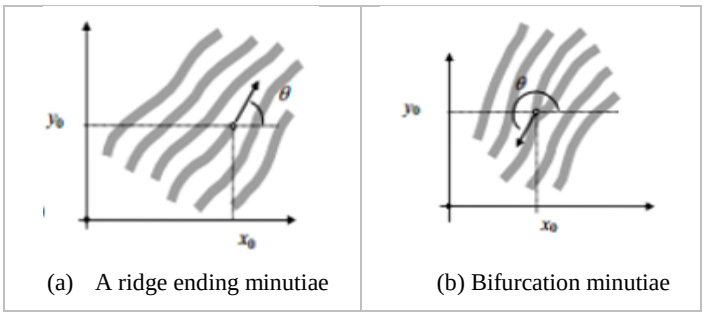


Figure 2.11. Some of the common minutiae types [16, 21]

Among these minutiae types, ridge ending and ridge bifurcation are the two most significant and widely used features, since all other types of minutiae can be seen as the combinations of these two feature types. A ridge ending is defined as the ridge point where a ridge ends abruptly and is also called termination. A ridge bifurcation is defined as the ridge point where a ridge forks or diverges into two branch ridges [4].

The point $[x_0, y_0]$ in Figure 2.12 are the coordinates and θ is the angle that the minutiae tangent forms with the horizontal axis. Minutiae based representation is characterized by a high saliency i.e. it is relatively stable to fingerprint impression conditions, image resolutions, and global distortion when compared to other representations. This representation also has a good privacy issues since one cannot reconstruct the original image by using only minutiae information [16].



(a) A ridge ending minutiae (b) Bifurcation minutiae

Figure 2.12. Minutiae's and their Coordinate Points[4]

Landmarks such as termination (or ridge ends) and ridge bifurcations are extracted with a reliable minutiae extraction algorithm. The algorithm mainly consists of three blocks namely image enhancement, feature extraction and matching. After the image enhancement and fingerprint ridge thinning, marking minutiae points takes place. In general, for each 3×3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch while if the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending (see in Figure 2.13). A fingerprint recognition system that uses minutiae extraction algorithm achieves a very high accuracy [16].

0	1	0
0	1	0
1	0	1

a) Bifurcation

0	0	0
0	1	0
0	0	1

b) Termination

Figure 2.13. Minutiae Features in Pixel Level [16]

2.5.5.3. *Intra-ridge Detail*

At the very-fine level, intra-ridge details can be detected in each ridge of a fingerprint. On every ridge of the finger epidermis, there are many tiny sweat pores and are considered to be highly distinctive in terms of their numbers, sizes, positions, and shapes [16]. This feature is the most important fine-level details and are illustrated in Figure 2.14 where minutiae (indicated as black-filled circles), sweat pores (indicated as empty circles) on a single ridge line. However, extracting very-fine details including pores is feasible only in high-resolution (e.g., 1000 dpi) fingerprint images of good quality and therefore this kind of representation is not practical for most applications [4].

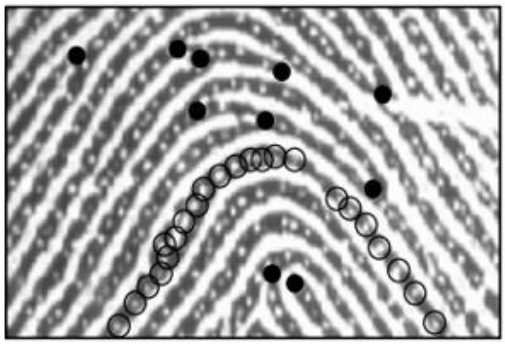


Figure 2.14. Intra – Ridge Details *[4, 21]*

2.6. **Fingerprint image Processing**

2.6.1. Fourier Transform

Fourier transform is a transformation technique that transforms the image from spatial domain into frequency domain. It provides a better image processing, a conceptual insights in spatial-frequency information (smooth, moderate change, fast change, etc.) and also computation is fast (convolution vs. multiplication) in Fourier transform [26].

2.6.2. The 2-D Discrete Fourier Transform

Let $f(x, y)$, for x = 0, 1, 2, …, M-1 and y = 0, 1,2,… ,N-1 denote an M × N image. The 2-D, discrete Fourier Transform (DFT) of $f(x, y)$, denoted by $F(u, v)$, is given by the equation [26]

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \tag{2.1}$$

for u = 0, 1, 2, ..., 31 , v = 0, 1, 2, ..., 31 and $e^{-j2\pi\left(\frac{um}{M}+\frac{vn}{N}\right)}$ is the 2D Fourier basis function.

The frequency domain is simply a coordinate system spanned by $F(u, v)$ with u and v as frequency variables. The value of the transform at the origin of the frequency domain i.e. $F(0, 0)$ is called the dc component of the Fourier. Even if $f(x, y)$ is real, its transform in general is complex. Letting $R(u, v)$ and $I(u, v)$ represent the real and imaginary components of $F(u, v)$ respectively, the Fourier magnitude spectrum is defined as [26]

$$|F(u,v)| = \sqrt{R^2(u,v) + I^2(u,v)} \tag{2.2}$$

The phase angle of the Fourier transform is defined as [26]

$$\varphi(u,v) = tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right] \tag{2.3}$$

The Fourier transform can be expressed in polar form as [26]

$$F(u,v) = \left|F(u,v)\right| e^{-j\varphi(u,v)} \tag{2.4}$$

The power spectrum is defined as the square of the magnitude [26]

$$P(u,v) = \left|F(u,v)\right|^2 = R^2(u,v) + I^2(u,v) \tag{2.5}$$

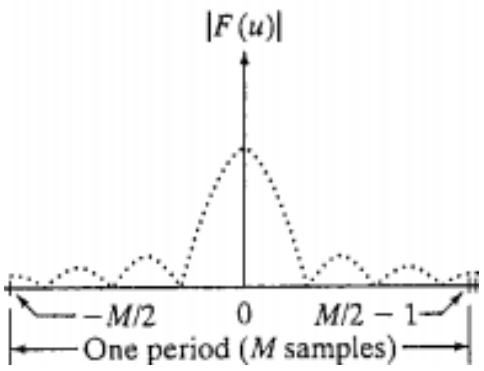


Figure 2.15. Fourier magnitude Spectrum [26]

The inverse, discrete Fourier transform, $F^{-1}(F(u,v))$ is given by [26]

$$f(x,y) = F^{-1}\left(F(u,v)\right) = \frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v) e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \tag{2.6}$$

For x = 0, 1, 2,…31 and y = 0, 1, 2,……31. The values of $F(u,v)$ in this equation are referred to as the Fourier coefficients of the expansion.

2.6.3. Normalization

Normalization is the process of setting the mean and variance of the image $f(x,y)$ to a pre-specified and/or required values of mean and variance. Due to imperfections in the fingerprint image capturing process such as non-uniform ink intensity or non-uniform contact with the

fingerprint reader, a fingerprint image may exhibit distorted levels of variations in grey-level values along the ridges and valleys. By normalization, the grey-level values are made to fall within certain range that is good enough for improved image contrast and brightness [28]. Thus, normalization is used to reduce the effect of these variations, which facilitates the subsequent image enhancement steps [29]. The normalized image $N(x, y)$ is defined by [23] [28]

$$N(x,y) = \begin{cases} M_0 + \sqrt{\dfrac{V_0 \times (f(i,j) - M)^2}{V}} & ,if\ f(x,y) > M \\ M_0 - \sqrt{\dfrac{V_0 \times (f(x,y) - M)^2}{V}} & ,Otherwise \end{cases} \tag{2.7}$$

Where M_0 and V_0 are the desired (predefined) mean and variance values, respectively while M and V are the estimated ones as follows [28].

Mean of the image is

$$M(f) = \frac{1}{N^2} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \tag{2.8}$$

And the variance is

$$V(f) = \frac{1}{N^2} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (f(x,y) - M(f))^2 \tag{2.9}$$

Generally, image normalization is done [16, 28]

- ✓ To reduce the variation in the gray-level values along ridges and valleys
- ✓ To have images with similar characteristics
- ✓ To remove the effect of the sensor noise
- ✓ To facilitate the subsequent processing steps

2.6.4. Image Segmentation

A captured fingerprint is usually composed of two regions namely the foreground region and the background region. The foreground region corresponds to the clear fingerprint area containing the

ridges and valleys, which is the area of interest while the background region is the region outside the borders of the fingerprint area, which do not contain any valid information [30, 31].

Segmentation is a process which is used to separate the fingerprint area (foreground region) in the image from the image background region. When feature extraction algorithms are applied to the background regions of an image, it results in the extraction of noisy and false features i.e. inclusion of noisy background can pose problems to the following enhancement, feature extraction and matching performance. Thus, accurate segmentation of a fingerprint should be employed to discard these background regions, which facilitate the reliable extraction of minutiae and will greatly reduce the computational time complexity of the subsequent processing steps, and discard many spurious minutiae [29].

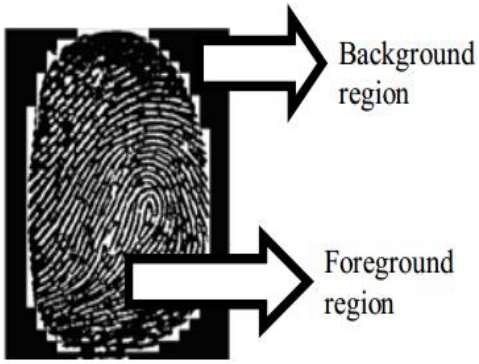


Figure 2.16. A fingerprint image and its foreground and background regions[28]

There are two types of segmentation namely, the global and adaptive thresholding.

Global Thresholding

In a fingerprint image, the background regions generally exhibit a very low grey-scale variance value, whereas the foreground regions have a very high variance. Hence, a method based on variance thresholding can be used to perform the segmentation. Firstly, the image is divided into blocks and the grey-scale variance is calculated for each block in the image.

The grey-level variance for a block of size $W \times W$ is defined as [28]:

$$V(k) = \frac{1}{w^2} \sum_{i=0}^{w-1} \sum_{j=0}^{w-1} \left(I(i,j) - M(k) \right)^2 \qquad (2.10)$$

Where $V(k)$ is the variance for block *k*, $I(i,j)$ is the grey-level value at pixel (i,j), and $\mathrm{M}(i,j)$ is the mean grey-level value for the block *k*.

If the variance is less than the global threshold, then the block is assigned to be a background region; otherwise, it is assigned to be part of the foreground. The variance based segmentation with global threshold T_h is given by

$$S(x,y)=\begin{cases}1\,,\ if\ V(x,y)\geq T_h\\ 0,\ Otherwise\end{cases} \tag{2.11}$$

Local Adaptive Thresholding

Consider a greyscale document image in which $g(x, y) \in [0, 255]$ be the intensity of a pixel at location (x, y). In local adaptive thresholding techniques, the aim is to compute a threshold $T_h(x,y)$ for each pixel such that [32]

$$S(x,y)=\begin{cases}0\,,\ if\ g(x,y)\leq T_h\\ 255\,,\ Otherwise\end{cases} \tag{2.12}$$

In Sauvola's binarization method [32], the threshold $T_h(x,y)$ is calculated using the mean $m(x,y)$ and standard deviation $\delta(x,y)$ of the pixels within a window of size $\boldsymbol{w} \times \boldsymbol{w}$ using [32]

$$T_h(x,y)=m(x,y)\left[1+k\left(\frac{\delta(x,y)}{R}-1\right)\right] \tag{2.13}$$

where R is the maximum value of the standard deviation (R = 128 for a grayscale document), and $\boldsymbol{k}$ is an experimentally determined bias, which takes positive values in the range of [0.2, 0.5].

The value of the threshold adapt the value of local mean $m(x,y)$ and standard deviation $\delta(x,y)$ according to the contrast in the local neighborhood of the pixel. When there is high contrast in some region of the image, $\delta(x,y) \sim \mathrm{R}$, the threshold adapts the value of the local mean, i.e. $T(x,y) \sim m(x,y)$. The parameter *k* controls the value of the threshold in the local window such that the higher the value of *k*, the lower the threshold from the local mean. Experiments with different values of k shows that *k = 0.34* gives the best results. In general, the algorithm is not very sensitive to the value of *k*. This method of thresholding gives a very good results even for severely degraded

documents. However in order to compute the threshold $T(x, y)$, local mean and standard deviation have to be computed for each pixel. Computation of $m(x, y)$ and $\delta(x, y)$ in a naive way results in a computational complexity for an image of large size [32].

Segmentation based on Morphological Processing

In local adaptive technique, a threshold is calculated for each pixel, based on some local statistics such as mean, range or variance of the neighborhood pixels. This algorithm uses the block range as a feature to achieve fingerprint segmentation which is suitable for different sensors and doesn't need empirical thresholds or a well-trained model. Then, some Morphological closing and opening operations are performed, to extract the foreground from the image. Segmentation is achieved through three main steps. First, the grayscale fingerprint image is decomposed into a set of non-overlapping blocks of a specific size (normally 3×3), and the range over these blocks is computed. Next, the resulting range image is converted to a binary image using adaptive thresholding [33]. Finally, a morphological opening and closing operations are applied to extract the fingerprint foreground [34].

2.6.5. Ridge orientation Estimation

An orientation image is a matrix of direction vectors representing the ridge orientation at each pixel location in the image. The gradient-based approach is used to calculate the orientation [35], which uses the fact that the orientation vector is orthogonal to the gradient. The gradient vectors, $[G_x, G_y]^T$, are first estimated using Cartesian coordinates as [12]

$G_x(x, y) = \frac{\partial f(x, y)}{\partial x}$, is the differences (gradient) in x (horizontal) direction.

$G_y(x, y) = \frac{\partial f(x, y)}{\partial y}$, is the differences (gradient) in y (vertical) direction.

The simplest operator to approximate the gradient components is the first order numerical derivative of one – dimensional function and it can be approximated by [36]

$$\begin{aligned} G_x &= f(x+1, y) - f(x, y) \\ G_y &= f(x, y+1) - f(x, y) \end{aligned} \tag{2.14}$$

Where $f(x, y)$ is the gray level value in the image at position (x, y) (Figure 2.17).

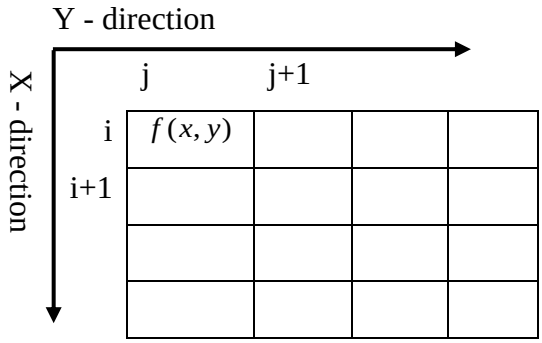


Figure 2.17. Pixel Position in image[35]

Let's consider a matrix $f(x, y)$ which is a unit-spaced two dimensional fingerprint image of size $M \times N$ that has both horizontal and vertical gradient $[G_x, G_y] = gradient(f(x, y))$. Then, the gradient values of the image $f(x, y)$ along the edges and the interior of the matrix are calculated with single-sided differences as follows.

The exterior gradient values are given by [36]

$$\begin{aligned} G_x(1,:) &= f(2,:) - f(1,:) \\ G_x(M,:) &= f(M,:) - f(M-1,:) \end{aligned} \tag{2.15}$$

and

$$\begin{aligned} G_y(:,1) &= f(:,2) - f(:,1) \\ G_y(:,N) &= f(:,N) - f(:,N-1) \end{aligned} \tag{2.16}$$

The interior gradient values, $G(x,:)$ and $G(:,y)$ are [36]:

$$\begin{aligned} G_x(x,:) &= \frac{1}{2}(f(x+1,y) - f(x-1,y)) \\ G_y(:,y) &= \frac{1}{2}(f(x,y+1) - f(x,y-1)) \end{aligned} \tag{2.17}$$

Where x varies between 2 and M-1 and y varies between 2 and N-1.

The gradient vector can be converted to polar coordinates, in which it is given by $[G_\rho , G_\varphi]^T$. This conversion is given by [35]

$$\begin{bmatrix} G_\rho \\ G_\varphi \end{bmatrix} = \begin{bmatrix} \sqrt{G_x{}^2 + G_y{}^2} \\ tan^{-1}(G_y / G_x) \end{bmatrix} \tag{2.18}$$

The gradient vector is converted back to it Cartesian representation by [35]:

$$\begin{bmatrix} G_x \\ G_y \end{bmatrix} = \begin{bmatrix} G_\rho cos G_\varphi \\ G_\rho sin G_\varphi \end{bmatrix} \tag{2.19}$$

Using trigonemetric identites, an expression for the doubled angle and squared gradient vectors $[G_{s,x} , G_{s,y}]^T$ can be found as [35]:

$$\begin{bmatrix} G_{s,x} \\ G_{s,y} \end{bmatrix} = \begin{bmatrix} G_\rho{}^2 cos 2G_\varphi \\ G_\rho{}^2 sin 2G_\varphi \end{bmatrix}$$

$$\begin{bmatrix} G_{s,x} \\ G_{s,y} \end{bmatrix} = \begin{bmatrix} G_\rho{}^2 \left(cos^2 G_\varphi - sin^2 G_\varphi \right) \\ G_\rho{}^2 \left(2 sin G_\varphi cos G_\varphi \right) \end{bmatrix}$$

$$\begin{bmatrix} G_{s,x} \\ G_{s,y} \end{bmatrix} = \begin{bmatrix} G_x{}^2 - G_y{}^2 \\ 2 G_x G_y \end{bmatrix} \tag{2.20}$$

This result can also be obtained directly by using the equivalent of doubling the angle and squaring the length of a vector to squaring a complex number [35]:

$$G_{s,x} + j.G_{s,y} = \left(G_x + j.G_y \right)^2$$

$$G_{s,x} + j.G_{s,y} = (G_x{}^2 - G_y{}^2) + j.\left(2 G_x G_y \right) \tag{2.21}$$

In polar form

$$G_{s,x} + j.G_{s,y} = (G_\rho e^{jG_\varphi})^2$$

$$G_{s,x} + j.G_{s,y} = G_{\rho}^{2} e^{j2G_{\varphi}} \tag{2.22}$$

Next, the average square gradient $[\overline{G_{s,x}}, \overline{G_{s,y}}]^T$ can be calculated. It is averaged in a local neighborhood, using a not necessary uniform window w [35]:

$$\begin{bmatrix} \overline{G_{s,x}} \\ \overline{G_{s,y}} \end{bmatrix} = \begin{bmatrix} \sum_w G_{s,x} \\ \sum_w G_{s,x} \end{bmatrix} = \begin{bmatrix} \sum_w G_x^{\,2} - G_y^{\,2} \\ \sum_w 2G_x G_y \end{bmatrix}$$

$$\begin{bmatrix} \overline{G_{s,x}} \\ \overline{G_{s,y}} \end{bmatrix} = \begin{bmatrix} G_{xx} - G_{yy} \\ 2G_{xy} \end{bmatrix} \tag{2.23}$$

In this expression, the estimate for the covariance and cross covariance of G_x and G_y , averaged over the window w are [35]

$$G_{xx} = \sum_w G_x^{\,2} \tag{2.24}$$

$$G_{xy} = \sum_w G_x G_y \tag{2.25}$$

$$G_{yy} = \sum_w G_y^{\,2} \tag{2.26}$$

Now the average gradient direction G_{φ}, is given by [35]:

$$G_{\varphi} = \frac{\overline{G_{s,y}}}{\overline{G_{s,x}}} = \frac{1}{2} \arctan\left(\frac{2G_{xy}}{G_{xx} - G_{yy}} \right) \tag{2.27}$$

Where G_{φ} is perpendicular to the ridge structure and is aligned by adding $\pi / 2$ it. The orientation vector, O which is orthogonal to the gradient is given by [4, 37]

$$O = \frac{\pi}{2} + G_{\varphi}$$

$$O = \frac{\pi}{2} + \frac{1}{2} \arctan\left(\frac{2G_{xy}}{G_{xx} - G_{yy}} \right) \tag{2.28}$$

The orientation given in Eq. (2.28) is positive in the clockwise direction.

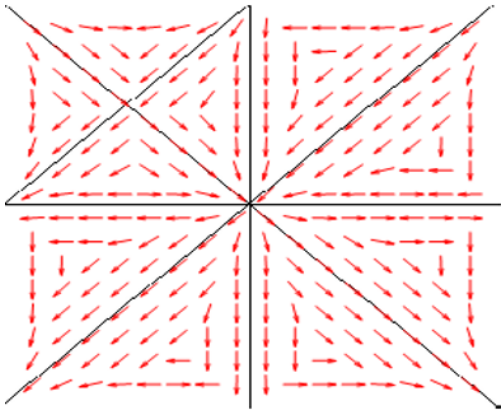


Figure 2.18. Estimated Orientation Fields

2.6.6. Ridge frequency Estimation

The local ridge frequency is defined as the frequency of the ridge and valley structures contained in a local neighborhood along a direction orthogonal to the local ridge orientation and this is an important parameter that is used in the construction of the Gabor filter [38]. The ridge frequency varies slowly and hence it is computed only once for each non-overlapping block of the image. The local ridge frequency is then estimated by counting the average number of pixels between two consecutive peaks of gray levels along the direction that is normal to the ridge orientation [23] (Figure 2.19).

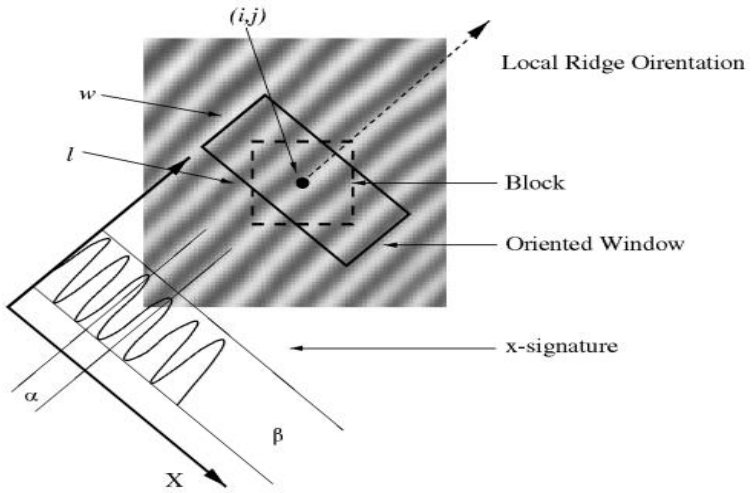


Figure 2.19. Oriented Window and X – Signature[23]

Let $S(i,j)$ be the ridge spacing computed by counting the median number of pixels between consecutive minima points of a block image in a projected waveform. Then, the ridge frequency $F(i,j)$ for a block centered at pixel (i,j) is defined as [23]:

$$F(i,j) = \frac{1}{S(i,j)} \tag{2.29}$$

2.6.7. Frequency Domain Digital Filters

Filtering means removing parts of the frequency spectrum of a signal. Depending on the part which is removed from the signal, there are several basic filter response types namely, low pass, high pass and band pass filters [26].

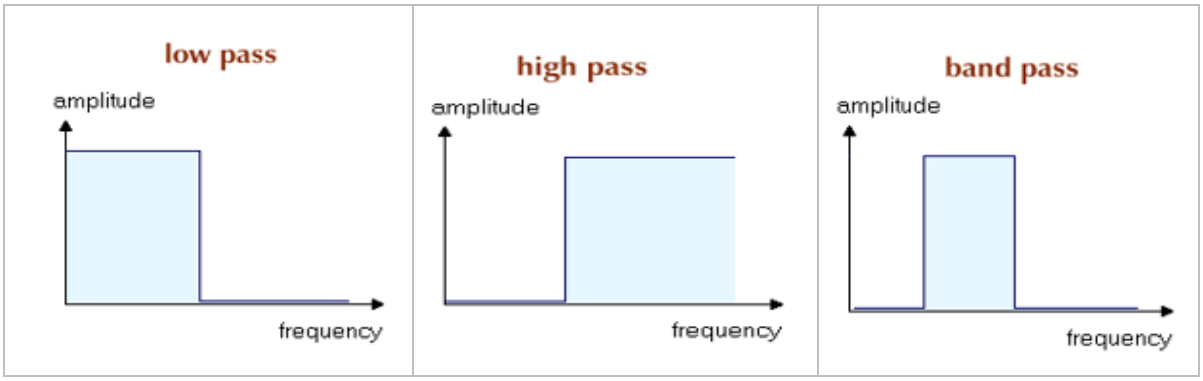


Figure 2.20. Frequency responses of digital image filters[26]

2.6.7.1. *Low-pass Filters*

Low pass filter is a filter that attenuates the range of high frequency components of $F(u,v)$ while leaving the low frequencies relatively unchanged. The net result of a low pass filter is image blurring (smoothing). The purpose of smoothing filter is blurring and noise reduction. Blurring means removal of small details from image prior to object extraction and bridging of small gap in line curves [26].

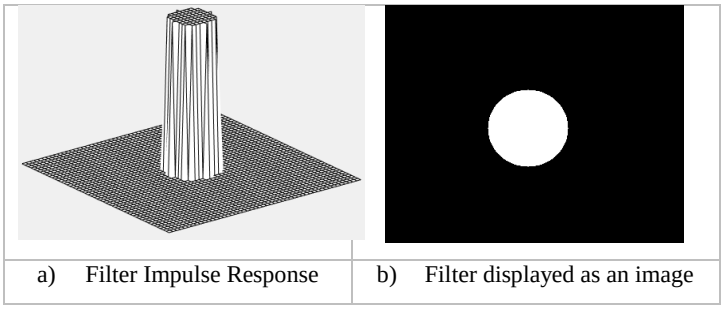
a) **Ideal Low pass Filter (ILPF):-** An ideal low pass filter is very sharp and its transfer function is given by [26]

$$H(u,v) = \begin{cases} 1, & if \ D(u,v) \le D_0 \\ 0, & if \ D(u,v) > D_0 \end{cases} \tag{2.30}$$

Where D_0 is specified nonnegative number, $D(u,v)$ is the distance from point (u,v) to the center of the filter. If the origin (Centered) of the filter is at $\left(\frac{M}{2},\frac{N}{2}\right)$, then

$$D(u,v)=\sqrt{\left(u-\frac{M}{2}\right)^2+\left(v-\frac{N}{2}\right)^2} \tag{2.31}$$

The locus of points for which $D(u,v)=D_0$ is a circle. Since the filter H multiplies the FFT of an image, it is clear that an ideal filter cuts off (multiplies by 0) all components of F outside the circle and leaves unchanged (multiplied by 1) all components of F inside the circle [26].



a) Filter Impulse Response b) Filter displayed as an image

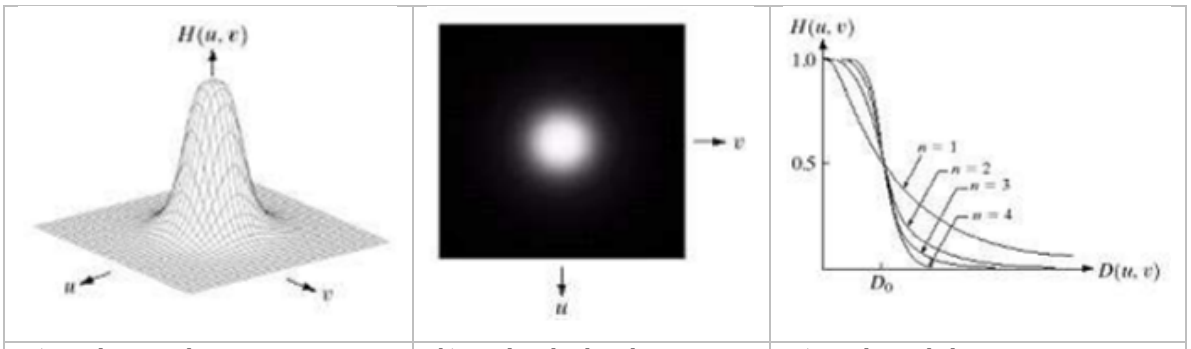
Figure 2.21. Low pass Filter[26]

b) **Butterworth Low pass Filter**

The Butterworth filter is a type of filter designed to have a frequency response as flat as possible in the passband region. It is also referred to as a maximally flat magnitude filter. Low – pass Butterworth filter of order n, with a cutoff frequency at a distance D_0 from the origin, has the transfer function of the form [26]

$$H(u,v)=\frac{1}{1+\left[\frac{D(u,v)}{D_0}\right]^{2n}} \tag{2.32}$$

Where n and D_0 are the controlling parameters and as *n* approaches to infinity, the filter response becomes a rectangular function and the frequencies that are below D_0 will be passed with gain 1, while frequencies above D_0 are suppressed. For smaller values of *n*, the cutoff will be less sharp. Unlike ideal low pass filter, the Butterworth low pass filter transfer function does not have a sharp discontinuity at D_0 [26]



a) Filter Impulse Response | b) Filter displayed as an image | c) Filter radial cross sections

Figure 2.22. Butterworth low pass filter transfer function[26]

c) **Gaussian Low pass Filter**

The Gaussian (very smooth) low pass filter has a transfer function of the following form [26]

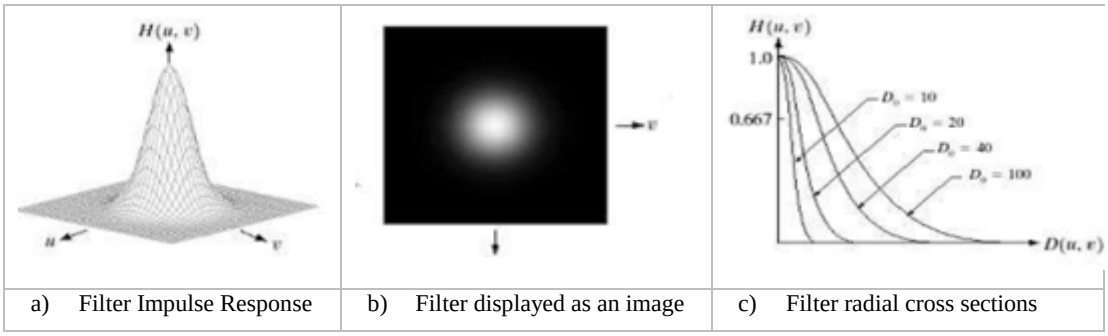
$$H(u,v) = e^{-\frac{D^2(u,v)}{2\sigma^2}} \tag{2.33}$$

Where σ is the standard deviation and $D(u,v)$ is give in Eq. (2.31).

By letting $\sigma = D_0$, we obtain the following expression in terms of the cutoff parameter D_0 [26].

$$H(u,v) = e^{-\frac{D^2(u,v)}{2D_0^2}} \tag{2.34}$$

When $D(U,v) = D_0$, the filter is down to 0.607 of its maximum value of 1. The filter transfer function of Gaussian low pass filter and the filter radial cross section of different orders is shown Figure 2.23.



a) Filter Impulse Response | b) Filter displayed as an image | c) Filter radial cross sections

Figure 2.23. Gaussian low pass filter transfer function[26]

2.6.7.2. *High Pass Filters*

High pass Filter is a filter that attenuates low frequency components of an image while leaving high frequencies of the Fourier transform relatively unchanged. As the low pass filtering blurs an image, high pass filtering performs the opposite process, i.e. it sharpens the image. The low-pass filter can be modified into a high-pass filter, or placed in series with others to form band-pass and band-stop filters, and higher order versions of these [26].

Given the transfer function $H_{lp}(u,v)$ of a low pass filter, the transfer function of the corresponding high pass filter can be obtained by using the relation [26]

$$H_{hp}(u,v) = 1 - H_{lp}(u,v) \tag{2.35}$$

Where

- ✓ $H_{lp}(u,v)$ is the transfer function of the corresponding low pass filter
- ✓ $H_{hp}(u,v)$ is the transfer function of the corresponding high pass filter

The transfer function of the three high pass functions is shown in Figure 2.24.

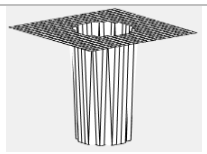
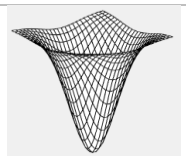
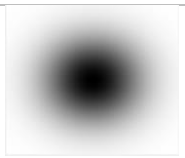
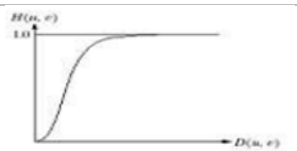
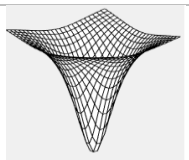
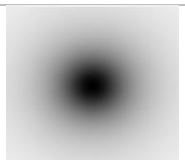
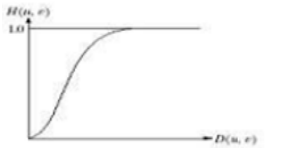
Ideal High pass Filter			
Guassian High pass Filter			
Butterworth High pass Filter			

Figure 2.24. High pass Filter Transfer Functions[26]

a) Ideal High pass Filter

An ideal high pass filter has the transfer function of the form [26]

$$H(u,v)=\begin{cases}0, \ if \ D(u,v)\le D_0\\ 1, \ if \ D(u,v)>D_0\end{cases} \quad (2.36)$$

Where

- ✓ D_0 is specified nonnegative number and
- ✓ $D(u,v)$ is the distance from point (u,v) to the origin of the filter.
- ✓ Origin: $\left(\frac{M}{2},\frac{N}{2}\right)$ (Centered), then $D(u,v)=\sqrt{\left(u-\frac{M}{2}\right)^2+\left(v-\frac{N}{2}\right)^2}$

b) Butterworth High pass Filter

The Butterworth high pass filter of order n with a cutoff frequency distance D_0 is obtained by substituting the low pass filter in Eq. (2.32) into Eq.(2.35) [26]

$$H_{hp}(u,v)=1-H_{lp}(u,v)$$

$$H(u,v)=1-\frac{1}{1+\left[\frac{D(u,v)}{D_0}\right]^{2n}}$$

$$H(u,v)=\frac{1}{1+\left[\frac{D_0}{D(u,v)}\right]^{2n}} \quad (2.37)$$

Where,

$$D(u,v)=\sqrt{\left(u-\frac{M}{2}\right)^2+\left(v-\frac{N}{2}\right)^2}$$

c) Gaussian High pass Filter

Substituting the low pass Gaussian filter given in Eq. (2.33) into Eq.(2.35), to get [26]

$$H_{hp}(u,v)=1-H_{lp}(u,v)$$

$$H(u,v)=1-e^{-\frac{D^2(u,v)}{2D_0^2}} \quad (2.38)$$

2.6.7.3. *Band Pass Filter*

Bandpass filer is a filter that allows to pass specified frequency components of between two ranges and attenuates the other frequency components. Band-pass filters are formed by the combination of low pass and high pass filters so that only frequencies within a certain range (band) can pass the filter [26].

a) **Gaussian Band pass Filter:** is obtained by [26]

$$H_{GBp} = H_{Glp}(u,v) * H_{Ghp}(u,v)$$

$$H_{GBp}(u,v) = e^{-\frac{D^2(u,v)}{2D_0^2}}\left(1 - e^{-\frac{D^2(u,v)}{2D_0^2}}\right) \tag{2.39}$$

b) Butterworth Band pass Filter: is obtained by [26]

$$H_{BW} = H_{lpBw}(u,v) * H_{hpBw}(u,v)$$

$$H(u,v) = \frac{1}{1+\left[\frac{D(u,v)}{D_0}\right]^{2n}} * \frac{1}{1+\left[\frac{D_0}{D(u,v)}\right]^{2n}}$$

$$H(u,v) = \frac{1}{2+\left(\frac{D(u,v)}{D_0}\right)^{2n}+\left(\frac{D_0}{D(u,v)}\right)^{2n}} \tag{2.40}$$

As the order of the filter n, increases, the filter becomes an ideal (sharp) bandpass filter as it is shown in Figure 2.25.

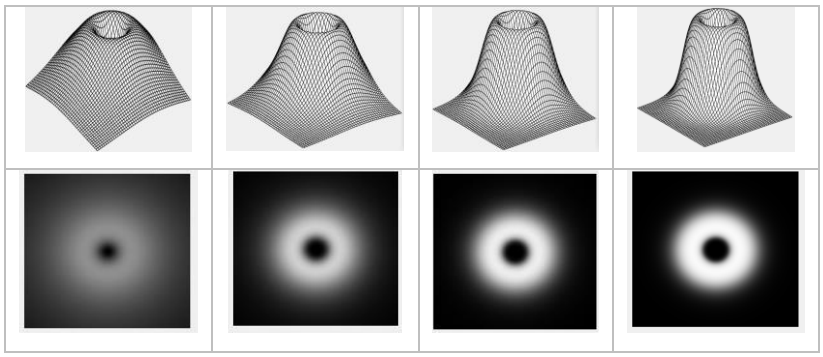


Figure 2.25. Butterworth Band pass Filter Transfer Function, for n =1, 2, 3 & 4 respectively[26]

2.6.7.4. *Gabor Filter*

Gabor filters are band pass filters that have both frequency-selective and orientation-selective properties so that the filters can be effectively tuned to specific frequency and orientation values. The Cosine/Sine form of Gabor filter is suitable for modeling ridge/valley structures and smoothing out noise [29].

2.6.7.4.1. Introduction to Gabor Wavelets

Wavelets are scaled and translated copies of a finite-length, fast-decaying oscillating waveform and are used for signal processing. Their main advantage is that they allow multiresolution analysis (analysis at different scales, or resolution). The Gabor wavelet is essentially a sinusoidal wave modulated by a Gaussian envelope and is given by [39].

$$G_w(t) = e^{-\left(\frac{t-t_0}{a}\right)^2} e^{-jf_0 t} \tag{2.41}$$

Where f_0 is the modulating frequency, t_0 dictates the position and a controls the bandwidth of the Gaussian envelope. An example of Gabor wavelet is shown in Figure 2.26 which shows the real and the imaginary parts where the modulus is the Gaussian envelope. Increasing the value of f_0 increases the frequency content within the envelope whereas increasing the value of a spreads the envelope without affecting the frequency [39].

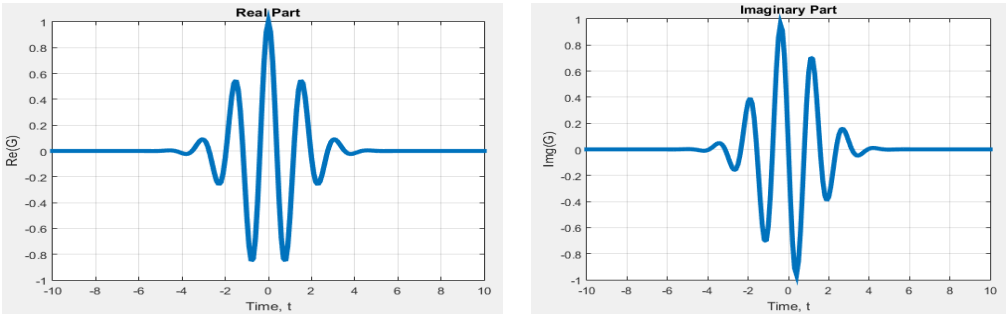


Figure 2.26. Example of Real and Imaginary Parts of Gabor Wavelet

The general form of 2D Gabor wavelets is defined by [39]

$$G(x, y, \theta, f) = \exp\left\{-\frac{1}{2}\left[\frac{(x-x_0)^2}{\delta_x^2} + \frac{(y-y_0)^2}{\delta_y^2}\right]\right\} \times e^{j2\pi fx} \tag{2.42}$$

Where

- ✓ x and y define the filter coordinate frame and are functions of θ
- ✓ x_0 and y_0 control the position(shifting) of the Gabor wavelet
- ✓ f_0 controls the frequency of modulation along either axis
- ✓ θ controls the *direction* (rotation or orientation) of the Gabor wavelet
- ✓ δ_x and δ_y control the envelope's spread of the Gabor wavelet

To analyze the Gabor filter in terms of the even-symmetric and odd-symmetric, the above equation is expressed in the complex form as [39]

$$G = G_{even} + iG_{odd} \tag{2.43}$$

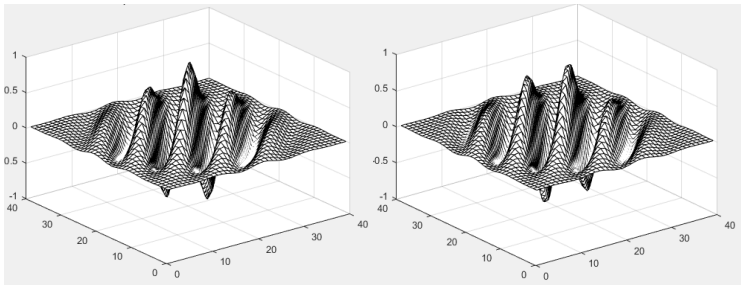
where, the even part of the Gabor filter is

$$G_{even}(x, y, \theta, f) = \exp\left\{-\frac{1}{2}\left[\frac{(x-x_0)^2}{\delta_x^2} + \frac{(y-y_0)^2}{\delta_y^2}\right]\right\} \times \mathrm{Cos}(2\pi fx) \tag{2.44}$$

and the odd part is given by

$$G_{odd}(x, y, \theta, f) = \exp\left\{-\frac{1}{2}\left[\frac{(x-x_0)^2}{\delta_x^2} + \frac{(y-y_0)^2}{\delta_y^2}\right]\right\} \times \mathrm{Sin}(2\pi fx) \tag{2.45}$$

Figure 2.27, shows that an example of 2D Gabor wavelet, i.e. the real and imaginary parts are even and odd functions, respectively.



a) Even-symmetric b) Odd Symmetric

Figure 2.27. Gabor filter Transfer Function [16]

As the frequency increases, the resolution of Gabor kernel becomes denser. The Gabor kernels with four different frequencies and four different orientations is shown in Figure 2.28.

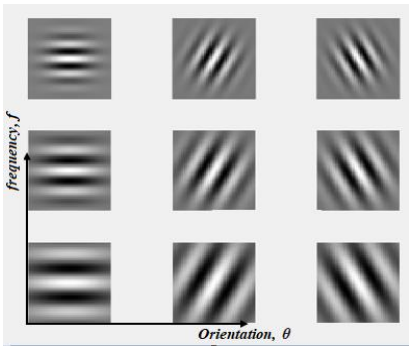


Figure 2.28. Gabor Kernels at different frequency and orientation [16]

2.6.8. Binarization

Minutiae extraction algorithm operates on binary images where there are only two levels of interest namely the black pixels that represent ridges, and the white pixels that represent valleys. Binarization is the process of converting a grayscale image to a binary (black and white) image. This improves the contrast between the ridges and valleys in a fingerprint image, and consequently facilitates the extraction of minutiae. This process involves examining the grey-level value of each pixel in the enhanced image and if the value is greater than a global threshold, the pixel value is set to a binary value of one, otherwise, it is set to zero. The outcome is a binary image containing two levels of information, the foreground ridges and the background valleys. Mathematically, the binary image is given by [29]

$$Binary(i,j) = \begin{cases} 1\ ,\ if\ \ f(x,y) > T_h \\ 0\ ,\ if\ \ otherwise \end{cases} \tag{2.46}$$

where $f(x,y)$ is the fingerprint grayscale image and T_h is the threshold value.

2.6.9. Thinning

Thinning is a morphological operation that successively reduces away the width of each ridge pixels until they become one pixel wide to form a skeletonized image by preserving the connectivity of the ridge structures. This algorithm is applied on the binary image and is accessible in MATLAB via the 'thin' operation under the "bwmorph" function. Then the thinned image is filtered by using the hbreak, clean and spur MATLAB functions to remove some H breaks, isolated points and spikes. The minutiae points are the extraction from this skeletonized image [11].

Chapter 3

System Model of Fingerprint Recognition System

3.1. Introduction

Fingerprint recognition is the process of comparing between a fingerprint in question and a known fingerprint template from a database to determine if the impressions are from the same finger or not via the features extracted from the scanned fingerprint images [21]. The most important stages of AFRS are enhancement stage, features extraction stage, and matching stage (Figure 3.1).

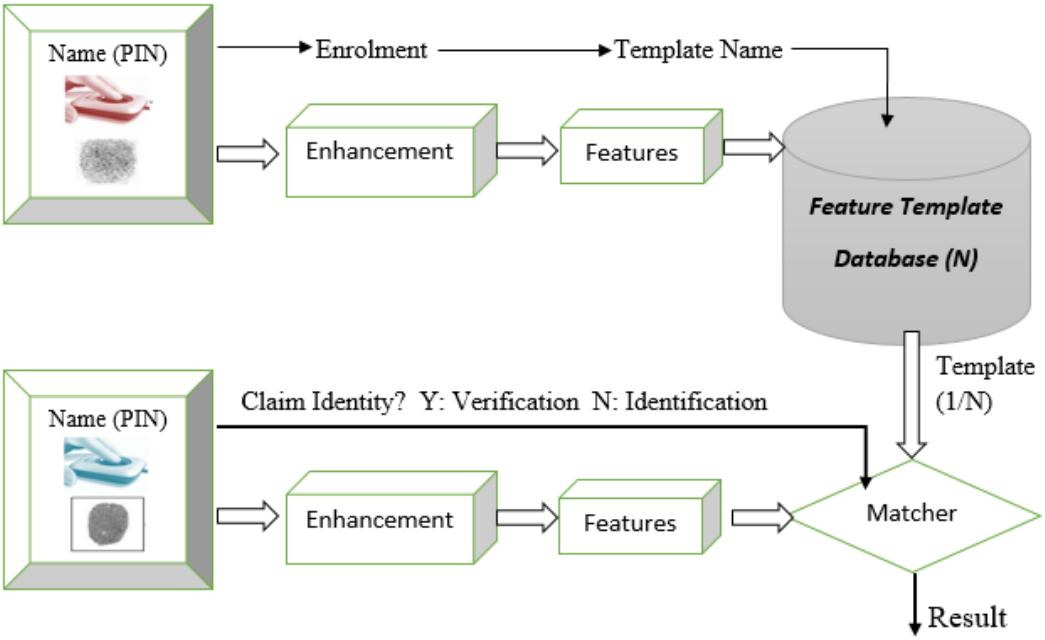


Figure 3.1. Schematic diagram of Fingerprint Recognition System[21]

A number of methods are used to acquire fingerprint images. Among them, the inked impression method remains the most popular one. Inkless fingerprint scanners are also used to eliminate the intermediate digitization process. They have high efficiency and accuracy except for some cases that the individual's finger is too dirty or dry [12].

The scanned image is first enhanced to increase the image quality, then features are extracted to be used for matching purpose. The minutiae extraction algorithm is the most accurate and widely used algorithm in extracting the unique features from the fingerprint that are used for recognition

purpose. Hence, the fingerprint image quality is very important since it affects directly the minutiae extraction algorithm as well as the matching algorithm [23].

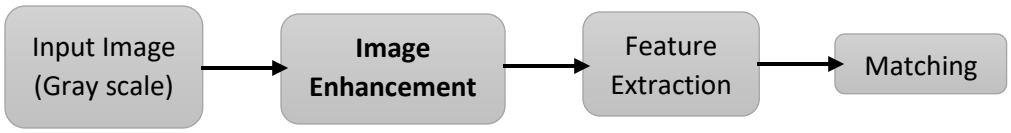


Figure 3.2. Fingerprint Recognition Block Diagram [11]

3.2. Fingerprint Image Enhancement

The main purpose of the fingerprint image enhancement stage is to increase the clarity of the fingerprint image, convert poor quality image to good quality image, and prepare the image for features extraction stage [23].

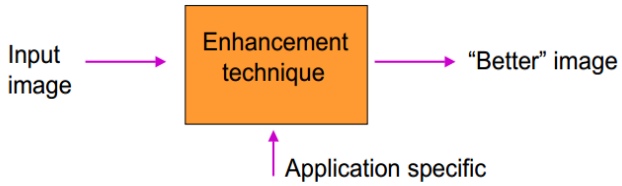


Figure 3.3. Basic Block Diagram of image Enhancement[23]

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip and it is unique for each individual. The uniqueness of a fingerprint is exclusively determined by the two most prominent local ridge characteristics called minutiae points [16, 21, 24] (Figure 3.4).

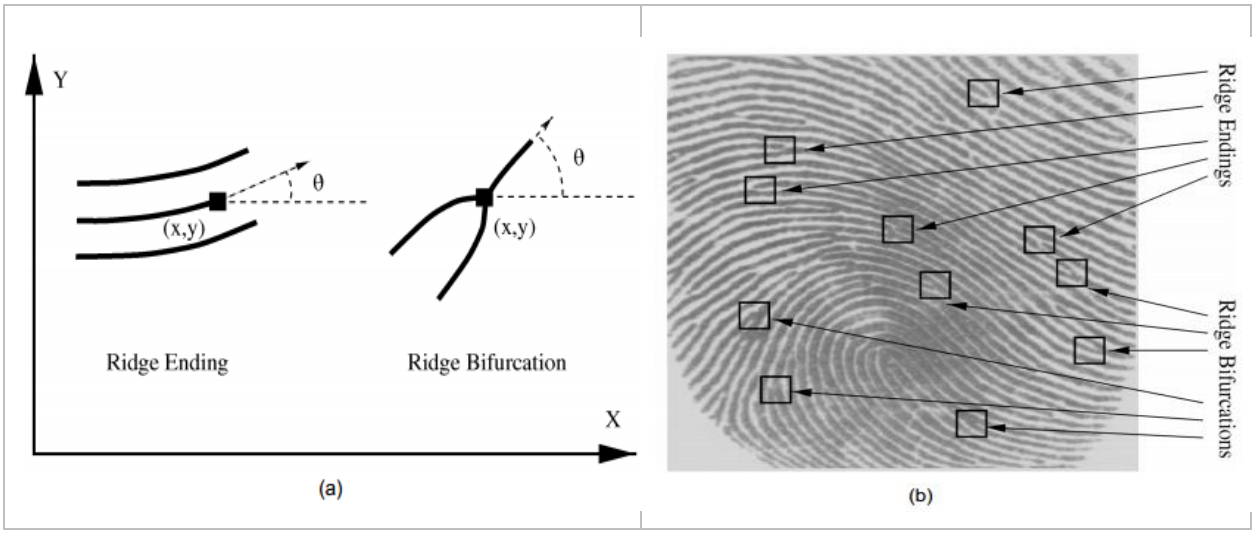


Figure 3.4. Examples of Minutiae Points [23]

Most of them depend heavily on the impression conditions and quality of fingerprints. In a good quality rolled fingerprint image, typically there are about 40 to 100 minutiae points, but the number of minutiae is much less in low quality images (approximately 20 to 30) and these points are used for the matching algorithm as an input data [23].

Automatic fingerprint matching depends on the comparison of these 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 raw 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. Figure 3.4b shows an example of good quality live-scan fingerprint image. However, practically a significant percentage of the acquired fingerprint images is of poor quality due to variations in impression conditions, skin conditions, noise from the acquisition devices, and non-cooperative attitude of subjects, etc. Two types of degradation usually affect fingerprint images [12, 23]:

1) The ridge lines are not strictly continuous since they sometimes include small breaks (gaps)
2) Parallel ridge lines are not always well separated due to the presence of cluttering noise.

This leads to the following problems:

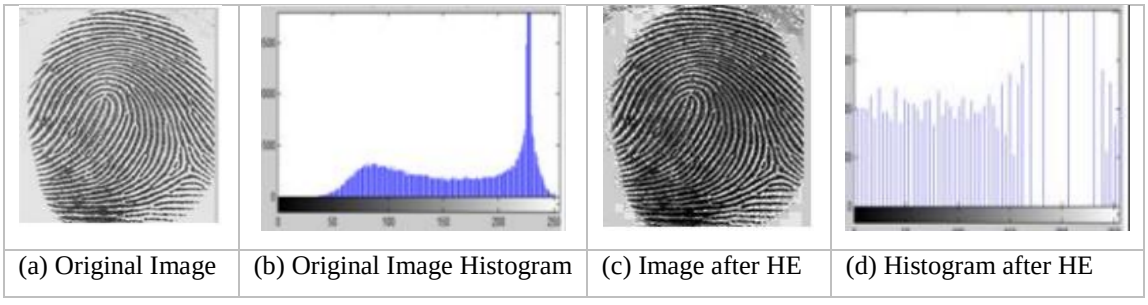
a) A significant number of spurious minutiae may be created,
b) A large percent of genuine minutiae may be ignored, and
c) Large errors in their localization (position and orientation) may be introduced.

The ridge structures in poor-quality fingerprint images are not always well-defined and hence, they cannot be correctly detected. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In order to ensure that the performance of an automatic fingerprint identification/verification system will be robust with respect to the quality of input fingerprint images, it is essential to incorporate a fingerprint image enhancement algorithm in the minutiae extraction module [23]. Section 3.2.1 presents fingerprint enhancement techniques such as HE, FFT, Gabor Filter and the combined form of FFT with Gabor Filter.

3.2.1. Enhancement using Histogram Equalization (HE)

HE is an image processing technique used for adjusting image intensities to enhance contrast of the fingerprint image. Contrast is defined as the difference in color or intensity between two objects in an image. If the contrast is too low, it is impossible to distinguish between two objects and they are seen as a single object. An intensity histogram is a histogram containing the distribution of all the possible intensities. The main idea of this technique is to re-estimate the intensity values of image pixels to make the intensity distribution uniform so that the whole available range of intensities contributes to the image [11, 38].

An 8-bit image has 256 different intensity values and thus the x-axis will contain 256 different values and the y-axis will display how many of each intensity values there are. A typical intensity histogram from an 8-bit grayscale image is shown in Figure 3.5. A typical example of good histogram is shown in Figure 3.5d where almost all of the pixels are used. This is good because the whole available range of intensities contributes to the image [11].



(a) Original Image	(b) Original Image Histogram	(c) Image after HE	(d) Histogram after HE

Figure 3.5. HE based Enhanced Image and its Histogram [11]

In the histogram shown in Figure 3.5b, the pixels are much more concentrated at intensities in the right side of the spectrum. All pixels are between 58 and 256. The available intensity values outside of this range are not used. The contrast in this image is low because only a portion of the available pixel values are used. The image can be altered so that all the available pixel intensities are used. This is known as histogram equalization [11].

Procedure: Consider $f(x, y)$ be a given grayscale fingerprint image represented as (M x N) matrix of integer pixels intensity values ranging from *0* to *(L-1)* gray level. Where *L* is the number of possible intensity values, often *256*.

The probability of an occurrence of a pixel of level *i* in the image is [11]

$$P_r = \frac{n_i}{T_N} \ , \ 0 \le i \le 255 \tag{3.1}$$

Where n_i is the number of pixels with intensities *i*, and T_N is the total number of pixels (if the image is 8 x 8 Matrix, i.e. $T_N = 64$). The cumulative distribution function is define as [11]:

$$cdf_r\left(i \le t\right) = \sum_{j=0}^{t} P_r\left(j\right) \tag{3.2}$$

Eq. (3.2) describes the CDF for the probability that a pixel has the intensity equal or lower than t. The values are often normalized, so that the total probability is 1. The goal is to create some transformation, $T_h(i)$ that creates a new image with a uniform pixel distribution. Mapping the image pixels to new pixel values that will increase the overall contrast in the image is then done using the general HE formula [11]:

$$T_h\left(i\right) = round\left(\frac{cdf_r\left(i\right) - cdf_{min}}{\left(m\,x\,n\right) - cdf_{min}} x\left(L-1\right)\right) \tag{3.3}$$

where cdf_{min} is the minimum value of the cumulative distribution function, $(m\,x\,n)$ gives the total number of image's pixels, and L is the number of grey level, often 256.

Consider the image given in Figure 3.6 below where the histogram of the image tells us that, most of the image pixels have values around 5.

6	2	3	4	5
5	5	6	7	5
5	6	4	8	6
4	7	4	3	4
8	5	6	6	7

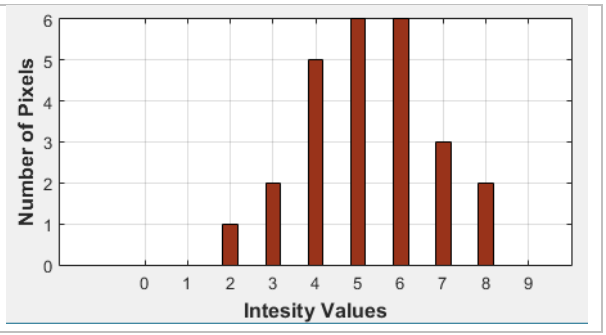


Figure 3.6. Sample Image and its Histogram

Table 3.1 shows the procedures of calculating and mapping the histogram equalization for a sample image of size 5 x 5 with L=10. The function round, rounds up or down to the nearest integer. For example, a pixel value of 3 in the original will be mapped to the pixel value of 1, 4 to 3 and so on.

Table 3.1. HE Calculation and Mapping Procedure

Gray Level	$Freq = n_k$	$p_n = \frac{n_k}{\sum_n n_k}$	$cdf = \sum p_n$	$T_h(i)$	round
0	0	0	0	0	0
1	0	0	0	0	0
2	1	0.04	0.04	0.36	0
3	2	0.08	0.12	1.08	1
4	5	0.2	0.32	2.88	3
5	6	0.24	0.56	5.04	5
6	6	0.24	0.8	7.2	7
7	3	0.12	0.92	8.28	8
8	2	0.08	1	9	9
9	0	0	1	9	9
	$\sum_n n_k = 25$	$\sum_n p_n = 1$			

The resulting equalized image and its histogram is shown in Figure 3.7.

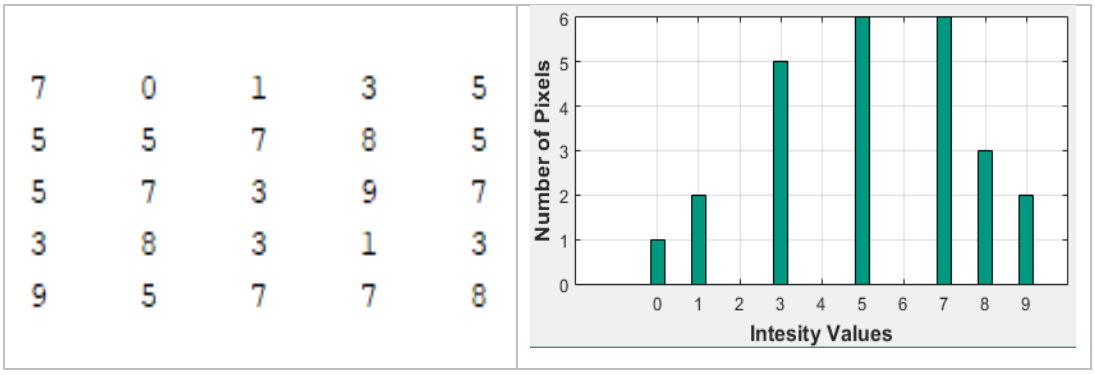


Figure 3.7. Equalized Image and its Histogram

The resulting image histogram is much better distributed across the whole range and this will result in a much higher overall contrast across all pixels.

3.2.2. Enhancement using Fourier Transform

The Fourier transform is widely used in signal and image processing in particular, for detection of high or low frequencies. This algorithm consists Normalization, Segmentation, Fourier Transform, Filtering, Root Filtering, Inverse Fourier Transform, Reconstruction and contrast enhancement. These steps are shown in Figure 3.8. Normalization is applied on the original gray scale image $f(x, y)$ to reduce the effect of noise and variations in the gray-level values along ridges and valleys to facilitate the subsequent image enhancement steps. It is a linear and pixel wise operation and doesn't change the ridge and valley structure. Segmentation is also applied on the original image to separate the foreground region from that of the noisy region that do not contain any valid information to minimize the computational complexity and to avoid false feature extraction [29]. The normalized image $N(x, y)$ is defined in Eq. (2.7) by

$$N(x,y) = \begin{cases} M_0 + \sqrt{\dfrac{V_0 \times (f(x,y) - M)^2}{V}} & : if\ f(x,y) > M \\ M_0 - \sqrt{\dfrac{V_0 \times (f(x,y) - M)^2}{V}} & : Otherwise \end{cases}$$

Where M_0 and V_0 are the desired (predefined) mean and variance values respectively, while M and V are the estimated ones.

Thus, to enhance a fingerprint image, it is first normalized and segmented. The segmented fingerprint image is divided into blocks of small size (e.g. 32×32). Generally, the blocks are constructed using an overlapped windows in order to avoid the border effect of the Fourier transform. For each block, FFT is applied, filtered using a bandpass Butterworth filter transfer function to remove a Gaussian noise and then finally multiplied by its power spectrum to level up the image quality. Thereafter inverse fast Fourier transform (IFFT) is applied to the resulting image. Figure 3.8 shows the frequency domain enhancement processing sequence [40, 26].

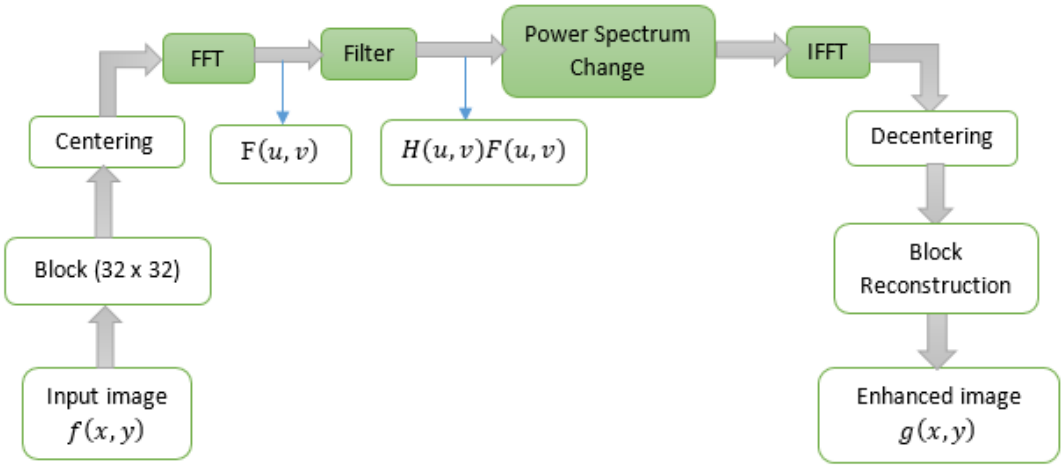


Figure 3.8. Frequency Domain Enhancement [26, 40]

The Fourier transform of the block image, $f(x,y)$, of size M×N is performed according to the equation [40]:

$$F(u,v)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \tag{3.4}$$

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

In order to enhance a specific block by its dominant frequencies, the Fourier transform of the block is multiplied by its power spectrum (or the square of its magnitude), where the magnitude of the original Fourier is defined as [40]

$$FFT=abs\left(F(u,v)\right)=\left|F(u,v)\right| \tag{3.5}$$

and the power spectrum is defined as [26]

$$P(u,v)=\left(|(F(u,v)|\right)^2 \tag{3.6}$$

The enhanced block is given according to the equation [26]

$$E(x,y)=F^{-1}\{F(u,v)\times P(u,v)\}$$

$$E(x,y)=F^{-1}\left\{F(u,v)\times\left|F(u,v)\right|^2\right\} \tag{3.7}$$

Where the inverse Fourier transform, $F^{-1}(F(u,v))$ is done by [40]

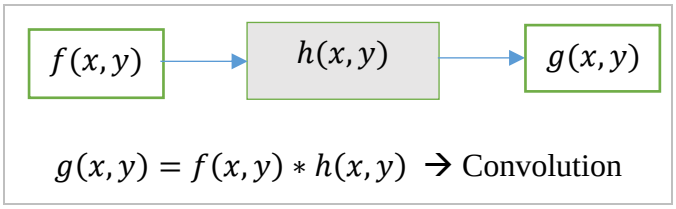
$$f(x,y)=\frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}F(u,v)e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \tag{3.8}$$

For x = 0, 1, 2,…31 and y = 0, 1, 2,……31

The value of overlap is an experimentally determined value, which is set between 3 and 6. Having a smaller value of overlap improves the appearance of the ridges, filling up small holes in ridges, while having too high value of overlap can result in false joining of ridges [40]. Figure 3.9 illustrates the use of enhancement using FFT transform.

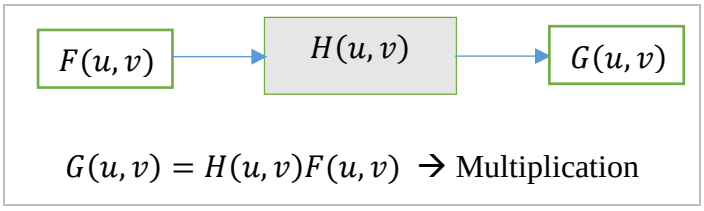
Filtering in spatial domain consists of convolving an image $f(x,y)$ with a filter mask $h(x,y)$.

In pixel domain [26]:



According to the convolution theorem, we can obtain the same result as in frequency domain found by multiplying $F(u,v)$ by $H(u,v)$, where $H(u,v)$, is the Fourier transform of the spatial filter $h(x,y)$. However, enhancement in spatial domain using is computationally complex. Therefore, frequency domain bandpass filter is used to remove the low and high frequency components [26].

In frequency domain [26]:



The filer output is given by [26]

$$G(u,v) = H(u,v)F(u,v) \tag{3.9}$$

Where H(u,v) is the filter transfer function and for Butterworth case, it is given as [26]

$$H(u,v) = \frac{1}{1+\frac{D(u,v)}{D_0}} \tag{3.10}$$

The general steps of filtering on image Enhancement using FFT are [26]

1) Centering - Multiply the block image $f(x,y)$ by $(-1)^{x+y}$
2) Compute F(u,v) – FFT
3) Filtering - Multiply F(u,v) by H(u,v)
4) Root filtering - Multiply the filtered result in step 3 by the power spectrum
5) Compute the IFFT of the result found in step 4
6) Obtain the real part of the result
7) Decentering - Multiply by $(-1)^{x+y}$

An IFFT is then applied to the filtered block image and reconstruction process takes place to get the full size of the fingerprint image. Finally, contrast enhancement is applied to the reconstructed image to get the final enhanced image.

Figure 3.9. Original Fingerprint Image and its Enhanced Image by FFT[40]

The enhanced image after FFT has the improvements in connecting some broken ridges and in removing some spurious connections between ridges.

3.2.3. Enhancement using Gabor Filter

The main purpose of this stage is to remove noise that exists between ridges and preserve the ridge and valley structures. One of the most important advantages of Gabor filters is that they have both orientation-selective and frequency-selective properties. This advantage allows Gabor filters to be tuned to the corresponding local orientation and frequency for each local neighborhood and give optimal response to the ridges in the fingerprint image. The necessary parameters of Gabor filter are local ridge orientation, ridge frequency and the standard deviations of the Gaussian envelope [38]. This algorithm consists of Normalization, Segmentation, Orientation estimation, Frequency estimation, Gabor Filtering and Binarization. Since the ridges poses the structure of repeated and parallel lines, it is possible to determine the frequency and ridge orientation from the FFT based enhanced fingerprint image. These steps are shown in Figure 3.10. The Normalization and Segmentation parts are already explained in the previous section [29].

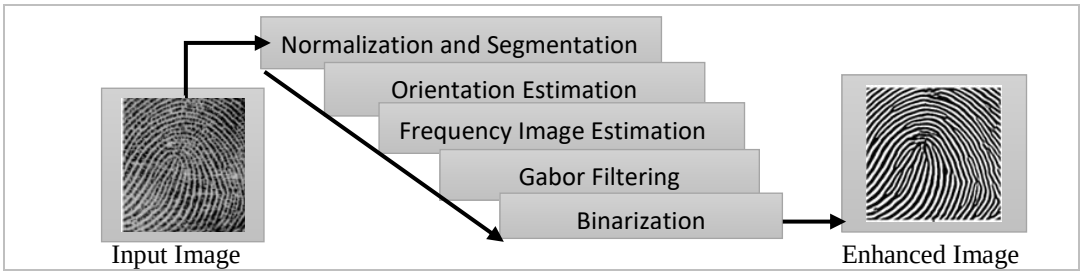


Figure 3.10. A Block Diagram of Gabor Filter based Fingerprint Enhancement [29]

3.2.3.1. *Orientation Estimation*

The Gabor filtering stage of the enhancement process relies heavily on filtering along the local ridge orientation in order to enhance the ridge structure and reduce noise [29]. An orientation image is a matrix of direction vectors representing the ridge orientation at each location in the image. The gradient-based approach is used to calculate the orientation, which makes uses fact that the orientation vector is orthogonal to the gradient. Firstly, the gradient is calculated for every pixel of the fingerprint image, in the *x* and *y* directions. The orientation vector for each block is derived by performing an averaging operation on all the vectors orthogonal to the gradient pixels in the block [35].

Intuitive Analysis

Gradients cannot be directly averaged in a local neighborhood, since opposite gradient vectors will cancel each other, although they indicate the same ridge-valley orientation. This is caused by the fact that local ridge-valley structures remain unchanged when rotated over 180 degrees [35].

A solution to this problem is, squaring the length and doubling the angles of the gradient vectors before averaging. After doubling the angles, opposite gradient vectors will point in the same direction and therefore will reinforce each other, while perpendicular gradients will cancel. After averaging, the gradient vectors have to be converted back to their single angle representation. The ridge-valley orientation is then perpendicular to the direction of the average gradient vector [6].

Formal Analysis

The intuitive analysis that was described in the previous section is formalized. The orientation vector, O which is orthogonal to the gradient is given in Eq. (2.28) by [6]

$$O = \frac{\pi}{2} + \frac{1}{2}\arctan\left(\frac{2G_{xy}}{G_{xx} - G_{yy}}\right)$$

Where G_{xx}, G_{yy} and G_{xy}, are the estimated covariance and cross covariance of the gradients G_x and G_y. This orientation is positive in the clockwise direction.

3.2.3.2. *Orientation Smoothing*

Due to the presence of noise in the fingerprint, such as corrupted minutiae, ridge and valley structures, etc., the local ridge orientation may not always be correctly determined in the formal analysis step. Since the local ridge orientation varies slowly in a local neighborhood, the orientation image can be smoothed using a Gaussian low-pass filter to modify the incorrectly estimated local ridge orientation or to reduce the effect of outliers [23].

The first step in orientation smoothing is to convert the orientation image into a continuous vector field, which is defined as follows [23]:

Let,

$$\theta = \frac{1}{2}\arctan\left(\frac{2G_{xy}}{G_{xx} - G_{yy}}\right)$$

Then, this equation is converted into continuous vector using [38]

$$\varphi_x(i,j) = \cos(2\theta(i,j))$$
$$\varphi_y(i,j) = \sin(2\theta(i,j)) \tag{3.11}$$

Where φ_x *and* φ_y are the x and y components of the vector filed, respectively. The Gaussian low-pass filter (G) of size $w_\varphi \times w_\varphi$ can then be applied as follows [38]:

$$\varphi'_x(i,j) = \sum_{u=-\frac{w_\varphi}{2}}^{\frac{w_\varphi}{2}} \sum_{v=-\frac{w_\varphi}{2}}^{\frac{w_\varphi}{2}} G(u,v)\varphi_x(i-uw, j-vw)$$
$$\varphi'_y(i,j) = \sum_{u=-\frac{w_\varphi}{2}}^{\frac{w_\varphi}{2}} \sum_{v=-\frac{w_\varphi}{2}}^{\frac{w_\varphi}{2}} G(u,v)\varphi_y(i-uw, j-vw) \tag{3.12}$$

The final smoothed orientation filed is computed by using the following equation [41].

$$O(i,j) = \frac{\pi}{2} + \frac{1}{2}\tan^{-1}\frac{\varphi'_x(i,j)}{\varphi'_y(i,j)} \tag{3.13}$$

3.2.3.3. *Frequency Estimation*

The next step in image enhancement process using Gabor filter is estimation of the local ridge frequency image. First, the image is divided into non overlapping square blocks and an oriented window is calculated for each block. Next, an x-signature signal is constructed using the ridges and valleys in the oriented window for each block. The x-signature is the projection of all the grey level values in the oriented window along a direction orthogonal to the ridge orientation.

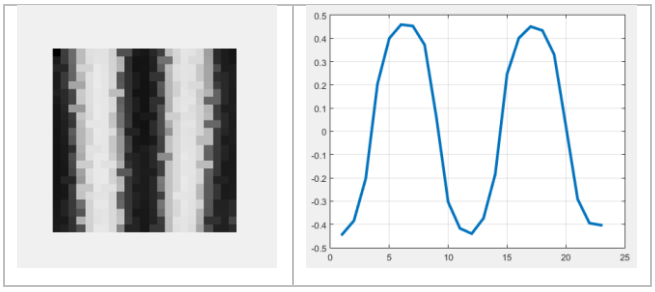


Figure 3.11. Local X-Signature and its Estimated Waveform

Consequently, the projection forms a sinusoidal-shape wave in which the center of a ridge maps itself as a local minimum in the projected wave. Finally, the distance between consecutive peaks in the x-signature is used to estimate the frequency of the ridges [25]. Let $S(i,j)$ is the ridge spacing that is computed by counting the median number of pixels between consecutive minima points in the projected waveform. Hence, the ridge frequency $F(i,j)$ for a block centered at pixel (i,j) is defined in Eq. (2.29) as:

$$F(i,j) = \frac{1}{S(i,j)}$$

3.2.3.4. *Mathematical Model of Gabor Filter*

Once the ridge orientation and ridge frequency information of the fingerprint is determined, these parameters are used to construct the even-symmetric Gabor filter. A two dimensional Gabor filter consists of a sinusoidal plane wave of a particular orientation and frequency, modulated by a Gaussian envelope [4]. Gabor filters are employed because they have frequency-selective and orientation-selective properties. These properties allow the filter to be tuned to give maximal response to ridges at a specific orientation and frequency in the fingerprint image. Therefore, a properly tuned Gabor filter is used to effectively preserve the ridge structures while reducing noise.

The even-symmetric Gabor filter is the real part of the Gabor function, which is given by a cosine wave modulated by a Gaussian (see Figure 2.3). The even-symmetric Gabor filter in the special domain has the general form as it is stated in Eq. (2.44) [38].

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

The coordinate values are given by [38]

$$x_\theta = x\cos\theta + y\sin\theta$$
$$y_\theta = -x\sin\theta + y\cos\theta$$

Where θ is the orientation of the Gabor filter, f is the frequency of the cosine (a sinusoidal plane) wave, δ_x and δ_y are the space constants (standard deviations) of the Gaussian envelope along the x and y axes, respectively, and x_θ and y_θ define the x and y axes of the filter coordinate frame,

respectively. Since the local ridge structures of fingerprints come with a well-defined local frequency and orientation, f is set to the reciprocal of the average inter-ridge distance and m as the number of orientations for $\theta = \frac{\pi(k-1)}{m}$, k=1, … ,m. Also the Cosine/Sine form and the sinusoidal-shape of Gabor filter is suitable for modelling ridge/valley structures and smoothing out noise, respectively [42].

3.2.4. Gabor Filter Parameter Selection

The Gabor filter parameters σ_x and σ_y control the bandwidth of the filter, and must be chosen carefully. The Gabor filter bandwidth, which specifies the range of frequency to which the filter responds to, is determined by the standard deviation parameters σ_x and σ_y. σ_x determines the degree of contrast enhancement between ridges and valleys, and σ_y determines the amount of smoothing applied to the ridges along the local orientation. Since the bandwidth of the filter is tuned to match with the estimated local ridge frequency, σ_x and σ_y should related to the ridge estimated ridge frequency. A drawback of using fixed values is that it forces the bandwidth to be constant, which does not take into account the variation that may occur in the values of the ridge frequency. For example, if a filter with a constant bandwidth is applied to a fingerprint image that exhibits significant variation in the frequency values, it could lead to non-uniform enhancement or other enhancement artefacts. Thus, rather than using fixed values, it is better the values of σ_x and σ_y to be a function of the ridge frequency parameter, which are defined as [37]:

$$\sigma_x = \frac{k_x}{F(i,j)}$$
$$\sigma_y = \frac{k_y}{F(i,j)} \tag{3.14}$$

where *F* is the ridge frequency image, k_x is a constant variable for σ_x, and k_y is a constant variable for σ_y.

This allows a more adaptable approach, as the values of σ_x and σ_y can be specified adaptively according to the local ridge frequency of the fingerprint image.

Large values of σ_x and σ_y lead to enhancement artefacts and a significant amount of blurring of the ridge structures. This blurring occurs due to the over-smoothing of the image by the Gabor

filter while too small values of σ_x and σ_y, lead the filter to be not effective in removing noise from the image and the resulting image is simply a smoothed version of the original image. This smoothing of the image occurs due to the Gabor filter evolving into the shape of a pure low pass filter. Hence, it can be seen that the selection of σ_x and σ_y involves a trade-off between values that are too small and values that are too large. Experiments conducted with the Gabor filter for varying values of σ_x and σ_y have shown that using $k_x = 0.5$ and $k_y = 0.5$ provides a reasonable trade – off [37].

3.2.4.1. *Gabor Filter Enhancement*

Based on the local orientation and ridge frequency around each pixel, the Gabor filter is applied to each pixel location in the fingerprint image by spatially convolving the image with the filter. The effect is that the filter enhances the ridges oriented in the direction of the local orientation, and decreases anything oriented differently.

Enhancement *E* is performed as follows [43]:

$$E(i,j) = \sum_{u=-\frac{w_x}{2}}^{\frac{w_x}{2}} \sum_{v=-\frac{w_y}{2}}^{\frac{w_y}{2}} G\left(u, v; O(i,j), F(i,j)\right) N(i-u, j-v) \tag{3.15}$$

where *O* is the estimated orientation, *F* is the estimated ridge frequency image, *N* is the normalized fingerprint image, and w_x and w_y are the width and height of the Gabor filter mask, respectively.

The filter size controls the spatial extent of the filter, which ideally should be able to accommodate the majority of the useful Gabor waveform information. A fixed filter size is not optimal since it does not allow the accommodation of Gabor waveforms of different sized bandwidths. Hence, to allow the filter size to vary according to the bandwidth of the Gabor waveform, the filter size have to be set a function of the standard deviation parameters [29]:

$$\begin{aligned} w_x &= 6\sigma_x \\ w_y &= 6\sigma_y \end{aligned} \tag{3.16}$$

where w_x and w_y are the width and height of the Gabor filter mask, respectively, and σ_x and σ_y are the standard deviations of the Gaussian envelope along the *x* and *y* axes, respectively.

3.2.5. Enhancement using FFT and Gabor Filter

Here, the fingerprint image is first enhanced using FFT filtered by a bandpass Butterworth filter. Next, the orientation and the local ridge frequency of the FFT enhanced image are estimated using equations (2.29) and (3.13). Then, again, the image is enhanced using Gabor filter that is modeled using the estimated new parameters. This is used to provide better image quality than of the others implemented independently.

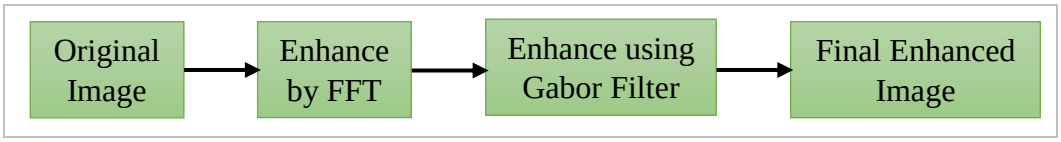


Figure 3.12. FFT Cascaded with Gabor Filter

3.2.6. Binarization and Thinning

One useful property of the Gabor filter is that it has a DC component of zero, which means the resulting filtered image has a mean pixel value of zero. Hence, straightforward binarization of the image can be performed using a global threshold of zero. The binary image of the Gabor enhanced fingerprint grayscale image, $E(i, j)$ is given by [29]

$$Binary(i, j) = \begin{cases} 1 \text{ , } if \;\; E(i, j) > 0 \\ 0 \text{ , } if \;\; otherwise \end{cases} \tag{3.17}$$

The final step in the enhancement using Gabor filter performed prior to the feature extraction is thinning which is used to form a skeletonized version of the binary image. This skeleton image is then used in the subsequent extraction of minutiae.

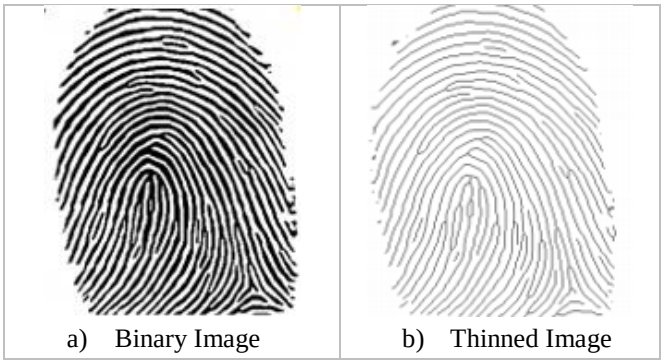


Figure 3.13. Binary Images [44]

3.3. Feature Extraction

Features such as the type, location and direction of the minutiae are taken into account when performing feature extraction. The set of minutiae types are restricted into only two types, namely terminations (ridge endings) and bifurcations as shown in Figure 3.14 [23]. Terminations are the points where a ridge curve comes to an end, and bifurcations are the points where a ridge splits from a single path into two separate paths at a Y-junction. The coordinates (x_0, y_o) tell us about the position that where the feautere exists while the orientation angle θ tells us the flow of the angular direction of that specific feature [4].

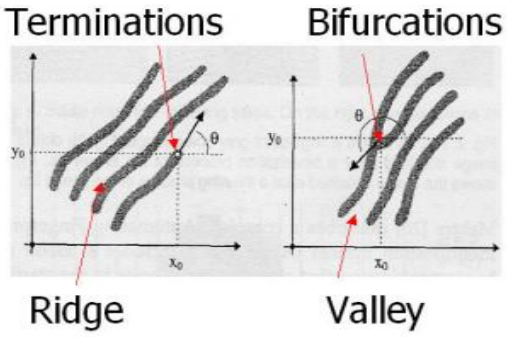


Figure 3.14. Termination and Bifurcation [20]

3.3.1. Crossing Number Concept

The minutiae extraction algorithm uses the Crossing Number (CN) concept to extract terminations and bifurcations. This method uses the skeletonized image where the ridge flow pattern is 8-connected. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3×3 window as shown in Figure 3.15. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood. The CN value is computed as [44]

$$CN = \frac{1}{2}\sum_{i=1}^{8}\left|P_i - P_{i+1}\right|, \quad P_9 = P_1 \tag{3.18}$$

where P_i is the pixel value in the neighborhood of P_c. For a pixel P_c, its eight connected neighboring pixels are scanned in an anti-clockwise direction as it is indicated in Figure 3.15.

P_4	P_3	P_2
P_5	$\mathbf{P_c}$	P_1
P_6	P_7	P_8

Figure 3.15. A 3 × 3 pixel Window [44]

After the CN is computed, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point according to the property of the CN shown in Table 3.2 [44].

Table 3.2. Properties of the Crossing Number [44]

CN	**Property**
0	Isolated Point
1	Ridge Ending ***
2	Continuing Ridge
3	Ridge Bifurcation ***
4	Crossing

For example, as shown in Figure 3.16, a ridge pixel with a Crossing Number of one corresponds to a ridge ending, a Crossing Number of three corresponds to a bifurcation and a Crossing Number of two corresponds to a continuing ridge.

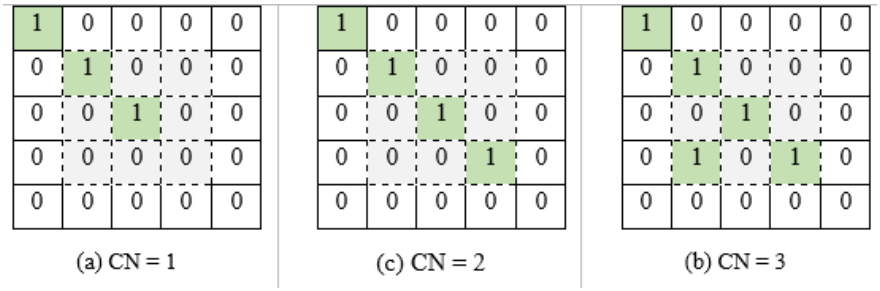


Figure 3.16. Examples of a continuing ridge, ridge ending and bifurcation pixel [13]

The information that completely characterize for each extracted minutiae point are [44]

- ✓ The x and y coordinates of the minutiae point,
- ✓ Type of minutiae (ridge ending or bifurcation), and
- ✓ Orientation of the associated ridge segment

3.3.2. Feature Direction Estimation

Bifurcation angle is the angle between the horizontal line and the opposite direction of the valley ending between the two ridges that are close to each other. The bifurcation is broken into three terminations. The three new terminations are the three neighbor pixels of the bifurcation and each of the three ridges connected to one common point to form a bifurcation and all have their own direction [29] (Figure 3.17).

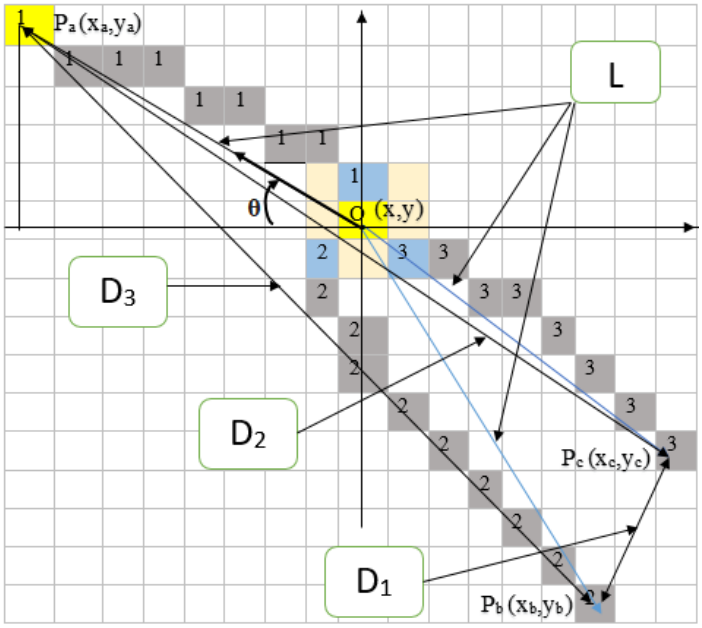


Figure 3.17. Geometric Representation of a Bifurcation

The orientation of each bifurcation at the point $O(x, y)$ is estimated by considering the orientation of the three ridges as follows. A ridge segments are traced from the starting point $O(x, y)$ to the termination points $P_a(x_a, y_a)$, $P_b(x_b, y_b)$ and $P_c(x_c, y_c)$ which have a path length of L. Then the distances between each the three points are calculated using [44]

$$D_1 = \sqrt{(x_b - x_c)^2 + (y_b - y_c)^2}$$

$$D_2 = \sqrt{(x_a - x_c)^2 + (y_a - y_c)^2} \quad (3.19)$$

$$D_3 = \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}$$

Then again the point that is opposite to the smallest distance, in this case D_1, is taken where the point is $P_a(x_a, y_a)$ and the direction is found from the equation

$$\theta = \tan^{-1}\left(\frac{y - y_a}{x - x_a}\right) \tag{3.20}$$

Termination Angle is the angle between the horizontal line and the direction of the ridge. The orientation of each termination is estimated by tracing a ridge segment from the starting point $P_0(x, y)$ to the termination point $P_a(x_a, y_a)$ which has a path length of L (Figure 3.18).

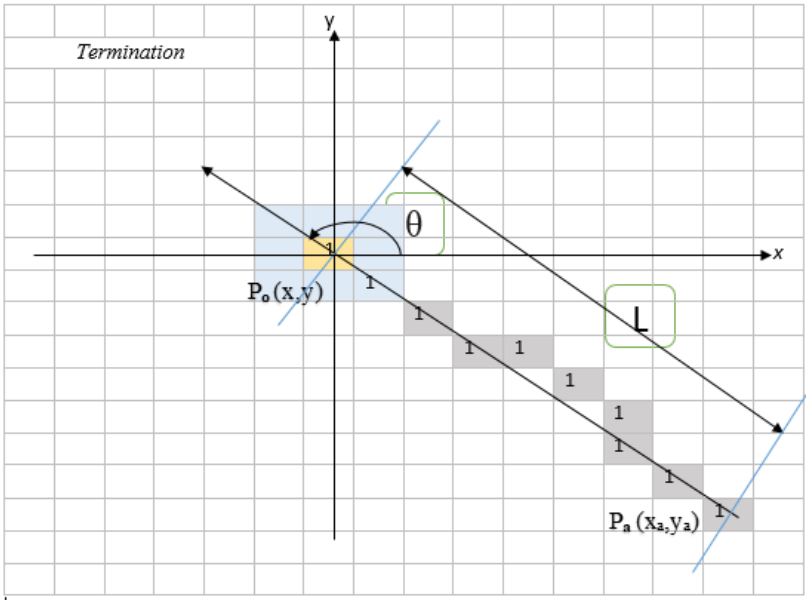


Figure 3.18. Geometric Representation of a Termination

Similarly, the direction of the termination is obtained using Eq. (3.20).

$$\theta = \tan^{-1}\left(\frac{y - y_a}{x - x_a}\right)$$

3.4. **Matching**

The fingerprint matching module is performed to check whether two fingerprints belong to the same person or not. Fingerprint recognition includes two sub-domains namely fingerprint verification and fingerprint identification [45].

3.4.1. Verification

Fingerprint verification is the process of verifying the authenticity of one person by his fingerprint together with his identity information like his identification (ID) number. The fingerprint verification system retrieves the fingerprint template according to the ID number and matches the template with the real-time acquired fingerprint from the individual. It is a one-to-one comparison to confirm whether the claim of identity by the individual is true or not [17].

3.4.2. Identification

Fingerprint identification is the process of specifying one person's identity by his fingerprint(s) without knowledge of the person's identity i.e. the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database. It is especially useful for criminal investigation cases [17].

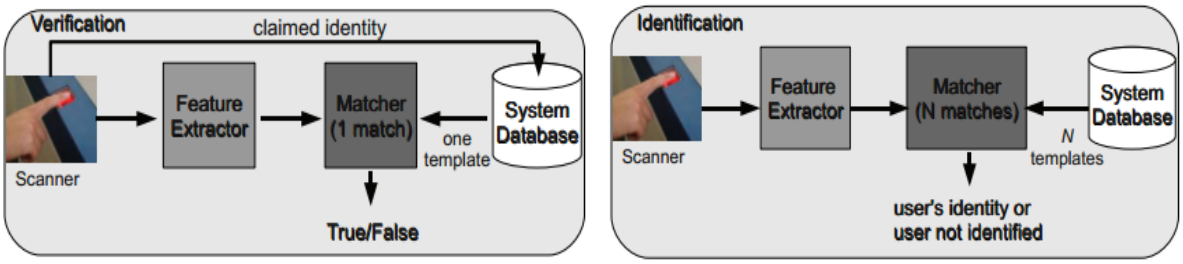


Figure 3.19: Basic model for fingerprint verification and identification processes [6]

3.4.3. Minutiae Match

The fingerprint matching module computes a minutiae match score between two set of feature points of fingerprints, to check whether they belong to the same person or not. The minutiae match score should be high for fingerprints that come from the same finger and low for those that come from different fingers. Minutiae-based matching algorithms are largely dependent on the extracted minutiae information [25]. The general processes of a fingerprint matching algorithm is presented in Figure 3.20.

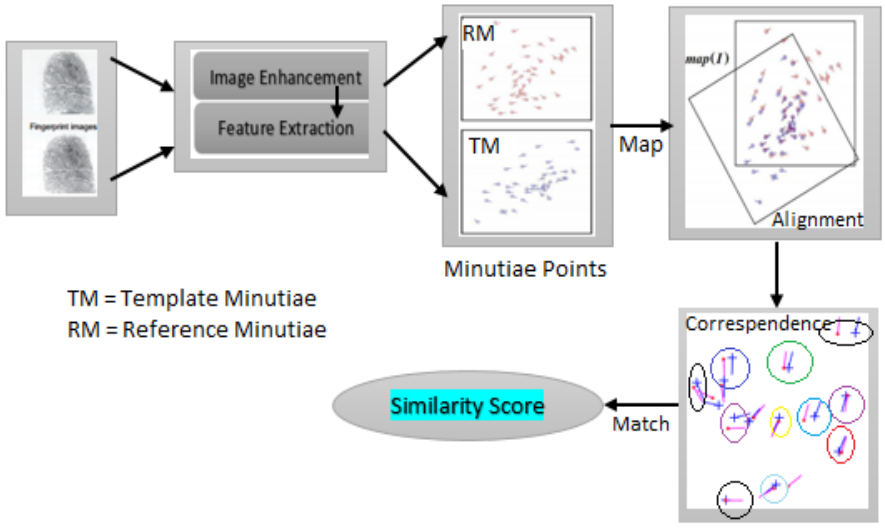


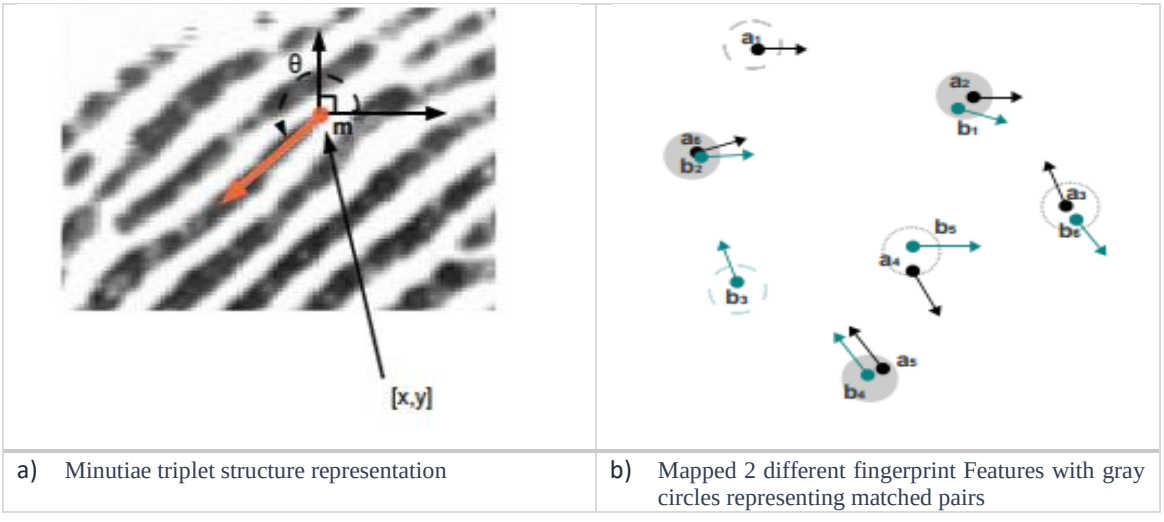
Figure 3.20. General process of minutiae based fingerprint matching [45]

3.4.3.1. *Minutiae representation*

In minutiae-based matching, the features are commonly represented as minutiae structures called minutiae triplets, where a minutiae is described as [44]

$$M_i = \{x, y, \theta, t\} \tag{3.21}$$

Where (x, y) representing the coordinates of the minutiae point, θ represents the angular direction of the main ridge and t is the type of the minutiae point (Figure 3.21a).



a) Minutiae triplet structure representation

b) Mapped 2 different fingerprint Features with gray circles representing matched pairs

Figure 3.21. Minutiae Representation and Mapping after Registration [45]

The main focus of minutiae-based matching algorithm is to perform a one-to-one mapping or pairing of minutiae points from a test image (reference fingerprint) minutiae set [45]

$$M_A = \left\{ M_{A_1}, M_{A_2}, \ldots, M_{A_p} \right\}$$

Where

$$M_{A_i} = \left\{ x_{A_i}, y_{A_i}, \theta_{A_i}, t_{A_i} \right\} \textbf{ and } 1 \le i \le p$$

to a template fingerprint from a database minutiae set

$$M_B = \left\{ M_{B_1}, M_{B_2}, \ldots, M_{B_q} \right\}$$

Where

$$M_{B_j} = \left\{ x_{B_j}, y_{B_j}, \theta_{B_j}, t_{B_j} \right\} \textbf{ and } 1 \le j \le q$$

forming the minutiae pairs (M_{A_k}, M_{B_k}) and returns similarity score $S(M_A, M_B)$. However, it is not possible to proceed to find the minutiae pairs directly from the triplets without some pre-processing for the following critical reasons [45]:

1) Fingerprint impressions can differ in orientation, deeming the direction field in the triplet useless,
2) Fingerprint impressions can differ in offset, deeming the x-y fields in the triplet useless, and
3) Skin elasticity creates non-linear distortion or 'warping' to occur when different directional pressure is applied causing triplet x-y and θ variations to occur.

In general, the lack of invariant characteristics of the triplet structure prohibits it to aid the process of finding minutiae pairs. In order to address these issues concerning the lack of invariance of the triplet structure, global alignment (or registration) is required before matching takes place.

3.4.3.2. *Alignment (Registration) Stage*

For matching regular sized fingerprint images, a brute-force matching method, which examines all the possible solutions is not feasible since the number of possible solutions increases exponentially with the number of feature points on the fingerprints [29, 44]. Thus, transformation of input minutiae set is the most important step in order to maximize the value of similarity score. Global registration concerns the alignment and overlay of the template and test fingerprints so that corresponding regions of the fingerprints have minimal geometric distance to each other. Registration is achieved geometrically by applying a guided affine transform to the fingerprint minutiae set, where minutiae triplet field values are updated to a new coordinate system [45]. For each fingerprint, all minutiae are translated and rotated with respect to the reference minutiae according to the following formulas [12]:

$$x_{new} = x_{\Delta} * Cos(\theta) - y_{\Delta} * Sin(\theta)$$
$$y_{new} = x_{\Delta} * Sin(\theta) + y_{\Delta} * Cos(\theta)$$
$$\theta_{new} = \theta_{\Delta}$$

In Matrix form this can be written as [12]

$$\begin{bmatrix} x_{new} \\ y_{new} \\ \theta_{new} \end{bmatrix} = \begin{bmatrix} Cos(\theta) & -Sin(\theta) & 0 \\ Sin(\theta) & Cos(\theta) & 0 \\ 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} x_{\Delta} \\ y_{\Delta} \\ \theta_{\Delta} \end{bmatrix} \tag{3.22}$$

Where θ_{Δ} is the orientation difference and (x_{Δ}, y_{Δ}) is the displacement difference in order to super-impose one fingerprint impression on top of the other with accurate overlap and uniform direction [12].

$$\begin{bmatrix} x_{\Delta} \\ y_{\Delta} \\ \theta_{\Delta} \end{bmatrix} = \begin{bmatrix} x - x_r \\ y - y_r \\ \theta - \theta_r \end{bmatrix} \tag{3.23}$$

where $\{x, y, \theta\}$ are the minutiae representation parameters and $\{x_r, y_r, \theta_r\}$ is the parameters of the reference minutiae.

Equation (3.22) can be written as [12]

$$\begin{bmatrix} x_{new} \\ y_{new} \\ \theta_{new} \end{bmatrix} = TM * \begin{bmatrix} x_{\Delta} \\ y_{\Delta} \\ \theta_{\Delta} \end{bmatrix} \tag{3.24}$$

Where TM is usually called the transformation matrix [12]

$$\mathrm{TM} = \begin{bmatrix} \mathrm{Cos}(\theta) & -\mathrm{Sin}(\theta) & 0 \\ \mathrm{Sin}(\theta) & \mathrm{Cos}(\theta) & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{3.25}$$

The determinant of TM is 1 and this shows that it has no effect of scale of the transformed features.

$$\det(\mathrm{TM}) = \det \begin{vmatrix} \mathrm{Cos}(\theta) & -\mathrm{Sin}(\theta) & 0 \\ \mathrm{Sin}(\theta) & \mathrm{Cos}(\theta) & 0 \\ 0 & 0 & 1 \end{vmatrix} = 1 \tag{3.26}$$

3.4.3.3. *Matching Stage*

Fingerprint matching is the process of comparing two fingerprints against each other to verify whether they belong to same person or not. A minutiae-based fingerprint matching system usually returns the number of matched minutiae on both test and template fingerprints and uses it to generate similarity score. Following the registration process, the geometric constraints for the discovery of minutiae matching pairs, including geometric Euclidean distance is produced. The minutiae pair $\mathrm{M}_{\mathrm{A_i}}$ and $\mathrm{M}_{\mathrm{B_j}}$ are considered to be match if and only if the Euclidean distance between their position and the difference in their directions are lower than a specified tolerance values. The Euclidean distance is given by [44]

$$dist_r(M_{A_i}, M_{B_j}) = \sqrt{(x_{A_i} - x_{B_j})^2 + (y_{A_i} - y_{B_j})^2} < r_0 \tag{3.27}$$

and the minutiae angle difference is given by [44],

$$dist_\theta(M_{A_i}, M_{B_j}) = \min\left(\left| \theta_{A_i} - \theta_{B_j} \right| ,\ 360 - \left| \theta_{A_i} - \theta_{B_j} \right| \right) < \theta_0 \tag{3.28}$$

The geometric tolerance r_0 is in place to account for distortion that may occur, whereas θ_0 is the tolerance for angular differences that may arise due to error in orientation estimations and image rotation. Now, the local search can be performed, in order to match minutiae in the neighborhood that meet the constraints in equations (3.27) and (3.28) (Figure 3.22). Once the minutiae pairs are produced, a metric of similarity, usually called the similarity score, is calculated using the following equation [45].

$$sim(A,B) = \sqrt{\frac{n^2_{match}}{n_A n_B}} \tag{3.29}$$

Where n_{match} is the number of matched minutiae pairs, n_A and n_B are the number of minutiae in the overlapped regions of the test and template fingerprints. The value of the similarity score is always less than or equal to 1.

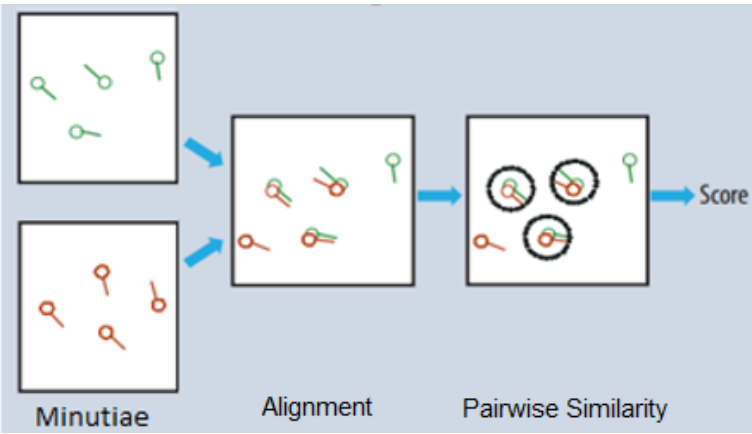


Figure 3.22. Typical minutiae matching algorithm[25]

3.4.4. System Errors

A fingerprint matcher can make two types of errors. The first is a false match, in which the matcher declares a match between images from two different fingers. When a fingerprint matches with the fingerprint of same individual, we call it true accept or if it doesn't, it is called false reject. The second type of error is a false non match, in which it does not identify images from the same finger as a match. If the fingerprint of different individuals match, we call it a false accept or if it rejects them, it is true reject. FMR and FNMR are the error rates which are used to express matching accuracy [12].

The similarity score values are used to estimate the FMR and FNMR for different threshold values using Equations (3.30) and (3.31) respectively. The probability that the system will decide to allow access to an imposter, FMR is defined by [12, 13]:

$$FMR(t) = \frac{FA(t)}{N} \times 100\ \%$$

$$FMR(t) = \frac{NFP(t) - N_{TA}(t)}{N} \times 100\ \% \tag{3.30}$$

Where, FA(t) = Number of False Accepts or False Matches at the threshold t which is given by $FA(t) = NFP(t) - N_{TA}(t)$, where $NFP(t)$ is the number of fingerprints matched at the threshold t, $N_{TA}(t)$ is the number of true or actual accepted fingerprints at the threshold t out of the total expected fingerprints and N is the total number of verifications.

The probability that the system denies access to an approved individual, FNMR is defined by [12]:

$$FNMR(t) = \frac{FR(t)}{N_{EM}} \times 100\ \%$$

$$FNMR(t) = \frac{N_{EM} - N_{TA}(t)}{N_{EM}} \times 100\ \% \tag{3.31}$$

Where, FR(t) = Number of False Rejects, N_{EM} is the number of total expected fingerprint per individual to be matched and $N_{TA}(t)$ is the number of true or actual accepted fingerprints at the threshold t out of the total expected fingerprints. The threshold, t, varies from 0 up to 1 with some uniform interval.

As it is indicated in Equations (3.30) and (3.31), a system's FMR and FNMR are both functions of the operating system threshold *t*, a large threshold score leads to a small FMR at the expense of a high FNMR. There is a strict tradeoff between FMR and FNMR in every biometric system. If the threshold *t*, is decreased to make the system more tolerant with respect to input variations and noise, then FMR(*t*) increases. On the other hand, if the threshold *t*, is increased to make the system more secure, then FNMR(*t*) increases. Therefore, for a given fingerprint matching system, it is impossible to reduce both these errors simultaneously [4, 15].

The terms shown in Figure 3.23 are described as follows

- ✓ EER: denotes the error rate at the threshold *t* for which both FMR and FNMR are identical, i.e. FMR(*t*) = FNMR(*t*)
- ✓ *Zero FNMR*: is defined as the lowest FMR at which no false non-matches occur.
- ✓ *Zero FMR*: is defined as the lowest FNMR at which no false matches occur.

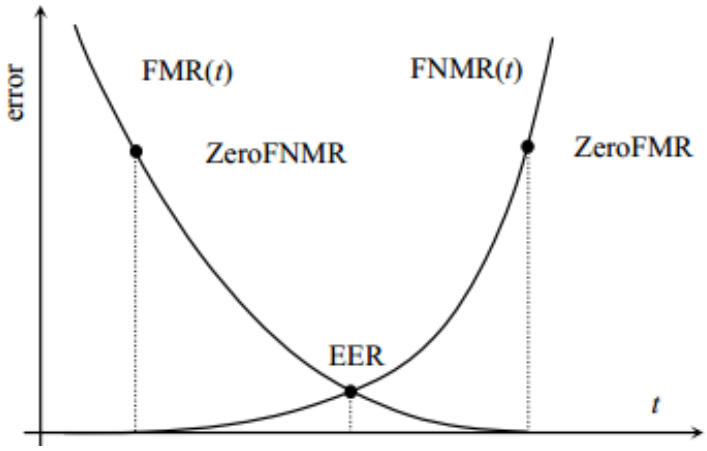


Figure 3.23. An example of FMR and FNMR Curves[4, 15]

The accuracy requirements of a biometric recognition system are very much application dependent. For example, in forensic applications such as criminal identification, it is the FNMR that is of more concern than the FMR, that is, we do not want to miss identifying a criminal even at the risk of manually examining a large number of potential false matches identified by the system. On the other extreme, a very low FMR may be the most important factor in a highly secure access control application where the primary objective is not to let in any impostors. Operating the system at a very low FMR will potentially lead to inconvenience to legitimate users due to the resulting in high FNMR. There are several civilian and commercial applications in between these two extremes, where both FMR and FNMR need to be considered. For example, in applications such as verifying a customer at a bank ATM, a false match means a loss of several hundred dollars whereas a high FNMR may upset the genuine customers [4].

Chapter 4

Simulation Results and Discussions

4.1. Introduction

In the previous chapters, the theoretical background and basic principles of fingerprint image enhancement, feature extraction and matching algorithms are developed. This chapter presents the MATLAB simulation results and discussions on the obtained results. MATLAB - based simulation is used to investigate the performances of the fingerprint image enhancement techniques on the matching stage. The features that made every individual unique called the minutiae points are extracted using the crossing number concept from the skeletonized image.

4.2. System Model Block Diagram

The overall system model block diagram of AFRS is shown in Figure 4.1.

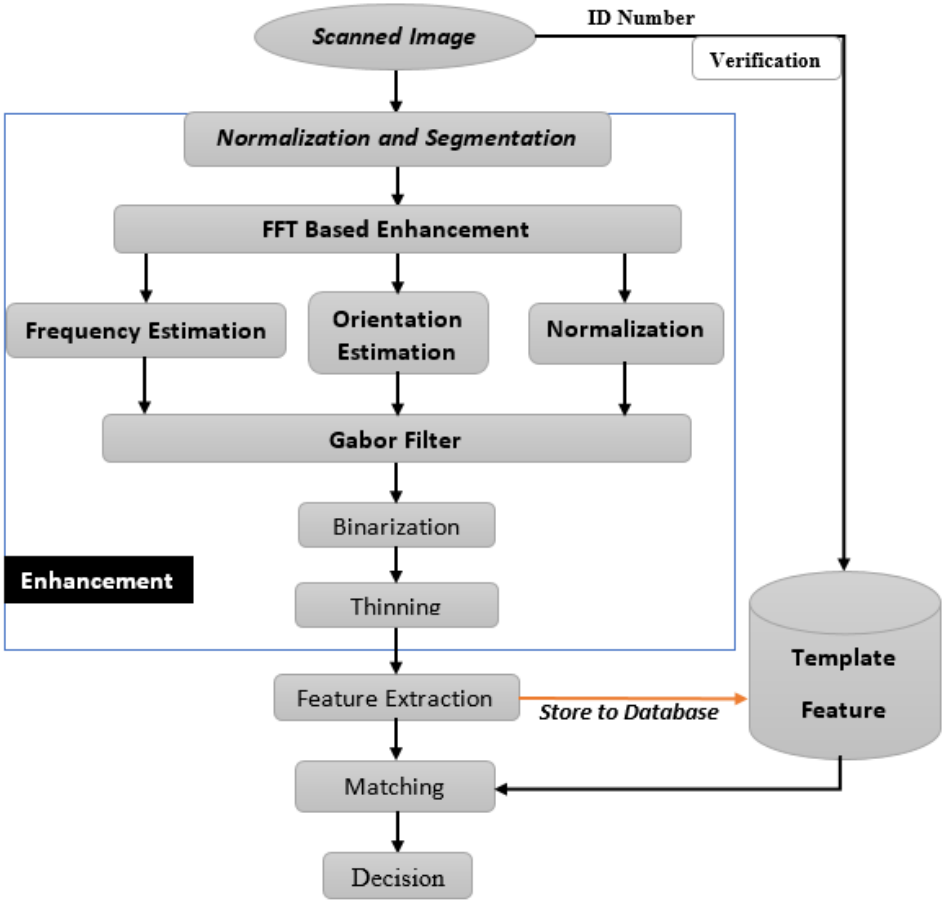


Figure 4.1. System Model of Automatic Fingerprint Recognition System

The scanned image is first normalized and segmented. Then FFT based image enhancement is performed on the segmented fingerprint image to improve the image quality. Next, frequency estimation, orientation estimation and again normalization is performed on the FFT based enhanced image and these parameters are used to model the frequency and orientation selective Gabor filter. The image is again enhanced using the Gabor filter based on the local estimated frequency and orientation. Binarization process takes place on the Gabor enhanced image with threshold value set to zero. Then, the binarized image is thinned to make the ridges one pixel wide forming a skeletonized image. Features are extracted from the skeletonized image using the crossing number concept and matching is done according to these features. In this thesis, the Fingerprint Verification Computation (FVC) fingerprint database is used as an input data where there are ten fingerprint from different persons with 8 fingerprints for each persons which composes a total of 80 fingerprint images. The eight fingerprints are taken in such a way that they have a difference in image quality, slight difference in orientation, scale, and shifted versions as well.

4.3. **Simulation Parameters**

Some of the simulation parameters used for performance evaluation of fingerprint image enhancement and system performance are listed in Table 4.1.

Table 4.1. Simulation Parameters

Parameters	**Values**
Database	FVC
Number of Persons	10
Number of fingerprints	80
Enhancement Methods	HE, FFT and Gabor filter
System Errors	FMR, FNMR and EER

4.4. **Simulation Results and Discussions**

The MATLAB simulation results for HE, FFT based, frequency and orientation selective bandpass Gabor filter and the combination of both FFT and Gabor filters using the above listed parameters are given in the following section in the form of figures and tables.

4.4.1. Image preprocessing

The image shown in Figure 4.2a is a high quality image so that the features can be extracted directly without bulky image preprocessing with minimum error. However, Figure 4.2b is a poor quality image in which the ridges are disconnected in their paths and features cannot be directly extracted from this image without image enhancement.

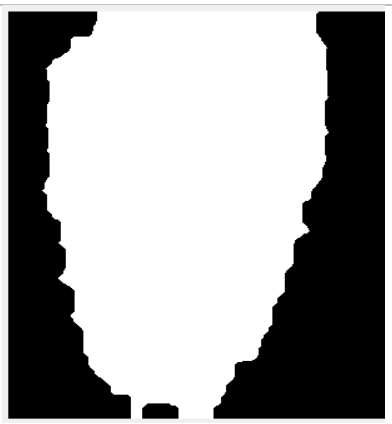
a) Original High Quality Image

b) Original Low Quality Image

Figure 4.2. High and Low Quality sample Images

4.4.1.1. *Normalization and Segmentation*

As it is shown in Figure 4.3, the low quality fingerprint image shown in Figure 4.2b is normalized and segmented based on the ROI.



a) Region of Interest (ROI)

b) Normalized and Segmented

Figure 4.3. Region of Interest and Normalized images

This avoids the noisy part of the image and facilitates the subsequent processing. The effect of the enhancement techniques to be applied for the two images i.e. for high image quality and low image quality are discussed in the following section.

4.4.2. Histogram Equalization based Enhancement

Histogram equalization simply equalizes the pixel intensity distribution and is usually used for good quality fingerprint image.

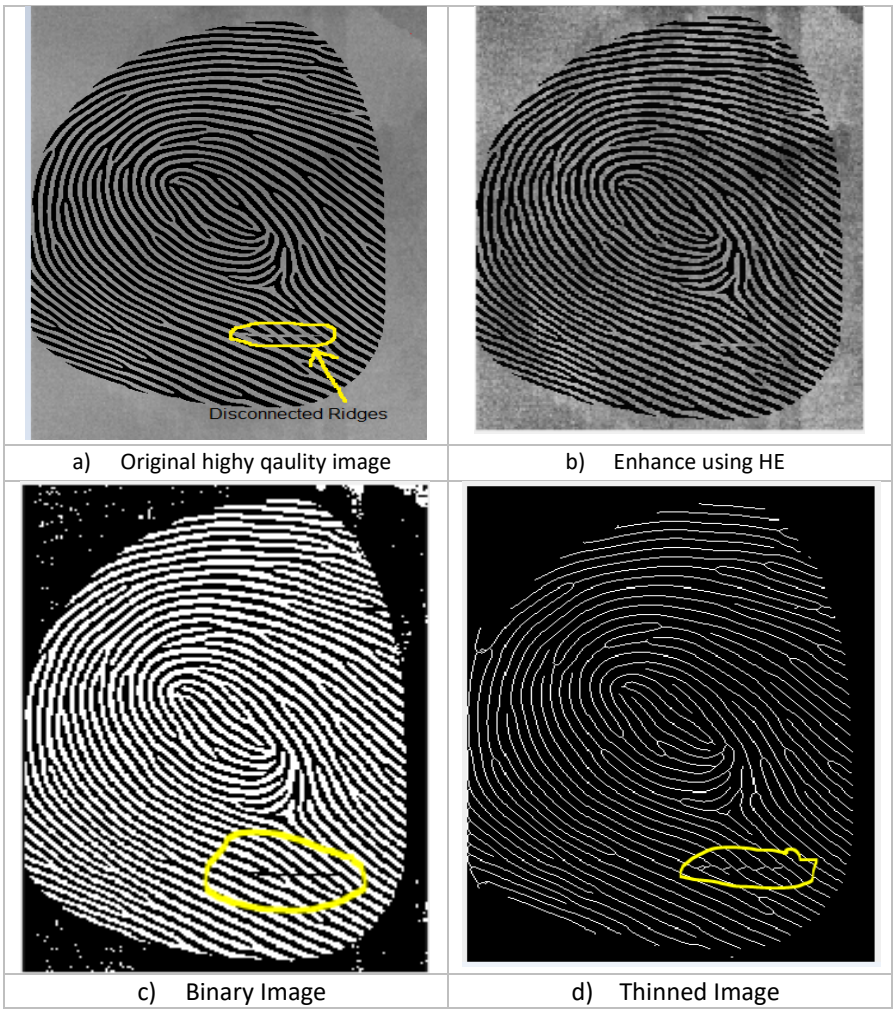


Figure 4.4. HE Based Enhanced Images for High Quality Image

As shown in Figure 4.4, HE has no ability to connect the damaged ridges even in good quality images with less affected ridges. For a bad quality image, the HE based enhanced image is shown in Figure 4.5 where the damaged and disconnected ridges are still remained disconnected and has

a lot of artifacts and cross overs after the thinning process as shown in Figure 4.5d. As a result, there is a number of false detected features from the low quality image. This causes a very high FMR, FNMR, EER and also takes more processing time in the matching stage.

Figure 4.5. HE Based Enhanced Images for Low Quality Image

4.4.3. FFT based Enhancement

The Fourier transform taken on the normalized and segmented block fingerprint image is filtered with a Butterworth filter before it is multiplied by its power spectrum to remove noise and increase the ridge image quality. As shown in Figure 4.6, the high quality original image is enhanced using FFT and the disconnected ridges indicated by the circle are modified. The enhanced image is then

locally binarized, thinned and finally multiplied by the ROI image to remove the background region of the fingerprint.

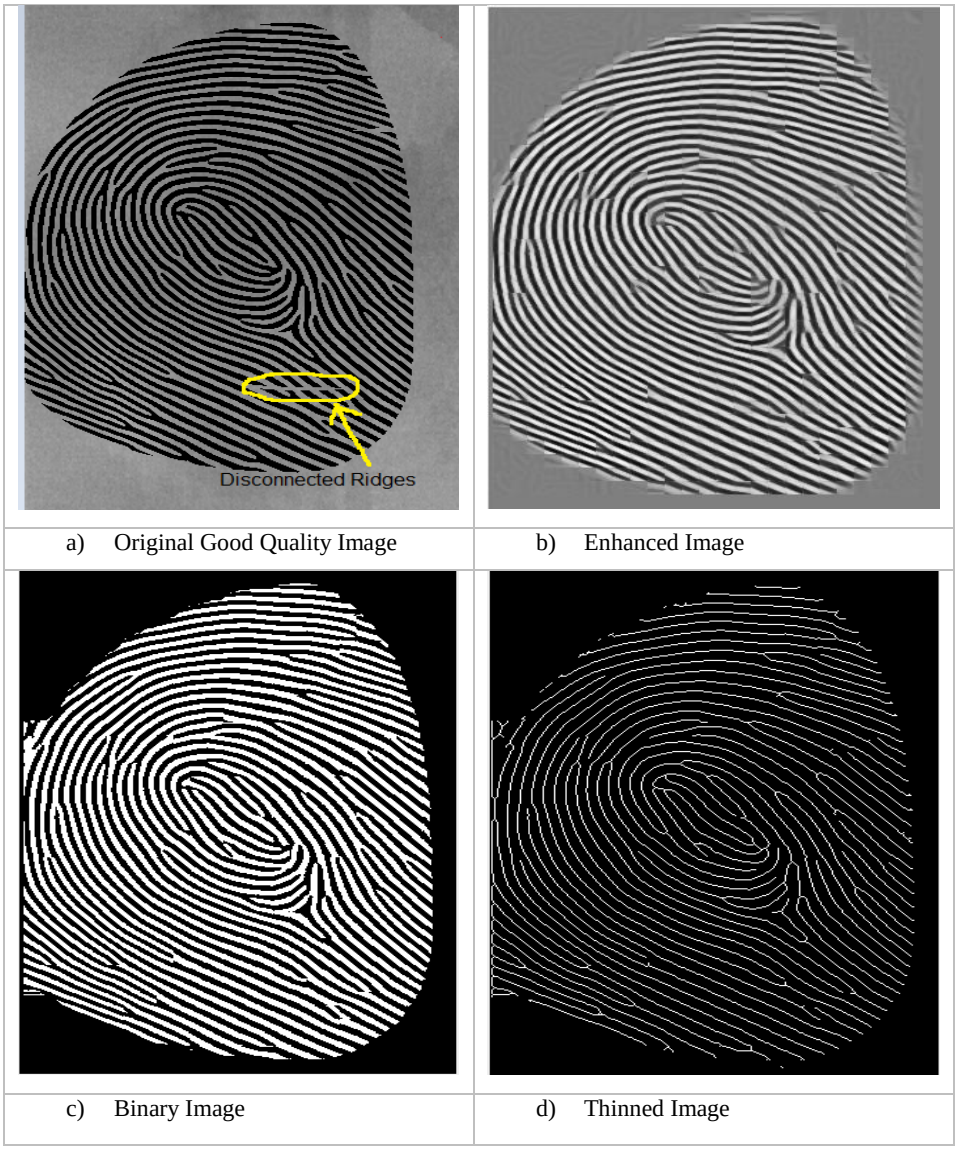


Figure 4.6. FFT Based Enhanced Images for High Quality Image

FFT is a fast method of enhancement that removes noise between the ridges and connects the fairly damaged ridges in high quality image as well as in poor quality image (Figure 4.7). However, it introduces artifacts and cross overs after the thinning process which results in false feature detection as shown in Figure 4.7d. This false feature detection in turn results in high EER, high FMR, high FNMR, and hence the system performance gets low.

a) Original Image

b) Enhanced Image

c) Binary Image

d) Thinned Image

Figure 4.7. FFT Based Enhanced Images for Low Quality Image

4.4.4. Gabor Filter based Enhancement

Gabor filter needs estimation of the local ridge frequency image and the local ridge orientation image of the original low quality fingerprint image as an input parameters. Here, the noisy part of the fingerprint image is masked before finding the parameters in order to simplify computational complexity.

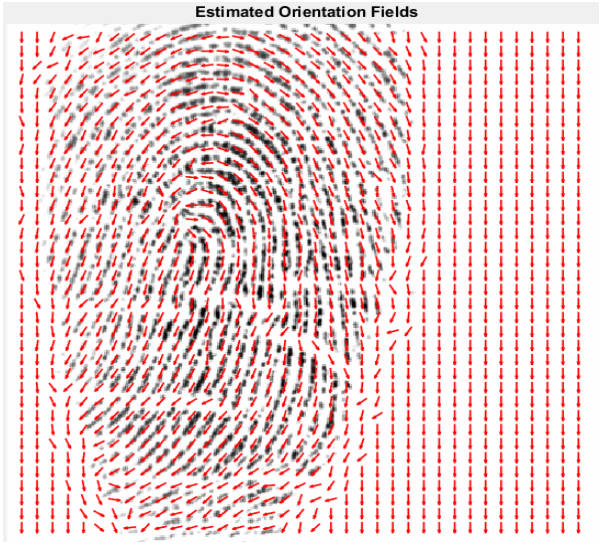


Figure 4.8. Estimated Local Ridge Orientation Image

As it is indicated in Figure 4.8, the orientation fields follow the ridge curvature but, errors occur when the ridges are significantly damaged i.e. when there is a ridge breaks and the gradient becomes maximum towards the valley created due to the ridge breaks.

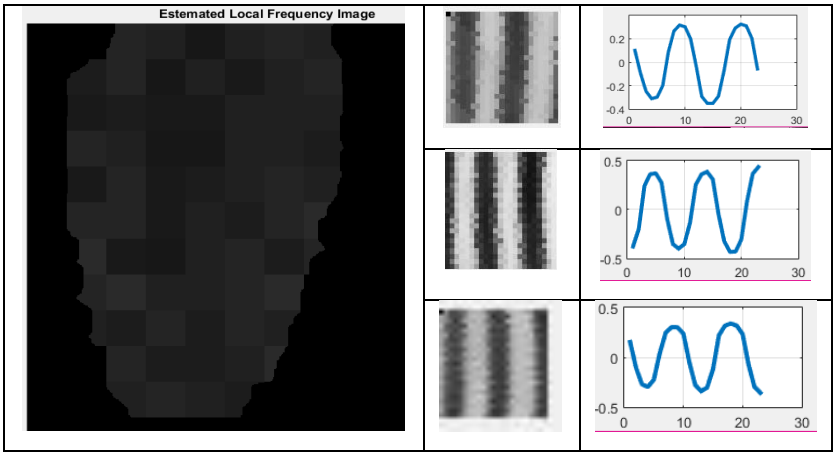


Figure 4.9. Estimated Local Ridge Frequency Image

Figure 4.9 indicates the locally estimated ridge frequency image where it is zero outside of the fingerprint part and sample oscillations for some local ridges of the fingerprint.

Gabor Kernels: are the Gabor filters modelled at different frequencies and orientations. These kernels varies with frequency and orientation and the Gabor filter parameter are set to the estimated ridge orientation and local ridge frequency. The x-axis indicates variation in orientation and the y-axis indicates variation in frequency (Figure 4.10).

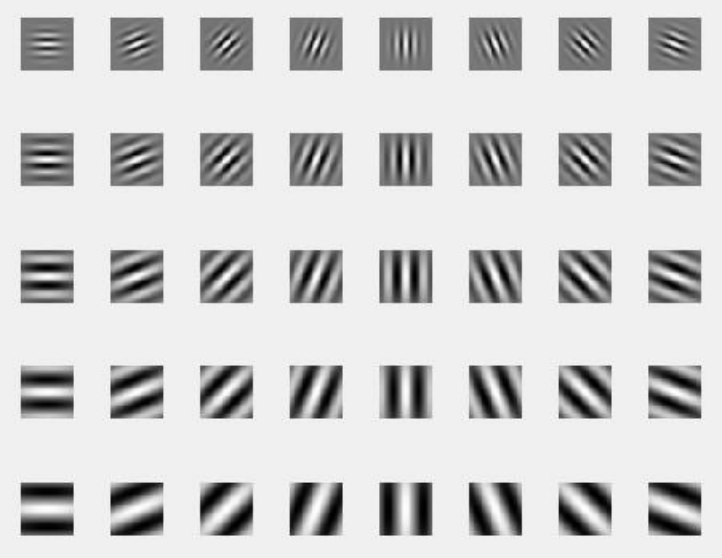
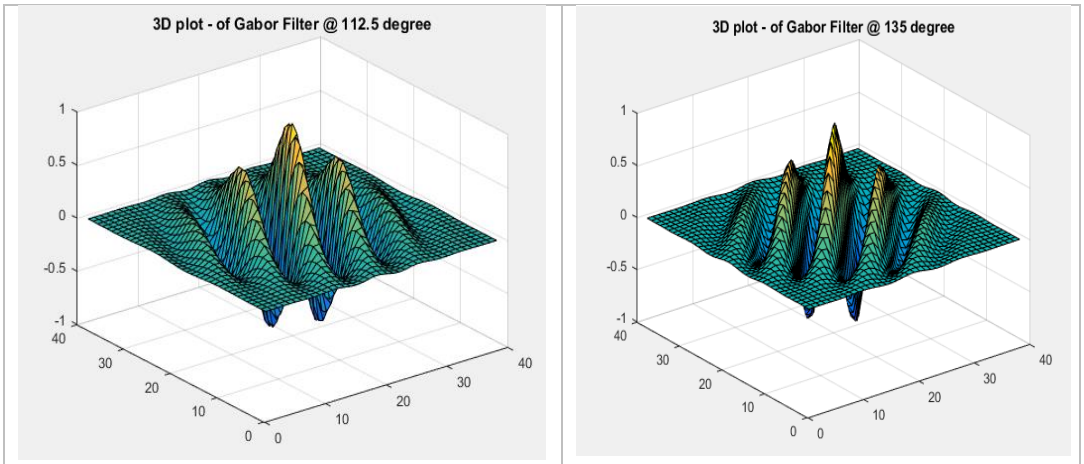


Figure 4.10. Gabor Kernels at different Frequency and Orientation

The 3D plot of the Gabor filter kernel for the frequency of 0.19 Hz is shown in Figure 4.11 below



a) Gabor Filter at 112.5 degree

b) Gabor Filter at 135 degree

Figure 4.11. 3D plots of Gabor Filter

The Gabor filter is applied to the local ridge of the fingerprint having the same frequency and oriented in the same direction with the filter to enhance the ridges oriented in the same direction while removing any other ridge and noise oriented differently. One property of the Gabor filter is that it is symmetric and it has a mean value of zero. This property is used to convert the Gabor enhanced image into binary image by setting the threshold value to zero. Thinning is then applied on the binary image to form a skeletonized version of the binary image.

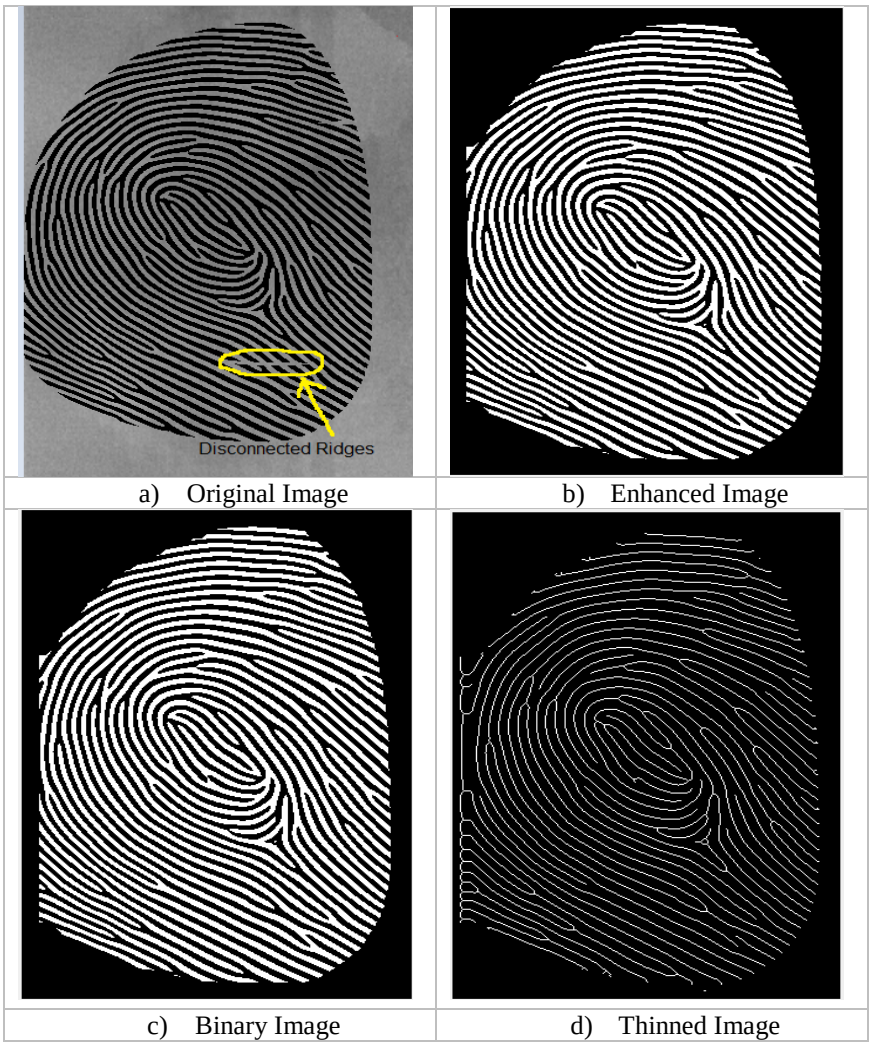
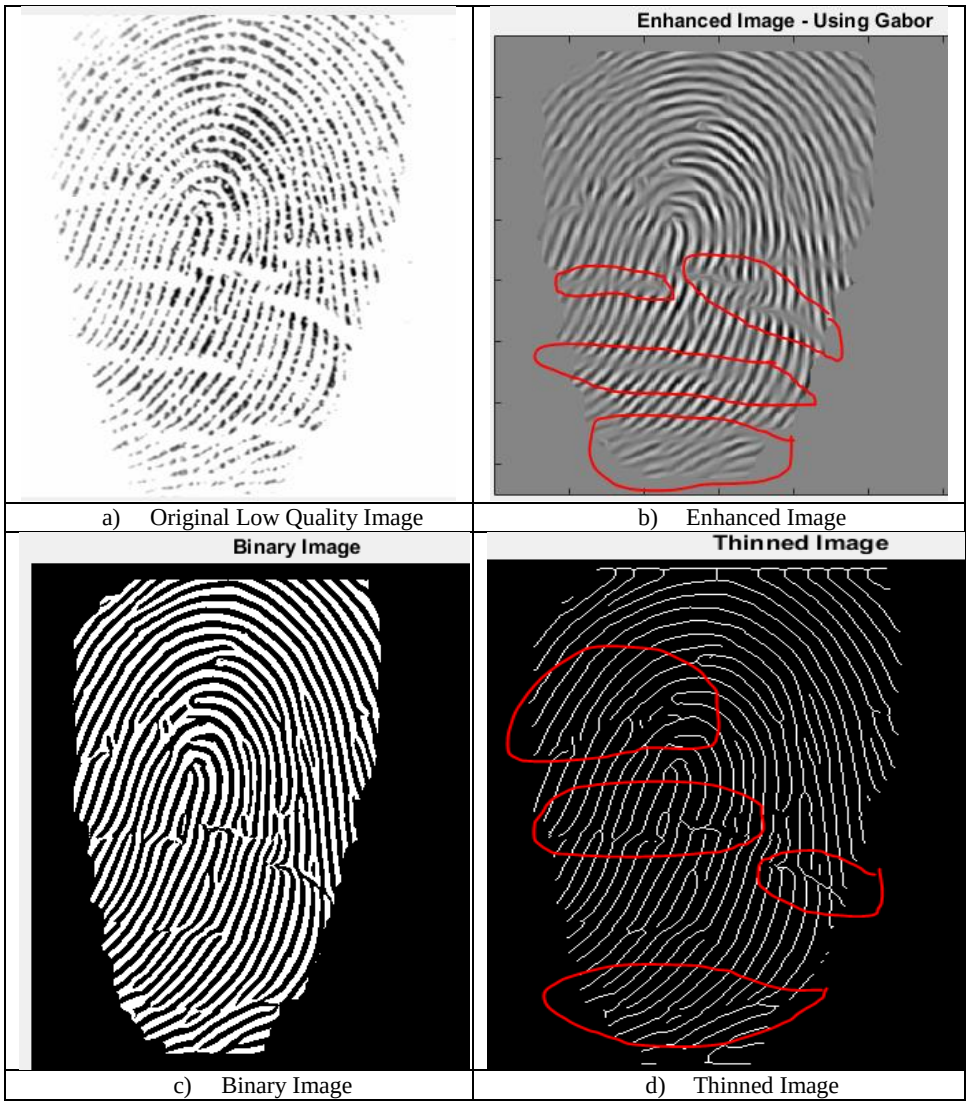


Figure 4.12. Gabor Filter Based Enhanced Images for High Quality Image

Figure 4.12 shows the enhanced image using Gabor filter for good quality image and gives almost the same result as FFT, whereas for low quality images, Gabor Filter slightly connects the significantly damaged ridges. However, after the thinning process, there are some falsely enhanced ridges like crossover and artifacts evolved due to the error happening in estimating the orientation and frequency from the original low quality image as shown in Figure 4.13. These errors affect the performance of the matching algorithm and also needs a post false minutiae removal processing.



a) Original Low Quality Image
b) Enhanced Image
c) Binary Image
d) Thinned Image

Figure 4.13. Gabor Filter Based Enhanced Images for Low Quality Image

4.4.5. FFT and Gabor based Enhancement

In this method, the Gabor Filter is modelled from the local ridge frequency and ridge orientation that are estimated from FFT based enhanced fingerprint image to get a better estimation.

As shown in Figure 4.14a, the damaged ridges result errors in the estimation of local ridge frequency and ridge orientation that are estimated directly from the poor quality image as indicted by circles. It can be observed however in Figure 4.14b that the orientation is smoothed when it is estimated from the FFT based enhanced image.

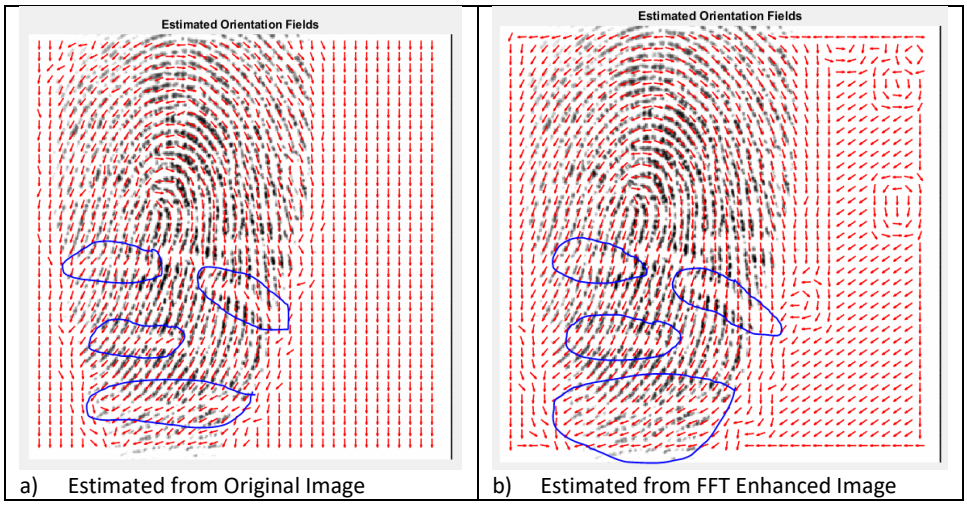


Figure 4.14. Estimated Ridge Orientations

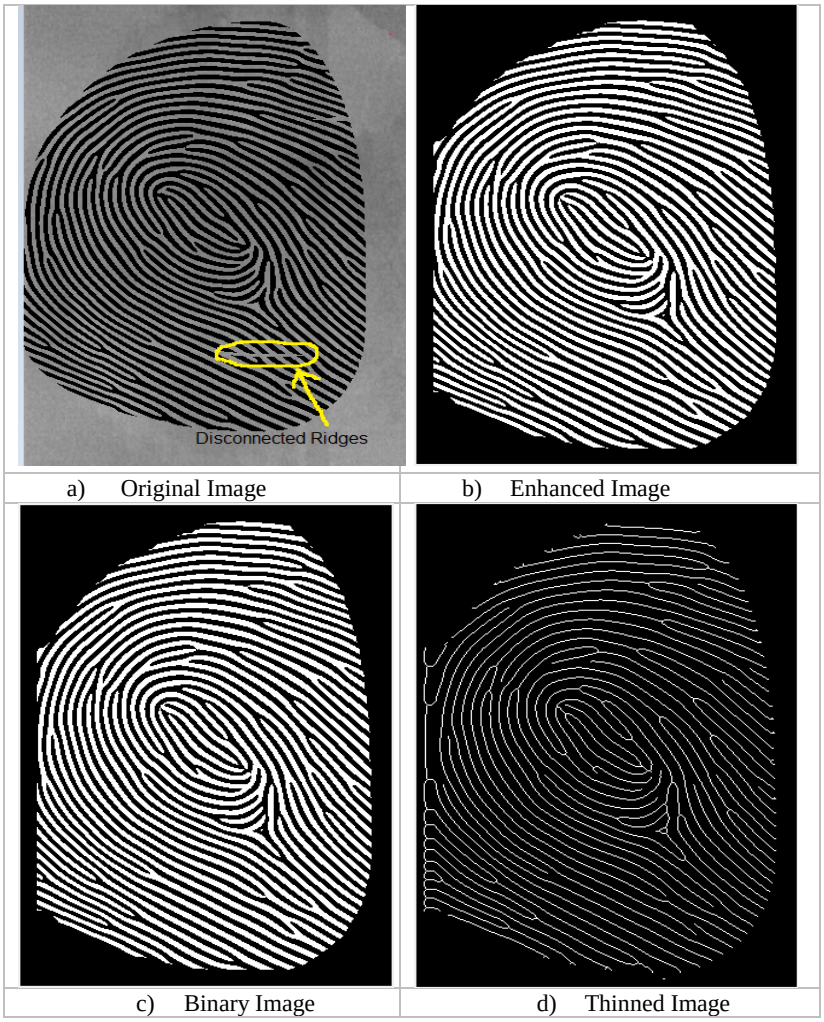
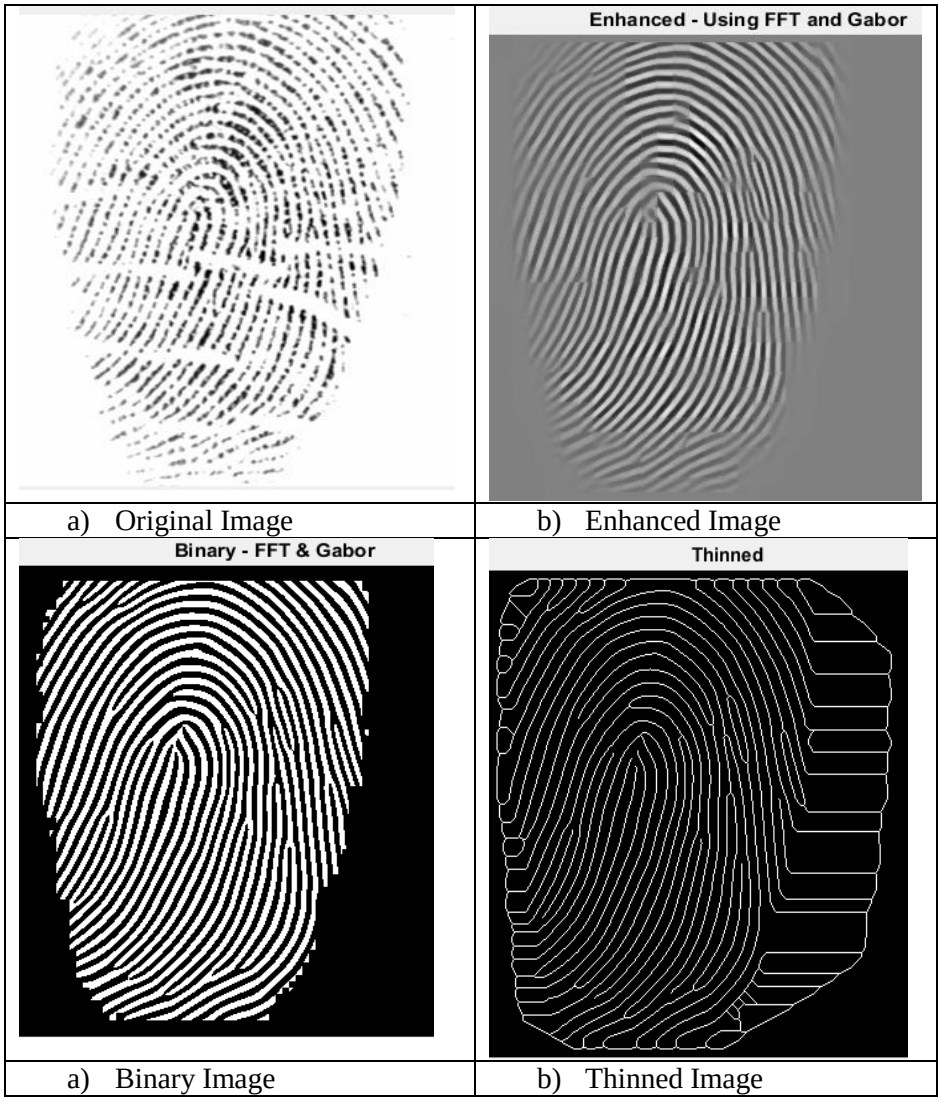


Figure 4.15. Gabor and FFT Based Enhanced Images for High Quality Image

It can be noted subjectively from Figure 4.15 that there is no significant difference in the quality of the enhanced version of the original image using FFT cascaded with Gabor Filter as it is compared with the enhanced images using FFT and Gabor methods. However, Figure 4.16 shows that, the FFT combined with Gabor filter gives a better result when it is applied on low quality image than the other methods discussed previously. The false features like crossover and artifacts are minimized because the ridge orientation and local ridge frequency are estimated from an FFT based enhanced image to get better estimation values.



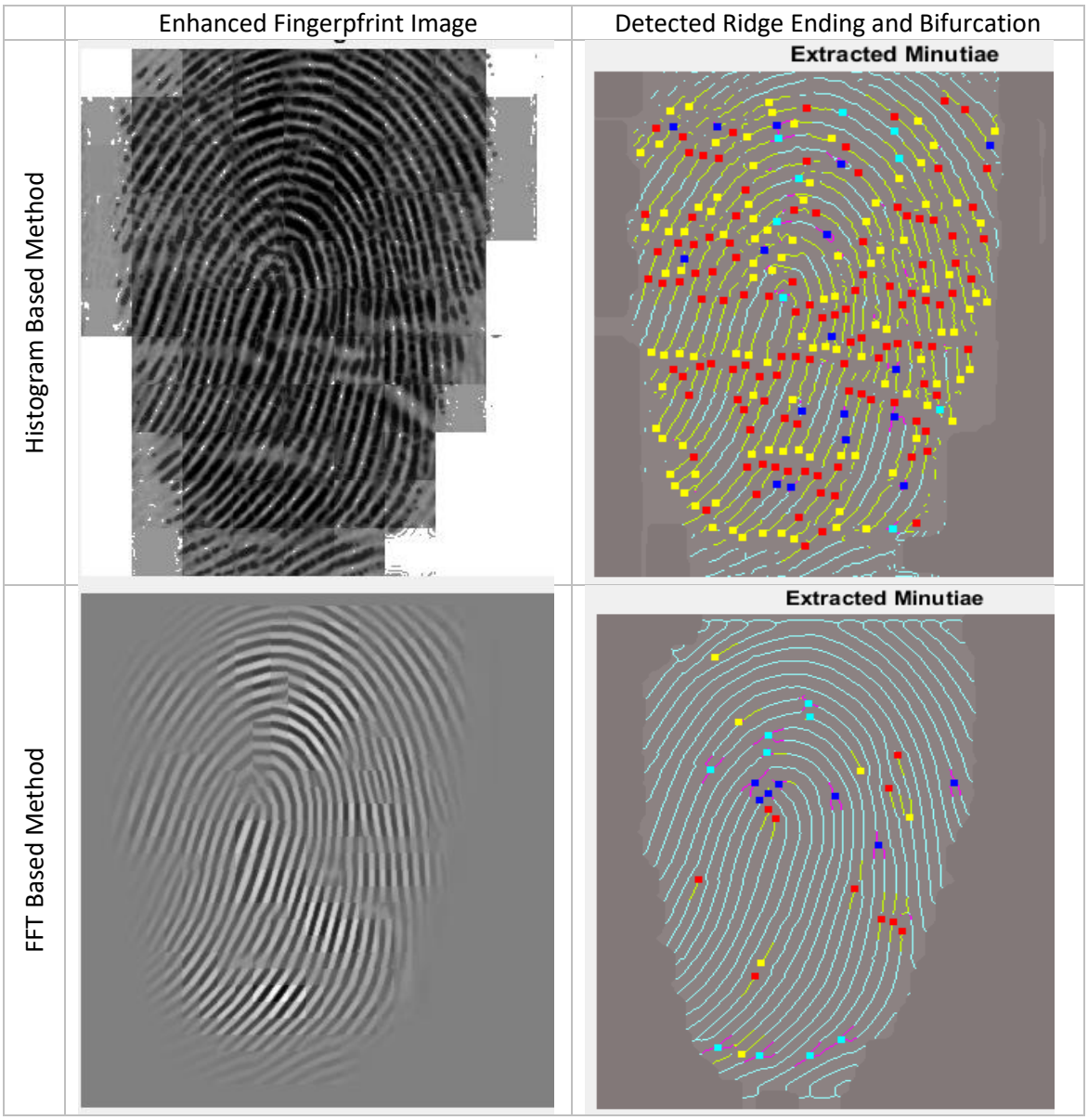
a) Original Image b) Enhanced Image

a) Binary Image b) Thinned Image

Figure 4.16. Gabor and FFT Based Enhanced Images for Low Quality Image

4.5. **Extracted Feature Weights**

The skeletonized image is used for extraction of unique features namely the minutiae of each individual. The crossing concept is used to extract the type, location and the angle of direction of the minutiae. Boundary elimination is applied during feature extraction to remove false features that exist at the border of the thinned image. The weight of the extracted features from a fingerprint is different based on the type of enhancement technique applied on it. The number of extracted features from a well enhanced image is much less than that of a poorly enhanced image as shown in Figure 4.17.



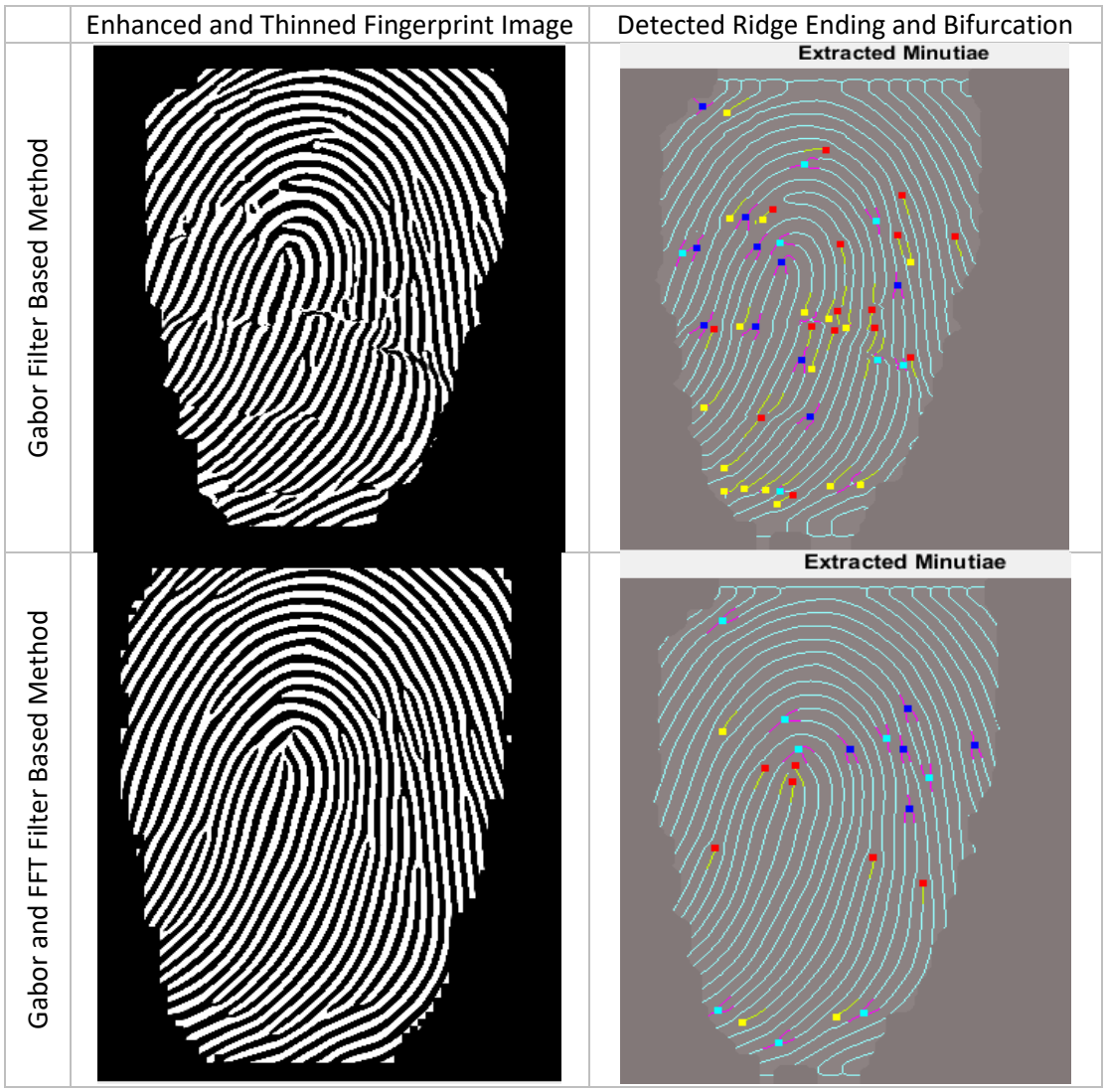


Figure 4.17. Comparison of Enhancement Techniques

Table 4.2 shows the number of features detected and average computational time for the enhancement techniques. The higher the number of detected features, the lower the quality of the image.

Table 4.2. Extracted Feature Weights for Enhancement Techniques on Different Images

	Number of Detected Features					Time
Enhancement Method						Average CT in Sec.
HE	62	141	233	213	155	0.95
FFT	49	21	38	32	27	2.04
Gabor	53	39	67	61	43	2.21
FFT and Gabor	48	20	42	34	21	5.85

4.6. **Performance Analysis of Enhancements**

4.6.1. Error Rates of FFT based Enhancement

The EER for FFT enhancement method is about 9.43% and occurs at the threshold value of 0.36 i.e. the system provides 90.57% accuracy if the threshold is set to 0.36. Zero FMR occurs at the threshold of 0.53 and the value of FNMR at this value of threshold is around 37%.

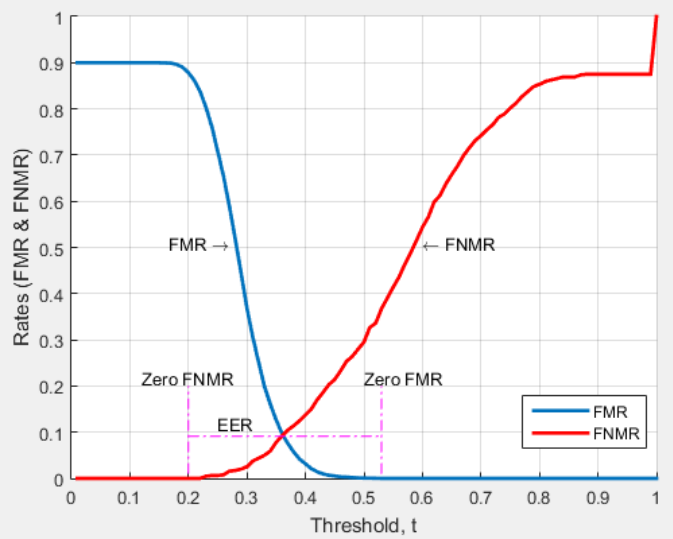


Figure 4.18. Threshold Vs FMR & FNMR for FFT based Enhancement

4.6.2. Error Rates of Gabor Filter based Enhancement

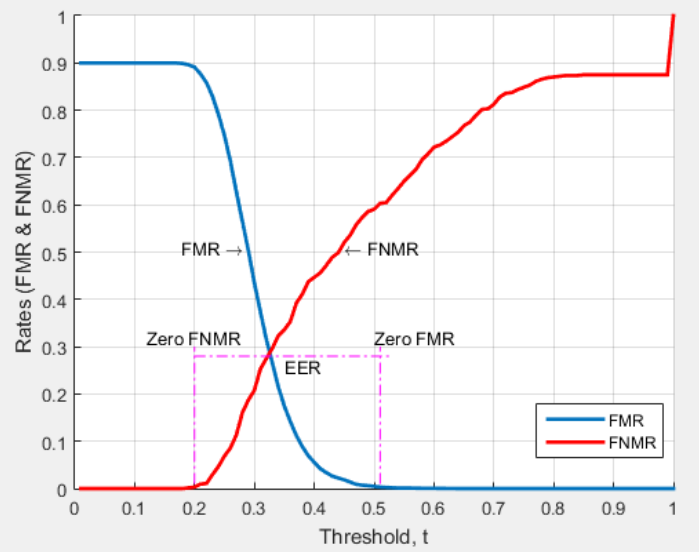


Figure 4.19. Threshold Vs FMR & FNMR for Gabor Filter based Enhancement

The EER for Gabor enhancement is around 27% and occurs at the threshold value of 0.32 i.e. the system provides 73% accuracy if the threshold is set to 0.32. Zero FMR occurs at the threshold of 0.5 and the value of FNMR at this value of threshold is around 60%.

4.6.3. Error Rates of FFT Cascaded with Gabor Filter based Enhancement

The EER of FFT cascaded with Gabor filter is 4.5% and occurs at the threshold value of 0.38 i.e. the system provides 95.5% accuracy if the threshold is set to 0.38. Zero FMR occurs at the threshold of 0.47 and the value of FNMR at this value of threshold is around 10%.

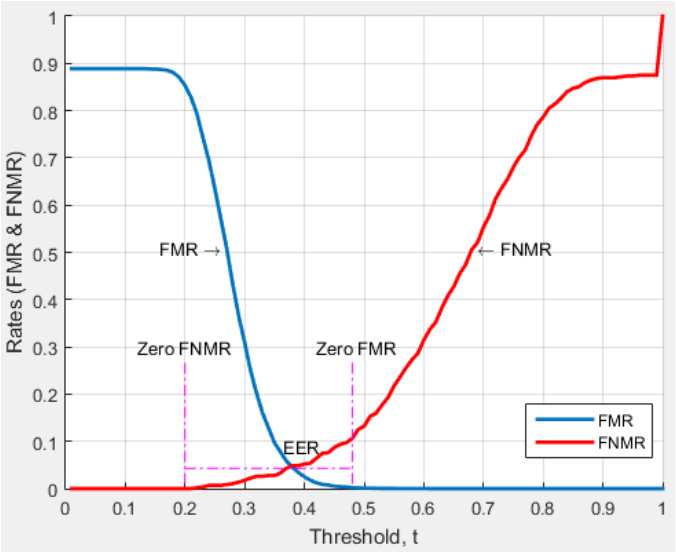


Figure 4.20. Threshold Vs FMR & FNMR for FFT cascaded with Gabor Filter

Table 4.3 describes a comparison between the enhancement methods with respect to the number of features detected, EER and computational time taken for enhancement, feature extraction, and matching stages. It shows that FFT cascaded with Gabor filter gives better result as it provides good image quality, extracts minimum number of features, and provides minimum EER, low computational time and high accuracy.

Table 4.3. Simulation Results and Comparison of Enhancement Techniques

Enhancement Technique	No of Features	EER	Enhancement CT (Sec)	Feature Extraction Time (Sec)	Matching Time (Sec)
HE	150	-	0.83	5.98	-
FFT	26	0.0943	1.25	2.02	1.75
Gabor Filter	57	0.270	1.74	1.28	10.24
FFT and Gabor	22	0.045	5.25	1.24	1.02

4.7. **Matching**

The similarity score must accurately describe how similar two fingerprints are, taking into account all of the relevant information obtained from its earlier stages, such as number of genuine minutiae pairs and how similar each pair is. The features extracted shown in Figure 4.21 and Figure 4.22 are taken from the same finger whereas the features shown in Figure 4.23 and Figure 4.24 are from other the same person. The threshold value for decision making for FFT cascaded with Gabor is taken from zero FMR value to be 0.47 in order to avoid false match totally.

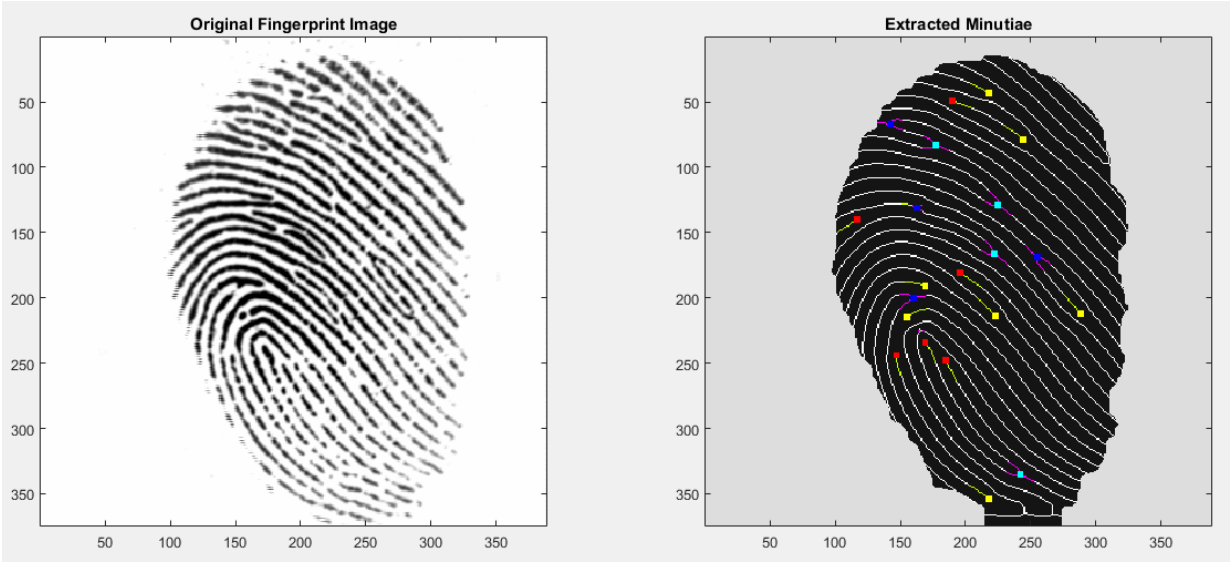


Figure 4.21. Extracted Features from Fingerprint 101_1

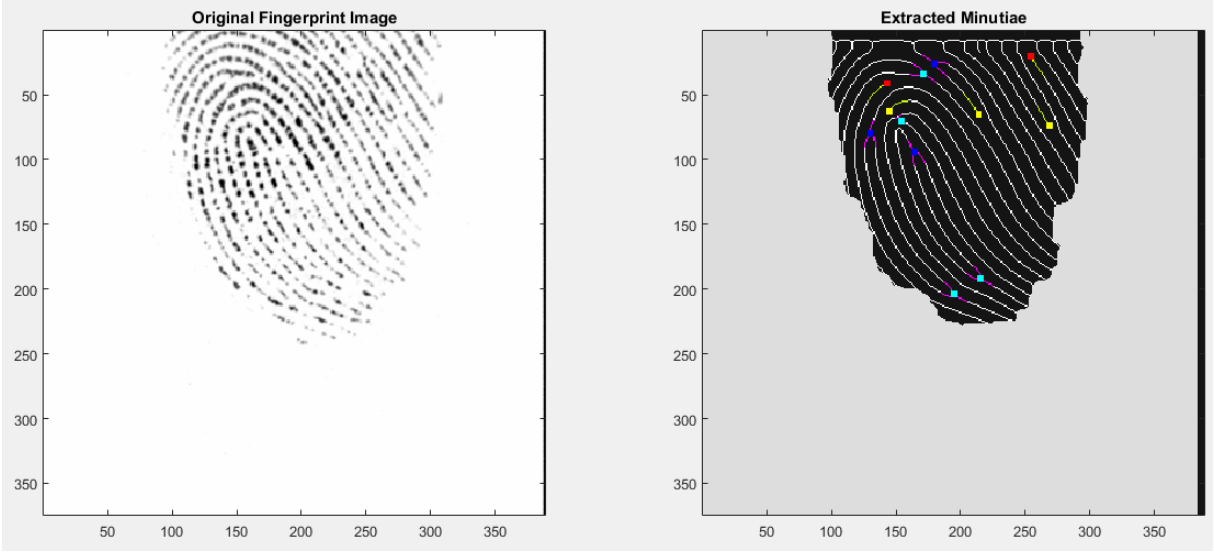


Figure 4.22. Extracted Features from Fingerprint 101_5

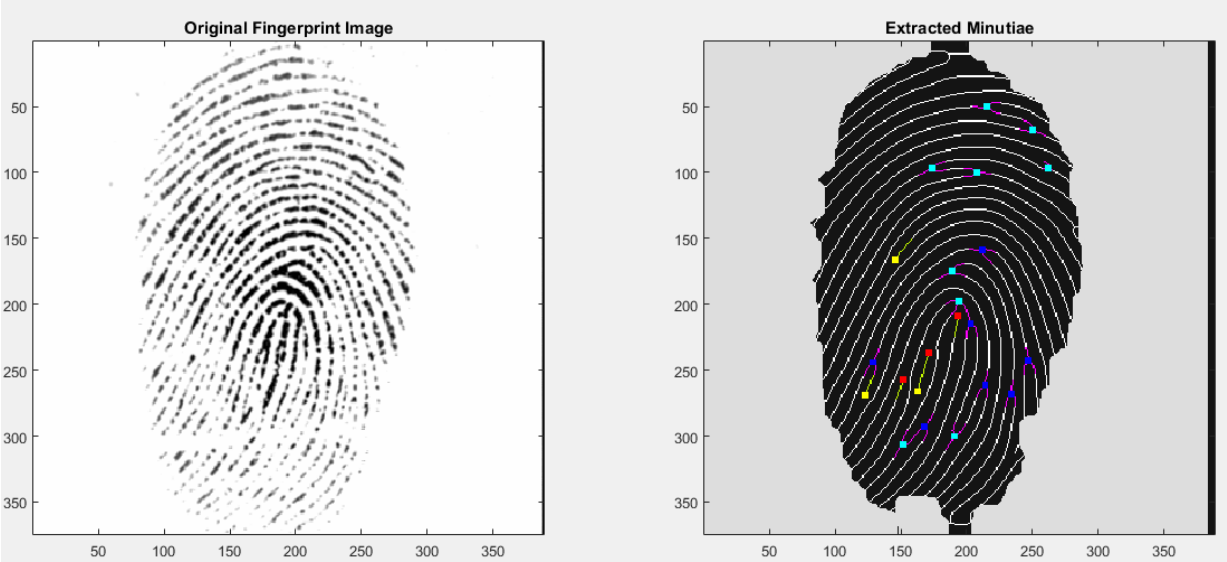


Figure 4.23. Extracted Features from Fingerprint 102_7

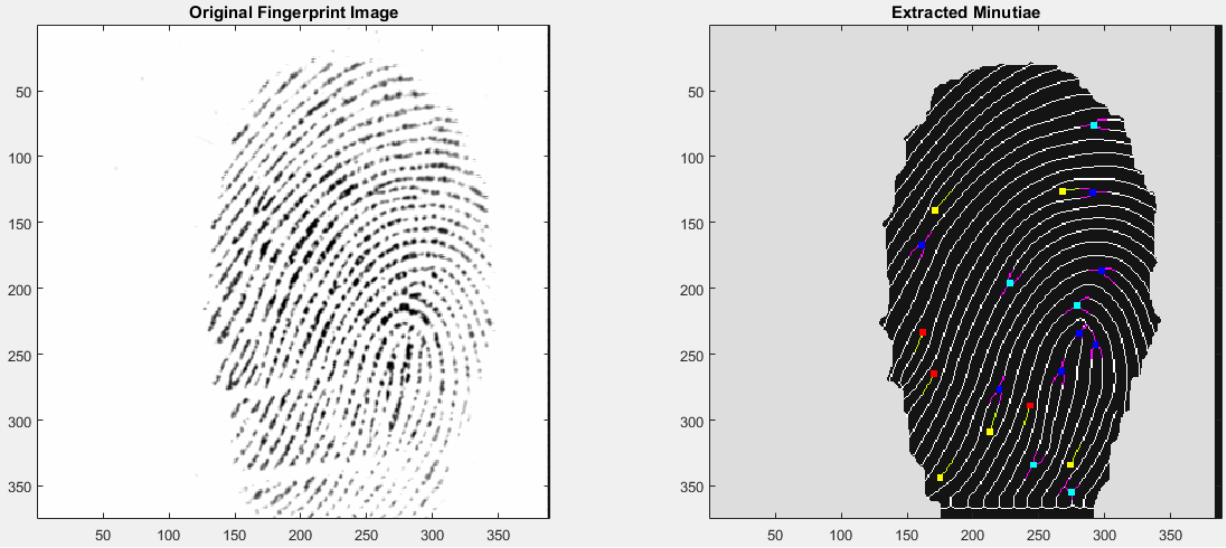
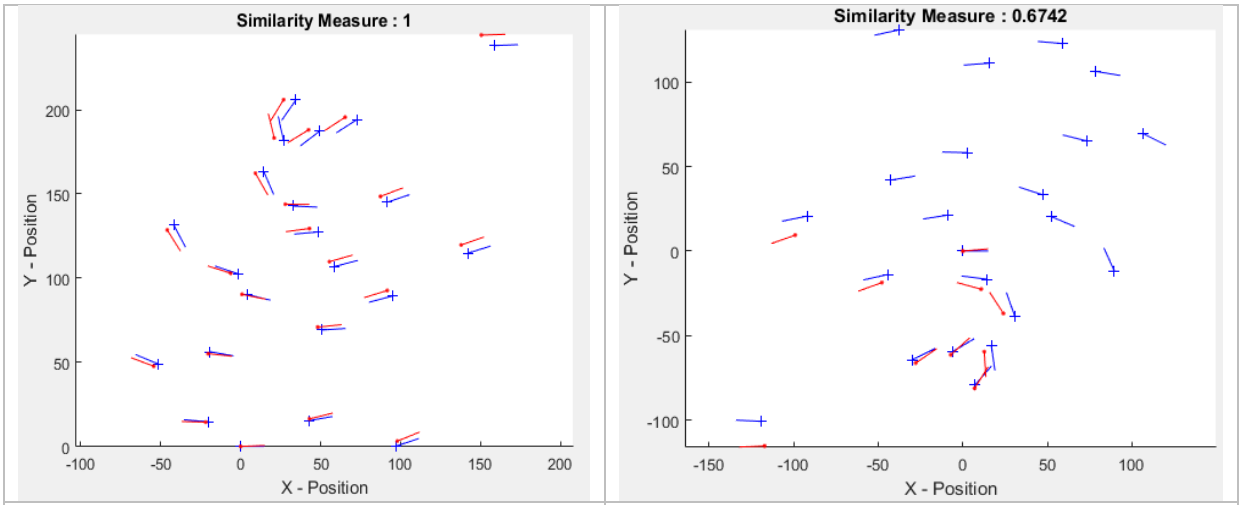


Figure 4.24. Extracted Features from Fingerprint 102_8

4.8. **Similarity Measure**

Similarity measure (or score) determines how two fingerprints are similar based on their extracted features. The extracted features are registered before matching stage takes place. The results of similarity score for the extracted features from 101_1 shown in Figure 4.21 with itself, with 101_5 shown in Figure 4.22, with 102_7 shown in Figure 4.23 and with 102_8 shown in Figure 4.24 are shown in Figure 4.25 and Figure 4.26.

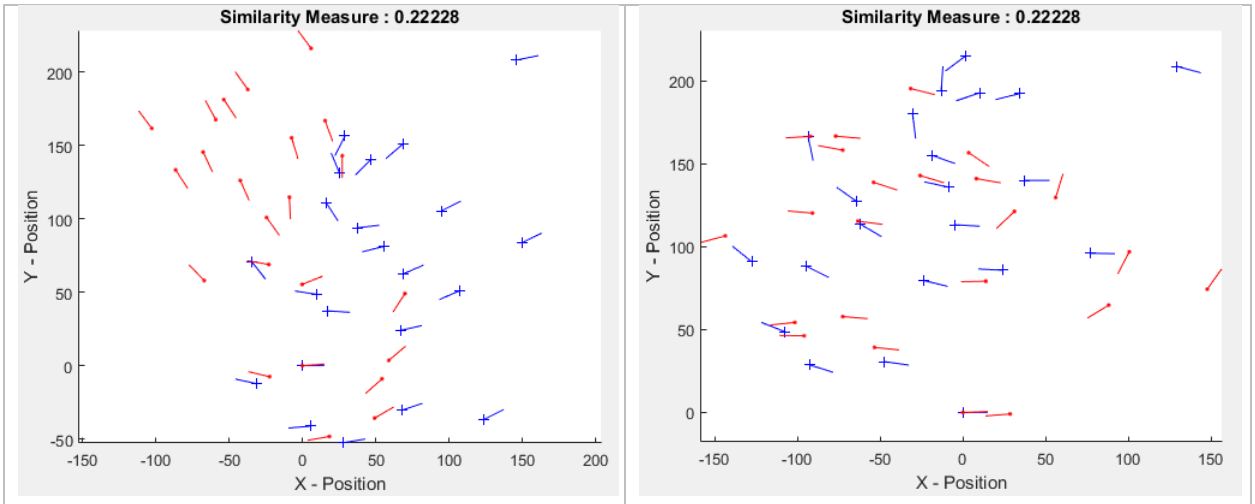
The arrow points on Figure 4.25 and Figure 4.26 indicate that the location and direction of the matched features just after guided Affine transformation is applied and have minimum geometric distance.



a) Similarity Score between 101_1 and 101_1

b) Similarity Score between 101_1 and 101_5

Figure 4.25. Similarity Measures between Fingerprints of the same Person



a) Similarity Score between 101_1 and 102_7

b) Similarity Score between 101_1 and 102_8

Figure 4.26. Similarity Measures between Fingerprints of different Persons

According to the theory of matching, the fingerprints from the same person gives high similarity score which is greater than decision threshold 0.47 whereas the fingerprints from different persons gives low similarity score which is below threshold 0.47. (See Figure 4.25 and Figure 4.26)

Chapter 5

Conclusions and Recommendations

5.1. Conclusions

In this thesis, a review of different fingerprint recognition systems and fingerprint image enhancement techniques namely HE, FFT and Gabor Filter is given. The minutiae extraction method is used to extract the features because the minutiae features have the ability to tolerate the variations in scale, shift, and rotation. However, the performance of the minutiae extraction highly depends on the image quality of the scanned fingerprint.

The crossing number concept is used to extract the minutiae feature points, namely the termination and bifurcation from the segmented skeletonized image with the attributes that make for every individual unique. The number of feature points for the same fingerprint image but enhanced with different enhancement technique is different. When the image is enhanced using poor enhancing technique, unwanted false features are evolved and the performance of the matching becomes poor. Similarity score is generated from these feature points for each fingerprints. The system errors namely the FMR, FNMR and EER are calculated from the similarity score.

Then the performance of HE, FFT, Gabor, and FFT cascaded with Gabor Filter enhancement techniques on the feature extraction stage and matching stage based on the computational time, FMR, FNMR and EER are compared.

Based on the performance analysis the FFT cascaded with Gabor filter gives better performance than of the HE based, Gabor Filter and FFT based when applied individually. This method of enhancement provided an EER of 0.045 at the threshold value of 0.38. This implies the system provides 95.5% accuracy on the decision making stage.

5.2. **Recommendation and Future Work**

The minutiae algorithm is an accurate feature extraction algorithm from a scanned fingerprints for AFRS. However, it highly depends on the quality of the fingerprint image that it is still time consuming especially in the enhancement stage. Therefore, it is better to scan the fingerprint image with high processing devices where the enhancement stage is embedded in them and the feature extraction will be applied directly to the scanned image. The performance of AFRS can also be increased by extracting the singular points and intra ridge detail features like sweat pores from the high quality scanned image. Finally, the system can be fooled using a cut fingerprint from a dead person. Hence, it is better to integrate a liveness detection system within the device of fingerprint image reader.

References

[1] Romulo Ferrer L. Carneiro, Jessyca Almeida Bessa, Jermana Lopes de Moraes, Edson Cavalcanti Neto, Auzuir Ripardo de Alexandria, "Techniques of Binarization, Thinning and Feature Extraction Applied to a Fingerprint System," *International Journal of Computer Applications,* vol. 103, pp. 1-8, October 2014.

[2] Pankaj Bhowmik, Kishore Bhowmik, at el., "Fingerprint Image Enhancement and its Feature Extraction for Recognition," *International Journal of Scientific and Technology Research Volume,* vol. 1, no. 2, pp. 117-121, 2012.

[3] Kulwinder Singh, Kiranbir Kaur, Ashok Sardana, "Fingerprint Feature Extraction," *InternatIonal Journal of Computer Science and Technology,* vol. 2, no. 3, pp. 237 - 240, September 2011.

[4] Davide Maltoni, Dario Maio, Anil K. Jain,Salil Prabhakar, Handbook of Fingerprint Recognition, 2 ed., Verlag,London: Springer, 2009, pp. 4-260.

[5] Pankaj Deshmukh , Siraj Pathan , Riyaz Pathan, "Image Enhancement Techniques for Fingerprint Identification," *International Journal of Scientific and Research Publications,* vol. 3, no. 3, pp. 5 - 9, March 2013.

[6] A. M. Bazen, "Fingerprint Identification, Feature Extraction, Matching and Database Search," Netherlands, August 19, 2002.

[7] Marius Tico,Eero Immonen, Pauli Ramo, Pauli Kuosmanen, and Jukka Saarinen, "Fingerprint Recognition using Wavelet Features," Tampere, Finland, 2001.

[8] Aneesha Karar, Prof.Amarjeet kaur at el, "Fingerperprint Enhancement and feature extraction.," *International Journal of Advanced Research in Computer Engineering & Technology,* vol. 4, no. 6, pp. 2621-2624, June 2015.

[9] T. Tang, "Fingerprint Recognition Using Wavelet Domain Features," in *International Conference on Natural Computation*, Chengdu, China, 2012.

[10] Kondreddi Gopi and J.T Pramod, "Fingerprint Recognition Using Gabor Filter And Frequency Domain Filtering," *Journal of Electronics and Communication Engineering,* vol. 2, no. 6, pp. 17-21, Oct 2012.

[11] Dr. Neeraj Bhargava, Dr. Ritu Bhargava, Manish Mathuria, Pooja Dixit, "Fingerprint Minutiae Matching using Region of Interest," *International Journal of Computer Trends and Technology,* vol. 4, no. 5, pp. 515-518, April 2013.

[12] A. Tukur, "Fingerprint Recognition and Matching using Matlab," *The International Journal Of Engineering And Science,* vol. 4, no. 12, pp. 1-6, 16 December 2015.

[13] Ravi. J, K. B. Raja, and Venugopal. K. R, "Fingerprint Recognition using Minutiae Score Matching," *International Journal of Engineering Science and Technology,* vol. 1, no. 2, pp. 35-42, December 2009.

[14] P. Namburu, "A Study of Fingerprint Image Enhancement and Minutiae Extraction Techniques," Rourkela, 2007.

[15] C. Vincenzo, S. Vitabile and M. Conti, "Biometric authentication overview: a fingerprint recognition sensor description," *International Journal of Biosensors & Bioelectronics,* vol. 2, no. 1, pp. 26-31, 2017.

[16] S. Chakraborty, "Fingerprint Enhancement by Directional Filtering," University of Texas at Arlington, December 2011.

[17] T. Sultan, "Fingerprint Identification by Using Wavelet Transform and Statistical Texture Measures," Mousl, May, 2015.

[18] R. Verma, "Wavelet Based Fingerprint Authentication System Review," *in Electrical and Electronics Engineering,* vol. 5, pp. 61-72, February 2016.

[19] C. B. e. al, "The FBI compression standard for digitized fingerprint images," *Proceedings of SPIE,* vol. 2847, pp. 344-355, Aug 1996.

[20] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu, "Fingerprint Verification System using Minutiae Extraction Technique," *World Academy of Science, Engineering and Technology,* pp. 497-502, 2008.

[21] C. Wu, "Advanced Feature Extraction Algorithms for Automatic Fingerprint Recognition Systems," New York, April, 2007.

[22] I. Moccagatta, M.Z. Coban and H.H. Chen, "Wavelet-based image coding: Comparison of MPEG-4 and JPEG-2000," in *Conference record of the thirty-third asilomar conference on Signals, Systems and Computers*, Oct. 1999.

[23] Lin Hong, Yifei Wan, and Anil Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," *IEEE Transactios on pattern Analysis and Machine Intelligence,* vol. 20, no. 8, pp. 777-789, August 1998.

[24] B. Bhanu and T. Xuejun, "Learned Templates for Feature Extraction in Fingerprint Images," in *Computer Vision and Pattern Recognition (CVPR)*, 2001.

[25] A. K. Jain, L. Hong, and B. R, "On-line fingerprint verification," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 19, no. 4, pp. 302-314, 1997.

[26] Rafael C.Gonzalez, Richard E.Woods and Steven L.Eddins, Digital Image Processing using MATLAB, Printice Hall, 2004, pp. 65-425.

[27] B. Bir and T. Xuejun, "Fingerprint indexing based on novel features of minutiae triplets," *Pattern Analysis and Machine Intelligence, IEEE Transactions,* vol. 5, no. 25, pp. 616-622, 2003.

[28] Iwasokun Gabriel Babatunde, Akinyokun Oluwole Charles, Alese Boniface Kayode and Olabode Olatubosun, "Fingerprint Image Enhancement: Thinning and Segmentation," *International Journal of Advanced Computer Science and Applications,* vol. 3, no. 1, pp. 15-24, 2012.

[29] R. Thai, "Fingerprint Image Enhancement and Minutiae Extraction," Australia, 2003.

[30] Asker M. Bazen and Sabih H. Gerez, "Segmentation of Fingerprint Images," *Workshop on Circuits, Systems and Signal Processing,* pp. 1-6, November 2001.

[31] Gabriel Babatunde and Oluwole Akinyokun, "Fingerprint Singular Point Detection Based on Modifed Poincare Index Method," *International Journal of Signal Processieng, Image Processing and Pattern Recognition,* vol. 7, no. 5, pp. 259-272, 2014.

[32] T.Romen Singh, Sudipta Roy, O.Imocha Singh, Tejmani Sinam and Kh.Manglem Singh, "A New Local Adaptive Thresholding Technique in Binarization," *International Journal of Computer Science,* vol. 2, no. 6, pp. 271-277, November 2011.

[33] Robert Fisher, Simon Perkins, Ashley Walker and Erik Wolfart, "Image Processing: Adaptive Thresholding," HIPR2, Oct 2000. [Online]. Available: https://homepages.inf.ed.ac.uk/rbf/HIPR2/adpthrsh.htm. [Accessed 21 April 2018].

[34] M F. Fahmy and M A. Thabet, "A Fingerprint Segmentation Technique Based on Morphological Processing," Assiut, Egypt, 2013.

[35] Asker M. Bazen and Sabih H. Gerez, "Systematic Methods for the Computation of the Directional Fileds and Singular Points of Fingerprints," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 27, no. 4, pp. 905-919, July 2002.

[36] D. Jacobs, "Image Gradients," Class Notes for CMSC, 2005.

[37] Shaikh Mohammed Sayeemuddin, Sima K Gonsai and Dharmesh Vandra, "Efficient Fingerprint Image Enhancement Algorithm Based on Gabor Filter," *International Journal of Research in Engineering and Technology,* vol. 3, no. 4, pp. 809-813, April 2014.

[38] Hany Hashem Ahmed, Hamdy M. Kelash, Maha Tolba and Mohamed Badawy, "Fingerprint Image Enhancement based on Threshold Fast Discrete Curvelet Transform and Gabor Filter," *International Journal of Computer Applications,* vol. 110, no. 3, pp. 33-41, January 2015.

[39] Mark S. Nixon and Alberto S.Aguado, Feature Extraction and Image Processing, 1 ed., Delhi: Replika Press Pvt Ltd, 2002, pp. 60-70.

[40] Indira Chakravarthy, Dr.VVSSS.Balaram and Dr.B.Eswara Reddy, "Overview of Fingerprint Image Enhancement and Minutiae Etraction," *International Journal of Computer Science and Information Technologies,* vol. 4 (1), pp. 5-9, 2013.

[41] Gehan A. Bahgat, A.H. Khalil, N.S. Abdel Kader and Samiha A. Mashali, "Fast and accurate algorithm for core point detection in Fingerprint Images," *Egyptian Informatics Journal,* vol. 1, no. 2, pp. 15-24, March 2013.

[42] Chih-Jen Lee and Sheng-De Wang, "Fingerprint Feature Extraction using Gabor Filters," *Electronics Letters,* vol. 35, no. 4, 18 Februray 1999.

[43] Qiang Tong and Jia-xiong Zhu, "Research of Improved Gabor Based on Fingerprint Enahnced Algorithm in Wavelet Domain," *Scientific Research Funded Projects by Sichuan Provincial Eduation,* pp. 17-18, 2012.

[44] L. Wieclaw, "A Minutaie Based Matching Algorithms in Fingerprint Recognition," *Journal of Medical Informatics and Technologies,* vol. 13, pp. 66-70, 2009.

[45] Joshua Abraham, Paul Kwan and Junbin Gao, "Fingerprint Matching using A Hybrid Shape and Orientation Descriptor," *State of the art in Biometrics,* pp. 25-55, 2011.

[46] Mela G. Abdul-Haleem, Loay E. George, Huda M. Al-Bayti, "Fingerprint Recognition Using Haar Wavelet Transform and Local Ridge Attributes Only," *in Advanced Research in Computer Science and Software Engineering,* vol. 4, no. 1, pp. 122-130, January 2014.