FINGERPRINT MATCHING USING ZERNIKE MOMENTS ON CONCENTRIC CIRCLES AROUND CORE POINT

By

Sadaf Ashraf
(2010-NUST-MS-PhD-CSE(E)-02)

Submitted to the Department of Computer Engineering in
fulfillment of the requirements for the degree of
Master of Science in **Computer Software Engineering**

Supervisor
Brig. Dr. Muhammad Younus Javed

COLLEGE OF ELECTRICAL & MECHANICAL ENGINEERING
NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY
2013

Declaration

I hereby declare that I have implemented this thesis completely on the basis of my personal efforts under the guidance and supervision of Dr. Muhammad Younus Javed. All the sources used in this thesis have been cited and the contents of this thesis are not plagiarized. No portion of the work presented in this thesis has been submitted in support of any application for any other degree of qualification to this or any other university or institute of learning.

_____

Sadaf Ashraf

Approval

It is certified that the content and form of the thesis entitled “Fingerprint Matching using Zernike Moments on Concentric Circles around Core Point” submitted by Sadaf Ashraf have been found satisfactory for the requirement of the degree.

Supervisor: **Brig. Dr. Muhammad Younus Javed**

Signature: _____

Date: _____

Committee Member: Dr. Umer Munir

Signature: _____

Date: _____

Committee Member: Dr. Arslan Shaukat

Signature: _____

Date: _____

Committee Member: Dr. Assia Khanum

Signature: _____

Date: _____

Abstract

Accurate and reliable automatic personal identification is critical in wide range of application domains such as National ID card, Electronic Commerce, ATMs etc. Biometrics which refer to automatic identification of a person based on his physiological or behavioral characteristics is inherently more reliable in differentiating an authorized person from an imposter, than traditional password and PIN number based methods. Among all the biometric techniques, fingerprint based authentication is mostly used because of its reliability, low cost and ease of integration.

Fingerprint indexing is an efficient technique that greatly improves the performance of Automated Fingerprint Identification Systems. Continuous fingerprint indexing method based on location, direction estimation and correlation of fingerprint singular points has been analyzed in detail. There have been many approaches introduced in the design of feature extraction. Based on orientation field, firstly, it is divided into blocks to compute the Poincare Index. Secondly, the blocks which may have singularities are detected in the block images.

For fingerprint matching, an approach based on localizing the matching regions has been proposed. The location of region of interest is determined using only the information related to core points based on feature vectors extracted for each fingerprint image by Zernike moment invariant. Zernike moment is selected as feature descriptor due to its robustness to image noise, geometrical invariants and orthogonal property.

Using the singular points, the area around the core point has been cropped into four concentric circles and Zernike moment is applied on each of them. To find out the matching difference among Zernike moment invariant feature, normalized Euclidean distance is calculated among the two corresponding Zernike moments invariant features, stored template and query fingerprint image.

This idea is applied on FVC 2002 Database which consists of 100 classes, each class having 4 training and 4 testing images. The parameters used to compute the performance are false acceptance rate and false rejection rate. A genuine match is done by matching a testing image of a

class to a training image of the same class, whereas for an imposter match is done by matching the testing image of a class to the training image of another class. To calculate the Equal Error rate Zernike moments orders were varied from 0 to 15. By increasing the moment order the EER started to deteriorate, but at order 13 and onwards the results started to converge and EER started to increase rather than decrease. So the best moment order selected for this approach was 12 which resulted in giving a minimum error rate of 16.59%. This results in a recognition rate of 83.41% of the proposed system.

Acknowledgment

Praise be to Almighty Allah for bestowing upon me strength and knowledge, to conclude this aspiration in time and to craft a useful contribution.

I would like to acknowledge all the people who have assisted me during my MS study in Computer Software Engineering at College of Electrical and Mechanical Engineering, National University of Sciences and Technology, Rawalpindi. I am most grateful to my supervisor, Brig. Dr. Muhammad Younus Javed, for his professional and personal advice, help and guidance. He has been very helpful and supportive. I am very fortunate to have him as an adviser. I would like to especially thank Dr. Umer Munir for his valuable advice, help and suggestions.

My sincere thanks go to my family for their never-fading love, care, understanding and encouragement. I could not have accomplished anything without their prayers and support.

Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Automatic Personal Identification

To move with the world, we need to get connected with it and for this electronic technology is being universally. As e-commerce, electronic banking and smart-cards are in common, they should be secured as well. So in this regard various databases are used to keep personal identification record. By personal identification it is meant to associate a person only to his/her identity. Identity of an individual plays a vital role in this electronic world, in which a simple question needs to be answered: "*Is the person authenticated or not, should he/she be allowed or not?".* Authentication of person is checked by millions of organization in government sector, electronic commerce, banks, health care etc. This automatic identification should be very reliable and accurate, as it is used extensively in different applications which include usage of passport, ATMs and mobile phones.

Traditionally, many types of automatic personal approaches are used, which are basically, token based and knowledge based [1]. In token based identification, a person is identified by any identity material that could be passport, driving license or ID card. The knowledge based technique is something in which a person's memory is used, that is usage of PIN numbers or passwords. Both techniques have some disadvantages, where PIN could be guessed by an imposter or token may be lost. Therefore these techniques are not considered very reliable and effective for personal identification. A very secure way to identify an individual is via a biometric device, which has no concern with memory or any material. As we all know a very common fact that every individual has unique fingerprints, so this could be one approach to differentiate a genuine fingerprint from an imposter one. In this thesis, the proposed system is focused on fingerprint-based biometric identification system.

1.2 Biometrics

Any device that is used to identify a distinct physiological and behavioral characteristic of an individual is known as biometric device. It has automatically the ability to differentiate between

an authenticated and unauthenticated person. An individual's physiological characteristics include his retina iris, fingerprint and face, etc. Whereas a person's behavioral characteristics lie in his gait, signature, keystroke dynamics etc. Verifying a person from these characteristics is more reliable than knowledge and token based techniques, because the physiological and behavioral characteristics are unique to every person [2, 3]. Using these features is more reliable because here the person's presence is necessary. However, some fraud elements even get successful in compromising these biometrics devices, and once they are hacked, they can't be replaced. This is one of the biggest drawbacks of biometric device identification. In this regard token based and knowledge based techniques are better, as they can be changed if hacked.

A basic block diagram of a biometric system is shown in Figure 1.1 [3]. An individual's fingerprint, face, retina, hand geometry, iris, facial thermo gram, signature, voice print, gait, hand vein, odor, ear, keystroke dynamics can be used as a biometrics devices . Among these all the most reliable is fingerprint verification systems. Hence it can be said that Biometrics provides security solution for individuals in this electronically connected world, and it is going to become a dominant personal identification in near future.

1.3 Biometrics Modes

A biometrics system is operated in two modes [4, 5].

(i) Mode 1: Verification

(ii) Mode 2: Identification

The mode of verification is decided, based on system requirement. The difference among both is as following:

1.3.1 Verification Mode

In the verification mode, the user enters his user name and presents his biometrics e.g. face or fingerprint as password. The biometrics system searches for the user name and if the user name is found in the database then the biometrics data (face or fingerprint) presented by the user is compared with the stored biometrics data. If the user is genuine person, then the biometrics system successfully matches the biometrics data. If the user is an imposter, then

the biometrics data is not matched. In this mode, only *one to one* matching is performed. This requires very less amount of time for matching as matcher is run only once.

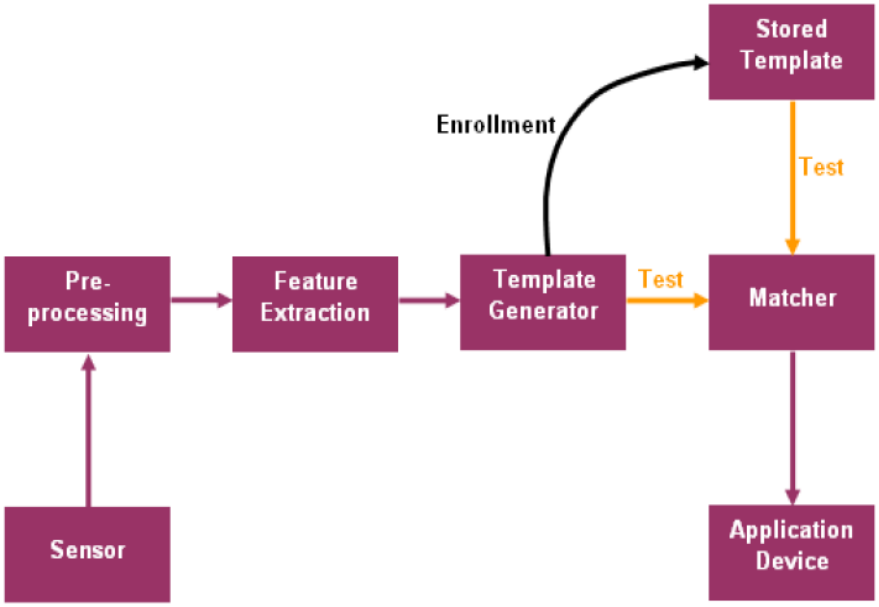

Figure 1.1: Block Diagram for a Biometric System

1.3.2 Identification Mode

In identification mode, user only presents his biometrics e.g. face, fingerprint, iris etc. The biometrics system compares the biometric data of the user with all the biometrics data stored in the database. In this case, if the biometrics data of the user matches with the stored data, then the user is successfully identified. In this mode, one to many matching is performed. Large amount of time is required for matching as the matcher compares the presented biometrics data of user with the biometrics data of all the users stored in the database until the match is found. The matching algorithms used in identification mode must be very efficient as thousands of matches have to be performed to identify a person.

1.4 Biometric Applications

Mostly biometrics is used in such applications where identification matters a lot. This technology has a bright future to be used in many civilians application also. The usage of biometric for civilians can be classified in two:

(i) Firstly, the usage can be in application such as banking, electronic commerce. Biometric will replace all the usage of token based and knowledge based technique.

(ii) Secondly, the applications which include person's immigration will be identified with biometric. This process has neither been handled by knowledge based nor by token base technique.

Usage of electronic device has made life easy but made security a crucial factor. Electronic banking which includes fund transfers, security for ATMs, cash checking, security of credit cards, online transactions, security of smart cards, and web access even needs security at high level. For this, biometric applications usage was very important and a reliable way to identify genuine users. Some applications which traditionally used physical access now use biometric technologies. The web access application used knowledge based technique, have also shifted to the biometrics with the passage of time and rapid growth of technology. As the technology is becoming more and more reliable the usage of biometrics is increasing very rapidly in coming years. Attendance, immigration at airports, Welfare payment, national ID card, voter registration and driving license are some of the biometric applications.

1.5 Biometric System

Pattern recognition systems are operated on fixed criteria. The biometric data is acquired from the person; its features of interest are extracted and are compared to the template in database. Depending on the application requirement, the biometric device works in a specific mode:

(i) In the verification mode, the user enters his user name and presents his biometrics e.g. face or fingerprint as password. The biometrics system searches for the user name and if the user name is found in the database then the biometrics data (face or fingerprint) presented by the user is compared with the stored biometrics data. If the user is genuine person, then the biometrics system successfully matches the biometrics data. If the user is an imposter, then the biometrics data is not matched. In this mode, only *one to one* matching is performed. This requires very less amount of time for matching as matcher is run only once. This is actually a positive test performed to match an identity.

(ii) In identification mode, user only presents his biometrics e.g. face, fingerprint, iris etc. The biometrics system compares the biometric data of the user with all the biometrics data stored in the database. In this case, if the biometrics data of the user matches with the stored data, then the user is successfully identified. In this mode, one to many matching is performed. Large amount of time is required for matching as the matcher compares the presented biometrics data of user with the biometrics data of all the users stored in the database until the match is found. The matching algorithms used in identification mode should be very efficient as thousands of matches have to be performed to identify a person. This mode is used to perform the negative test. The purpose of this test is to keep a check and balance of the record of a single user; so that a single user doesn't use multiple identities. In some case negative test are more important to perform than positive ones, and for his purpose biometric are a good approach. Positive test are mostly done by token and knowledge based techniques.

1.6 Biometric Technologies

Multiple biometric technologies exist and are used in a variety of applications. All biometric devices have their pros and cons and selection of that technology depends on the usage of that application. No biometric device is complete to fulfill all security measures, and in other words no biometric device is flawless. The match of the biometric device with the application depends a lot on the level of security. Commonly used biometric technologies are briefly discussed as following [6]:

1.6.1 Face

Face is a basic identity of a person; everyone has a unique facial expression. Identical twins even have minor differences. Recognition of person by face is a non-interfering method, and these images are the most commonly used biometric characteristic of a person to identify. Recognition of face is one of the most detailed topic on which researched have proposed many good ideas. Face recognition research is running from static controlled identification to dynamic. Usually the context used for personal identification, is through static and controlled full frontal position of the face. By static recognition, it is meant that the facial image is still and the frontal image of the face processed. By controlled, it is meant that during the image acquisition process the background intensity and the distance between acquisition device and the face is fixed. In such a controlled and static situation, segmentation and the processing of the image become easier and simpler. For the last 30 years, great efforts have been devoted to face recognition systems. In the early 1970's, face recognition was only based on fixed distance measurable techniques, that was to measure the difference from eyes to eyebrows, eyes to nose, nose to lips, and so on. As the resources were not sufficient, only a selected number of tests were performed to compute the results and end with a conclusion. In late 1980's and early 1990's, a rebirth to face recognition techniques evolved, efforts to attribute based techniques continued and resulted in new techniques including linear discriminant analysis (LDA), principal component analysis (PCA), singular value decomposition (SVD), local feature analysis and a range of neural network based techniques. An impressive performance was observed in the system using these techniques.

Although humans depend heavily on facial images and attributes to identify individuals, it is widely known that humans utilize a large amount of contextual information in performing face recognition. Without the contextual information, it is questionable whether the face itself is sufficiently effective to make a personal identification with high level of confidence. For example, in context-less image of face in Figure 1.2, it will be very difficult for both humans and machine vision systems to conclude that they are all of same person. Some approaches used to recognize face were either from *(i)* the placement of facial attributes; eyebrows, eyes, nose and lips or *(ii)* the complete analysis of face image that is represented as a weighted combination.

Figure 1.2: Same person with Multiple Personalities
(The New York Times Magazine, September 1, 1996/section 6, pages 48-49)

As discussed, the background illumination and resolution of the image matter a lot for the static verification. For this sometimes restrictions are imposed on the image and background style, but it too is not possible for some application. So for a face biometric that works well in all aspects of systems it should have the following property:

(i) Detection of face in image.
(ii) If face is detected, then detect how many face are there (one or more than one).
(iii) Use a general viewpoint (any pose) to recognize the face.

1.6.2 Fingerprint

Some lines on a finger, in furrows and ridges shape form a fingerprint, as shown in Figure 1.3. These lines are actually build-upon a human finger edge. In the first seven months of a human development, its formation is determined. Biologically fingerprints are 100% unique for each person. This characteristic has been used by humans from centuries to recognize an individual [7]. In fact, this characteristic of recognizing a person is so common that often people use biometrics as synonym of fingerprint recognition.

Fingerprints of even identical twins [8] are not even same and even the five fingers of each person doesn't have same prints on their finger [7]. Today, this technology is so advanced and common that every security measure uses this characteristic. Even the laptops are protected in

this. When biometrics is ordered in a bulk, still they cost $20, which shows its importance in our electronic society. The reliability of the fingerprint recognition systems used currently is good enough for small-medium systems, which include few hundred users. Additional information is required when users increase from hundreds to millions and system size from medium to large. Fingerprint recognition system also has some drawbacks: large computational effort is required, whether working in identification mode or verification mode. Similarly the areas where small fraction of fingerprint is used, biometrics won't be that suitable. Number of cuts and bruises on an individual finger changes every day, making recognition false in some cases.

Figure 1.3: Fingerprint Image

1.6.3 Iris

An Iris, as shown in Figure 1.4, is defined in its initial stages of embryonic mesoderm. The annular region of the eye, surrounded by pupil, is known an iris of a human eye. The texture of iris is formed into the early stages and stabilizes in first two years of life and is unique for each individual and never changes.

One of the most secured biometric characteristics is iris, as it cannot be changed even from surgery. It has no connection with the external environment. This characteristic can't be copied by any imposter using contact lens or through a surgery. The iris texture carries very distinctive information. The accuracy and speed of this biometric is very reliable and authenticated. Even the iris of twins doesn't match to each other, so this biometric is reliable for millions of user and for large systems. The iris systems are usually used where high

security is required; because of its expensive hardware it is not affordable by every small organization. In the current technological advanced environment it has become a very user friendly application.

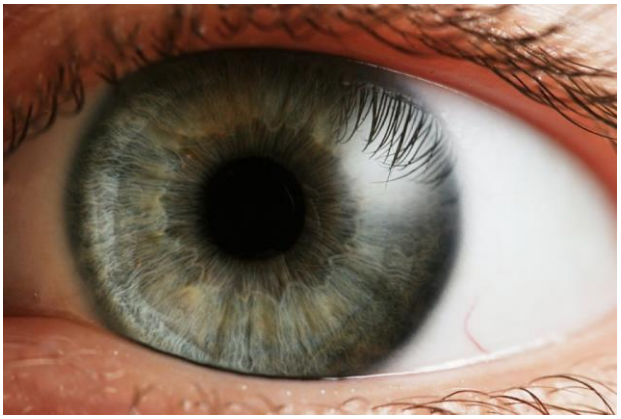

Figure 1.4: Iris Image

1.6.4 Facial, Hand and Hand Vein Infrared Thermogram

Heat radiation from a human body is another unique feature used as biometrics. The pattern of this radiation is different for every human body. This feature of human body is captured via infrared camera, just like a visible photograph. This biometric system does not require physical's contact, but in uncontrolled environments image acquisition becomes a bit challenging. Environment such as where heat is also an external factor, produced due to heaters, can be a difficult situation to detect a human identity. Another technology using infrared is by scanning the hand vein image of the person. These infrared sensors and thermograms devices are expensive, so its usage is limited.

1.6.5 Deoxyribo Nucleic Acid (DNA)

A generic code in every human body is known as Deoxyribo Nucleic Acid (DNA). As shown in Figure 1.5, it is a body code for one's individuality (one dimensional), but this code is identical for twins. It is still used in many forensic applications for individual recognition, but its usage is not very common. The reason lies in the following three pints:

(i) Stealing a piece of DNA sample is easier and can be used to access any personal or secured data.

(ii) This process is a real time recognition process, involves a lot of expert skills and the usage is even not very friendly.

(iii) Using DNA samples of an individual leaks its privacy as well. A person having a certain disease can be diagnosed from DNA sample of that person, which may result in discrimination for a person having any disease.

Figure 1.5: DNA Image

1.6.6 EAR

Ear shape can also be taken into consideration for identifying one's identity. Research says that the ear structure and shape is unique of an individual. Structure of cartilaginous tissues in pinna is distinctive; the measuring the distance among prominent points of the pinna structure can help identify a person. But this approach is not very reliable and authenticated, so not used commonly. A structure of ear image is shown in Figure 1.6.

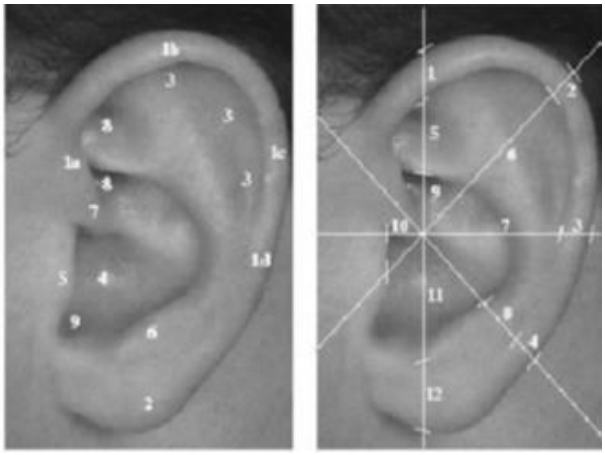

Figure 1.6: Ear Image

1.6.7 Gait

Walking style of a human being, as shown in Figure 1.7, is known as Gait. The device used to identify the uniqueness is called spatio-temporal biometric. This feature is not supposed to be very distinctive with each other, and can only be used where security is a low priority. Gait is known to be a behavioral biometric, and will keep on changing due to variation in body weight, or any major injury involving joints. This biometric uses video sequence footage to observe a person walk at different movements of the joint, for this a person needs o be observed for a long time. Hence used very rarely as it is a computationally expensive biometric technology.

1.6.8 Odor

A unique smell of an individual is also a good approach to identify a person, but unfortunately computers and automated systems do not smell as human do. Some research has been conducted in this area so far but still as people's distinction cannot be done reliably by odor. This unreliability is due to perfumes or deodorants smells or any smell due to chemical composition in environment.

Figure 1.7: Gait Image

1.6.9 Hand and Finger Geometry

Another behavioral biometric is known as hand and finger geometry recognition systems. This is based on different measurement of human hand, which includes size, shape, length, width, and difference between the fingers. Figure 1.8 shows that this biometric is an easy and simple technique but again is not very reliable as others. This technology cannot be used for thousands of user identifications. Its reliability is less, not due to any fault in technology but due to some facts. The hand and finger geometry keeps on changing as a person grows and its identification can be false by wearing a jewelry item or a glove in hand.

The technology has proved some good results by only measuring the geometry of some fingers (index and middle) not the complete hand. The devices used for this technology is too

big in size, but as it is just used for finger geometry the size has shrunk but not that small as other biometrics.

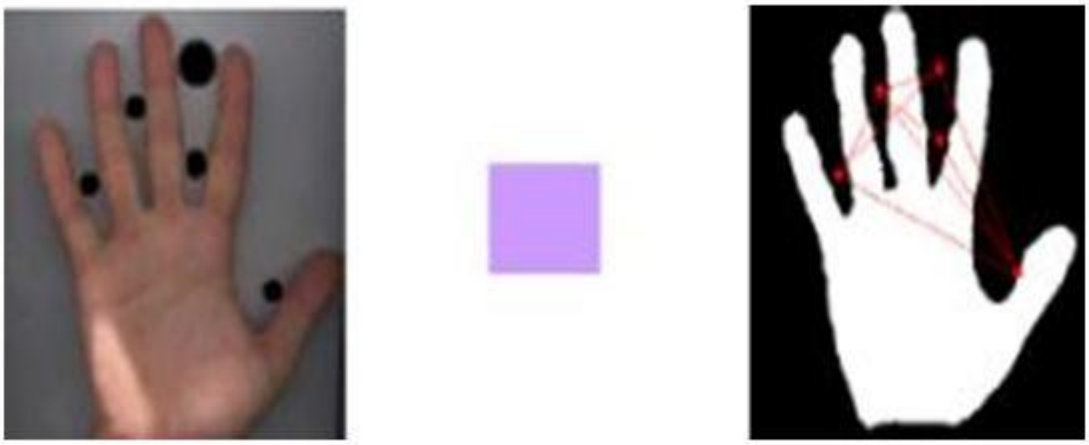

Figure 1.8: Hand and Finger Geometry Image

1.6.10 Keystroke

According to the imagination of some physiologists, it has been observed that each person types on keyboard in a different style. This behavioral characteristic computed as biometric is not expected to be very unique but gives enough information to distinguish a person's identity. Keystroke is a dynamic behavioral biometric, it is often observed that the keystroke style varies from person to person. A person is monitored as he is typing and thereby identified. A keystroke style is shown below in Figure 1.9.

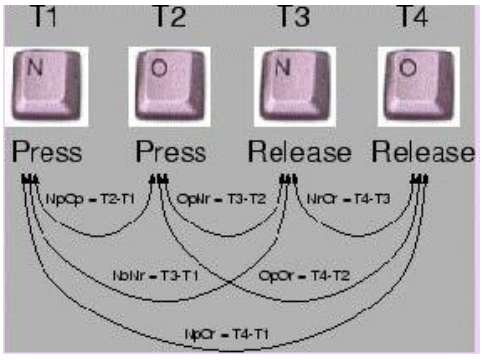

Figure 1.9: keystroke Style Image

1.6.11 Palm print

Human palm is another feature that consists of ridges and valleys, as shown in Figure 1.10. This biometric is bigger in size than a fingerprint biometric and obviously provides more authenticated results. Human palm also is more reliable because it can also identify by taking hand and finger geometry in consideration. The scanners used for this biometric are bulkier and expensive. The more the resolution of scanner would be, the better results would be observed but at the same time, it would be more expensive.

Primary lines and wrinkles of a hand can also be detected with a low resolution scanner. Usage of high resolution scanner considers all features and becomes a perfect biometric device. The features that could be used for verification in a palm can be, ridges and valleys features, singular points, hand and finger geometry, wrinkles and principal lines.

Figure 1.10: Palmprint Image

1.6.12 Retinal Scan

The retinal veins in human eyes, shown in Figure 1.11, form very stable and repeatable patterns and these are called retinal patterns. These retinal patterns are unique to each individual. As it is not easy to change a retina, so its scan is proved to be most authenticated biometric technology. The device used to capture the image of the retinal patterns is expensive; moreover, acquiring the image of the retina is a difficult task also. The image

acquisition is a laborious task and so its usage adversely affects the public acceptability for this technology.

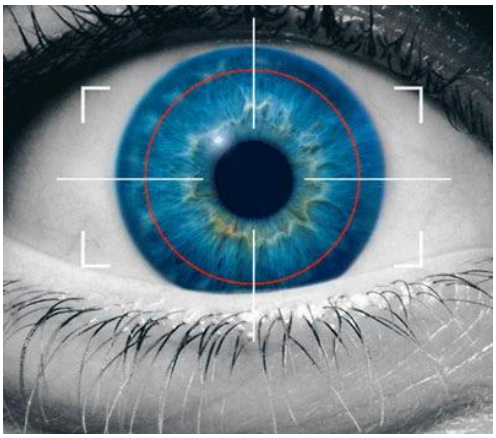

Figure 1.11: Retinal Scan Image

1.6.13 Signature

Signature is a kind of biometric that can be used to make a personal identification. Every individual has its own writing style so the way he/she signs will be different as well. Signature shown in Figure 1.12 is a very common way to verify a person's identity and has also been used in every legal and commercial process. Signatures of an individual change with the passage of time, but whenever it is changed, the authorities are informed about it. Some signature are too unique and difficult to be copied by professionals but still can be copied with lots of practice. This system of verification is the easiest but again has some security issue of being copied, to fool the human eye or signature matching system.

Figure 1.12: Signature Image

1.6.14 Voice

The vocal characteristics of humans are totally determined by the mouth, vocal tract, nasal cavities, and other vocalizations process of human body. These are unique to each individual and are known as voice prints. Voice verification is either text independent or text dependent. A text independent system is one in which the individuals speaks any phrase of their own choice. A text-dependent voice recognition system is based on specific phrase that an individual utters. The text dependent system is very easy to design, but text independent system is more reliable to protect against fraud.

Text independent system is more complicated to design, so usually the text dependent system is used by organization. But this technology cannot be used for thousands of people's identification. Voice recognition is not reliable even in the sense that voice might change due to age factor or any vocal disease. Another disadvantage of voice based recognition system can be the influence of the surrounding factors which might not authenticate the person. A voice verification system is shown in Figure 1.13.

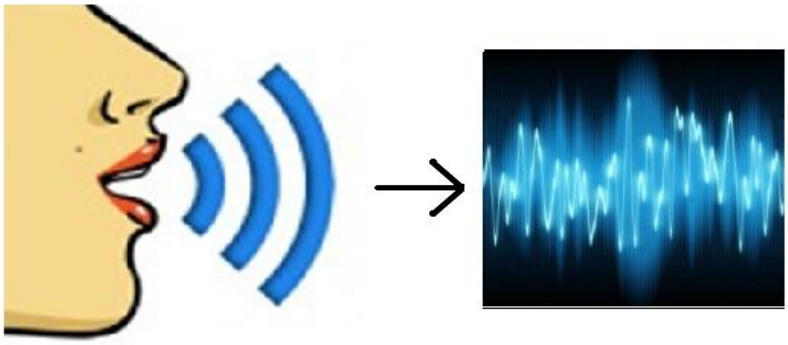

Figure 1.13: Voice Image

1.7 Comparison of Biometric Technologies

Based on seven different factors, a comparison of all biometric technologies is given in Table 1.1. Selection of biometric technology totally depends on the application requirements. Each of the biometric technique discussed above has its own advantages and disadvantages [6].

No technology can fit in all application domains. From the details of technologies so far discussed, it can be concluded that fingerprint and iris technology proves to be the best. Whereas in some applications biometrics are not applicable (i.e. tele-banking).

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

Table 1.1: Results for different Biometric technologies (H=High, M=Medium, L=Low)

1.8 Thesis Objective

The main objective of this thesis is to study the fingerprint matching techniques and propose new fingerprint matching framework in order to enhance the matching performance of fingerprint identification systems.

1.9 Research Findings

The fingerprint is first normalized and then its direction field is computed. The core point computed with the Poincare index is cropped in a unique way. The region of interest has been shrunk in smaller concentric circles and then using the geometric moment, the fingerprint is matched. This technique utilizes the Zernike moments features to compare images in matching

stage. The Zernike moments are rotation invariant and this property is utilized to handle rotation in a fingerprint image. Experimental results show that Zernike moment based fingerprint matching technique outperforms the traditional matching techniques in computation time.

1.10 Thesis Outline

The rest of this thesis is organized as follows: Chapter 2 discusses the fingerprint identification algorithms and sets up the background for remaining chapters. Chapter 3 computes the direction field and the region of interest. Chapter 4 discusses the fingerprint matching algorithm based on Zernike moments. In Chapter 5, experimental results of fingerprint matching are discussed. The thesis ends in Chapter 6, where conclusions and future work are presented.

1.11 Summary

In the chapter, biometrics has been discussed in details. Biometric have two modes; verification and identification. The usage of biometric has replaced the token and knowledge based technique used for security. Multiple biometric technologies exist and are used in a variety of application. All biometrics application has their advantages and disadvantages. No biometric device is complete to fulfill all security measures. Fingerprint and Iris technology is the most reliable technology to use for security. The iris technology is not mostly used because of its complexities whereas the fingerprint biometric is economical and has no complications.

Chapter 2: Fingerprint Identification

2.1 Introduction

Utilizing the underside image of individual's finger, the process of verifying a person can be performed very effectively. This image consists of curve lines, which are totally unique from each other. Even a person's five fingers do not have same pattern of curve. The curves with light shade are known as ridges, whereas the dark shaded curves are known as valleys. A fingerprint is based on these two types of curves. Figure 2.1 shows these curves very clearly. Note that a fingerprint image is actually a reverse of the original print on a person's finger. That is, the ridges are represented as the dark-shaded areas, where the valleys are the light-shaded areas. The flow of these ridges and valleys form up a unique fingerprint pattern, and creating an automated process that matches fingerprints based on this pattern is the objective of fingerprint identification.

Although the notion of identifying a person through his fingerprint has been in practice since the 16^{th} century, the first scientific study of fingerprints was carried out in the late 19th century. The research that was carried out at that time formed the foundation for which modern fingerprint authentication systems operate. The research was primarily carried out by two individuals, E. Henry and F. Galton [9, 10] towards the end of the nineteenth century. Each researcher investigated different facets of fingerprint identification, and both of their work has provided a valuable contribution to the area of fingerprint identification. Their study led to the formal acceptance of fingerprints as a valid means of identifying an individual.

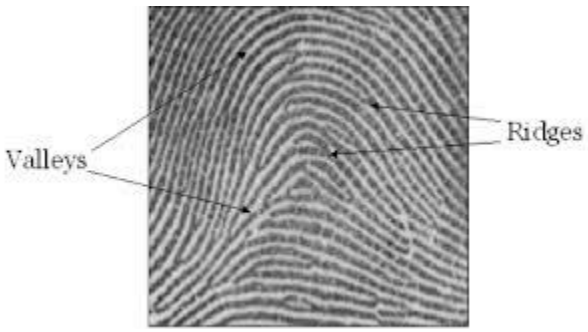

Figure 2.1: Fingerprint Ridge and Valley

2.2 Fingerprint Classification

The research carried out by Henry [11] dealt with the global or macro structures of fingerprint patterns. He analyzed many sets of prints, and his results from this analysis have produced a classification system for fingerprints, known as the *Henry System*. This classification scheme categorizes all fingerprints into 5 broad groups, which are known as global structure of a fingerprint pattern. These categories are: Left Loop, Right Loop, Whorl, Twin Loop, Tented Arch and Arch as shown in Figure 2.2 [12].

The three basic ridge patterns found in fingerprints are the loop, arch, and whorls. Approximately 65% of all fingerprints have loop patterns, 30% arch patterns, 4% whorl patterns, and 1% has patterns other than the basic types [12, 13, 14].

2.3 Features and Uniqueness in Fingerprints

The research carried out by Galton [9, 10] dealt primarily with two separate topics. In one area of research, he investigated the uniqueness of a fingerprint. Up until then, fingerprints were assumed to be relatively unique, but there was no certainty that the unique property held. Galton's findings have now ensured that every fingerprint is in fact unique.

Galton also examined the changes in the fingerprint pattern structure over age. His results showed that a fingerprint pattern remains the same through age, and this finding together with the uniqueness property has allowed authentication through fingerprint recognition a possibility.

Galton's other area of research dealt with the micro structure of a fingerprint pattern. He revealed the existence of small discontinuities in the fingerprint ridge pattern flow, called *minutiae* points. Furthermore, he was able to classify these minutiae points into categories based on the type local discontinuity that existed. The significance of the finding was that these minutiae points could be used as reference points to aid in the authentication of a person through their fingerprint.

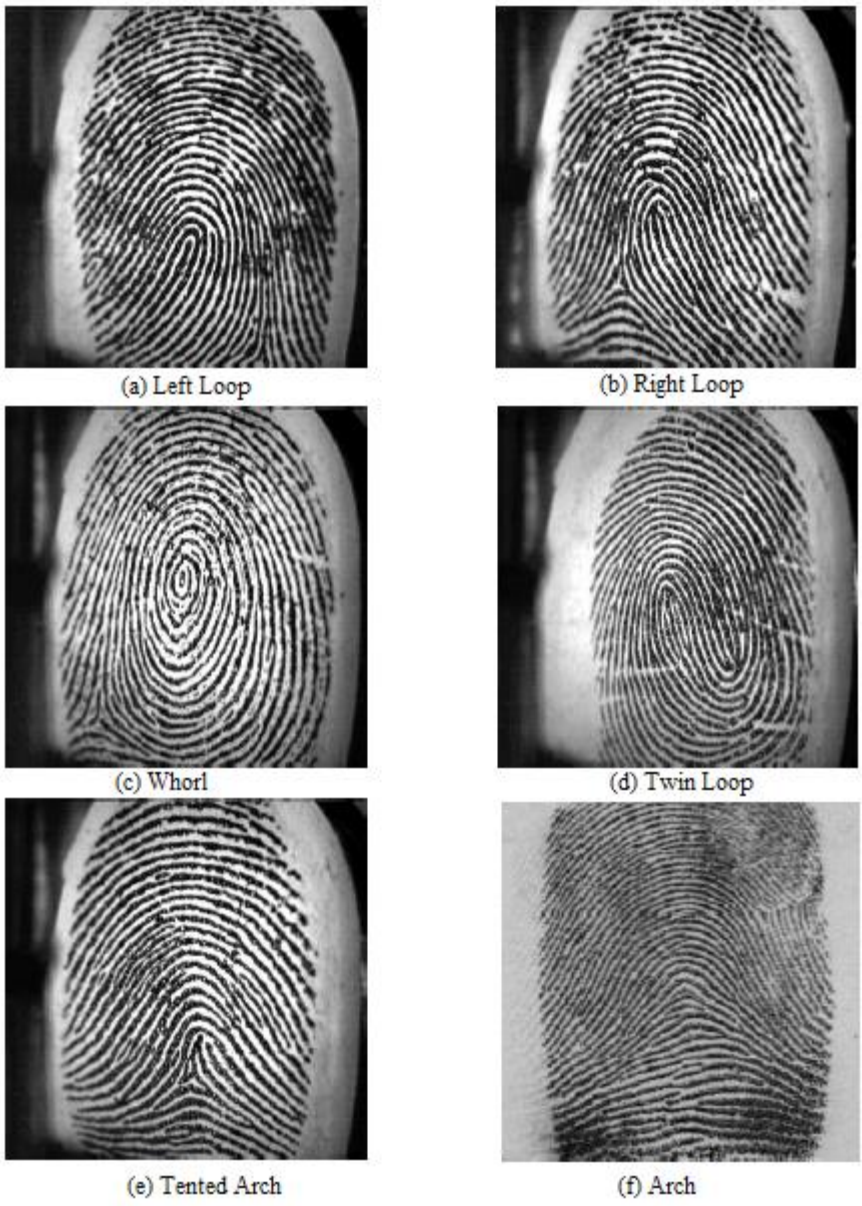

Figure 2.2: Different Patterns of Fingerprints

The original set of minutiae points or Galton features, consisted of four feature types. This set has now been extended to incorporate more minutiae point types, and is referred to as the Extended Galton Feature set. The contents of this set are: Ridge End, Lake or Enclosure, Bifurcation, Short Ridge, Crossover or Bridge, and Spur as shown in Figure 2.3 [15].

Figure 2.3: Extended Galton Feature Set

Two more key features of a fingerprint are the core and delta points. These are also called as the singularity points of the fingerprint. The top most point in the innermost ridge is called the core point and a point where three curves meet each other is called a delta point. Figure 2.4 shows core and delta points of a fingerprint [15].

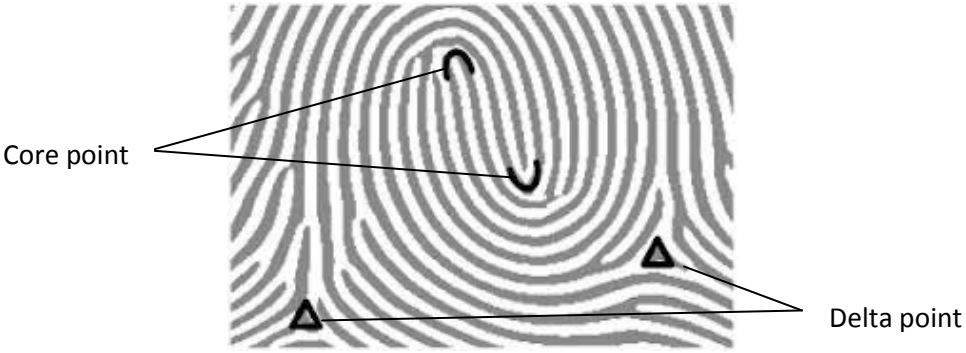

Figure 2.4: Singular Points (core and delta)

2.4 Fingerprint Matching

In fingerprint matching, first the fingerprint image is acquired through fingerprint scanner and then preprocessing is done on a fingerprint image. Next features are extracted from a fingerprint image and these features are stored as template in a database. When a query input image is presented to a fingerprint matching system, the features are extracted and compared with the stored templates of fingerprints in a database. Then based on some threshold values, it is decided that fingerprint image is matched or not. The query and template fingerprint image alignment is a major problem in a fingerprint matching. When acquired through fingerprint scanner, the query fingerprint image may be translated (displaced) left, right, up or down as compared to template image. Also the query fingerprint image may be rotated as compared to a template image. So before matching, translation and rotation issue of a query fingerprint image must be resolved. Both the query and template fingerprint images should be aligned with respect to each other and there should be no translation and rotation difference.

Some fingerprint matching algorithms operate directly on grayscale fingerprint image [16, 17, 18] while most others require that an intermediate representation of fingerprint image is derived through feature extraction stage.

Fingerprint matching is not as easy a task as it appears, because there are large intra-class variations (translation and rotation in different prints of a finger). The main reasons for these intra class variations are given below:

(i) The person can place the finger at different area of fingerprint scanner surface so the fingerprint image may be displaced left, right, up and down. Hence instead of capturing complete fingerprint image, only its partial left or right portion may be captured.

(ii) The fingerprint can be rotated at different angles by the person on the fingerprint scanner surface during acquisitions of fingerprints.

(iii) In fingerprint scanning, the three dimensional shape of finger is mapped on to a surface that is two dimensional. This mapping into two dimensional frameworks results in a

non-linear distortion of images. This is due to the skin texture in different fingerprint acquisitions.

(iv) The ridge and valley structure of a fingerprint would be captured accurately if the ridges and valleys of a fingerprint were in uniform contact with the scanner. Due to the difference in fingerprint pressure, skin dryness, moisture in the air and grease, the finger is not uniformly contacted with the scanner surface.

(v) There is a noise which is caused by surface of fingerprint scanner. The surface of scanner may get dirty after large number of fingerprint acquisitions. Therefore acquired fingerprint image can be very noisy.

(vi) The feature extraction algorithms are not 100 percent perfect and errors are introduced by these algorithms at different stages [15].

2.5 Fingerprint Matching Techniques

There are many fingerprint matching methods [17, 19, 20, 21, 22, 23, 24, 25]. These fingerprint matching methods can be mainly classified into three categories.

(i) Fingerprint matching based on Minutiae
(ii) Fingerprint matching based on Feature
(iii) Fingerprint matching based on Correlation

2.5.1 Minutiae based fingerprint matching

This is the most popular technique in fingerprint matching. This technique is based on matching process used by human fingerprint examiners. Minutiae are extracted from the fingerprint image and stored as feature vectors. These feature vectors contains minutiae coordinates, their orientation, their angle with respect to other minutiae and their distance from other minutiae.

The minutia based technique [19], first finds the minutiae in query fingerprint image and matches their features in a stored template fingerprint [16]. 60 to 80 minutiae are found in a good quality fingerprint image, but there are different numbers of minutiae in different fingerprints.

The main steps of the minutiae-based matching system are following:

(i) Estimate the direction field to establish the orientation of curves in the fingerprint.
(ii) Perform adaptive filtering to reduce noise.
(iii) Obtain a binary image of the fingerprint by maintaining thresholds.
(iv) Perform thinning to obtain ridges with a width of 1 pixel.
(v) Extract minutiae points from the thinned image.
(vi) Remove false minutiae points from the thinned image.
(vii) Register minutiae templates in the biometrics database.
(viii) Match the fingerprints by comparing the freshly captured fingerprint with the registered minutiae templates.

2.5.2 Feature based fingerprint matching

In Minutiae based matching approaches, the low quality class fingerprint images are a major problem as minutiae points cannot be easily obtained from these poor quality fingerprints. There are other fingerprint features which include ridge frequency, ridge shape, ridge orientation and texture information. These fingerprint features can be extracted more reliably than minutiae. In ridge feature based matching, fingerprints are compared in terms of their extracted features from ridge pattern. This technique is a feature-based technique that captures the ridge features from a fingerprint image and stores them as a feature vector [15, 20, 21]. The fingerprint matching is based on the similarity between the two corresponding feature vectors and therefore the matching process is very fast. There are other feature based approaches in which features are Zernike features, invariant features, frequency features and wavelet features. These features can easily be extracted from a fingerprint, and matching based on these features is very fast.

The main steps of the ridge feature based matching system are following:

(i) Estimate the direction field to establish the orientation of curves in the fingerprint.
(ii) Perform filtering to reduce noise in direction field.
(iii) Find the reference point in fingerprint image.
(iv) Tessellate the image in circular sectors or in square grid.
(v) Apply bank of Gabor filters to region of interest in fingerprint image.
(vi) Calculate variance in the filter image (feature vector).
(vii) Compute Euclidean distance between template image and query image.

2.5.3 Correlation based fingerprint matching

Correlation-based techniques rely on the broader and overall correlation between two images. Depending upon the correlation technique, two fingerprint images are aligned and a correlation between corresponding pixel values is computed. Correlation based technique [22, 23, 24] matches the global patterns of holistic features of the fingerprints and therefore these are more tolerant to fingerprint image degradation.

To use the correlation-based verification system:

(i) Obtain the characteristic information from the captured fingerprint image.
(ii) Create a primary template of the fingerprint by performing image normalization.
(iii) Find the characteristic positions in the primary template using correlation computation technique.
(iv) Match the characteristic positions of the primary template with the secondary template stored in the biometric database.
(v) Find the maximum correlation in both the primary and secondary template to decide whether the prints match, match for the correlation value.

2.6 Problem Description and Scope

Since the last four decades, fingerprint matching is done through minutia based techniques. This matching technique has faced many problems, such as orientation and location errors of minutiae.

Along with this, a major drawback of minutiae technique was occurrence of false minutiae and the non-appearance of genuine minutiae. It was a very challenging task to overcome the problem of non linear distortion, which was introduced when a three dimensional fingerprint was mapped to two dimensional mapping fingerprint technique for matching. The scope of this paper is totally different from the minutiae based technique, as fingerprint authentication technique is now based on moments.

The first step for this verification system proposed is to compute the directional field; the second was to normalize the directional field. Then the Poincare index technique is applied on the normalized estimation field [26]. As a result singular points are detected in the image. Using the detected singular point, the area of interest is modified. The proposed approach of modification of area of interest is described in detail in chapter 3.

After Computation of the Singular point for fingerprint, the next step is of matching the fingerprint. For this, one of the Geometric moments has been used. Moments were introduced by Hu [27, 28] and its usage showed high results in image processing. Its results showed that the moments are translational and scale invariant. The most powerful moment was known to be Zernike moment. Teague was the first one to use it, and used it in many applications. Zernike moment, due to their orthogonal and rotation invariant property is far better than Minutiae based technique. The basic advantage of using moment is that it is less complex and efficient algorithm. Zernike moment is applied on the ROI feature of fingerprint. To compute matching, Euclidean distance is calculated among those two ROI features of fingerprint. Zernike moments are beneficial, as they are orthogonal polynomials. Due to this property, it allows maximum separation of data points, and reduces redundancy among moments. Zernike polynomials are used for reconstruction also. Furthermore Zernike moments are rotational invariant, which was its plus point to be used in fingerprint matching. As some fingerprints which are genuine but slightly rotated, are matched using Zernike moments [27].

So after computing the singular points and modifying the area of interest, Zernike moments are applied. The matching difference is computed using Euclidean distance and chapter 5 shows the result of this approach.

2.7 Summary

In this chapter, different types of fingerprint classes based on singular points have been briefly discussed. Major issues in fingerprint matching have also been highlighted which cause problems in matching. These issues must be resolved by a fingerprint matching algorithm to get the best results in matching. Different categories of fingerprint matching methods have also been explained in this chapter.

Chapter 3: Fingerprint Preprocessing

3.1 Introduction

Each person in the world is known by his/her unique fingerprints. This makes people identification easier by matching their fingerprints. Classification of fingerprints can be done into six different classes: whorl, arch, twin loop, tented arch, right loop and left loop.

From long time the matching is performed by minutiae, which is done by extracting ridges and branching points of a fingerprint. Using this technique the similarity of fingerprints was determined by comparing the sets of minutiae.

This technique was not that helpful as it only helped in comparing a right loop image with another right loop image in database. And when the proportion of images increases, coarse level classification results lose their authentication. For automation systems this was a drawback, as the system had to intake the global directions and its connectivity.

Taking another approach of fingerprint into consideration was helpful, that was their direction oriented patterns. These directions were formed by the ridges and valleys. The area of interest is known as singular point area. This area where the curvature of the ridge is higher than normal and the ridge changes its direction very quickly.

Mostly the algorithms used for fingerprint verification and classification have this feature of extracting precise location in a very efficient way. Before verification of fingerprint, its classification is an important step for partitioning the large database of fingerprint. In this process, the input image of fingerprint is processed and then a search process is conducted into the template database for the class, which the input fingerprint belongs to. The pattern area of fingerprint is an important area for classification. Ridges that are surrounded by typelines exist in pattern area of fingerprint. These typelines are the innermost ridges that encircle that central part of the fingerprint image. This is actually the area of interest [26]. A clear description of the pattern area with typelines ‘A’ and ‘B’ have been highlighted in Figure 3.1.

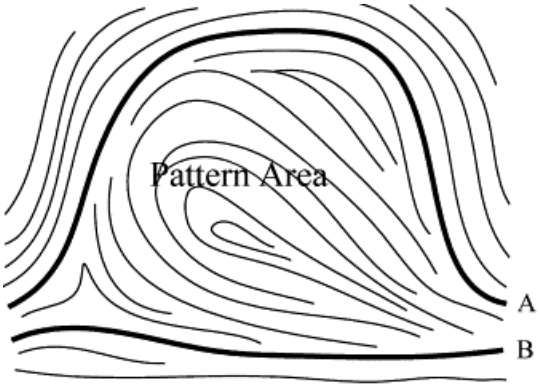

Figure 3.1: Pattern Area and Typelines

The pattern area consists of two singular points, core and delta. Identification of these two points should be done very accurately and precisely. As more accurate the identification of points be, the lesser will be the probability of error [26, 29]. Core point marked as circle and delta point marked as delta, are highlighted in Figure 3.2.

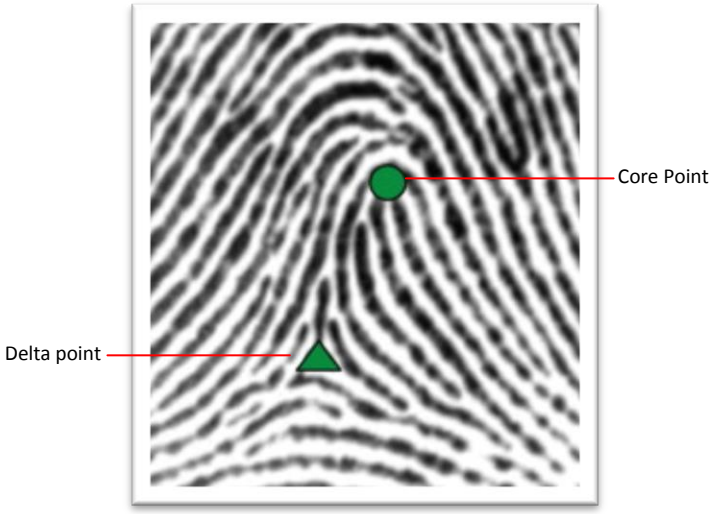

Figure 3.2: Singular Points Highlighted

The detection of singular points (core and delta), accurately and reliably, is very important for classification and matching of fingerprints. An approach mostly used for core point detection is based on *SIFT (Scale Invariant Feature Transform)* operation [30]. Firstly, SIFT points are extracted, and then reliability and ridge frequency criteria are applied to reduce the candidate point required to make a decision on the core point. Finally a suitable mask is applied to detect an accurate core point [31]. The problem lies in extracting the SIFT points, for bad quality images if

initially these point are extracted wrong, all remaining effort for ridge frequency and applying a mask to detect core point is of no use.

Another technique used for point detector is *SURF (Speeded Up Robust Feature).* It is a performant scale-and rotation-invariant interest point detector and descriptor**.** It approximates or even out performs previously proposed schemes with respect to repeatability, distinctiveness, and robustness, yet can be computed and compared much faster. This is achieved by, relying on integral images for image convolutions, building on the strengths of the leading existing detectors and descriptors (using a Hessian matrix-based measure for the detector, and a distribution-based descriptor) and simplifying these methods to the essential. This leads to a combination of novel detection, description, and matching steps [32]. This technique was not considered due to its complex algorithm to compute the core point. And although this technique is used in many image processing point detector task but have not given successful results for detecting core point in a finger print image.

For detection of the Core point and delta point, a practical method known as Poincare Index is used. This technique helps in detection of singularities of a fingerprint whose orientation is well defined. The method accurately judges the singular points for the images whose quality is high, for low quality images the results are not very accurate. For reliable results on weak images, the image first needs to be enhanced. The traditional method of Poincare index detects the presence of singular point but does not detect the points accurately. For this Poincare index technique is modified, which firstly detects the region where singular points exist and then singular points are detected at 1 pixel level, which gives more accurate results. Figure 3.3 gives a brief introduction of the steps followed to achieve the objective of detecting singular points using Poincare index.

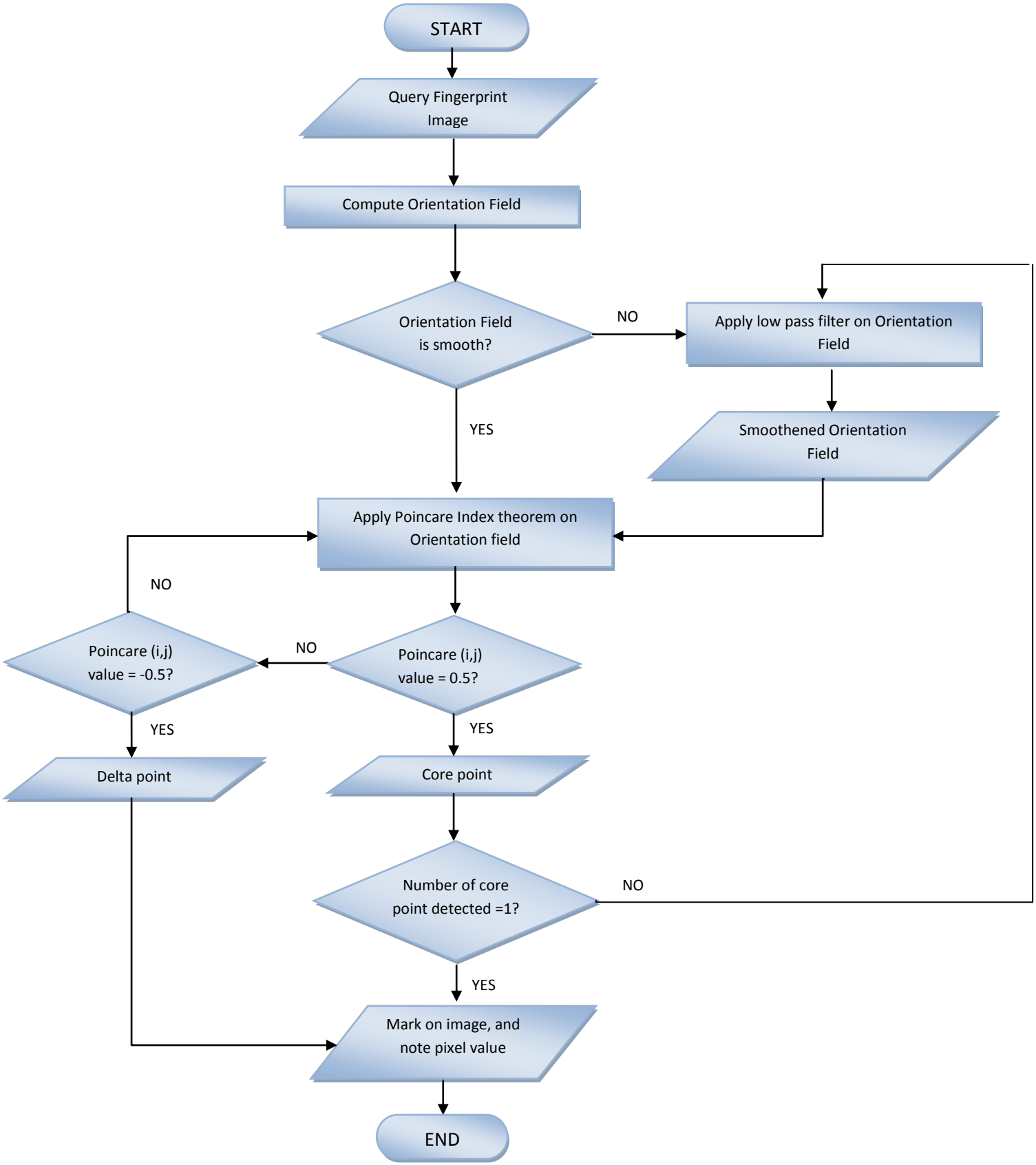

Figure 3.3: Flowchart to Detect Core Point of Fingerprint

3.2 Orientation Field Estimation

An important preprocessing step in fingerprint matching is direction estimation. The direction field computed should be reliable and of good quality. Computing singular point is also based on the directional field quality and reliability. The method used to compute the direction estimation is least mean square algorithm [26].

To compute directional field following steps are performed:

(i) Input image *I* is divided into non overlapping blocks of a constant size *w*×*w*.

(ii) Compute the gradient horizontally $\partial x(i, j)$ and vertically $\partial y(i, j)$ at each pixel of the image (i, j). The gradient is computed using Sobel operator [33].

(iii) At each block the estimation field, which is center of the block (i, j), is computed using the following equation:

$$\mathrm{v_x(i,j)} = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{\mathrm{v=j-\frac{w}{2}}}^{\mathrm{j+\frac{w}{2}}} 2\,\partial_{\mathrm{x}}(\mathrm{u,v})\,\partial_{\mathrm{y}}(\mathrm{u,v}) \qquad (3.1)$$

$$\mathrm{v_y(i,j)} = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{\mathrm{v=j-\frac{w}{2}}}^{\mathrm{j+\frac{w}{2}}} \partial_{\mathrm{x}}^2(\mathrm{u,v})\,\partial_{\mathrm{y}}^2(\mathrm{u,v}) \qquad (3.2)$$

$$\mathrm{O(i,j)} = \frac{1}{2}\tan^{-1}\left(\frac{\mathrm{v_y(i,j)}}{\mathrm{v_x(i,j)}}\right) \qquad (3.3)$$

O(i,j) is known as least square mean estimation of each block centered at pixel. As it is computed for each block, so it is known as local orientation estimation. It is actually the orthogonal representation of the Fourier spectrum of the window sized *w x w*.

Similarly local orientation is computed for each block. And further the orientation field is smoothened and represented as O`. The smoothening is performed using a low pass filter. A continuous vector field is required for the filter to be applied for smoothening, defined in following equations:

$$\emptyset x(i,j) = \cos(2O(i,j)) \tag{3.4}$$

And

$$\emptyset y(i,j) = \sin(2O(i,j)) \tag{3.5}$$

Øx and Øy are the continuous vector field components. Low pass filtering can be performed with these vector fields, mentioned in the following equations:

$$\emptyset`x(i,j) = \sum_{u=-\frac{w_\emptyset}{2}}^{\frac{w_\emptyset}{2}} \sum_{v=-\frac{w_\emptyset}{2}}^{\frac{w_\emptyset}{2}} W(u,v)\, \emptyset_x(i-uw, j-vw) \tag{3.6}$$

And

$$\emptyset`y(i,j) = \sum_{u=-\frac{w_\emptyset}{2}}^{\frac{w_\emptyset}{2}} \sum_{v=-\frac{w_\emptyset}{2}}^{\frac{w_\emptyset}{2}} W(u,v)\, \emptyset_y(i-uw, j-vw) \tag{3.7}$$

Where *W* is a low pass filter with two dimensional integral. The filter size is $w_\emptyset$ x $w_\emptyset$. Block by block the smoothening of the field is done, and the smoothed orientation filed *O`* is computed as follows:

$$\mathrm{O`(i,j)} = \frac{1}{2}\tan^{-1}\left(\frac{\emptyset`_{\mathrm{y}}(\mathrm{i,j})}{\emptyset`_{\mathrm{x}}(\mathrm{i,j})}\right) \tag{3.8}$$

The orientation field computed from the above equation clearly defines the directional estimation of the fingerprint, highlighted as in Figure 3.4.

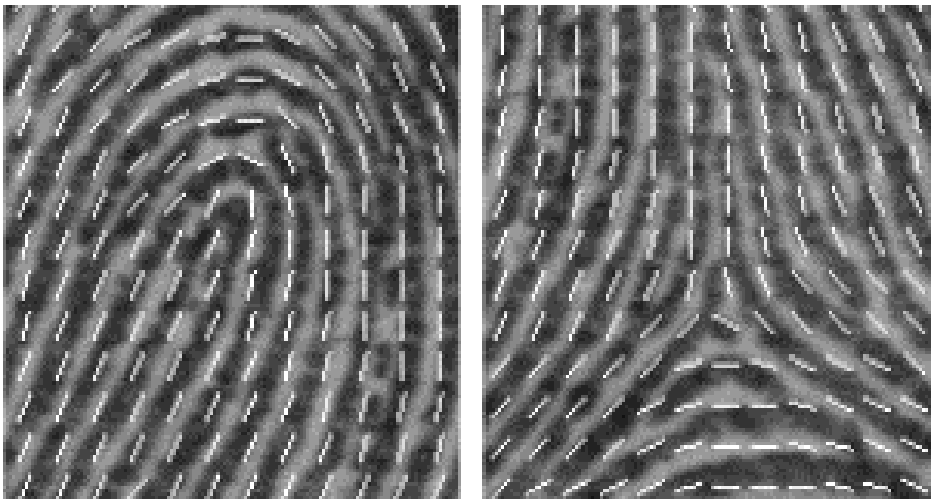

Figure 3.4: Orientation Field for Core and Delta Area

3.3 Normalization

Another important step of preprocessing is normalization. The area of interest is normalized to a constant value of mean and standard variation. This process is done to remove noise factor and fingerprint pressure difference.

Normalization is performed at block level, where I(x,y) is the pixel value of the image, M_i and V_i are the estimated value of mean and variance of each block. $N_i(x,y)$ is the normalized value at specified pixel location (x,y).

The normalization for all pixels in a block is defined as following :

$$N_i(x,y) = \begin{cases} M_o + \dfrac{\sqrt{(V_o) \times (I(x,y) - M_i)^2}}{V_i}, & I(x,y) > M_i \\ M_o - \dfrac{\sqrt{(V_o) \times (I(x,y) - M_i)^2}}{V_i}, & otherwise \end{cases} \quad (3.9)$$

M_o is desired mean and V_o is the desired variance value. As mentioned earlier, normalization is pixel wise operation, when done for whole image it will not compensate for the intensity variation

which was caused due to fingerprint pressure. Normalization performed on each block resolves this problem.

3.4 The Poincare Index value

The method which have proposed the singular point detection, most commonly is Poincare Index algorithm.

Poincare index have specific threshold values for digital images. A fingerprint having two core points has Poincare index value as 1, single core point threshold value by default as ½ and delta point threshold value as -½. The Poincare algorithm is applied on the orientation field.

For an *M x N* fingerprint image, $\theta(x,y)$ denotes the direction for a pixel in image and the Poincare at a pixel location (x,y) can be computed by following the equation mentioned below:

$$Poincare(x,y) = \frac{1}{2\pi}\sum_{k=0}^{N-1}\Delta(k) \tag{3.10}$$

Where,

$$\Delta(k) = \begin{cases} \delta(k) & |\delta(k)| < \frac{\pi}{2} \\ \delta(k) + \pi & |\delta(k)| \leq -\frac{\pi}{2} \\ \pi - \delta(k) & |\delta(k)| \geq \frac{\pi}{2} \end{cases} \tag{3.11}$$

$$\delta(k) = \theta\left(x_{(k+1)modN}, y_{(k+1)modN}\right) - \theta(x_k, y_k) \tag{3.12}$$

The Poincare index algorithm works in counter clockwise direction. The pixel highlighted in the mask shown in Figure 3.5, are used in counter clock wise direction to compute the value for the index (x,y).

(x+2,y-2)	(x+2,y-1)	(x+2,y)	(x+2,y+1)	(x+2,y+2)
(x+1,y-2)	(x+1,y-1)	(x+1,y)	(x+1,y+1)	(x+1,y+2)
(x,y-2)	(x,y-1)	(x,y)	(x,y+1)	(x,y+2)
(x-1,y-2)	(x-1,y-1)	(x-1,y)	(x-1,y+1)	(x-1,y+2)
(x-2,y-2)	(x-2,y-1)	(x-2,y)	(x-2,y+1)	(x-2,y+2)

Figure 3.5: Mask for Detecting Singular Points

The size of the mask shown above can increased as well, but then the location of singular points gets affected too. The size of the mask can be increased only when it is detecting for than one core point within the pattern area. The poincare index not only considers the rotation angles but also the rotational vectors in the orientation field.

3.5 Singular Point Detection

The Poincare algorithm is applied over the orientation field to find out the singular point. The mask discussed above is applied all over the orientation field. If Poincare (i,j) value is equal to 0.5 then the block M(i,j) has detected a *core* in image. If Poincare (i,j) value is equal to -0.5 then the block has detected a *Delta* in image. If the value is none of them then the block M(i,j) has detected no singular point. If the numbers of core points or delta points are more than two, the orientation field is smoothened until the singular points detection becomes lesser than two [27].

3.6 Summary

In this chapter, singular point detection on fingerprint has been explained in detail. Preprocessing steps required for this are also discussed. Thus to find out the singular points (core and delta), the direction estimation field computation makes the detection process easy. Then by simply applying Poincare index algorithm on the directional field, the core point and delta point is detected.

Chapter 4: Zernike Moments

4.1 Introduction

Geometric moments have been used for image analysis since 1960s [14, 34, 35, 36, 37, 38]. One of the Geometric moments used very frequently by researchers is Zernike moment. This moment has been used and its algorithm has been enhanced by many researchers. Zernike moment is set of complex polynomial, which forms the image set over a circular disk of unit radius [39]. Usage of Zernike moment by researchers concluded that the problem of information redundancy in image is reduced [35]. Zernike moments [34, 40] have the property of rotational invariance, as they belong to the class of orthogonal moment. Changing the direction of image doesn't change the magnitude under the application of applying Zernike moment over the image. Moments are constructed by defining their order. Table 4.1 shows the features of Zernike when defining their order. Zernike moments have some disadvantages: they are sensitive to noise; bad quality images also don't respond well to Zernike moment. Hence Zernike moments has been applied on different images with different order of moment. The mathematical detail of Zernike moments is presented in Section 4.3 of this chapter.

4.2 Fingerprint Matching

There are over a hundred matching techniques for fingerprint. Few of them are very basic and commonly used; the mostly frequently used are minutiae based matching, image-based matching and hybrid approach of matching. In Minutiae-based fingerprint matching [41, 42, 43], the algorithm detects the minutiae on the fingerprint and then matches it with the template database.

Order	Dimensionality	Zernike moments
0	1	$A_{0,0}$
1	2	$A_{1,1}$
2	4	$A_{2,0}, A_{2,2}$
3	6	$A_{3,1}, A_{3,3}$
4	9	$A_{4,0}, A_{4,2}, A_{4,4}$
5	12	$A_{5,1}, A_{5,3}, A_{5,5}$
6	16	$A_{6,0}, A_{6,2}, A_{6,4}, A_{6,6}$
7	20	$A_{7,1}, A_{7,3}, A_{7,5}, A_{7,7}$
8	25	$A_{8,0}, A_{8,2}, A_{8,4}, A_{8,6}, A_{8,8}$
9	30	$A_{9,1}, A_{9,3}, A_{9,5}, A_{9,7}, A_{9,9}$
10	36	$A_{10,0}, A_{10,2}, A_{10,4}, A_{10,6}, A_{10,8}, A_{10,10}$
11	42	$A_{11,1}, A_{11,3}, A_{11,5}, A_{11,7}, A_{11,9}, A_{11,11}$
12	49	$A_{12,0}, A_{12,2}, A_{12,4}, A_{12,6}, A_{12,8}, A_{12,10}, A_{12,12}$

Table 4.1: Zernike Moments and Features from order 0 to 12

One by one each input fingerprint minutia with the template database image. This requires high quality input image, so that it detects minutiae perfectly. The performance of this technique is slow due to complex algorithm and the way the matching on minutiae is done. The second technique, Image-based fingerprint matching [21, 44, 45, 46, 47, 48, 49] uses the features of the fingerprint to perform the matching. The features used are the ridges and valleys, and along this the direction of the ridges and texture information is used to perform the matching. Combination of the above two mentioned techniques can also be used to match a fingerprint, but again the complexity of the technique touches sky. Combination of any two techniques is known as Hybrid fingerprint matching [19, 50, 51, 52].

Hasen et. al. [27] proposed a fingerprint matching technique based on Zernike moments. Their technique relies on the accurate detection of core-point in a fingerprint image to form the Region of Interest (ROI). Core-point detection is not a trivial task as core-point may be located along the edge of fingerprint image. Hence ROI may not be covering the ridge and valley structure of a fingerprint image properly. The core-point detected should be in the center of fingerprint image for proper formation of ROI. Also there is always some margin of error in the accurate detection of core-point location. But still our approach does rely on the detection of core-point location.

Image-based matching techniques [53] mostly have concerns with the detection of singular points. The inner most ridge on the finger print is known as Core point [46, 54, 55, 56]. The region around the core point is unique area so mostly the matching is done from applying the technique in this area. This area is known as region of interest. Extraction of ROI from around the core point is a weak approach, because detection of core point has some inadequacies:

(i) The ROI is the region around core point, what if any image doesn't has a core point, or the algorithm doesn't identifies the core point.

(ii) The ROI is not the complete image; it is just an area around core point. What if the core point is detected at the edge of image, then ROI will then have very less information of the image to be matched.

(iii) It is ideally believed the image will have one core point and with respect to it, one ROI will be extracted, what if the algorithms detects two core point in a image, how will the ROI selected and extracted?

4.3 Proposed approach using Zernike moment

Our matching technique fall under the category of image based matching systems. The core point is detected and further the ROI is enhanced. The Zernike moment is been applied on that enhanced ROI to return features.

Our proposed fingerprint matching technique has the following steps:

(i) Extraction of ROI around core point
(ii) Features of Zernike moments computation with order 12
(iii) Euclidean distance between the input image and template database image

The Figure 4.1 shows the flow chart of the recognition system proposed. This flow chart only provides a brief summary of this chapter, stating what steps are performed as pre and post processing for Zernike moment.

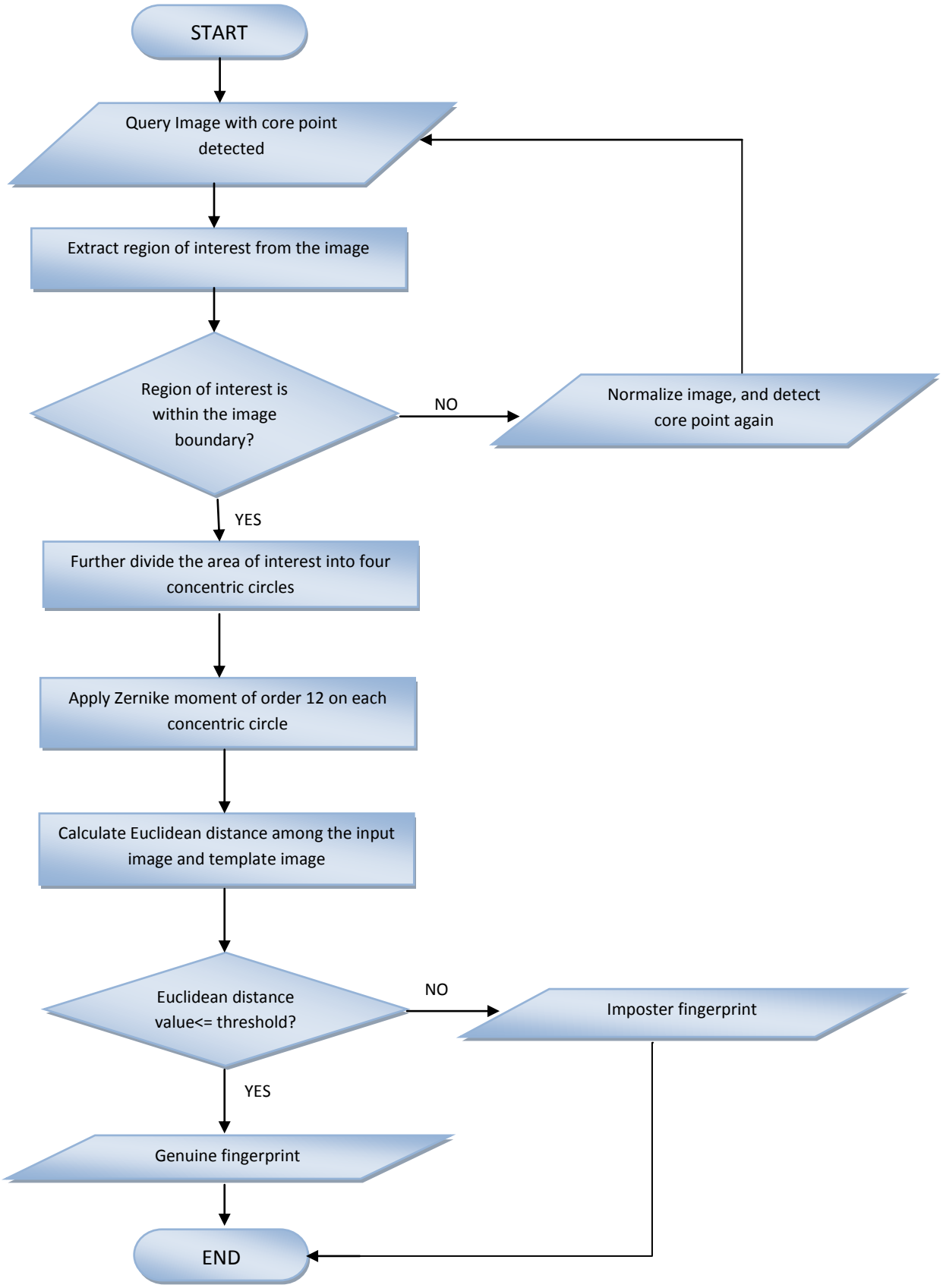

Figure 4.1: Flowchart to Match Fingerprint Image

4.3.1 Feature Extraction around Core point

While using the Zernike moment for fingerprint matching, it is known that this moment is neither translation and nor scale invariant. For this the image should be translation invariant, for this the algorithm needs other computation efforts in the logic. Scaling of the image is not necessary while using moments, because it depends on the image quality. In some cases the scanner is of good resolution, so scaling is not required. It automatically sets dots per pixel specification of the image.

Usually the area around core point is known as area of interest. For geometric moments the area of interest is generally circular region, cropped around core point. Figure 4.2 shows the generally used region of interest for moments. In this paper, the approach for area of interest is modified, and then Geometric moment is applied on it.

Figure 4.2: Area around Core Point

The area of interest is modified by dividing the above shown circular region in to four different concentric circles. The center of the all the four circles is the core point detected using Poincare index. This Modification is done to make region of interest more precise. The first circle closest to the core point has the smallest radius, and the fourth circle has the largest radius. The Zernike moments over small region gives a probability of better result. The size circle can be shrunk or expanded but is has its own disadvantages.

Figure 4.3 shows the concentric circles extracted from the region around core point shown in Figure 4.2. These concentric circle are known as region of interest (ROI).

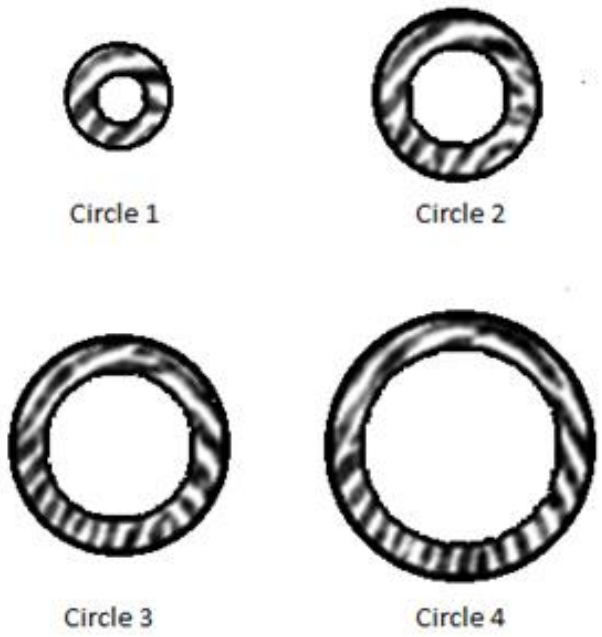

Figure 4.3: Concentric Circle Extracted from Region of Interest

One by one Zernike moments is applied on each circle. This handles the translation invariant property.

4.3.2 Zernike Moment calculation

One of the well-known Geometric moments is Zernike moment. The core of Zernike moment lies in its orthogonal and rotation invariant property.

Rotation invariance of image is handled very well by Zernike moments. To handle image translation invariance, some preprocessing is done on the function f(x,y) before being processed by Zernike.

Zernike moment is set of complex polynomial $\{V_{nm}(x,y)\}$,forming a orthogonal set over a unit disk. The unit disk is expressed as $x^2+y^2 \leq 1$. Defining of Zernike moment in polar coordinates is as follows:

$$V_{nm}(x,y) = V_{nm}(r,\theta) = R_{nm}(r)e^{jm\theta} \quad (4.1)$$

Where n is know as order of the polynomial and should ba a postive integer; m is integer subjected for contriants and n-|m| is an even value, and $|m| \leq n$; r is the radius of the unit disk, $r=\sqrt{x^2+y^2}$; θ is the angle between x axis and radius of the unit circle and the direction is counter clokwise, $\theta = \tan^{-1}(y/x)$; Radial polynamial R_{nm} is defined as following:

$$R_{nm}(r) = \sum_{s=0}^{(n-|m|)/2} \frac{(-1)^s (n-s)!}{s!\left[\frac{n+|m|}{2}-s\right]!\left[\frac{n-|m|}{2}-s\right]!} r^{n-2s} \quad (4.2)$$

Finalizing the equation for two dimensional Zernike moment with defining n as order and m as frequency factor, for function f(x,y) as following:

$$ZP_{nm} = \frac{(n+1)}{\pi} \iint_{unitdisk} f(x,y) V_{nm}^{*}(x,y) dxdy \quad (4.3)$$

Where,

$$V^{*}_{nm}(x,y)=V_{n,-m}(x,y) \quad (4.4)$$

Integrals in Zernike moment are used for continous image, computation for digital image is different. For this integrals are replaced by summations:

$$A_{nm} = \frac{(n+1)}{\pi} \sum_{x} \sum_{y} f(x,y) V_{nm}^{*}(x,y) \tag{4.5}$$

The function f(x,y) in the equation above is defined over the unit circle $x^2+y^2 \leq 1$.

Rotational invariance is an elementary feature of Zernike moments. This feature can be computed for a function f(x,y) by rotating it by angle α. Then the Zernike moment of the rotated image can be computed by the following equation:

$$Z_{nm}^{'} = Z_{nm} e^{-jm\alpha} \tag{4.6}$$

The Zernike magnitude for rotated image Z'_{nm} will be same as Z_{nm} [27].

4.3.3 Normalized Euclidean Distance based Matching

Two pahses are involved in a fingerprint recognition systems; the first phase includes enrollment process whereas the second phase consists of verification process. The verification process shows the reliabilty of the system, that how much fingerprint recognition system is valid and authenticated.

As enrollment process consits of preprocessing, similarly the verification process consists of some steps. These steps include making of a set of template images for training purposes. Zernike moment is applied on these template images and their A_{nm} value is stored into the database. In verification phase, the input image is processed by applying Zernike moment on it, and then its value is matched with the claimant's ZM feature stored as template in database. This will result in geeting a similarity measure. Usually Euclidean distance is measured between the two featured vectors, and then its value is compared to the threhold. If the value of the Euclidean distance is less than thethreshold, the user is accepted and known as a Genuine user. The mathematical detail for normalized Euclidean distance is as following:

$$\mu_i^k = \frac{1}{n}\sum_{j=1}^{n} x_{i,j}^k \tag{4.7}$$

$$\sigma_i^k = \sqrt{\frac{1}{n}\sum_{j=1}^{n}(x_{i,j}^k - \mu_i^k)^2} \tag{4.8}$$

$$d(x) = \sum_{i=1}^{m}(\frac{x_i - \mu_i^k}{\sigma_i^k})^2 \tag{4.9}$$

Where,

μ_i^k= the mean of the ith feature in class k;

σ_i^k= the standard deviation of the ith feature in class k;

$x_{i,j}^k$= the value of the ith feature of example j in class k;

n = the number of examples in class k;

m = the feature dimension;

$d(x)$ = the normalized distance between example x and class k;

Overall the database provided has eight images for each class. From each class four images were selected for training and four for testing. By training image, it is meant that four images of each class are used as template and their Zernike moment features are computed and saved into the database. Whereas by testing, it is meant that the four samples will be used to compare with the four other samples in database. The comparison is done by computing the difference using the normalized Euclidean distance technique [14].

4.4 Summary

In this chapter, an enhanced version of region of interest has been originated and then the Zernike moment has been applied over it. The ROI should be translational and scale invariant before the moment is been applied over it.

Fingerprint verification by applying Zernike moment on new approach of ROI extracted from core point is presented. Dividing the area of interest into circles and applying Zernike moment on limited image one by one proved a good approach than by applying Zernike moment on whole image. Along with the rotation and translational invariant, the new vector feature captures more global information on image. This approach can be very valuable in image understanding applications. It is a robust approach for noise and transformation. Hence, applying Zernike moments on the new approach of extracted area of interest resulted in an efficient fingerprint verification system.

Chapter 5: Experiment Results and Analysis

5.1 Experiment Results

The experiments using Zernike moments were performed on Fingerprint Verification Competition (FVC) 2002 database [57], which is known as Database 1 (Db1). The database consists of 800 images in total (100 different classes; 8 images in each class).

In a fingerprint recognition system, the results taken into consideration are of four types:

(i) Genuine Accept Rate (GAR)
(ii) Genuine Reject Rate (GRR)
(iii) False Reject Rate (FRR)
(iv) False Accept Rate (FAR)

In a recognition system the correct outcomes are GAR and GRR. The percentage in result of GAR and GRR should be the highest. Whereas the results of FRR and FAR should be very low, as these are the false outcomes. Obviously no system wants to reject a genuine input and accept any false input. No system is perfect; it does have some error rate, and the results in FRR and FAR help find out the error and performance of the system. The terms used to find out the system performance are False Accept Rate (FAR) that is 'Imposter Fingerprint Accepted' and False Reject Rate (FRR) that is 'Genuine Fingerprint Rejected'. Another term used is Equal Error Rate (EER), computed by plotting the graph among FAR and FRR. The point where FAR and FRR cancel each other on the plot, is EER of the recognition system.

To compute the difference among the template images and the query input images, Euclidean distance is computed. In this technique a threshold value is set. The fingerprint images below that threshold value are accepted as genuine fingerprint image and the images above the threshold value are rejected as imposter fingerprint.

The experiments for the FVC2002 database of fingerprint were performed on Dual core processor, with windows 7 operating system. The algorithm defined is implemented on MATLAB R2010b. The experiments consist of four training images and four testing images from a class. In total, there are 100 classes, each class having four testing images and four training images. So as a result, 400 training images and 400 testing images have been used for the experiments.

To compute the performance of the system, FAR and FRR were required to be computed. For this, genuine and imposter matches were done on the database. In a genuine match, the testing image of a class is matched with the training images of the same class. For an imposter match, the testing image is matched to training image of the other class.

Zernike moments have been used to analyze the effects of varying the number of moment features on fingerprint matching performance. A cycle of experiments has been conducted by varying the number of Zernike features and their effect was studied on matching performance. To the best of our knowledge, these experiments have not been done before, in fingerprint matching as only fixed number of Zernike features were used by other researchers. They did not analyze the effect of utilizing different number of moment features. It has been shown through these experiments that for different type of fingerprint images, the number of Zernike features were not the same to obtain the best matching results. Best matching performance has been obtained by using different numbers of Zernike features for Db1.

The Zernike moments up to order 15 have been calculated. EER was computed for different number of Zernike features. Experiments were performed by varying the number of Zernike features from 0 to 15 to get the best EER. Curves of FAR & FRR versus threshold values and Receiver Operating Curves (ROC) are also computed using different order of Zernike moments.

Table 5.1 shows the complete result for the proposed approach with different Zernike moment orders applied on the database (db1). When Zernike moment invariant order was selected to 1, an EER of 31.85% was observed. By increasing the order of Zernike moment the EER started to deteriorate. But at order 13 and onwards of Zernike moments, the results started to converge and EER started to rise rather than decrease. So the best Zernike moment order selected for this

approach is order 12, which resulted in giving a minimum error rate of 16.59%. The minimum error rate is highlighted at order 12 and an increase of 0.96% is observed in EER with increase in moment order to 15. As the error rate started to increase after order 12, so only the results till order 15 are shown.

Fingerprint Verification Competition 2002	
Zernike moment order	**Equal Error Rate (%)**
1	31.85
2	29.61
3	29.02
4	28.99
5	25.04
6	24.79
7	22.88
8	21.08
9	19.50
10	18.41
11	17.23
12	16.59
13	16.98
14	17.34
15	17.55

Table 5.1: Equal Error Rate on FVC 2002 Database by using Different Number of Zernike Moments

The recognition rate and the computation time of the system implemented at different Zernike moment order is shown in Table 5.2. Increase in moment order improves the recognition rate, but increases the computation time as well. The recognition rate started from 68.15% and improved to 83.41%. At order 13 and onwards the recognition rate started to decline but the computation time kept on increasing logically. Going beyond of order 12 is of no use except degrading system

performance. As there was no improvement on recognition rate after 12, only results till order 15 are shown.

Fingerprint Verification Competition 2002		
Zernike moment order	**Recognition rate (%)**	**Computation time (in seconds)**
1	68.15	5.39
2	70.39	5.51
3	70.98	5.58
4	71.01	5.73
5	74.96	6.02
6	75.21	6.42
7	77.12	6.63
8	78.92	7.20
9	80.5	7.61
10	81.59	8.22
11	82.77	8.54
12	83.41	9.57
13	83.02	10.13
14	82.66	10.98
15	82.45	11.45

Table 5.2: System Performance on FVC 2002 Database by using Different Number of Zernike Moments.

5.2 Analysis

An analysis of three different techniques using Zernike moments is done in this section. It can be proved from the results that the proposed method is better in performance for a fingerprint matching system.

The method used earlier was to simply crop the area around core point in circular form and apply Zernike moment on it. As an enhancement of this technique, the area around core point was

cropped into four concentric circles and Zernike moment was applied individually on each circle. The computation of Zernike moment with Discrete Fourier Transform (DFT) was done. This technique was to apply the DFT on the complete image and then apply the Zernike moment algorithm over it. EER was kept a parameter to compare the three different techniques for fingerprint matching using Zernike moment. Table 5.3 shows the comparison of EER.

		EER %
1	Zernike moment on Discrete Fourier Transform of image [58]	13.13
2	Zernike moment on complete circle around core point	22.38
3	Zernike moment individually on 4 concentric circle around core point	16.59

Table 5.3: EER Comparison for Matching Techniques

Applying Zernike moment on complete circle around core point resulted in 22.38 % EER, and by dividing the core point into concentric circles reduced the error rate to 16.59%. The DFT technique gives the minimum error rate of 13.13%. The computation time also is an important factor in measuring the performance of the recognition system. The DFT technique although gives the minimum error rate but the system performance gets slow. Comparison of the computation time for the three techniques has been given in the Table 5.4 and plotted in Figure 5.1.

From the results it can be clearly seen that the best computation time is for the technique proposed in this thesis. Taking computation time at order 10 as reference on the graph or table it can be compared very easily that Zernike moment with DFT technique takes 11.79 seconds and is the most time consuming technique. Then the second graph of computation time is for the technique proposed in this thesis, to extract 4 concentric circles around core point, it takes 8.22 seconds. The third graph of computation time is for the technique to apply Zernike moment on complete area of interest around core point. It provides computation time of 6.58 seconds that is minimum among all the three methods.

Fingerprint Verification Competition 2002			
Zernike moment order	**Computation time for ZM with DFT on complete image[58] (in seconds)**	**Computation time for ZM with Core point, 4 concentric circles (in seconds)**	**Computation time for ZM with Core point ,1 complete circle (in seconds)**
1	7.10	5.39	3.29
2	7.81	5.51	3.99
3	8.32	5.58	4.33
4	8.64	5.73	4.51
5	9.37	6.02	4.78
6	9.89	6.42	5.13
7	10.32	6.63	5.78
8	10.66	7.20	5.97
9	11.47	7.61	6.24
10	11.79	8.22	6.58
11	12.85	8.54	6.90
12	13.01	9.57	7.20

Table 5.4: Computation time by using Different Order of Zernike Moments on Different Techniques

The FAR and FRR graph; ROC graph with different number of Zernike moment is shown in Figure 5.2. The plot shows that as the moment order is increased the EER gets reduced. As it was justified before that the best results were obtained till order 12. So EER and ROC results are only shown till order 12. The Figure 5.2 (a) shows the FAR and FRR graph at order 5 of Zernike moment. FAR and FRR both intersect each other at 25.04%. The percentage shows that this amount images were falsely accepted and the genuine images were rejected. Figure 5.2 (b) shows ROC graph at order 5 of Zernike moment. The ROC curve is depicting the relative tradeoffs between true positive and false acceptance rate of the genuine scores versus impostor scores. The

graph depicts that minimum the area under the curve, the better is the performance of the system. Similarly Figure 5.2 (c) shows that the FAR and FRR meet at 18.41% for moment order 10. The graph shows as the moment order is increasing the lesser the Error rate is. Figure 5.2 (d) shows the performance of the system using ROC graph. It can be seen from the graph that there is lesser tradeoff between the true positive and false acceptance rate at order 10 of Zernike moment. Figure 5.2 (e) shows the minimum EER of 16.59% at the intersection of FAR and FRR. Figure 5.2 (f) shows best performance of the system with minimum area under the curve of the ROC plot at order 12 of Zernike moment.

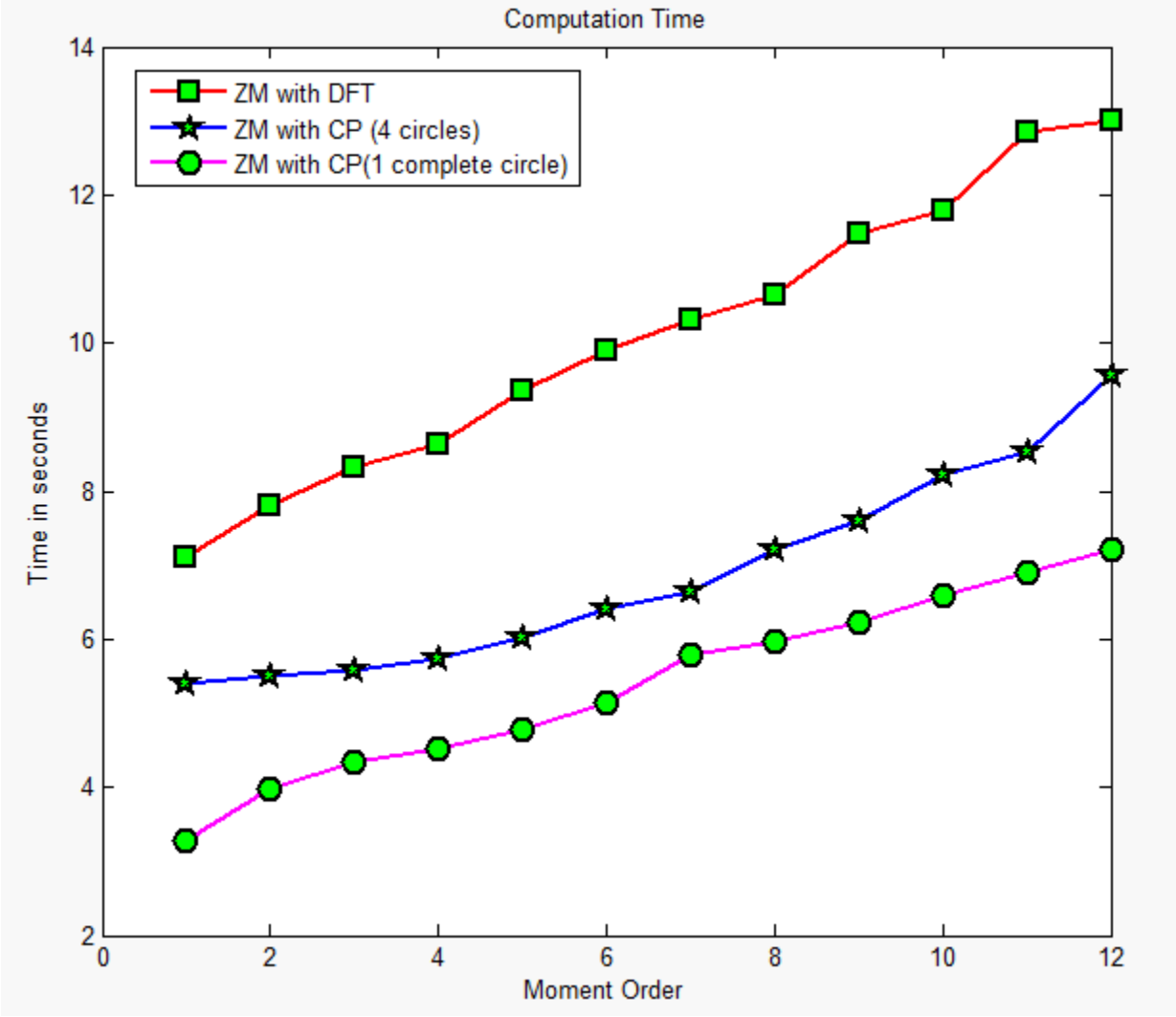

Figure 5.1: Computation Time Graph by using Different Number of Zernike Moments on Different Techniques

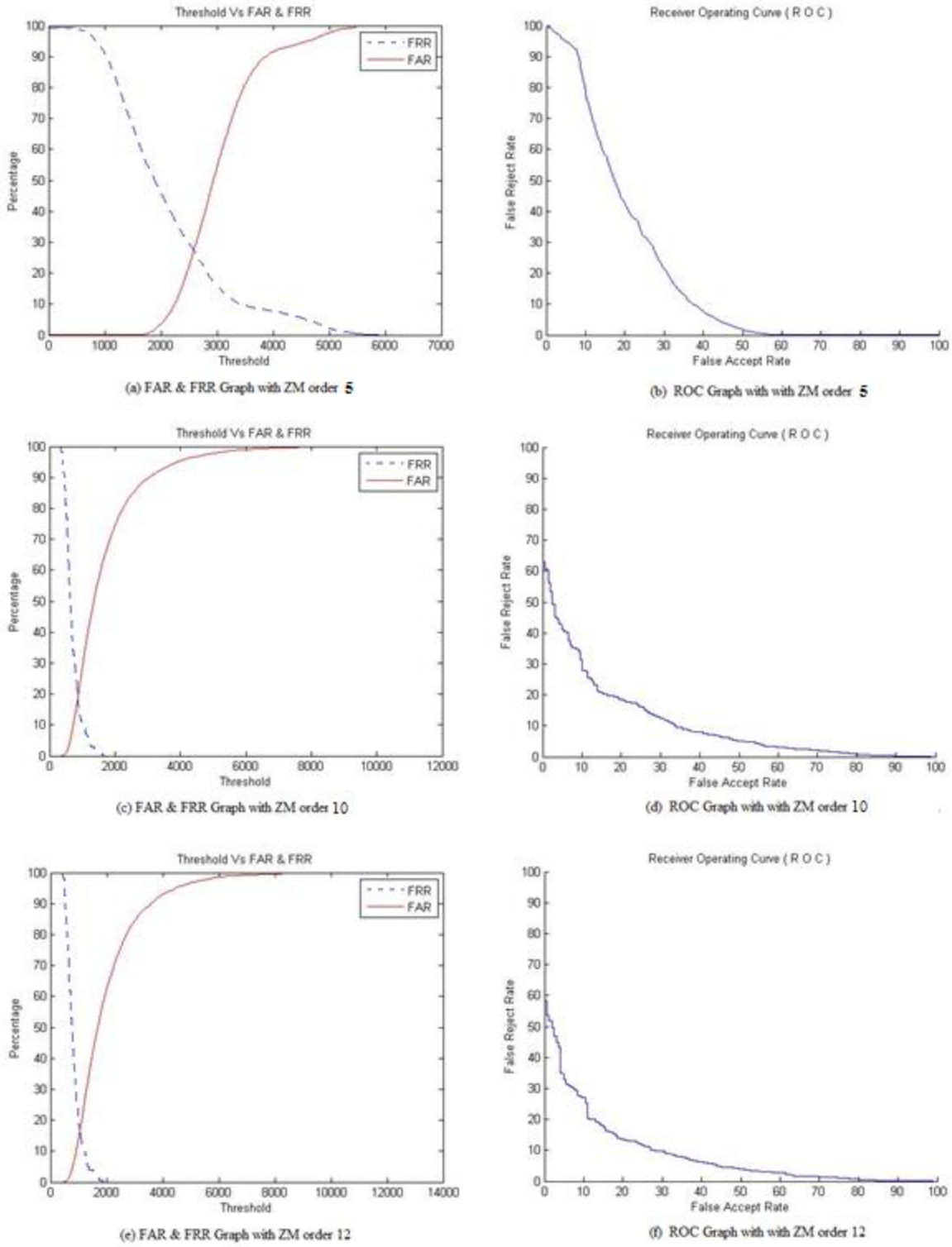

Figure 5.2: FAR and FRR graph; ROC graph by using Different Number of Zernike Moments

Table 5.5 shows the overall recognition rate results of the proposed system. The success rate achieved is 83.41%. This recognition is computed with the help of EER in the system. EER is computed at the point where FAR and FRR meet each other.

Recognition Type	Recognition Rate
True Success Rate (TSR)	83.41 %
False Acceptance Rate (FAR)	16.23%
False Rejection Rate (FRR)	16.41%
Equal Error Rate (ERR)	16.59 %

Table 5.5: Recognition Rate Results

Figure 5.3 shows a value where FAR and FRR cross each other. This plot is just to show the value used as a threshold. Equal Error rate value is also retrieved from this plot. The plot shows that a threshold value of 990 is obtained when the value of FAR is set equal to FRR.

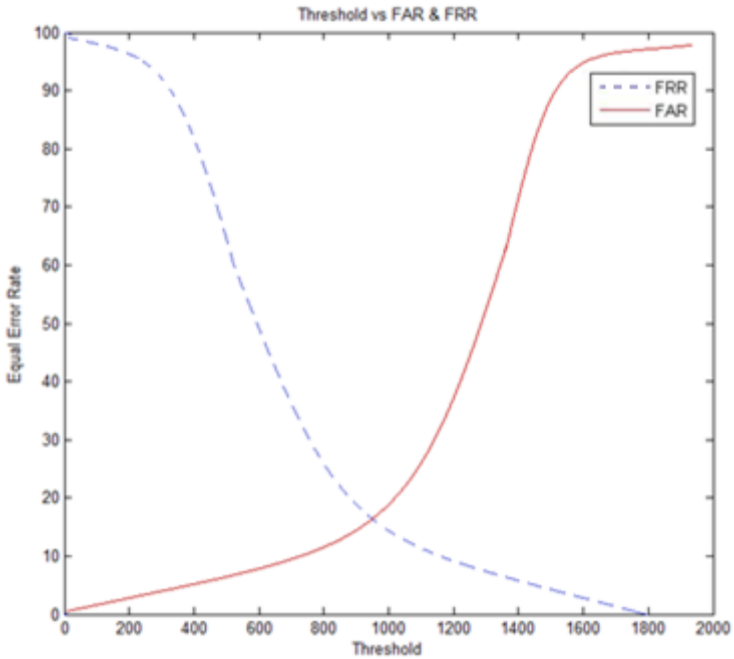

Figure 5.3: FAR-FRR Plot to obtain Threshold

The comparison of the proposed approach is also done with the FVC 2002 competition data. The results are given in the Table 5.6. The Table is highlights the algorithm name, organization name

and type of the data, and is taken from the FVC 2002 competition [57]. To compare the results of the algorithms only, the EER parameter is considered.

Algorithm	Organization	Type	EER
Algorithm PA22	AILab, Institute of Automation, The Chinese Academy of Sciences. China	Academic	17.34% (15.03%-19.64%)
Algorithm PA25	Department of Computer Science and Information Engineering, Da-Yeh University	Academic	35.00% (34.89%-35.11%)
Algorithm PA03	Biometrics System Lab, Beijing University of Posts and Telecommunications	Academic	50.00% (0.00%-100.00%)
Proposed Approach using Zernike Moments	Department of computer Engineering. National University of Science and Technology	Academic	16.59% (14.09%-18.50%)

Table 5.6: EER Comparison with the FVC 2002 Competition Data

As the equal error rate of the three algorithms is higher, it can be concluded that the proposed approach having the minimum EER of 16.59% is the best algorithm to be used for fingerprint matching.

5.3 Summary

Fingerprint verification by applying Zernike moments on new approach of image extracted from core point, is proposed in this thesis and has been tested on FVC 2002 Db1 database. Dividing the area of interest into circles and applying Zernike moments on limited image one by one proved a good approach than by applying Zernike moments on the whole image. The performance of Zernike moments can be seen in the result section and its comparison is also done with different algorithms mentioned in the FVC 2002 competition, the results shows that the recognition rate of the proposed system is greater. Along with are rotation and translational invariant, the new vector feature captures more global information on image. This approach can be very valuable in image understanding applications. This approach was also robust to noise and transformation. Hence this new approach with Zernike moments resulted in an efficient finger print verification system.

Chapter 6: Conclusions and Future Work

6.1 Conclusions

In this thesis, a novel fingerprint matching method based on Zernike moments has been proposed. For fingerprint matching, it is desirable to obtain a fingerprint representation invariant to translation and rotation. Translation invariance is achieved by transforming the image using zero moment orders. For rotation invariance, Zernike moments are calculated which are invariant to rotation.

The orientation field is computed for the fingerprint and then Poincare index technique core point is detected. The region of interest is cropped using core point and is enhanced and divided into smaller concentric circles. Then the magnitude of the Zernike moments is calculated by applying over the region of interest. The fingerprint matching is based on the normalized Euclidean distance between the two corresponding Zernike moments of stored template and query fingerprint image. Different number of Zernike features has been tested on FVC 2002 Db1 database. The number of Zernike features used in fingerprint matching varies to obtain the minimum EER.

Applying Zernike moment of the complete region of interest resulted in a recognition rate of 77.62%, whereas the enhanced region of interest has increased the recognition rate to 83.41%. The performance of the fingerprint recognition system implemented is evaluated by computing the plot of EER vs. Threshold. The system resulted in minimum error rate of 16.59% at order 12 of Zernike moment. Increasing the moment order started to converge the result and increase EER. The performance of the proposed algorithm is very good as it performed better as compare to other matching schemes as shown by experimental results discussed in Chapter 5.

6.2 Future Work

There are still many good approaches to be applied with Zernike moments to give better performance. One approach taken into account can be loss of precision due to high order computation of Zernike moments. To sort out this, we need to add some noise factor in the image,

and then compare the moment invariance value to the original image in its noisy counter-part. So the precision factor using higher order moments can be computed. The weight function could be computed by taking inverse of variance value and multiplying with their respective moment. This could be applied on the training set of the fingerprint images and then the weights could be applied on the testing images in database.

Weights can be applied on Zernike moment feature vector through machine learning.

Clustering algorithm is an important topic as Zernike moment feature vector does not perform that well under hierarchical clustering. Clustering the image won't need the scaling of images as well.

Another approach to improve the performance for fingerprint recognition using moment features is to use wavelet moment invariants. These moments not only handle rotation of images globally but also rotationally invariant local information of interested image.

For Zernike moments based fingerprint matching, further research need to be done on reducing the computation time that was 9~10 seconds. The EER can be reduced further. It can be done by increasing the ZMI feature (i.e. by increasing order of moment). Further different types of moments and techniques could be evolved, which could be combined with this approach to make it better in performance.

Some more areas of improvement are suggested below:

(i) Region selected to extract features from should be optimal.

(ii) By registering a fingerprint image, a better performance can be expected.

(iii) By exploring more on region of interest, a better system can be implemented.

(iv) By optimizing the algorithm for calculation of Zernike Moments, computational effort can be reduced.

(v) To increase verification accuracy in matching, two different fingers (thumb and right index) of a person can be used separately in verification. None of the two fingers of the same person are similar. This should improve verification accuracy.

(vi) In military application where security is very high, verification can be done using all the fingers of one hand. This means that 5 fingers are used in matching and this will increase the accuracy of biometric system.

Annexure A: List of Abbreviations

Abbreviations	Meanings
Db1	Database 1
EER	Equal Error Rate
FAR	False Accept Rate
FRR	False Reject Rate
FVC	Fingerprint Verification Competition
GAR	Genuine Accept Rate
GRR	Genuine Reject Rate
ROC	Receiver Operating Curve
ROI	Region of Interest
TSR	Total Success Rate
ZM	Zernike Moment

References

[1] Lin Hong, "Automatic Personal Identification Using Fingerprints", PhD Thesis, Michigan State University, 1998.

[2] Salil Prabhakar, "Fingerprint Classification and Matching Using a Filterbank", PhD Thesis, Michigan State University, 2001.

[3] R. W. Frischholz and U. Dieckmann, “Bioid: A Multimodal Biometric Identification System”, IEEE Computer, Vol. 33, No. 2, pp. 64-68, 2000.

[4] L. Hong, "Automatic Personal Identification Using Fingerprints", PhD Thesis, Michigan State University, 1998.

[5] A. K. Jain, L. Hong, and S. Pankanti, “Biometric identification”, Comm. ACM, pages 91–98, Feb 2000

[6] A. K. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition”, *IEEE* Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, pp. 4-20, January 2004.

[7] S. Pankanti, S. Prabhakar, and A. K. Jain, “On the individuality of fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 8, pp. 1010-1025, 2002.

[8] A. K. Jain, S. Prabhakar, and S. Pankanti, “On the similarity of identical twin fingerprints”, Pattern Recognition, vol. 35, no. 8, pp. 2653-2663, 2002.

[9] F. Galton, “Finger-Prints”, 1892.

[10] F. Galton, “Finger-Print Directories”, 1895.

[11] E. Henry, “The Classification and Uses of Finger Prints”, December 1900.

[12] S. Prabhakar, "Fingerprint Classification and Matching Using a Filterbank", PhD Thesis Michigan State University, 2001.

[13] Access Control Applications using Optical Computing. http://www.mytec.com/, 1997

[14] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer Verlag, June 2003.

[15] M. U. Munir, M. Y. Javed, “Fingerprint Quality estimation and matching algorithms”, National University of Science and Technology, College of Mechanical and Electrical engineering , 2013.

[16] N. Ratha, S. Chen, and A. K. Jain, “Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images”, Pattern Recognition, Vol. 28, No.11, pp. 1657-1672, 1995.

[17] S. Gold and A. Rangarajan, “A graduated assignment algorithm for graph matching”, IEEE Trans. Pattern Anal. Machine Intell., vol. 18, no. 4, pp. 377–388, 1996.

[18] D. Maio and D. Maltoni, “Direct gray-scale minutiae detection in fingerprints, "IEEE Transactions on PAMI, vol. 19, pp. 27-40, Jan 1997.

[19] A. K. Jain, A. Ross, and S. Prabhakar, “Fingerprint matching using minutiae and texture features," in Proc. International Conference on Image Processing (ICIP), (Thessaloniki, Greece), pp. 282{285, Oct 2001.

[20] A.K. Jain, S. Prabhakar, L. Hong and S. Pankanti, "FingerCode: A Filterbank for Fingerprint Representation and Matching", Proc. IEEE Conference on CVPR, Colorado, Vol. 2, pp. 187-193, June 23-25, 1999.

[21] A. K. Jain, S. Prabhakar, L. Hong and S. Pankanti, "Filterbank-based Fingerprint Matching", IEEE Transactions on Image Processing, Vol. 9, No.5, pp. 846-859, May 2000.

[22] A. Ross, J. Reisman, and A. K. Jain, Fingerprint Matching Using Feature Space Correlation. Proc. of Post-ECCV Workshop on Biometric Authentication, LNCS 2359, pp.48-57, Denmark, 2002.

[23] K. Ito, H. Nakajima, K. Kobayashi, T. A.T. Higuchi, “A Fingerprint Matching Algorithm Using Phase-Only Correlation”, IEICE Trans, Fundamentals, Vol. E87-A, No.3, March 2004.

[24] C.D. Kuglin and D.C. Hines, “The phase correlation image alignment method”, Proc. Int. Conf. on Cybernetics and Society, pp. 163-165, 1975.

[25] T. Kenji, T. Aoki, Y. Sasaki, T. Higuchi, and K. Kobayashi, “High-accuracy subpixel image registration based on phase-only correlation”, IEICE Trans. Fundamentals, vol.E86-A, no.8, pp.1925-1934, Aug. 2003.

[26] Jin Bo, Tang Hua Ping, Xu Ming Lan, “Fingerprint Singular Point Detection Algorithm by Poincaré Index”, ISSN: 1109-2777 Issue 12, Volume 7, December 2008.

[27] H. A. Qader, A. R. Ramli, S. Al-Haddad, “ Fingerprint Recognition Using Zernike Moments”, The International Arab Journal of Information Technology, Vol. 4, No. 4, 2007, pp. 372-376.

[28] Hu M. K, " Visual Pattern recognition by moments invariant", IRE transaction Information theory, vol. IT-8, no. 2, pp 179-187, 1962.

[29] Tan TZ, Ning XB, Yin YL, Zhan XS, Chen Y, "A method for singularity detection in fingerprint images" [J]. Journal of Software, 2003, 14(6):1082-1088.

[30] David G. Lowe, " Distinctive image features from scale-invariant keypoints", International Journal of Computer Vision, 60, 2 (2004), pp. 91-110.

[31] David G. Lowe, " Object Recognition from Local Scale-Invariant Features", Proc. of the International Conference on Computer Vision,Corfu (Sept. 1999).

[32] Herbert Bay , Andreas Ess , Tinne Tuytelaars , Luc Van Gool, "Speeded-Up Robust Features (SURF)", Computer Vision and Image Understanding 110 (2008) 346–359.

[33] K. Woods, W.P. Kegelmeyer, and K.W. Bowyer, "Combination of Multiple Classifiers Using Local Accuracy Estimates," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 4, pp. 405-410, Apr. 1997.

[34] A. Khotanzad, Y.H. Hong, "Invariant image recognition by Zernike moments", IEEE Trans.Pattern Anal. Mach. Intell. 12 (5) (1990) 489–497.

[35] M. R. Teague, "Image analysis via the general theory of moments", J. Opt. Soc. Amer. 70 (1980) 920-930.

[36] M.K. Hu, "Visual pattern recognition by moment invariants", IRE Trans. Info. Theory IT-8(1962) 179–187.

[37] R. Mukundan, "Image analysis by Tchebichef moments", IEEE Trans. on Image Proc. 10 (9) (2001) 1357-1364.

[38] C.-H. The, R.T. Chin, "On image analysis by the method of moments", IEEE Trans. Pattern Anal. Mach. Intell. 10 (4) (1988) 496–513.

[39] F. Zernike, Physica, vol. 1, p. 689, 1934.

[40] D. Sim, H. Kim, R. Park, "Invariant texture retrieval using modified Zernike moments", Image Vis. Comput. 22 (2004) 331–342.

[41] A.K. Jain, L. Hong, S. Pankanti and R. Bolle, "An Identity Authentication System Using Fingerprints", Proc. IEEE, 85 (9) (1997) 1365-1388.

[42] F. Benhammadi, M.N. Amirouche, H. Hentous, K.B. Beghdad, M. Aissani, "Fingerprint matching from minutiae texture maps", Pattern Recognit. 40 (1) (2007) 189–197.

[43] J. Liu, Z. Huang, K. Chan, “Direct minutiae extraction from gray-level fingerprint image by relationship examination”, International Conference on Image Proc. 2 (2000) 427–430.

[44] J. C. Yang, D. S. Park, “A fingerprint verification algorithm using tessellated invariant moment features”, Neurocomputing 71 (2008) 1939– 1946.

[45] L. Wang, G. Healey, “Using Zernike moments for the illumination and geometry invariant classification of multispectral texture”, IEEE Trans. on Image Proc. 7 (2) (1998) 196–203.

[46] D. Maio, L. Nanni, “An efficient fingerprint verification system using integrated gabor filters and Parzen Window Classifier”, Neurocomputing, 68 (2005) 208–216.

[47] T. Amornraksa, S. Tachaphetpiboon, “Fingerprint recognition using DCT features, Electron”. Lett. 42 (9) (2006) 522–523.

[48] A.T.B. Jin, D.N.C. Ling, O.T. Song, “An efficient fingerprint verification system using integrated wavelet and Fourier-Mellin invariant transform”, Image Vis. Comput. 22 (6) (2004) 503–513.

[49] M. Tico, P. Kuosmanen, J. Saarinen, “Wavelet domain features for fingerprint recognition, Electron”. Lett. 37 (1) (2001) 21–22.

[50] A. Ross, A. K. Jain, and J. Reisman, "A Hybrid Fingerprint Matcher", Pattern Recognit. 36 (7) (2003) 1661-1673.

[51] L. Nanni, A. Lumini, “A hybrid wavelet-based fingerprint matcher, Pattern Recognit”, 40 (11) (2007) 3146–3151.

[52] A.K. Jain, L. Hong and R. Bolle, "On-line Fingerprint Verification", IEEE Trans. Pattern Anal. Mach. Intell. 19 (4) (1997)302-314.

[53] L.Nanni, A.Lumini, “A novel method for fingerprint verification that approaches the problem as a two-class pattern recognition problem”, Neurocomputing, 69 (2006) 846–849.

[54] M. U. Munir, M. Y. Javed, “Fingerprint Matching using Ridge Patterns”, Proceedings of the 1st International Conference on Information & Communication Technologies (ICICT), pp. 116-120, Karachi, August 27-28, 2005.

[55] M. U. Munir, M. Y. Javed, “Ridge Feature based Fingerprint Verification”, Proceedings of National Conference on Information Technology and Applications, pp. 56-63, Quetta, Pakistan, April 21- 22, 2005.

[56] M. U. Munir, M. Y. Javed , “Fingerprint Matching using Gabor Filters”, Proceedings of the National Conference on Emerging Technologies (NCET), pp. 147-151, Karachi, December 18-19, 2004.

[57] D. Maio, D. Maltoni, R. Cappelli, FVC2002 Fingerprint Verification Competition. August 2000. http://bias.csr.unibo.it/fvc2002/databases.asp.

[58] M. U. Munir, M. Y. Javed, S. A. Khan, "Fingerprint Quality Estimation and Matching Algorithms", 2012