A Novel Approach to Fingerprint Identification

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Software Engineering

Submitted By
Ishdeep Singla
(Roll No. 801131012)

Under the supervision of:
Er. Karun Verma
Assistant Professor
C.S.E.D, Thapar University

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

June 2011

Certificate

I hereby certify that the work which is being presented in the thesis entitled, ***A Novel Approach to Fingerprint Identification,*** in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Software Engineering* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Er. Karun Verma* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Ishdeep Singla

Ishdeep Singla

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

15/7/13

Er.Karun Verma
C.S.E.D,
Thapar University

Countersigned by

(Dr. Maninder Singh)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. K. Mohapatra) 15/7
Dean (Academic Affairs)
Thapar University
Patiala

i

Acknowledgement

First of all, I am thankful to God for all the blessings and showing me the right direction. Due to the mercy of God, it has been made possible for me to reach so far.

I wish to express my deep gratitude to Er.Karun Verma, Assistant Professor, Computer Science and Engineering Department, Thapar University, Patiala for providing his support throughout the span of my thesis. This work would not have been possible without his encouragement and valuable guidance.

I am also thankful to Dr. Maninder Singh, Head, Computer Science and Engineering Department for his kind help and cooperation. I express my gratitude to all the staff member of Computer Science and Engineering Department for providing me all the facilities required for the completion of my thesis work.

I express my heartfelt thanks to my parents, my sisters and my well wishers for their cooperation, which they were always ready to extend. At the end, I want to express my appreciation to every person who contributed with either inspirational or actual work to this thesis.

Ishdeep Singla

Abstract

In biometrics fingerprint is the widely and oldest technology used as identification. In this thesis a database is has been created from the extracted minutiae points. Database is designed using B Tree indexing techniques. By using this technique there is no need of comparing fingerprint image with other fingerprint. The B Tree algorithm further works on the computational algorithm based on minutiae points distance calculations. Moreover, it is known that everyone has unique fingerprint, but no mathematical proof has been presented which can present as it's hard to match some fingerprint patterns with whole world's patterns. In this paper a mathematical proof on the basis of adjacent minutiae points distance calculation has been presented. This calculation shows that every fingerprint is unique. Further by using extracted minutiae a database has been designed. As no actual image comparison is presence hence it increase the searching speed and decrease the database size.

Table of Contents

List of Figures

List of Tables

Chapter 1

Biometrics

1.1 History

The word "biometrics" is combination of two Greek words bio (life) and metric (to measure). As biometrics was not in the use in most of the counties until the late nineteenth century, it was being used in China by at least the fourteenth century [5]. According to the writer Joao de Barros he has written that Chinese merchants used palm prints technology to distinguish children from each other. He used paper and ink for this purpose.

In the West, identification relied heavily on "photographic memory" until Alphonse Bertillon, a French police desk clerk and anthropologist, developed the "anthropometric" system (later known as Bertillonage) in 1883. It was the first precise, scientific system widely used to identify criminals. It turned biometrics into a field of study. It involved precisely measuring certain lengths and widths of the head and body, as well as recording individual markings such as tattoos and scars. Bertillon's system was widely adopted in the West until its flaws became apparent—mainly problems associated with differing methods of measurement and changing measurements [49]. After that, Western police forces turned to fingerprinting essentially the same system seen in China hundreds of years earlier.

Until recently, fingerprinting was used mainly for forensics and criminal identification. With the development of biometrics technologies, silicon-based sensors that produce digital images of the fingerprint have replaced printer's ink, and this new approach can be used as a means to secure access to a place (such as an office) or device (such as a computer)[50]. Moreover, the scope of biometrics has been expanded to include many different methods involving the measurement of various physical and behavioral traits.

1.2 Applications

Applications of biometrics can only be limited by limiting one's imagination. Biometric technology is now being used in almost every area. Not only that, but various types of biometric systems are being used to achieve various functionalities. We have shortlisted a few highly popular applications of biometrics technology. Although this list is no way complete it is simply an effort to list a few of the more popular biometric applications [14].

- Biometric Time Clocks or Biometric time and attendance systems, which are being increasingly used in various organizations to control employee timekeeping.
- Biometric safes and biometric locks, provides security to the homeowners.
- Biometric access control systems, providing strong security at entrances.
- Biometric systems are also developed for securing access to pc's and providing single logon facilities.
- Wireless biometrics for high end security and providing safer transactions from wireless device.
- Applications of biometrics technology in identifying DNA patterns for identifying criminals, etc.
- Biometrics airport security devices are also deployed at some of the world's famous airports to enhance the security standards.

1.3 Benefits of Biometrics

Biometrics allows you to replace "what you have" and "what you know" security adages with the all important "who you are" byword, hence contributing one of the most important benefits to the security arena [19].

Advantages of biometrics will help in your quest to curb the "Why Biometrics" question. We have enlisted some of the most sought after advantages of biometrics for you;

- **Increase security** - Provide a convenient and low-cost additional tier of security.

- Reduce fraud by employing hard-to-forge technologies and materials [1]. For e.g. minimize the opportunity for ID fraud, buddy punching.
- Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For e.g. prevent unauthorized use of lost, stolen or "borrowed" ID cards.
- Reduce password administration costs.
- Replace hard-to-remember passwords which may be shared or observed.
- Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access
- Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN!
- Offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time & Attendance.

1.4 Disadvantages of Biometric

So why do not we use biometrics everywhere instead of passwords because nothing is perfect, and biometric authentication methods also have their own shortcomings. As given bellow [23]:

- First of all the performance of biometric systems is not ideal yet. Biometric systems still need to be improved in the terms of accuracy and speed. Biometric systems with the false rejection rate under 1% (together with a reasonably low false acceptance rate) are still rare today. Although few biometric systems are fast and accurate (in terms of low false acceptance rate) enough to allow identification, (automatically recognising the user identity), most of current systems are suitable for the verification only, as the false acceptance rate is too high.
- The fail to enrol rate brings up another important problem. Not all users can use any given biometric system. People without hands cannot use fingerprint or hand-based systems. Visually impaired people have difficulties using iris or retina based techniques. As not all users are able to use a specific biometric system, the authentication system must be extended to handle users falling

into the FTE category. This can make the resulting system more complicated, less secure or more expensive. Even enrolled users can have difficulties using a biometric system. The FTE rate says how many of the input samples are of insufficient quality. Data acquisition must be repeated if the quality of input sample is not sufficient for further processing and this would be annoying for users [23].

- Biometric systems can potentially be quite troublesome for some users [1]. These users find some biometric systems intrusive or personally invasive. Even if no biometric system is really dangerous, users are occasionally afraid of something they do not know much about [23].
- Lack of standards (or ignorance of standards) may also possess a serious problem [13]. Two similar biometric systems from two different vendors are not likely to interoperate at present.
- The finger print of those people working in Chemical industries is often affected. Therefore these companies should not use the finger print mode of authentication.

1.5 Characteristics in Biometrics

These are the important factors necessary for any effective biometric system: accuracy, speed and throughput rate, acceptability to users, uniqueness [27] of the biometric organ and action, resistance to counterfeiting, reliability, data storage requirements, enrolment time, intrusiveness of data collection, and subject and system contact requirements [55].

Types of characteristics:

Accuracy: Accuracy is the most critical characteristic of a biometric identifying verification system. If the system cannot accurately separate authentic persons from impostors [29] [33], it should not even be termed a biometric identification system.

False Reject Rate: The rate, generally stated as a percentage, at which authentic, enrolled persons are rejected as unidentified or unverified persons by a biometric system is termed the false reject rate. False rejection is sometimes called a Type I error. In access control [44], if the requirement is to keep the “bad guys” out, false rejection is considered the least important error. However, in other biometric

applications, it may be the most important error. When used by a bank or retail store to authenticate customer identity and account balance [56], false rejection means that the transaction or sale (and associated profit) is lost, and the customer becomes upset. Most bankers and retailers are willing to allow a few false accepts as long as there are no false rejects [25].

False rejections also have a negative effect on throughput, frustrations, and unimpeded operations, because they cause unnecessary delays in personnel movements. An associated problem that is sometimes incorrectly attributed to false rejection is failure to acquire. Failure to acquire occurs when the biometric sensor is not presented with sufficient usable data to make an authentic or impostor decision. Examples include smudged prints on a fingerprint system, improper hand positioning on a hand geometry system, improper alignment on a retina or iris system, or mumbling on a voice system. Subjects cause failure to acquire problems, either accidentally or on purpose [27].

False Accept Rate: The rate generally stated as a percentage, at which unenrolled or impostor persons are accepted as authentic, enrolled persons by a biometric system is termed the false accept rate. False acceptance is sometimes called a Type II error. This is usually considered to be the most important error for a biometric access control system [19].

Crossover Error Rate (CER): This is also called the equal error rate and is the point, generally stated as a percentage, at which the false rejection rate and the false acceptance rate are equal. This has become the most important measure of biometric system accuracy.

All biometric systems have sensitivity adjustment capability [1]. If false acceptance is not desired, the system can be set to require (nearly) perfect matches of enrolment data and input data. If tested in this configuration, the system can truthfully be stated to achieve a (near) zero false accept rate. If false rejection is not desired, this system can be readjusted to accept input data that only approximate a match with enrolment data. If tested in this configuration, the system can be truthfully stated to achieve a (near) zero false rejection rate. However, the reality is that biometric systems can operate only on one sensitivity setting at a time. The reality is also that when system sensitivity is set to minimize false acceptance, closely matching data will be spurned, and the false rejection rate will go up significantly. Conversely, when system

sensitivity is set to minimize false rejects [2], the false acceptance rate will go up notably. Thus, the published (i.e., truthful) data tell only part of the story. Actual system accuracy in field operations may even be less than acceptable. This is the situation that created the need for a single measure of biometric system accuracy. The crossover error rate (CER) provides a single measurement that is fair and impartial in comparing the performance of the various systems. In general, the sensitivity setting that produces the equal error will be close to the setting that will be optimal for field operation of the system. A biometric system that delivers a CER of 2% will be more accurate than a system with a CER of 5% [15].

Speed and Throughput Rate: The speed and throughput rate are the most important biometric system characteristics. Speed is often related to the data processing capability of the system and is stated as how fast they accept or reject decision is annunciates. In actuality, it relates to the entire authentication procedure: stepping up to the system; inputting the card or PIN (if a verification system); input of the physical data by inserting a hand or finger, aligning an eye, speaking access words, or signing a name; processing and matching of data files; annunciation of the accept or reject decision; and, if a portal system, movement through and closing the door.

Generally accepted standards include a system speed of 5 seconds from start up through decision annunciation. Another standard is a portal throughput rate of 6 to 10/minute, which equates to 6 to 10 seconds/person through the door. Only in recent years have biometric systems become capable of meeting these speed standards, and, even today, some marketed systems do not maintain this rapidity. Slow speed and the resultant waiting lines and movement delays have frequently caused the removal of biometric systems and even the failure of biometric companies [25].

Acceptability to Users: System acceptability to the people who must use it has been a little noticed but increasingly important factor in biometric identification operations. Initially, when there were few systems, most were of high security and the few users had a high incentive to use the systems; user acceptance was of little interest. In addition, little user threat was seen in fingerprint and hand systems [25].

Biometric system acceptance occurs when those who must use the system — organizational managers and any union present — all agree that there are assets that need protection, the biometric system effectively controls access to these assets, system usage is not hazardous to the health of the users [3], system usage does not

inordinately impede personnel movement and cause production delays, and the system does not enable management to collect personal or health information about the users [51]. Any of the parties can affect system success or removal. Uncooperative users will overtly or covertly compromise, damage, or sabotage system equipment. The cost of union inclusion of the biometric system in their contracts may become too costly. Moreover, management has the final decision on whether the biometric system benefits outweigh its liabilities.

1.6 Types of Biometrics

This section describes the different types of biometric systems: fingerprint systems, hand geometry systems, voice pattern systems [21], iris pattern systems. For each system these characteristics are described: the enrolment procedure and time, the template or file size, the user action required [7], the system response time, any ant counterfeit method, accuracy, field history, problems experienced, and unique system aspects.

1.6.1 Fingerprint Systems

The information in this section is a compilation of information about several biometric identifying verification systems whose technology is based on the fingerprint [11].

Characteristics

1. Data Acquisition: Fingerprint data is acquired when subjects firmly press their fingers against a glass or polycarbonate plate [32]. The fingerprint image is not stored. Information on the relative location of the ridges, whorls, lines [27], bifurcations, and intersections is stored as an enrolled user data base file and later compared with user input data.

2. Enrolment Procedure and Time: As instructed, subject enters a 1- to 9-digit PIN on the keypad. As cued, the finger is placed on the reader plate and then removed. A digitized code is created. As cued, the finger is placed and removed four more times for calibration. The total enrollment time required is less than 2 minutes [13].

3. Template or File Size: Fingerprint user files are generally between 500 and 1,500 bytes.

4. User Actions Required: Nearly all fingerprint-based biometrics are verification systems. The user states identification by entering a PIN through a keypad or by using a card reader then places a finger on the reader plate [22].

5. System Response Time: Visual and audible annunciation of the confirmed and not confirmed decision occurs in 5 to 7 seconds [1].

6. Accuracy: Some fingerprint systems can be adjusted to achieve a false accept rate of 0.0%. Sandia National Laboratories tests of a top-rated fingerprint system in 1991 and 1993 produced a three-try false reject rate of 9.4% and a crossover error rate of 5%.

7. Field History: Thousands of units have been fielded for access control and identity verification for disbursement of government benefits, for example.

8. Problems Experienced: System operators with large user populations are often required to clean sensor plates frequently to remove built-up skin oil and dirt that adversely affect system accuracy [19].

9. Unique System Aspects: To avoid the dirt build-up problem [1], a newly developed fingerprint system acquires the fingerprint image with ultrasound. Claims are made that this system can acquire the fingerprint of a surgeon wearing latex gloves. A number of companies are producing fingerprint-based biometric identification systems.

1.6.2 Hand Geometry System

Hand geometry data, the three-dimensional record of the length, width, and height of the hand and fingers is acquired by simultaneous vertical and horizontal camera images [9].

Characteristics

1. Enrolment Procedure and Time: The subject is directed to place the hand flat on a grid platen, positioned against pegs between the fingers. Four finger-position lights ensure proper hand location. A digital camera records a single top and side view from above, using a 45º mirror for the side view. The subject is directed to withdraw and then reposition the hand twice more. The readings are averaged into a single code and given a PIN. Total enrolment time is less than 2 minutes [3].

2. Template or File Size: The hand geometry user file size is nine bytes.

3. User Actions Required: The hand geometry system operates only as an identification verifier. The user states identification by entering a PIN on a keypad or by using a card reader. When the "place hand" message appears on the unit display, the user places the hand flat on the platen against the pegs. When all four lights confirm correct hand position the data are acquired and a "remove hand" message appears [1].

4. System Response Time: Visual and audible annunciation of the acceptance decision generates in 3 to 5 seconds.

5. Ant counterfeit Method: The manufacturer states that "the system checks to ensure that a live hand is used."

6.Accuracy: Sandia National Laboratories tests have produced a one-try false accept rate less than 0.1%, a three-try false reject rate less than 0.1%, and crossover error rates of 0.2 and 2.2% (i.e., two tests) [16].

7. Field History: Thousands of units have been fielded for access control, college cafeterias and dormitories, and government facilities [1]. Hand geometry was the original biometric system of choice of the Department of Energy and the Immigration and Naturalization Service. It was also used to protect the Athlete's Village at the 1996 Olympics in Atlanta.

8. Problems Experienced: Some of the field applications did not perform up to the accuracy results of the initial Sandia test. There have been indications that verification accuracy achieved when user data bases are in the hundreds deteriorates when the data base grows into the thousands [19].

9. Unique System Aspects: The hand geometry user file code of nine bytes is by far the smallest of any current biometric system. Hand geometry identification systems are manufactured by Recognition Systems, Inc. A variation, a two-finger geometry identification system is manufactured by Biometric Partners.

1.6.3 Voice Pattern Systems

Up to seven parameters of nasal tones, larynx and throat vibrations, and air pressure from the voice are captured by audio and other sensors.

Characteristics

1. Enrolment Procedure and Time: Most voice systems use equipment similar to a standard telephone. As directed, the subject picks up the handset and enters a PIN on the telephone keypad. When cued through the handset, the subject speaks his or her access phrase, which may be his or her PIN and name or some other four- to six-word phrase. The cue and the access phrase are repeated up to four times. Total enrolment time required is less than 2 minutes.

2. Template or File Size: Voice user files vary from 1,000 to 10,000 bytes, depending on the system manufacturer.

3. User Actions Required: Currently, voice systems operate only as identification verifiers. The user states identification by entering the PIN on the telephone-type keypad. As cued through the handset (i.e., recorded voice stating "please say your access phrase"), the user speaks into the handset sensors [21].

4. System Response Time: Audible response (i.e., "accepted, please enter" or "not authorized") is provided through the handset. Some systems include visual annunciation (e.g., red and green lights or LEDs). Total transaction time is up to 10 to 14 seconds [11].

5. Anti counterfeit Method: Various methods are used including measuring increased air pressure when "p" or "t" sounds are spoken. Some sophisticated systems require the user to speak different words from a list of 10 or more enrolled words in a different order each time the system is used [19].

6. Accuracy: Sandia National Laboratories has reported crossover errors over 10% for two systems they have tested. Other voice tests are being planned [7].

7. Field History: Over 100 systems have been installed, with over 1,000 door access units, at colleges, hospitals, laboratories, and offices [9].

8. Problems Experienced: Background noise can affect the accuracy of voice systems. Access systems are located at entrances, hallways, and doorways, which tend to be busy, high-traffic, and high-noise-level sites.

9. Unique System Aspects: Some voice systems can also be used as an intercom or to leave messages for other system users. There are several companies producing voice-based biometric identification systems [13].

1.6.4 Iris Pattern System

The iris (i.e., the colored portion of the eye surrounding the pupil) has rich and unique patterns of striations, pits, freckles, rifts, fibers, filaments, rings, coronas, furrows, and vasculature. The images are acquired by a standard 1/3 inch CCD video camera capturing 30 images per second, similar to a camcorder[15].

Characteristics

1. Enrolment Procedure and Time: The subject looks at a mirror-like LCD feedback image of his or her eye, cantering and focusing the image as directed. The system creates zones of analysis on the iris image, locates the features within the zones, and creates an Iris Code. The system processes three images, selects the most representative, and stores it upon approval of the operator. A PIN is added to the administrative (i.e., name, address) data file. Total enrolment time required is less than 2 minutes [16].

2. Template or File Size: The Iris Code occupies 256 bytes.

3. User Actions Required: The Iris Scan system can operate as a verifier, but is normally used in full identification mode because it performs this function faster than most systems verify. The user pushes the start button, tilts the optical unit if necessary to adjust for height, and looks at the LCD feedback image of his or her eye, centering and focusing the image. If the system is used as a verifier, a keypad or card reader is interconnected [23].

4. System Response Time: Visual and audible annunciation of the identified or not identified decision occurs in 1 to 2 seconds, depending on the size of the data base. Total throughput time (i.e., start button to annunciation) is 2.5 to 4 seconds with experienced users.

5. Ant counterfeit Method: The system ensures that data input is from a live person by using naturally occurring physical factors of the eye [4].

6. Accuracy: Sandia National Laboratories' test of a preproduction model had no false accepts, low false rejects, and the system "performed extremely well." Sandia has a production system currently in testing. British Telecommunications recently tested the system in various modes [48] and will publish a report in its engineering journal. They report 100% correct performance on over 250,000 Iris Code

comparisons. “Iris recognition is a reliable and robust biometric. Every eye presented was enrolled. There were no False Accepts, and every enrolled eye was successfully recognized.” Other tests have reported a crossover error rate of less than 0.5%.

7. Field History: Units have been fielded for access control and personnel identification at military and government organizations, banks, telecommunications firms, prisons and jails, educational institutions, manufacturing companies, and security companies [9].

8. Problems Experienced: Because this is a camera-based system, the optical unit must be positioned such that the sun does not shine directly into the aperture.

9. Unique System Aspects: The iris of the eye is a stable organ that remains virtually unchanged from 1 year of age throughout life [46]. Therefore, once enrolled, a person will always be recognized, absent certain eye injuries or diseases. Iris Scan Inc. has the patents worldwide on iris recognition technology.

1.7 Working of Different Biometric Techniques

Workings of all biometric techniques are presented bellow.

1.7.1 Fingerprint Scanner

Fingerprints are one of those bizarre twists of nature. Human beings happen to have built-in, easily accessible identity cards. You have a unique design, which represents you alone, literally at your fingertips [45]. How did this happen? People have tiny ridges of skin on their fingers because this particular adaptation was extremely advantageous to the ancestors of the human species. The pattern of ridges and "valleys" on fingers make e it easier for the hands to grip things [1], in the same way a rubber tread pattern helps a tire grip the road. The other function of fingerprints is a total coincidence. Like everything in the human body, these ridges form through a combination of genetic and environmental factors. The genetic code in DNA gives general orders on the way skin should form in a developing fetus, but the specific way it forms is a result of random events. The exact position of the fetus in the womb at a particular moment and the exact composition and density of surrounding amniotic fluid decides how every individual ridge will form [25].

Figure 1: Finger Print Pattern

So, in addition to the countless things that go into deciding your genetic make-up in the first place, there are innumerable environmental factors influencing the formation of the fingers. Just like the weather conditions that form clouds or the coastline of a beach, the entire development process is so chaotic that, in the entire course of human history, there is virtually no chance of the same exact pattern forming twice. Consequently, fingerprints are a unique marker for a person, even an identical twin. And while two prints may look basically the same at a glance, a trained investigator or an advanced piece of software can pick out clear, defined differences. This is the basic idea of fingerprint analysis, in both crime investigation and security. A fingerprint scanner's job is to take the place of a human analyst by collecting a print sample and comparing it to other samples on record. In the next few sections, we'll find out how scanners do this.

1.7.2 Iris Scanning

Iris scanning can seem very futuristic, but at the heart of the system is a simple CCD digital camera. It uses both visible and near-infrared light to take a clear, high-contrast picture of a person's iris. With near-infrared light, a person's pupil is very black, making it easy for the computer to isolate the pupil and iris.

When you look into an iris scanner, either the camera focuses automatically or you use a mirror or audible feedback from the system to make sure that you are positioned correctly [1]. Usually, your eye is 3 to 10 inches from the camera. When the camera takes a picture, the computer locates:

- The centre of the pupil
- The edge of the pupil
- The edge of the iris
- The eyelids and eyelashes

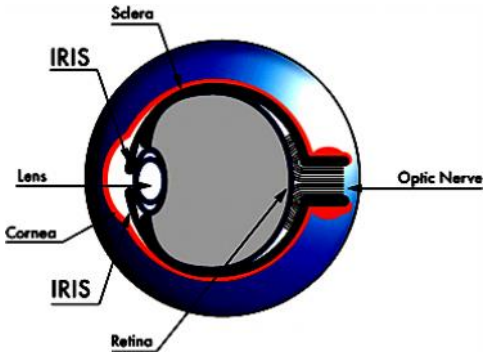


Figure 2: Internal Structure of eye [35]

It then analyzes the patterns in the iris and translates them into a code. Iris scanners are becoming more common in high-security applications because people's eyes are so unique (the chance of mistaking one iris code for another is 1 in 10 to the 78th power. They also allow more than 200 points of reference for comparison, as opposed to 60 or 70 points in fingerprints. The iris is a visible but protected structure [1], and it does not usually change over time, making it ideal for biometric identification. Most of the time, people's eyes also remain unchanged after eye surgery, and blind people can use iris scanners as long as their eyes have irises. Eyeglasses and contact lenses typically do not interfere or cause inaccurate readings [26].

1.7.3 Facial Recognition Technology

Pick someone's face out of a crowd, extract the face from the rest of the scene and compare it to a database of stored images. In order for this software to work [12], it has to know how to differentiate between a basic face and the rest of the background. Facial recognition software is based on the ability to recognize a face and then measure the various features of the face.

Every face has numerous, distinguishable **landmarks**, the different peaks and valleys that make up facial features. Facet defines these landmarks as **nodal points**. Each

human face has approximately 80 nodal points. Some of these measured by the software are:

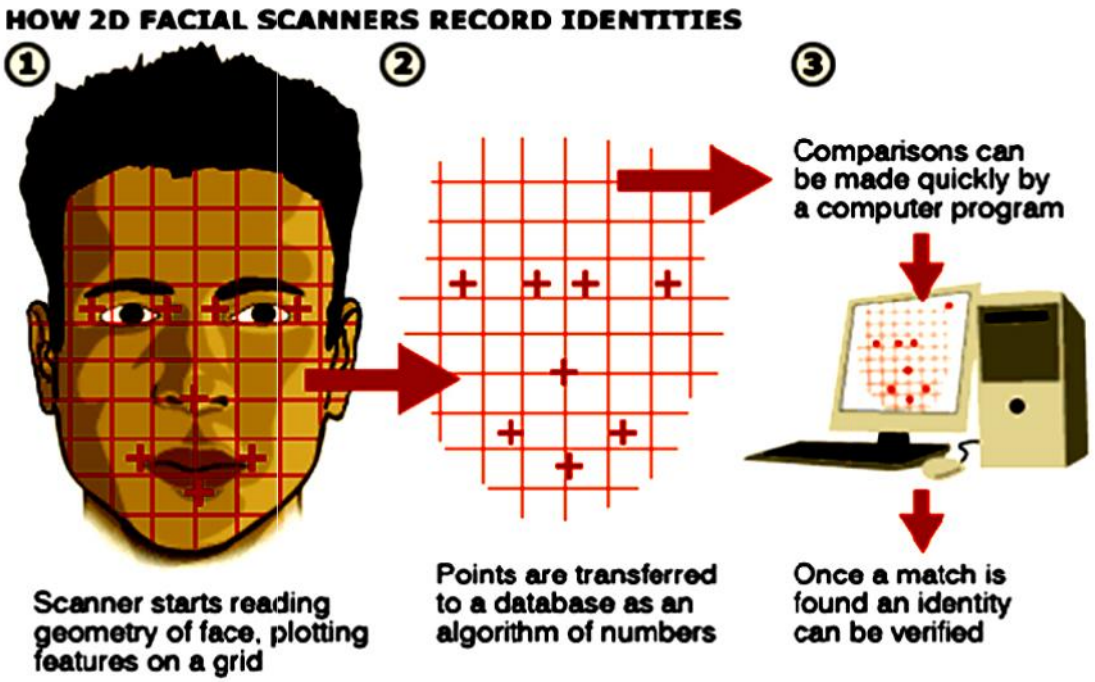


Figure 3: Working of face Scanner [29]

Distance between the eyes

- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

These nodal points are measured creating a numerical code, called a **face print**, representing the face in the database. In the past, facial recognition software has relied on a 2D image to compare or identify another 2D image from the database. To be effective and accurate, the image captured needed to be of a face that was looking almost directly at the camera, with little variance of light or facial expression from the image in the database. This created quite a problem. In most instances the images were not taken in a controlled environment. Even the smallest changes in light or orientation could reduce the effectiveness of the system, so they couldn't be matched to any face in the database, leading to a high rate of failure. In the next section, we will look at ways to correct the problem [24]

1.7.4 Hand and Finger Geometry

People's hands and fingers are unique -- but not as unique as other traits, like fingerprints or irises. That's why businesses and schools, rather than high-security facilities, typically use hand and finger geometry readers to authenticate users, not to identify them. Disney theme parks, for example, use finger geometry readers to grant ticket holders admittance to different parts of the park. Some businesses use hand geometry readers in place of timecards.

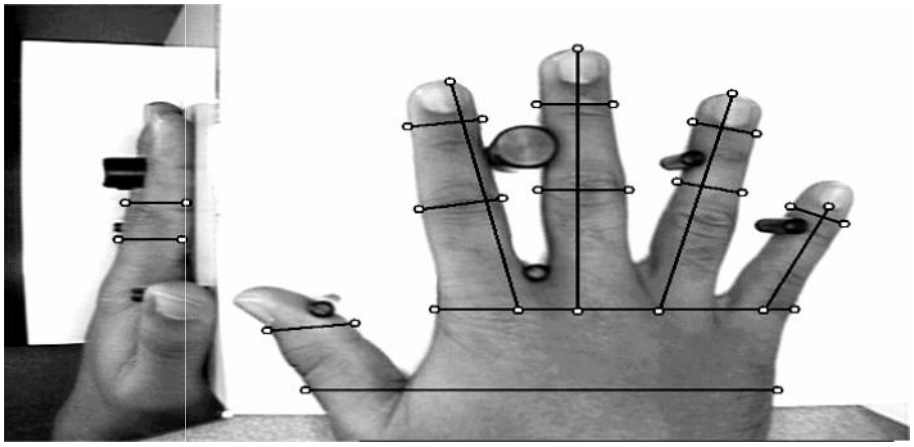


Figure 4: Hand Geometry Scanning [23]

Systems that measure hand and finger geometry use a digital camera and light. To use one, you simply place your hand on a flat surface, aligning your fingers against several pegs to ensure an accurate reading. Then, a camera takes one or more pictures of your hand and the shadow it casts. It uses this information to determine the length, width, thickness and curvature of your hand or fingers. It translates that information into a numerical template.

Hand and finger geometry systems have a few strengths and weaknesses. Since hands and fingers are less distinctive than fingerprints or irises, some people are less likely to feel that the system invades their privacy. However, many people's hands change over time due to injury, changes in weight or arthritis. Some systems update the data to reflect minor changes from day to day [2].

For higher-security applications, biometric systems use more unique characteristics, like voices. We'll look at those next.

Chapter 2

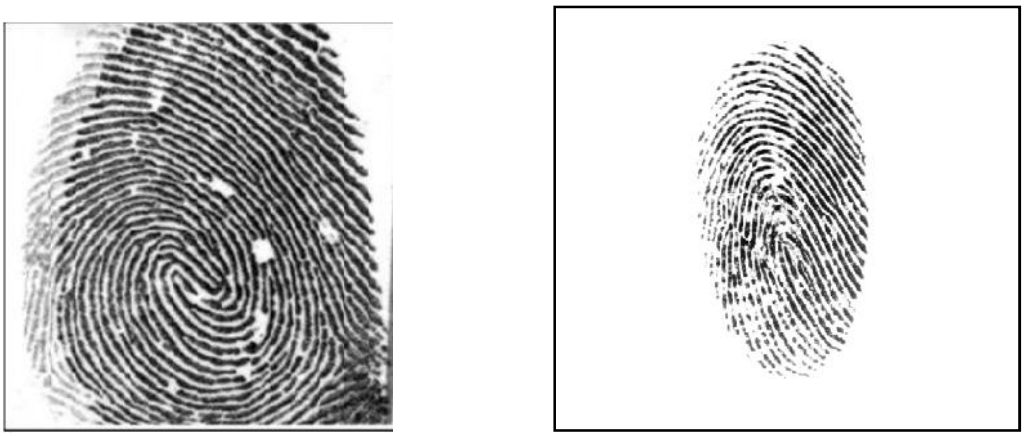
Fingerprint Techniques

2.1 Introduction

In an increasingly digital world, the control over entry of authorized person has become a vital thing. From the personal computer to National security there is big use of identity checking that is Authentication [49]. And biometrics provides automated access to the security systems. It's always better to use some automated methods instead of remembering and filling passwords. In biometrics fingerprint technology is widely used technology, using this technology we need not to carry any identity card. Finger works as identity card, meaning there no tension of forgetting and losing identity cards [2].

2.2 What is Fingerprint?

- Fingerprint is the graphical flow-like ridges. It is present on each and every finger of every human's fingers as shown in Figure 5. Ridges are embedded on all fingers from the very first day of our birth and do not change throughout the life. It may only change if a serious accident such as bruises and cuts or surgery on the fingertips occurs. This property makes fingerprints a very attractive biometric identifier and point of research. Basically, there are two resources for getting fingerprint pattern [1]:
- Scanning an inked impression of a finger is shown in Figure 5(a)
- Using a live-scan fingerprint scanner is shown in Figure 5(b).



(a) (B)

Figure 5: Fingerprint images (a) inked fingerprint (b) live-scan fingerprint [3].

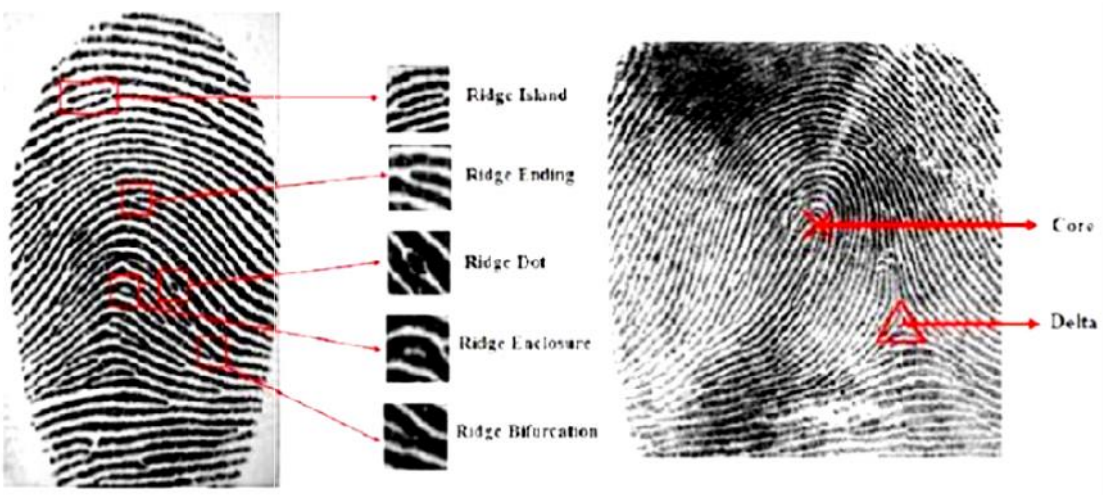
In the above figure 5(b) dark lines is called ridges and the white area that exists between the ridges is called valley or furrow.

2.3 Fingerprint Features

Fingerprint features are those attributes of a fingerprint that may be useful either to classify or to uniquely identify the fingerprint. There are two main types of features, namely, the local features and the global features. The figure 6 (a) shows the local features and the below Figure 6 (b) shows the global features.

2.3.1 Global Features

The fingerprint global features are identified by means of the local orientation of the fingerprint ridges, that is, the Orientation Field Curves (OFCs). As shown in figures 6 (b) the Core and the Delta are the features which have been located in central position of fingerprint. A Core is the area around the centre of the fingerprint loop and a Delta is the area where the fingerprint ridges tend to triangulate. Due to their unique property, both play an important role to compare one fingerprint with other fingerprints [4].



(a) (b)

Figure 6: (a) Local Features: Minutiae (b) Global Features: Core and Delta [3]

2.3.2 Local Features

The fingerprint local features are those attributes that give the minutiae details about the fingerprint pattern. Minutiae further provide various ways that the ridges can be discontinuous. A ridge can suddenly end (termination), or can divide into two ridges (bifurcation) as shown in figure 6(a). There is 40-100 minutiae point in a good quality image [8]. And in a fingerprint image of 300x300 pixels the distance between two fingerprints vary between 1-113 pixels. With these features and numerical figures local features has become more suitable to compare fingerprints [4]. There are many methods like cross number are available to extract the minutiae points.

2.4 Fingerprint Classification

It's obvious that with the increase database size complexity and automatic comparison time will also increase. So to reduce the search time and computational complexity, there is a need to classify fingerprint in a precise and consistent manner which will help to reduce search time with less number of comparisons. According to Galton-Henry classification (Galton, 1892 and Henry, 1900) classification, we classify fingerprint images into 5 major classes: plain arch, tented arch, left-loop, right-loop and whorl (a plain and twin loop, respectively).

Arch: In whole fingerprint arch covers only 5 % of the portion. These consist of ridges that run majorly in horizontal manner can say from left to right as shown in

figure 7. There are two types of arches [53] [13] Plain arches and Tented arches. Generally, plain arch has no singular points. While tented arch have one core and one delta.

Loop: Loops cover 60-70 % of whole fingerprint pattern. As the name suggests set of the ridges enters on either side of the fingerprint, bends, touches or crosses the line running from the delta to the core and run back in same direction of the side where the ridge or ridges entered as shown in figure 7. Each loop pattern has is one delta and one core. There can be left loop or right loop.

Whorl: 25-35 % of fingerprint pattern is covered by whorl. In a whorl, more than one ridges moves through at least one circuit. A whorl pattern always consists of two or more deltas. There are two types of whorl plain whorl and double whorl. A plain whorl is the pattern which consists of some ridges which make or partially make a complete circuit with two deltas. Double loop whorl consists of two separate and distinct loops.

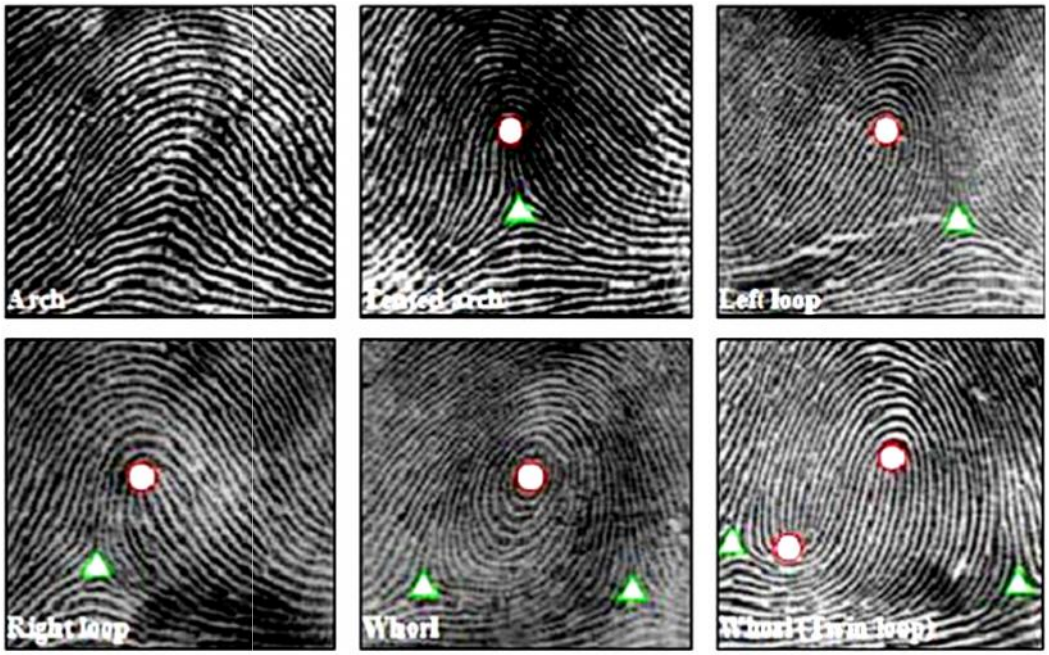


Figure 7: Fingerprint Classes [17]

Chapter 3
Literature Review

3.1 Fingerprint Matching Techniques

There a lot of techniques for matching a fingerprint. There are three most popular methods for matching fingerprints [1] are described below.

3.1.1 Correlation-based matching:

In this method one fingerprint image is superimposed on other. The correlation between corresponding pixels is computed for different alignments and on the basis of these correlations and computations decision is made.

3.1.2 Pattern-based (or image-based) matching:

In pattern based algorithms the basic fingerprint patterns (arch, whorl, and loop) are used to compare fingerprints, between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

3.1.3 Minutiae-based matching**:**

This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets that result in the maximum number of minutiae pairings. In this thesis we have implemented a minutiae based matching technique. This approach has been intensively studied, also is the backbone of the current available fingerprint identification products.

3.2 Minutiae Extraction

A minutiae point matching is the best approach for the matching of fingerprints. The work of minutiae extraction includes some important steps that are Ridge Thinning, Minutiae Marking, False Minutiae Removal and Minutiae Representation.

3.2.1 Ridge Thinning

The main aim of this step is to convert the redundant pixels of ridge into one pixel wide. This will be very helpful in finding minutiae points and to implement minutiae point algorithm. In Matlab there has one very popular morphological thinning function to perform this task.

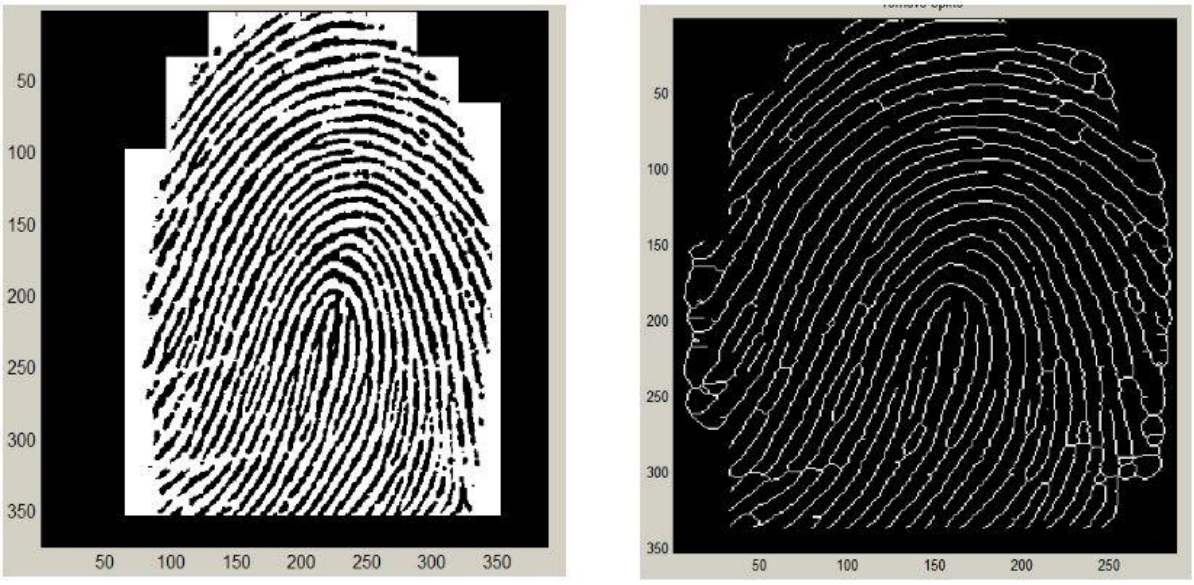
bwmorph(binaryImage,'thin',Inf)

The thinned image is then filtered, again using MATLAB's three morphological functions to remove some H breaks, isolated points and spikes (See Figure 8)

bwmorph(binaryImage,'hbreak',k) → For H breaks

bwmorph(binaryImage,'clean',k) → For isolated points

bwmorph(binaryImage,'spur',k) → Spikes



(a) (b)

Figure 8: Binaries image (b) Thinning image [32]

3.2.2 Minutiae Marking

The name of this algorithm is Crossing Number (CN). It is implemented thinned image. Iteratively a 3x3 pixels wide picture is selected from thinned image then check that if the central pixel is a ridge branch and the central pixel is 1 and has exactly three neighbors of 1's, then its **bifurcation** (See figure 9).

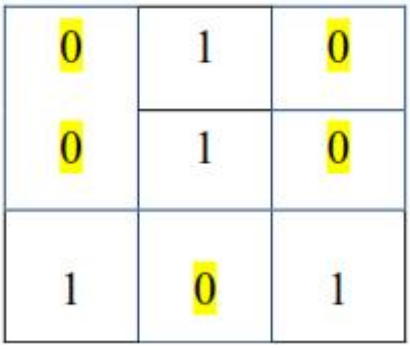


Figure 9: Ridge Bifurcation [9]

If there one central 1 with exactly one 1in its neighborhood, then it's a **ridge ending**. (figure 10).

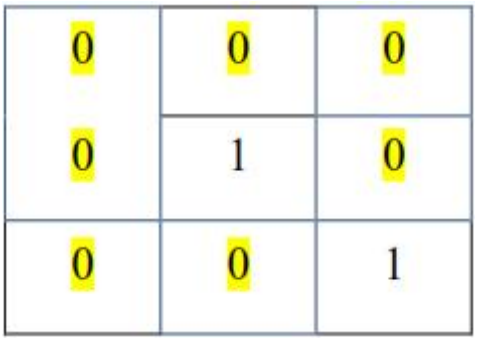


Figure 10: Ridge Termination [9]

3.3 Indexing Techniques

There are many indexing techniques available. But according to work and ease it has been observed that B Tree and B+ Tree techniques would be important for this work.

3.3.1 B Trees

B Trees are multi-way trees. That is each node contains a set of keys and pointers [43]. A B Tree with four keys and five pointers represents the minimum size of a B Tree node. A B Tree contains only data pages [54]. B Trees are dynamic. That is, the height of the tree grows and contracts as records are added and deleted.

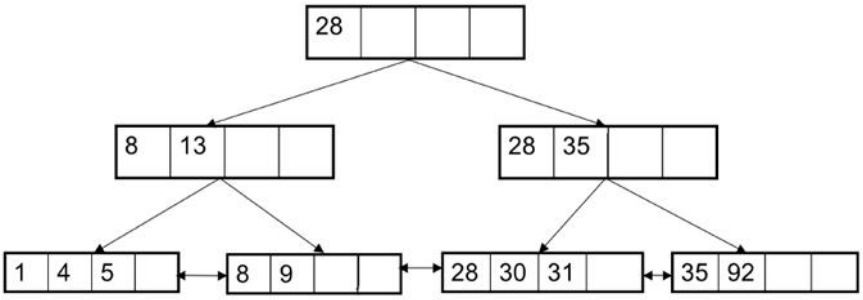


Figure 11: Example of B Tree [43]

3.3.1 B+ Trees

A B+ Tree combines features of ISAM (Indexed Sequential Access Method) and B Trees. It contains index pages and data pages. The data pages always appear as leaf nodes in the tree. The root node and intermediate nodes are always index pages. These features are similar to ISAM. Unlike ISAM, overflow pages are not used in B+ trees [34]. The 9index pages in a B+ tree are constructed through the process of inserting and deleting records. Thus, B+ trees grow and contract like their B Tree counterparts. The contents and the number of index pages reflect this growth and shrinkage. B+ Trees and B Trees use a "fill factor" to control the growth and the shrinkage. A 50% fill factor would be the minimum for any B+ or B tree. As our example we use the smallest page structure. This means that our B+ tree conforms to the following guidelines (figure12).

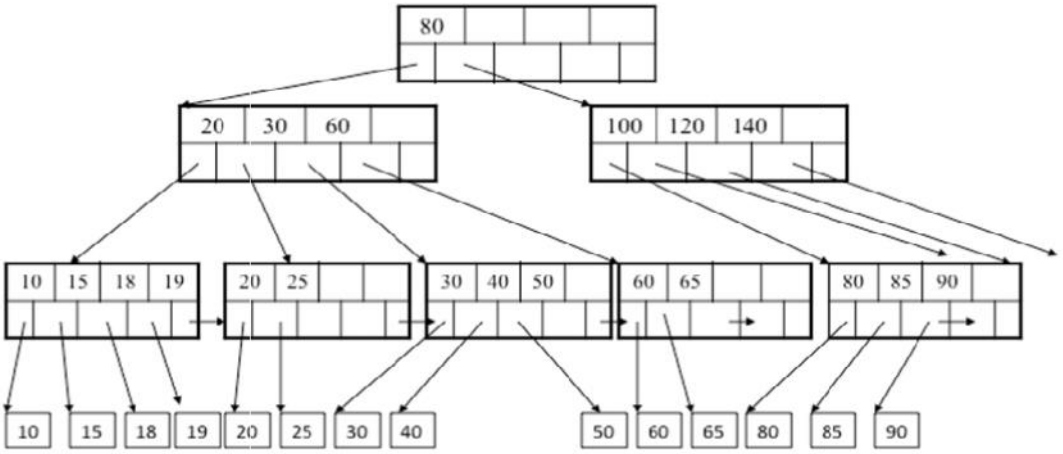


Figure 12: Example of B+ Tree [29]

There is no need to waste extra memory to store each node's pointer. Hence B Tree is best for this work.

Chapter 4

Problem Statement and Methodology

4.1 Problem Statement:

1) To design a system that can manage very large database of fingerprints
2) To design an efficient algorithm for comparing fingerprint.
3) To verify and validate the results.

4.1.1 Verification and Identification:

Two main parts come in the situation which divide whole picture in two parts. One is Identification (Validation) and another is verification.

Identification (1: many or 1: n): identifying an individual based upon comparison of biometrics collected against a database of previously collected samples. Essentially, technologies which are implemented for the purpose of identification will answer the question: "WHO AM I?" [28] Typically, systems established to perform identification are large, include substantial databases of previously collected information, are costly to deploy, and demand processing time to find a match within the database. These types of systems include those used by law enforcement personnel around the globe who maintain large databases of fingerprints or facial images.

Verification (1:1): verifying that an individual is the person that they claim to be, based upon validating a sample collected against a previously collected biometric sample for the individual. When biometric are implemented for verification purposes, they will answer the question: "IS I WHO I SAY I AM? [24] Still there are very less research work done in the field validation i.e. verification. So there must a world level search on the basis of fingerprints. To achieve this task initial and important step is to find correct minutiae points (see figure 13).

Figure 13: Minutiae Points Marking [44]

4.2 Methodology

Before finding minutiae points there are some important steps to be performed (figure 14). As it can see in figure 15 there few steps like Browsing the image, Enhancement, Linearization, Thinning, and minutiae points marking need to be performed.

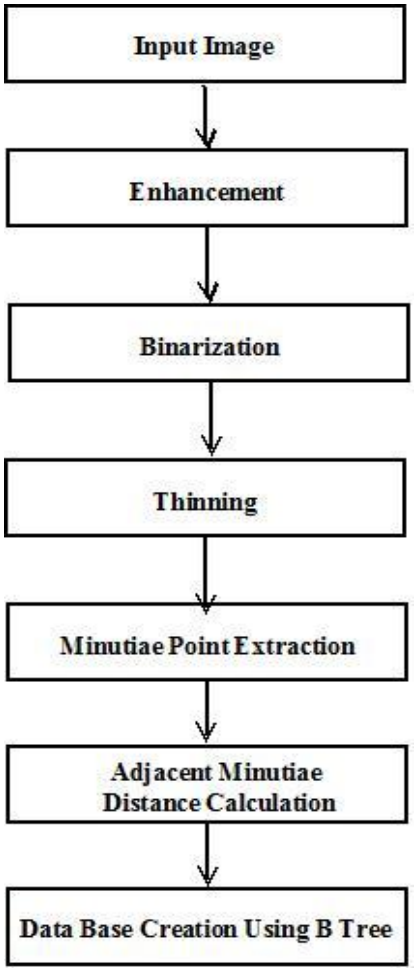


Figure 14: Methodology in Steps

4.2.1 Minutiae Point Extraction Detail

To understand whole work as shown in figure 15, let's understand it step by step.

Input an image:

This step is for selecting any image from our given database. In this step browse the image from set of fingerprint images.

Enhancement:

More recently, significant increasing need for biometric technology in forensic

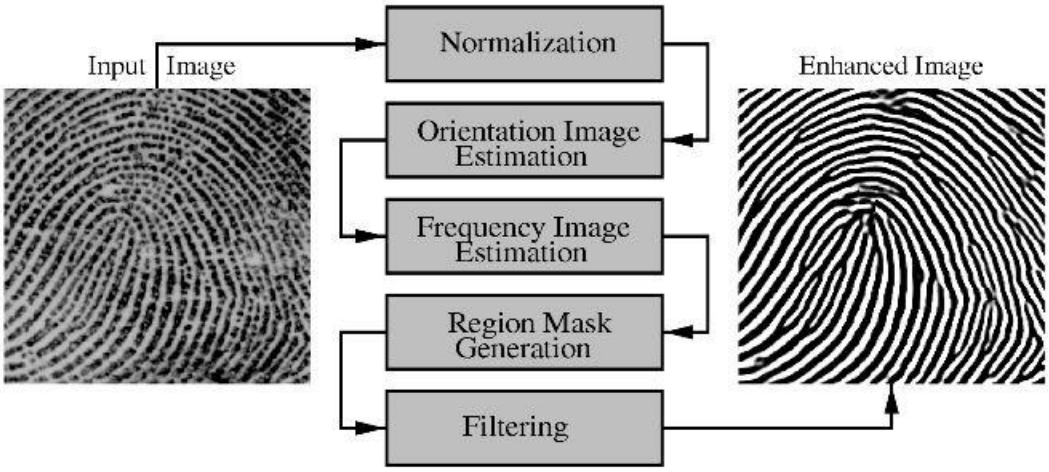


Figure 15: Enhancement [11]

Non-forensic applications invite a lot of efforts and researches for improving current biometric systems [31]. Fingerprint is the first biometric system adopted by law enforcement agencies, and now is also the most widely used system. Most AFISs are based on minutiae matching. The major minutiae features used by AFISs, are endings and bifurcations, which represent terminations and intersections of fingerprint ridge line flows. Although the automatic fingerprint recognition and identification have wide and long practical application, there still exist a lot of challenging and established image processing and pattern recognition problems [10]. Fingerprint image quality is of much importance to achieve high performance in Automatic Fingerprint Identification System (AFIS). Several researches [4] [6] [7] [2] [17] have proposed some enhancement techniques to this end. Enhancement of fingerprint images can be performed on either binary ridge images or direct gray images. Linearization before enhancement will generate more spurious minutiae structures

and lose some valuable original fingerprint information; it also poses more difficulties for later enhancement procedure. Therefore, most enhancement algorithms are performed on gray images directly. But there no need of enhancement because the quality of image is good.

Binarization:

Fingerprint Image Binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows are white. A locally adaptive binarization method is performed to binarize the fingerprint image [5]. Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs. Figure 16 shows the Fingerprint image after adaptive binarization: Binarized image (left), Enhanced gray image (right)

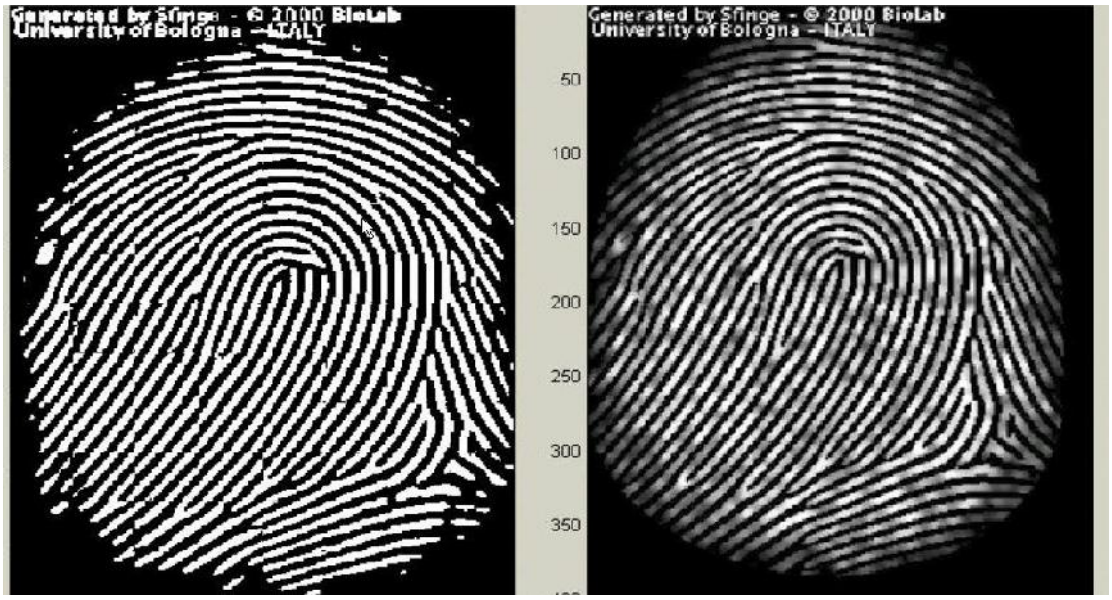


Figure 16: The Fingerprint Image after Adaptive Binarization [31]

Thinning:

Thinning plays a very important role in the preprocessing phase of automatic fingerprint recognition/identification systems. The performance of minutiae extraction relies heavily on the quality of skeletons used [4]. A good fingerprint thinning algorithm can depress image noise and promote the robustness of the minutiae

extraction algorithm which helps improve the overall performance of the system. Many thinning algorithms have been devised and applied to a wide range of applications including, Optical Character Recognition (OCR), biological cell structures and fingerprint patterns [30]. With so many thinning algorithms available, deciding which one is appropriate for a particular application has become very difficult. In an effort to assist fingerprint biometrics developers choose an appropriate thinning algorithm; a study was taken to compare performance of four different thinning algorithms. These four algorithms are implemented and their performance evaluated and compared. The algorithms are compared in terms of the quality of the skeletons they produce (i.e. connectivity and spurious branches) as well as the time complexity associated with each algorithm [9]. Results show that faster algorithms have difficulty preserving connectivity. Zhang and Suen's algorithm gives the least processing time, while Guo and Hall's algorithm produces the best skeleton quality [13] [20]. Thinning is a process of extracting a skeleton from an object in a digital image [10]. A skeleton of an image can be thought of as a one-pixel thick line through the middle of an object which preserves the topology of that object. Thinning is a fundamental preprocessing step in many image processing and pattern recognition algorithms [1]. Thinned images (skeletons) are easier to process and they reduce processing time for the subsequent operations. Many thinning algorithms have been developed in the past three decades [1]. Two major approaches of thinning digital patterns can be categorized into iterative boundary removal algorithms and non-iterative distance transformation algorithms (See Figure 17). Iterative boundary removal algorithms delete pixels on the boundary of a pattern repeatedly until only unit pixel-width thinned image remains. Non-iterative distance transformation algorithms are not appropriate for general applications since they are not robust, especially for patterns with highly variable stroke directions and thicknesses. Thinning based on iterative boundary removal can be divided into sequential and parallel algorithms [2].

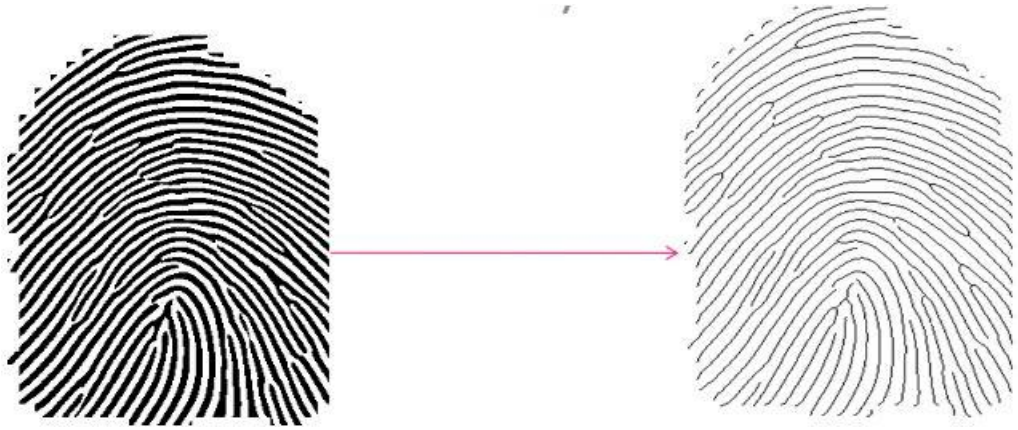


Figure 17: (a.) Binarized Image (b.) Thinned Image [52]

4.3 Create the database

1. Take input minutiae to the system and track it's all the minutiae points and then start drawing lines top to down and left to right starting from first minutiae point to second so on till end. (figure 19 showing minutiae track pattern)
2. Now measure the distances between two adjacent minutiae in millimeters. Measure lengths from above pattern in mm are 0.5, 0.6, 0.7, 0.3, 0.8, 1.1, 0.9, 0.5, 1.0, 0.5, and 0.6
3. Now write measure length in 05 06 07 03 08 11 09 05 10 05 06 called "trace" (say).

1. Even 's Sum	2. Odd's Sum	3. Multiple of 3's Sum

Figure 18: Trace Packet

4. Apply B+ tree algorithm on Even's Sum by considering as *first level,* Odd's Sum by considering as *second level* and Multiple of 3's sum by considering as *third level B+ Tree* as shown in Figure 19.

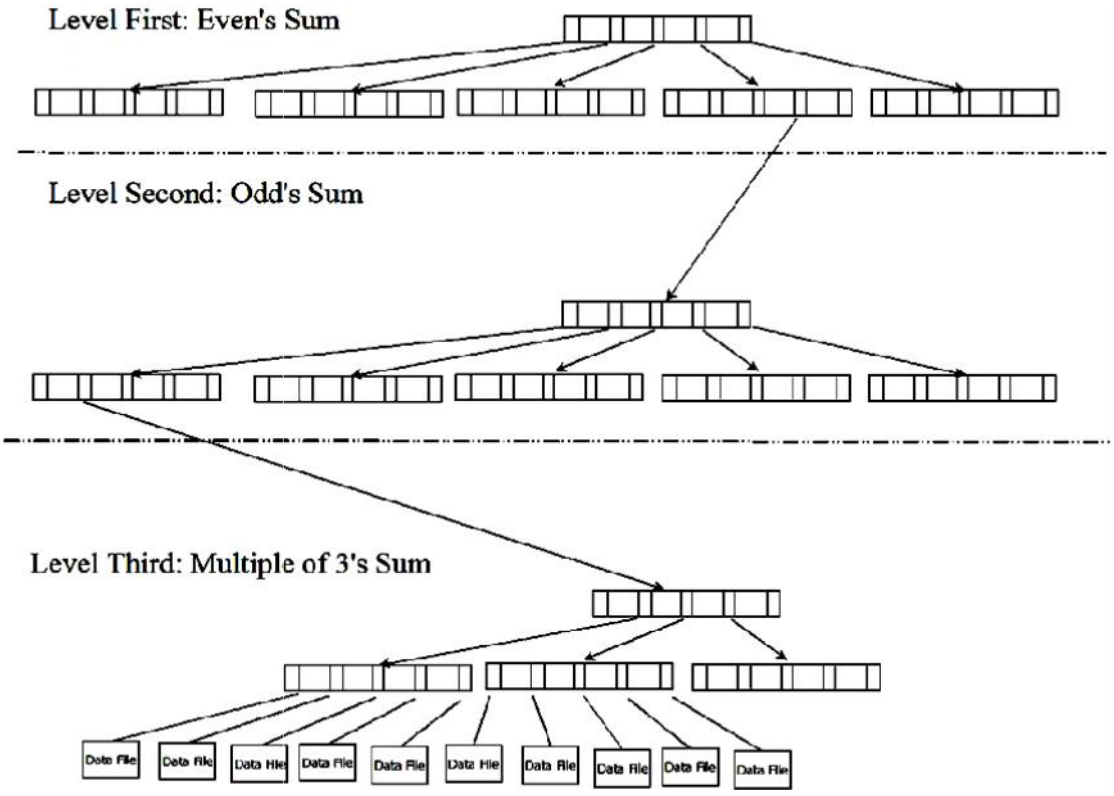


Figure 19: Three Stage Leveling of B+

4.3.1 First Level B+ Tree:

As the average minimum distance between two adjacent minutiae points can be 5mm and maximum average distance is 10mm. Hence it is clear that the sum the 70 minutiae points will lie between 70x5 =350mm to 70x 8=560mm.

But for the construction of B+ Tree half minutiae numbers are considered so range will reduce to 175mm to 285mm.

4.3.2 Second Level B+ Tree:

As per literature survey, the average minimum distance between two adjacent minutiae points can be 5mm and maximum average distance is 10mm. Hence it is clear that the sum the 70 minutiae points will lie between 70x5 =350mm to 70x 8=560mm.

But for the construction of B+ Tree half minutiae numbers are considered so range will reduce to 175mm to 285mm.

4.3.3 Third Level B+ Tree:

As the average minimum distance between two adjacent minutiae points can be 5mm and maximum average distance is 10mm. Hence it is clear that the sum the 70 minutiae points will lie between 70x5 =350mm to 70x 8=560mm.

But for the construction of B+ Tree will include 1/3 of total minutiae numbers i.e. range will reduced to 117mm to 187mm.

Chapter 5

Implementation and Results

5.1 Main Interface:

Figure 20 shows the implemented interface for Thumbprint minutiae extraction. Each step was implemented and called using designated buttons on the interface.

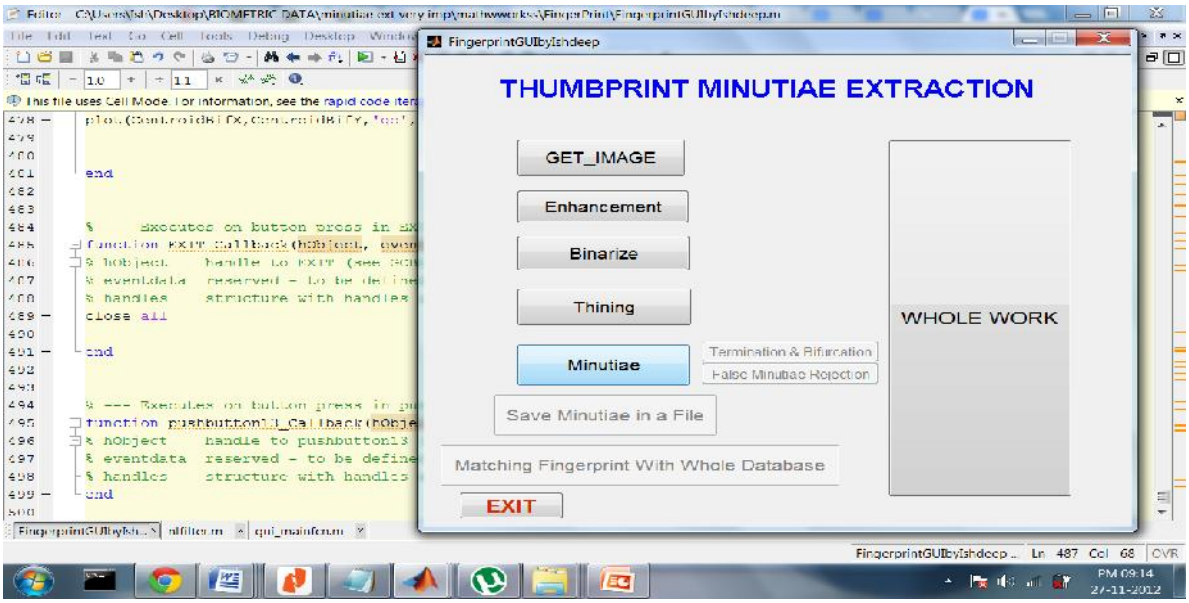


Figure 20: Screenshot of Main Interface

5.1.1 Step 1: Browsing the Image from Database

Select an image for the operation.

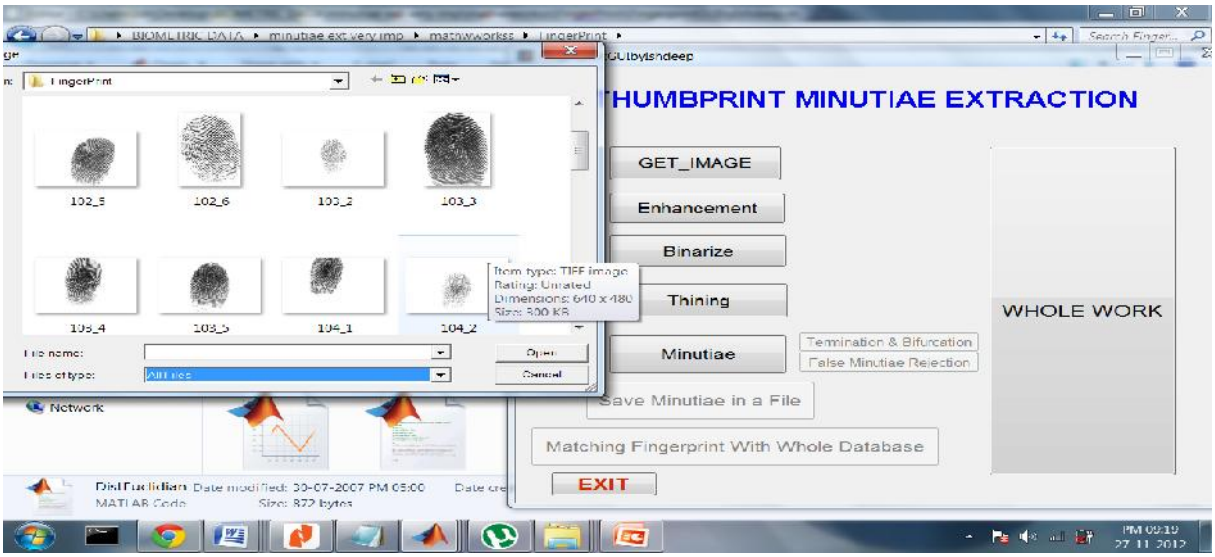


Figure 21: Browsing the Image from Database

5.1.2 Step 2: Enhancement

Second step is to enhance the image as in this project good quality fingerprint image have been used so there is no need of image enhancement here. In future project there is a scope of implementing it with fingerprint.

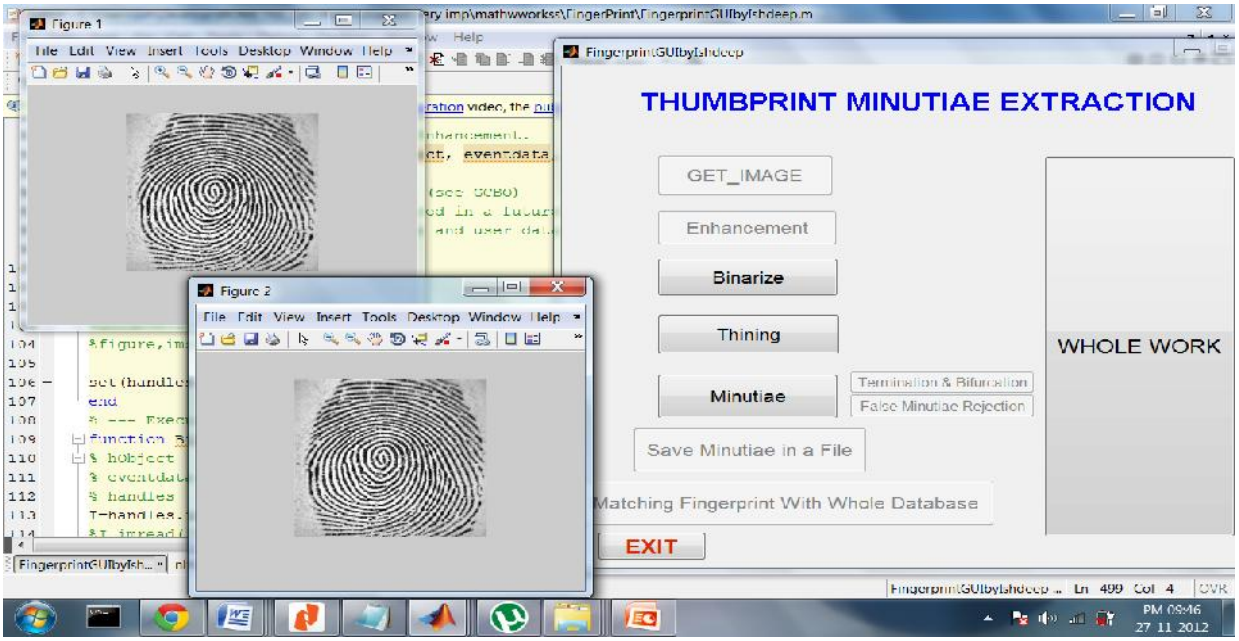


Figure 22: Screenshot of Enhancement

5.1.3 Step 3: Binarization

Before applying Thinning there is a strong requirement of binarizarion. The pixel values in the image have to be made in the range 0 to 1. Then, apply graythresh on the normalized image, it will return a threshold value between 0 and 1. Using the threshold you can easily binary image from the normalized image by making all the pixel values greater than the threshold equal to 1 and rest to 0

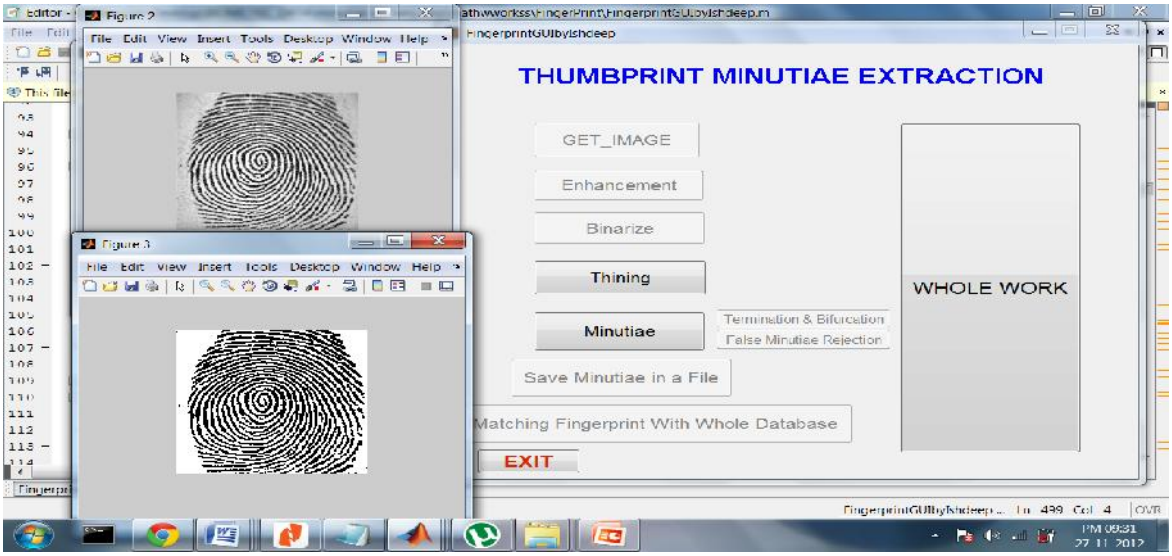


Figure 23: Screenshot of Binarization

The difference the difference between two windows figure 3 and figure 2 in figure 23 can notice. The false colors and pixels have been removed.

5.1.4 Step 4: Thinning

Skelton of the image has been prepared.

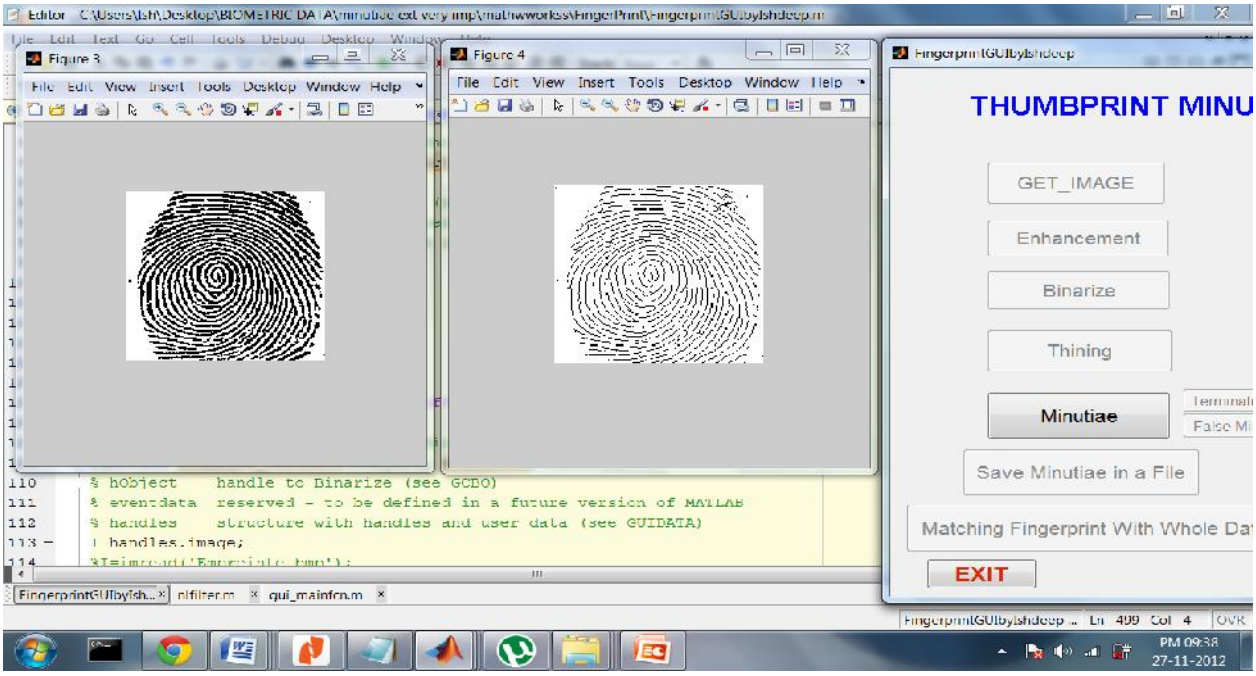


Figure 24: Screenshot of Thinning

5.1.5 Step 5: Minutiae Marking

In this window green sports means Bifurcation and red spots means Ridge Termination in the fingerprint.

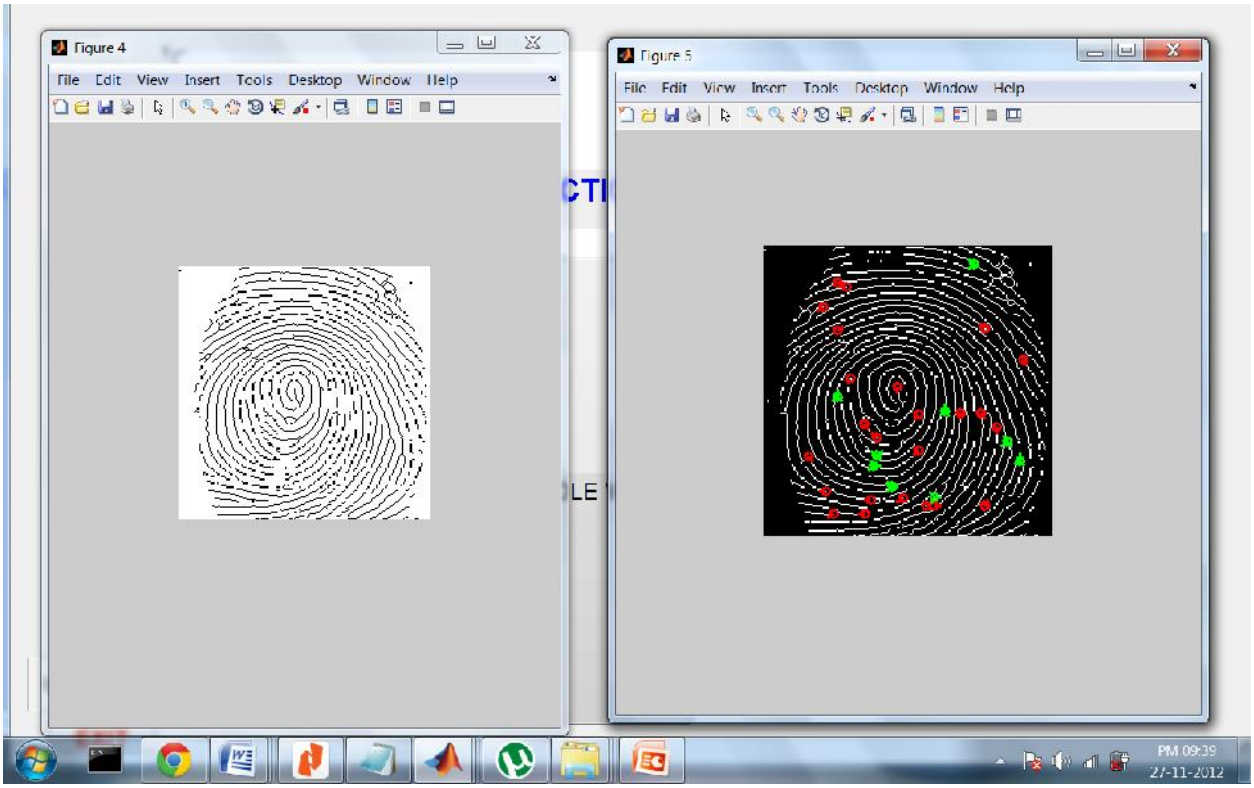


Figure 25: Screenshot of Minutiae Marking

5.1.6 Whole Work Button

To accomplish all steps in a single phase there exist a button named as *Whole Work.* By using this button all steps like Enhancement, Binarization,, Thinning, and Minutiae Extraction will be done.

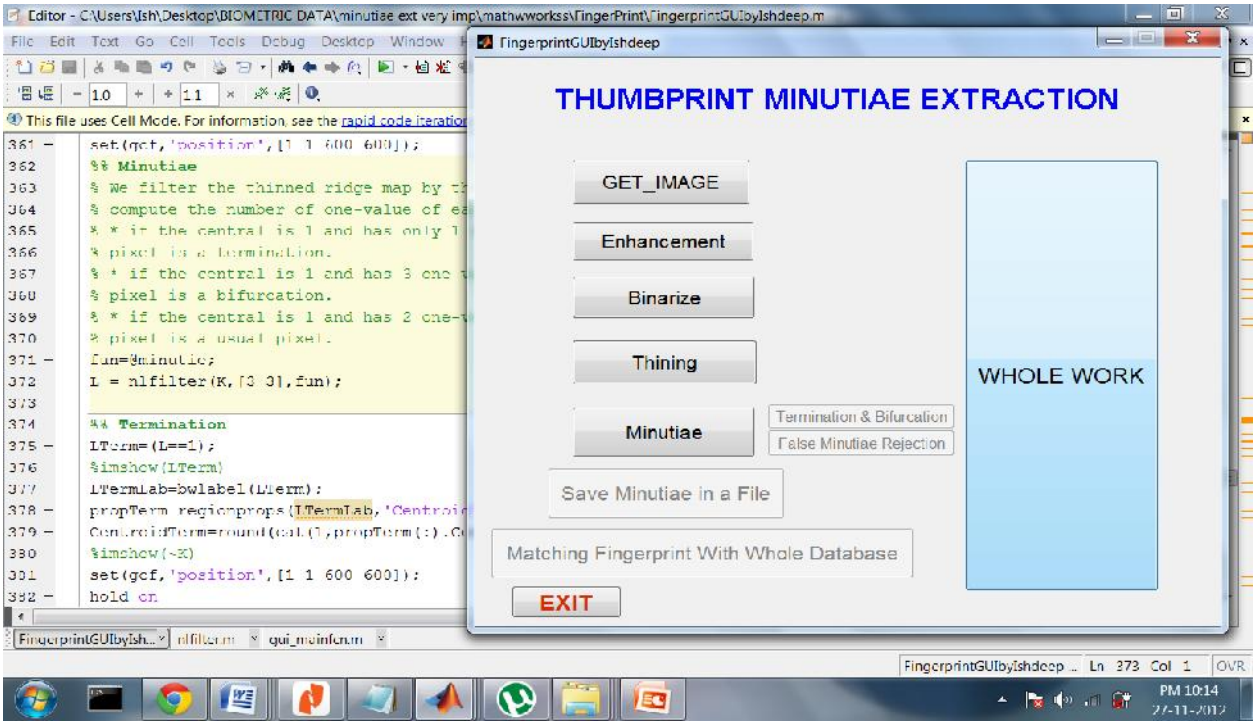


Figure 26: Screenshot of Whole Work Button

5.1.7 Outputs of Whole Work Button:

Figure 27: Browsing the Image

Figure 28: Enhancement Output

Figure 29: Binarization Output

Figure 30: Thinning Output

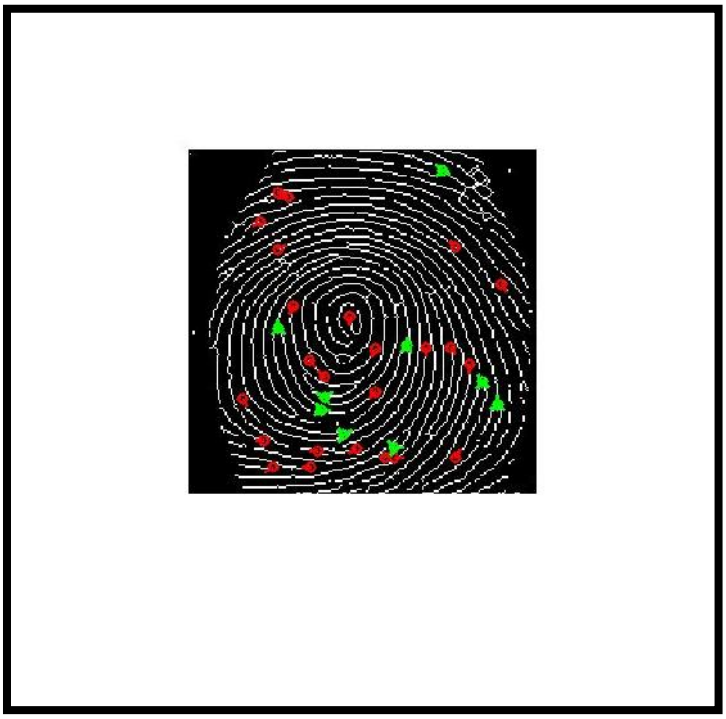


Figure 31: Minutiae Marking Output

5.2 Validation of Unification of Fingerprint

This mathematical calculation is based upon minutiae points. Based on statistical values available in the literature [17] On an average there are 40-100 minutiae points lie in a good quality image [18]. Normalizing from top to bottom and left to right (figure 32), distance between two adjacent minutiae points was noticed 1 to 113 pixels. Taking median of both values, it result 57 pixels as distance and 70 as number of minutiae points in a fingerprint image.

Figure 32: Calculating Distance of Two Adjacent Minutiae Points

Mathematically the total numbers of cobinations are $57^{\wedge 70}$ and it can be noticed very clearly that this count is much more than the whole universe's people's count. In simple words it can be said that the fingerprint can have $57^{\wedge 70}$ different patterns.

5.3 Implement B Tree

After finding the minutiae points and measuring the distance between each adjacent minutiae point's pair. There is requirement of implement B-Tree.

5.3.1Creating the B-Tree

This is the pseudo code to create an empty B-Tree [51].

Inputs: x, pointer to the root node of a subtree,

k, a key to be searched in that subtree.

```
B-TREE-CREATE(T)
    x ← ALLOCATE-NODE()
    leaf[x] ← TRUE
    n[x] ← 0
    DISK-WRITE(x)
    root[T] ← x
```

Splitting a node in B-Tree [58]

```
B-TREE-SPLIT-CHILD(x, i, y)
    z ← ALLOCATE-NODE()
    leaf[z] ← leaf[y]
    n[z] ← t − 1
    for j ← 1 to t − 1
        do key_j[z] ← key_{j+t}[y]
    if not leaf[y]
        then for j ← 1 to t
            do c_j[z] ← c_{j+t}[y]
    n[y] ← t − 1
    for j ← n[x] + 1 downto i + 1
        do c_{j+1}[x] ← c_j[x]
    c_{i+1}[x] ← z
    for j ← n[x] downto i
        do key_{j+1}[x] ← key_j[x]
    key_i[x] ← key_t[y]
    n[x] ← n[x] + 1
    DISK-WRITE(y)
    DISK-WRITE(z)
    DISK-WRITE(x)
```

Searching [19]:

```
function B-TREE-SEARCH(x, k) returns (y, i) such that key_i[y] = k or NIL
    i ← 1
    while i ≤ n[x] and k > key_i[x]
        do i ← i + 1
    if i ≤ n[x] and k = key_i[x]
        then return (x, i)
    if leaf[x]
        then return NIL
        else DISK-READ(c_i[x])
             return B-TREE-SEARCH(c_i[x], k)
```

5.3.2 Testing and Result of B-Tree:

Testing test is present for First Level Searching technique only because this same algorithm has to be repeated according to the problem. The input is taken as text file contain the all possible combination of sum of distances between adjacent minutiae points.

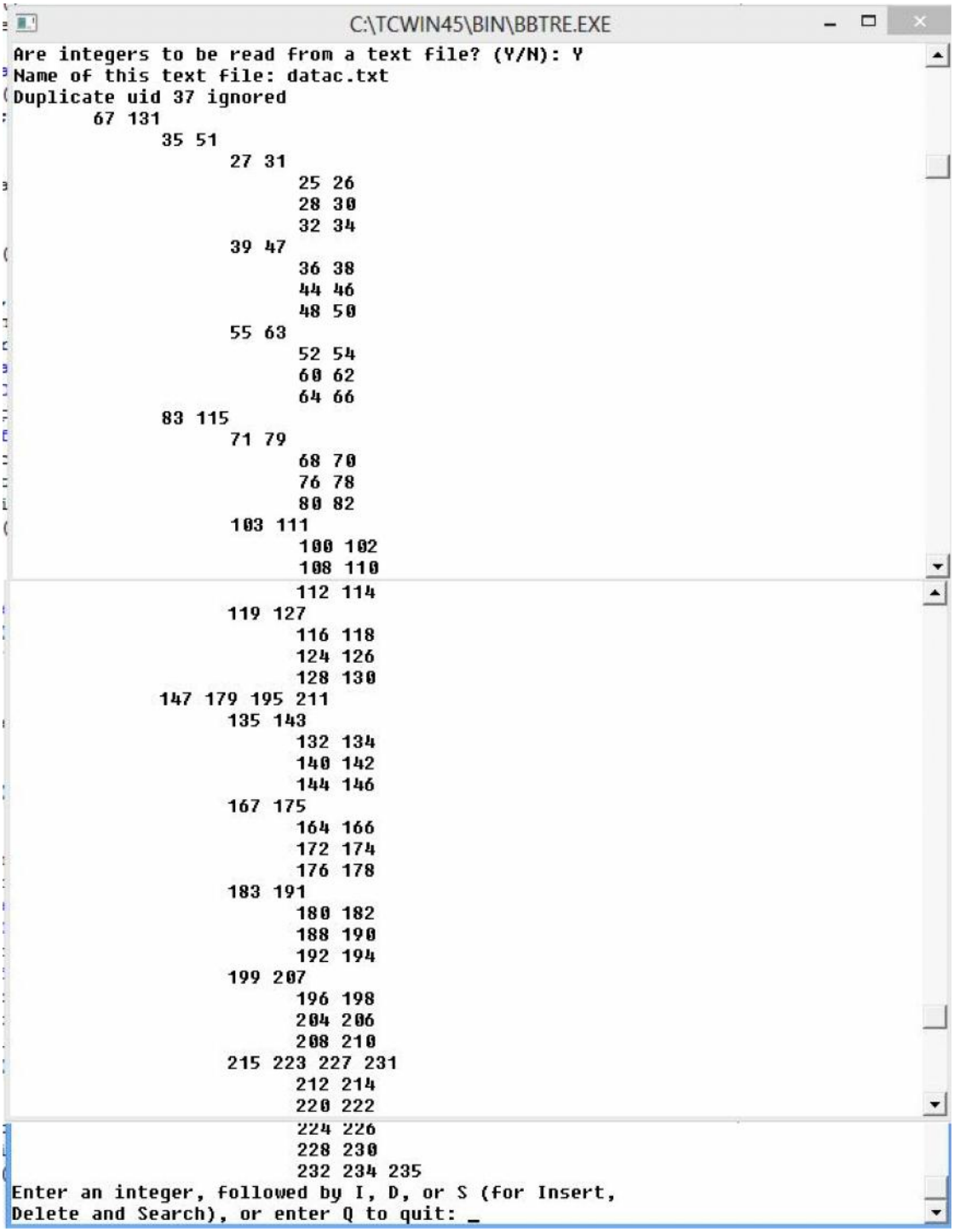


Figure 33: Input Window

5.3.3 Testing With Different Test Cases

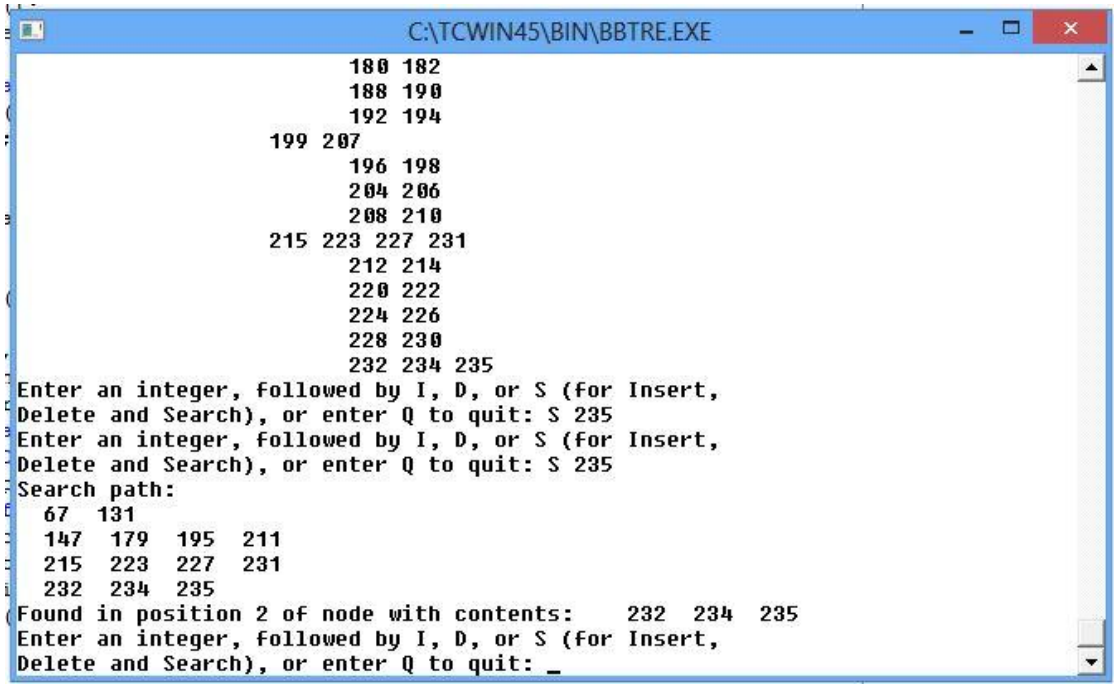


Figure 34: Testing & Result

This testing and Output belong to First Level Technique, But this same algorithm can be repeated for Second and Third level Searching Techniques. After applying this technique just there is requirement of applying *Linear or Binary* searching algorithm on very small size data. Searching speed of this algorithm is in nanoseconds.

5.4 Result

Table 1 : Time and Space Complexity of the Algorithm

S.No	Complexity	Average	Worst case
1.	Space	O(n)	O(n)
2,	Search	O(log n)	O(log n)
3.	Insert	O(log n)	O(log n)
4.	Delete	O(log n)	O(log n)

Chapter 6
Future Scope and Conclusion

In future there may be some possibility of few changes in minutiae extraction technique. In this thesis the minutiae points are extracted using CN method. Moreover there may be a possibility of use of better and fast indexing technique than B Tree. If someone wants to use this technology for the field of forensic only then there is scope of some improvement in enhancement of the picture. However it depends upon the type of work.

The work of the thesis is up to creation and searching an entity from database, but further there may be a good database management system can be used to traversing and storing the data.

References

[1] Ardovini, L. Cinque, F. Della Rocca, and E. Sangineto. A semi-automatic approach to photo identification of wild elephants. Pattern Recognition and Image Analysis, pages 225–232, 2007.

[2] B.M. Mehtre and B. Chatterjee,"Segmentation of fingerprint images–a composite method", Pattern Recognition, 22(4):381–385, 1989.

[3] Cappelli, R.; Ferrara, M.; Maltoni, D. Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. IEEE Trans. Pattern. Anal. Mach. Intell. 2010, 32, 2128–2141.

[4] Cappelli, R.; Maio, D.; Maltoni, D.; Wayman, J.L.; Jain, A.K. Performance evaluation of fingerprint verification systems. IEEE Trans. Pattern. Anal. Mach. Intell. 2006, 28, 3–18.

[5] Chen, X.; Tian, J.; Yang, X. A new algorithm for distorted fingerprints matching based on normalized fuzzy similarity measure. IEEE Trans. Image Process. 2006, 15, 767–776.

[6] Chen, X.; Tian, J.; Yang, X.; Zhang, Y. An algorithm for distorted fingerprint matching based on local triangle feature set. IEEE Trans. Inf. Forensics Secur. 2006, 1, 169–177.

[7] D. Gabor, "Theory of communication," J. Inst. Electr. Eng. Vol. 93, 1946, pp. 429-457.

[8] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition,Second Edition.London Springer, 2009.

[9] Feng, J. Combining minutiae descriptors for fingerprint matching. Pattern Recogn. 2008, 41, 342–352.

[10] Feng, Y.; Feng, J.; Chen, X.; Song, Z. A Novel Fingerprint Matching Scheme Based on Local Structure Compatibility. In Proceedings of the 18th International Conference on Pattern Recognition, Hong Kong, China, 20–24 August 2006; Volume 4, pp. 374–377.

[11] Fingerprint Minutiae Extraction, Department of Computer Science National Tsing Hua University Hsinchu, Taiwan 30043.

[12] Ghazvini, M.; Sufikarimi, H.; Mohammadi, K. Fingerprint Matching Using Genetic Algorithm and Triangle Descriptors. In Proceedings of the 19th Iranian Conference on Electrical Engineering Tehran, Iran, 17–19 May 2011; pp. 1–6.

[13] H. Blum and R. N. Nagel. Shape description using weighted symmetric axis features. Pattern Recognition, 10(3):167–180, 1978.

[14] H. Blum and R. N. Nagel. Shape description using weighted symmetric axis features. Pattern Recognition, 10(3):167–180, 1978.

[15] H. Demuth, and M. Beale, "Neural Network Toolbox for use with MATLAB", The MathWorks Inc,1998.

[16] Handbook of Fingerprint Recognition by David Maltoni (Editor), Dario Maio, Anil K. Jain, Salil Prabhakar.

[17] Hoyle, K. Minutiae Triplet-Based Features with Extended Ridge Information for Determining Sufficiency in Fingerprints. Master Thesis, Virginia Polytechnic Institute and State University, Burruss Hall Blacksburg, VA, USA, 2011.

[18] Ishmael S. Msiza, Brain Leke-Betechuoh, Fulufhelo V. Nelwamondo and Ntsika Msimang,"A Fingerprint Pattern Classification Approach Based on the Coordinate Geometry of Singularities",Proceedings of the IEEE International Conference on systems, Man, and Cybernetics San Antonio, TX, USA- October 2009.

[19] J. Neyman and E.S. Pearson, "On the problem of the most e□ cient tests of statistical hypotheses," Phil. Trans. Roy. Soc. London, Series A, Vol. 231, 1933, pp. 289-337.

[20] J.L. Wayman, "Technical testing and evaluation of biometric identification devices," in Biometrics: Personal Identification in Networked Society (A. Jain, R. Bolle, S. Pankanti, eds), Kluwer, Dordrecht, 1999, pp. 345-368.

[21] Jain, A. Bolle, R. and Pankanti, S (eds). 1998. Biometrics Personal Identification in networked society. Boston: Kluwer Academic Publishers.

[22] Jain, A.K.; Feng, J. Latent fingerprint matching. IEEE Trans. Pattern. Anal. Mach. Intell. 2011,33, 88–100.

[23] Jain, A.K.; Feng, J.; Nandakumar, K. Fingerprint matching. Computer 2010, 43, 36–44.

[24] Jea, T.Y. Minutiae-Based Partial Fingerprint Recognition. PhD Thesis, State University of NewYork, NY, USA, 2005.

[25] Jea, T.Y.; Govindaraju, V. A minutia-based partial fingerprint recognition system. Pattern Recogn. 2005, 38, 1672–1684.

[26] Jiang, X.; Yau, W.Y. Fingerprint Minutiae Matching Based on the Local and Global Structures. In Proceedings of the 15th International Conference on Pattern Recognition, Barcelona, Spain, 3–7 September 2000; Volume 2, pp. 1038–1041.

[27] K. Bradfield. Photographic identification of individual Archey's frogs, Leiopelma archeyi, from natural markings. Doc. Science Internal Series 191, Dept. Of Conservation, New Zealand, 2004.

[28] K. Bradfield. Photographic identification of individual Archey's frogs, Leiopelma archeyi, from natural markings. Doc. Science Internal Series 191, Dept. Of Conservation, New Zealand, 2004.

[29] K. Jain, L. Hong, S. Pantanki and R. Bolle, An Identity Authentication System Using Fingerprints, Proc of the IEEE, vol, 85, no.9,1365-1388, 1997.

[30] Kekre, H.B., T. Sarode and R. Vig, Fingerprint identification using sectorized cepstrum complex plane. Int. J. Comput. Appli., 8: 12-15, 2010.

[31] Kovcs-Vajna, Z.M. A fingerprint verification system based on triangular matching and dynamic time warping. IEEE Trans. Pattern. Anal. Mach. Intell. 2000, 22, 1266–1276.

[32] L. Hong, A. Jain, S. Pankanti and R. Bolle, Fingerprint Enhancement, Pattern Recognition, 202-207, 1996.

[33] Lin Hong, Yifei Wan and Anil Jain. Fingerprint Image Enhancement:Algorithm and Performance Evaluation. East Lansing, Michigan.

[34] Lin Hong,"Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.

[35] Maltoni, D.; Maio, D.; Jain, A.K.; Prabhakar, S. Handbook of Fingerprint Recognition, 2nd ed.; Springer-Verlag: London, UK, 2009.

[36] N. Ratha, S. Chen and A.K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, pp. 1657-1672, November 1995.

[37] Parziale, G.; Niel, A. A Fingerprint Matching Using Minutiae Triangulation. In Proceedings of the 1st International Conference on Biometric Authentication, Hong Kong, China, 15–17 July 2004; Volume LNCS 3072, pp. 241–248

[38] Prabhakar, S.; Ivanisov, A.; Jain, A.K. Biometric recognition: Sensor characteristics and imagequality. IEEE Instrum. Meas. Mag. 2011, 14, 10–16

[39] Qi, J.; Yang, S.; Wang, Y. Fingerprint matching combining the global orientation field with minutia. Pattern Recogn. Lett. 2005, 26, 2424–2430.

[40] R.V.L. Hartley, "Transmission of information," Bell Syst. Tech. J. Vol. 7, 1928, pp. 535-563.

[41] Raffaele Cappelli, Alessandra Lumini, Dario Maio and Davide Maltoni,"Fingerprint Classification by Directional Image Partitioning",IEEE Transactions On Pattern Analysis And Machine Intelligence, vol. 21, no. 5, pp.402-421, 1999.

[42] Reisman, J.; Uludag, U.; Ross, A. Secure Fingerprint Matching with External Registration. In Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '05), Tarrytown, NY, USA, July 2005; Volume LNCS 3546, pp. 720–729.

[43] S. Belongie, J. Malik, and J. Puzicha. Shape matching and object recognition using shape contexts. IEEE Trans. on Pattern Analysis and Machine Intelligence, pages 509–522, 2002.

[44] T. Burghardt and N. Campbell. Individual animal identification using visual biometrics on deformable coat patterns. In Proceedings of the 5th International Conference on Computer Vision Systems, Berlin,Germany.. Accessed, volume 9. Citeseer, 2007.

[45] Tan, X.; Bhanu, B. Fingerprint matching by genetic algorithms. Pattern Recogn. 2006, 39, 465–477.

[46] Tico, M.; Kuosmanen, P. Fingerprint matching using an orientation-based minutia descriptor. IEEE Trans. Pattern. Anal. Mach. Intell. 2003, 25, 1009–1014.

[47] Udupa U, R.; Garg, G.; Sharma, P. Fast and Accurate Fingerprint Verification. In Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA ’01), Halmstad, Sweden, 6–8 June 2001; Volume LNCS 2091, pp. 192–197.

[48] W.W. Peterson, T.G. Birdsall, and W.C. Fox, “The theory of signal detectability,” Trans. I.R.E. PGIT-4, 1954, pp. 171-212.

[49] Wang, W.; Li, J.; Chen, W. Fingerprint Minutiae Matching Based on Coordinate System Bank and Global Optimum Alignment. In Proceedings of the 18th International Conference on Pattern Recognition, Hong Kong, China, 20–24 August 2006; Volume 4, pp. 401–404.

[50] Wayman, J. Jain, A. Maltoni, D. and Maio, D. (eds). 2005. Biometric systems technology, design and performance evaluation. London: Springer.

[51] Woodward Jr, J.D. Orlans, N. M. and Higgins, P. 2002. Biometrics. McGraw-Hill Professional.

[52] Xu, W.; Chen, X.; Feng, J. A Robust Fingerprint Matching Approach: Growing and Fusing of Local Structures. In Proceedings of the 2nd International Conference on Biometrics, Seoul, Korea, 27–29 August 2007; Volume LNCS 4642, pp. 134–143.

[53] Y. Bulatov, S. Jambawalikar, P. Kumar, and S. Sethia. “Hand recognition using geometric classifiers”, ICBA’04, Hong Kong, China, pages 753–759, July 2004. Z. Sun, T. Tan, Y. Wang, and S.Z. Li, "Ordinal palmprint representation for personal identification", Proc. EEE Computer Vision and Pattern Recognition (CVPR), vol. 1, pp. 279-284, 2005.

[54] Zewail, R. Saeb, M. and Hamdy, N. 2004.Soft and hard biometrics fusion for improved identity verification. IN: The 47th IEEE Midwest Symposium on circuits and systems. IEEE pp 2255 228.

[55] Zhao, Q.; Zhang, D.; Zhanga, L.; Luoa, N. High resolution partial fingerprint alignment using pore-valley descriptors. Pattern Recogn. 2010, 43, 1050–1061.

[56] Zheng, J.D.; Gao, Y.; Zhang, M.Z. Fingerprint Matching Algorithm Based on Similar Vector Triangle. In Proceedings of the 2nd International Congress on Image and Signal Processing (CISP ’09), Tianjin, China, 17–19 October 2009; pp. 1–6.

List of Publications/ Communicated

1.) Karun Verma, Ishdeep Singla "Fingerprint and Minutiae points Technique" at AISC Series of **Springer**. (Presented in conference & accepted for Publishing by SPRINGER).

2.) Ishdeep Singla, Karun Verma "Minutiae Point Extraction and Database Creation Methodology" (Will be Communicated Shortly in a Good Journal).