

ONLINE FINGERPRINT VERIFICATION

A DISSERTATION

*Submitted in partial fulfilment of the
requirements for the award of the degree*

of

MASTER OF TECHNOLOGY

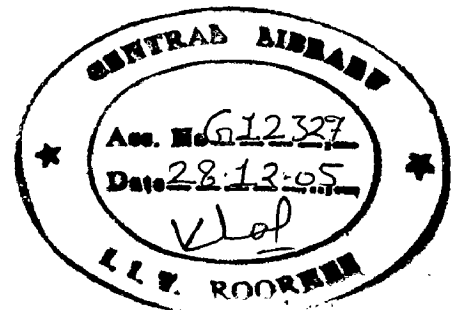
in

ELECTRICAL ENGINEERING

(With Specialization in Measurement & Instrumentation)

By

M. BHUSHAN KUMAR



DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE-247 667 (INDIA)

JUNE, 2005

CANDIDATE'S DECLARATION

I hereby declare that the work presented in this dissertation entitled "**ONLINE FINGERPRINT VERIFICATION**" submitted in partial fulfillment of the requirement for the award of Degree of **Master of Technology in Electrical Engineering** with specialization in **Measurement and Instrumentation**, in the Department of Electrical Engineering, **Indian Institute of Technology Roorkee, Roorkee** is an authentic record of my own work carried out from July 2004 to June 2005 under the guidance of **Dr. Vinod Kumar**, Professor, and **Dr. H.K.Verma**, Professor, Department of Electrical Engineering, Indian Institute of Technology Roorkee, Roorkee.

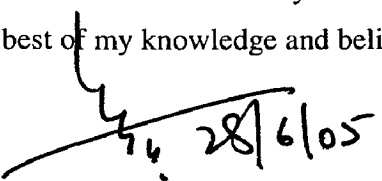
I have not submitted the matter embodied in this report for the award of any other degree or diploma.


28th
Date: June 2005
Place: Roorkee


(M.BHUSHAN KUMAR)

CERTIFICATE

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


(Dr. Vinod Kumar)
Professor
Department of Electrical Engineering
Indian Institute of Technology Roorkee
Roorkee-247667
India


(Dr. H.K. Verma)
Professor
Department of Electrical Engineering
Indian Institute of Technology Roorkee
Roorkee-247667
India

ACKNOWLEDGEMENTS

I express my foremost and deepest gratitude to **Dr. Vinod Kumar**, Professor, Department of Electrical Engineering, Indian Institute of Technology Roorkee, Roorkee for his valuable guidance, support and motivation throughout this work. I have deep sense of admiration for his innate goodness and inexhaustible enthusiasm. The valuable discussions and suggestions that I had with him have undoubtedly helped in supplementing my thoughts in the right direction for attaining the desired objective. I consider myself extremely fortunate for having got the opportunity to learn and work under his able supervision over the entire period of my association with him.

I am greatly indebted to my Co-guide **Dr. H.K.Verma**, Professor, Department of Electrical Engineering, Indian Institute of Technology Roorkee, Roorkee for extending moral support and guidance during my work. His co-operation has made my work possible.

My special thanks to the staff of the Instrumentation & Signal Processing lab for their kind co-operation. My special thanks go to my friends Murthy and Srikanth for extending their moral support for the completion of my work. I also thank my friends Ravi, Kesi Reddy, Shankar and others for their constant help and encouragement.

I'm highly indebted to my parents and family members whose undying love for me and their sincere prayers, best wishes, and encouragement have a constant source of strength and inspiration to me.

I also thank all those who helped me directly or indirectly in the successful completion of my dissertation.


(M.BHUSHAN KUMAR)

ABSTRACT

Present day need of our society is to have an identification or verification system, which is fast and reliable. We have various biometrics based verification systems, but fingerprint verification system is one of the fast and reliable systems. In fingerprint verification system minutiae-based representation is most widely used for identification / verification. But due to the limited amount of information present in the minutiae-based representation, it is desirable to explore alternative representations of fingerprints for verification or identification.

Various methods of biometric verifications are discussed here. Fingerprint biometrics has been illustrated in detail. In this dissertation a method based on filter bank representation for the verification of fingerprints has been developed. Overall performance of the system is tested on fingerprint database of 50 students named as IITRDB. Results obtained are FAR (False Acceptance Rate) of 23.65% and FRR (False Rejection Rate) of 27.67%. These are good enough for several applications. User friendly software has been developed and implemented for live demonstration and testing.

CONTENTS

	Page No.
CANDIDATE'S DECLARATION	i
ACKNOWLEDGEMENTS	ii
ABSTRACT	iii
LIST OF FIGURES	vi
1. INTRODUCTION	1
1.1. BIOMETRICS	1
1.2. WHY TO USE BIOMETRICS	1
1.3. VARIOUS BIOMETRIC TECHNIQUES	2
1.3.1. BEHAVIOURAL CHARACTERISTICS	2
1.3.2. PHYSIOLOGICAL CHARACTERISTICS	5
1.4. LITERATURE REVIEW	12
1.5. OUT LINE OF REPORT	13
2. FINGERPRINT BIOMETRICS	14
2.1. INTRODUCTION	14
2.2. COMMON TYPES OF FINGERPRINTS	14
2.3. ADVANTAGES AND DISADVANTAGES OF FINGERPRINT BIOMETRICS	16
2.4. FINGERPRINT SENSOR TECHNOLOGIES	16
2.4.1. OPTICAL TYPE	16
2.4.2. CAPACITANCE TYPE	19
2.4.3. THERMAL TYPE	21
2.4.4. ACOUSTIC (ULTRA SOUND) SENSORS	21
2.5. FINGERPRINT SENSOR USED	22
2.6. DATA ACQUISITION	23
2.6.1. FINGERPRINT IMAGE DETAILS	23
2.6.2. DATABASE DETAILS	24
3. FINGERPRINT VERIFICATION	25
3.1. INTRODUCTION	25
3.1.1. MINUTIAE BASED	25
3.1.2. FILTER BANK BASED	26
3.2. FILTER BANK BASED VERIFICATION	26
3.3. CENTER POINT DETECTION	28
3.3.1. ALGORITHM FOR CENTER POINT DETECTION	28
3.3.2. RESULTS	31
3.4. SECTORIZATION AND NORMALIZAION	32
3.4.1. INTRODUCTION	32
3.4.2. RESULTS	33

3.5. FILTERIZATION	34
3.5.1. INTRODUCTION	34
3.5.2. GABOR FILTER ANALYSIS	34
3.5.3. IMPLEMENTATION	35
3.5.4. RESULTS	36
3.6. FEATURE EXTRACTION	37
3.6.1. INTRODUCTION	37
3.6.2. FEATURE VECTOR	37
3.6.3. IMPLEMENTATION	38
3.6.4. RESULTS	38
3.7. FINGERPRINT MATCHING	39
3.7.1. INTRODUCTION	39
3.7.2. ACCEPT/REJECT DECISION	39
3.7.3. RESULTS	39
4. IMPLEMENTATION OF SOFTWARE AND GUI (GRAPHICAL USER INTERFACE)	42
5. CONCLUSIONS AND FUTURE SCOPE OF WORK	45
5.1. CONCLUSIONS	45
5.2. FUTURE SCOPE OF WORK	45

REFERENCES

LIST OF FIGURES

Figure 1.1	Voice recognition System	4
Figure 1.2	Image of Human Iris	6
Figure 1.3	Iris pattern with part of Iris eliminated	7
Figure 1.4	RSI Hand Geometry Reader and Image of the Hand	8
Figure 1.5	Facial Features of an Individual	9
Figure 1.6	Retina	10
Figure 1.7	a) Image of a fingerprint b) Minutiae in the fingerprint	12
Figure 2.1	Common types of Fingerprints	14
Figure 2.2	Common types of lines found in Fingerprints	15
Figure 2.3	Optical Type Sensor	17
Figure 2.4	KSI's (KC-901) Optical Fingerprint Sensor	17
Figure 2.5	Capacitive Sensing Type	19
Figure 2.6	Capacitive Sensing Type Fingerprint sensor	19
Figure.2.7	Thermal Sensing Type Fingerprint sensor	21
Figure 2.8	Touchchip™ Fingerprint Sensor (TCRU1 A)	22
Figure 3.1	Characterization of Minutiae.	25
Figure 3.2:	Flow chart for filter bank based verification.	27
Figure 3.3	Concave and convex ridges in a fingerprint image, 'X' marks the center point	28
Figure 3.4	Center point (marked as X) detected for various fingerprints	31
Figure 3.5	Results of the Sectorization and normalization	33
Figure 3.6	a) Gabor filter oriented at 0^0 b) Top view of Gabor filter	34

Figure 3.7	Filtered images	36
Figure 3.8	Feature vector of the fingerprints	38
Figure 3.9	Plot of FAR vs FRR for IITRDB database	41
Figure 4.1	Welcome page for the modules	42
Figure 4.2	Registration and Verification modules	43
Figure 4.3	Result window after verification	44

INTRODUCTION

1.1. BIOMETRICS

In this security arena, there is often a need to verify one's identity or someone's identity. Biometrics, which refers to automatic identification of a person based on the physiological or behavioral characteristics, is inherently more reliable and more capable in differentiating between an authorized person and a fraudulent imposter than traditional methods such as passwords and PIN numbers. The present day scenario has started using biometrics in every walk of life. Biometrics is derived from the root words Bio (means Life) and Metrics (means Measurement) which literally means "Life Measurement".[1]

1.2. WHY TO USE BIOMETRICS?

Several key reasons for the increasing popularity of biometrics are[2]

- ❖ **Convenient Authentication:** The convenience of quick-and-easy authentication makes for a smoother system of identity assurance than using keys, cards, tokens, or PINs.
- ❖ **Increased Need for Strong Authentication:** Unlike passwords and PINs which can be stolen, biometric features cannot be stolen and serves as an attractive method for guarding against stolen or lost identifiers such as cards or passwords.
- ❖ **Decreased Costs:** Over the years improvement in hardware and software technologies has brought down the cost of the biometric authentication to be affordable at the commercial market level. Advancements in computing power, networking, and database systems have allowed biometric systems to become easier over wide geographical and networked areas.
- ❖ **Increased Government and Industry Adoption:** Today, numerous public and private organizations are using biometrics keeping in view of the terrorist attacks in the present day scenario. Manufacturers are increasingly looking to provide biometrics with computer equipment and products. There are instances of

fingerprint sensors built right into keyboards, mice, and laptops and second generation sensors are becoming much more “plug and play”.

1.3. VARIOUS BIOMETRIC TECHNIQUES

There are various Biometric technologies discussed below [3], [4] and [5]

1.3.1. BEHAVIORAL CHARACTERISTICS

(i) SIGNATURE VERIFICATION:

Signature is a consistent graphical artifact with a unique shape, repeatable in appearance, where each instance of signature resembles another instance within a range of discrepancy. Although no two instances are exactly the same, common and consistent characteristics are maintained in signature.

Signature has at least three attributes: form, movement and variation, and since the signatures are produced by moving a pen on a paper, movement perhaps is the most important part of a signature. The movement is produced by muscles of the fingers, hand, wrist, and for some writers the arm and these muscles are controlled by nerve impulses. Once a person is used to signing his or her signature, these nerve impulses are controlled by the brain without any particular attention to detail. Furthermore, a person's signature does evolve over time and with the vast majority of users once the signature style has been established the modifications are usually slight. Hence the signatures are used to verify an individual. Signatures can be divided into offline and online signatures.

❖ **Offline Signatures:** Offline Signatures are the signatures scanned from paper documents where they are written in a conventional way. These signatures do not keep track of the dynamic features like timing of the signature, velocity, acceleration of signature etc. Hence Offline Signatures are also called **Static Signatures** as they just keep track of the shape of the signature.

❖ **Online Signatures:** Online Signatures are those signatures which in addition to the shape of the signature also keep track of the dynamics of the signature like timing of the signature, velocity, acceleration at various instants of Signature.

Hence these signatures are also called **Dynamic Signatures**.

The various steps in Signature Verification are

Data Acquisition: An off-line signature verification system receives an image as input from a camera or scanner. An on-line signature verification system gets its input from

an electronic pen, digitizer or from other input device (e.g. camera, mouse). The signature is then represented as one or several time-varying signals.

Preprocessing: The data obtained is preprocessed to reduce the noise and to normalize the length of the signature.

Feature Extraction: After the preprocessing the signature features are extracted from the signature. Some of the Signature features are

- ❖ Total Signing Duration
- ❖ Total Pen down duration
- ❖ Number of pen ups
- ❖ Time of second pen down etc.

Comparison Process: In the comparison process the obtained signature feature set of an user is compared with the reference signature feature set.

Accept /Reject Decision: The decision making on whether to accept or reject a user depends upon the similarity between the two compared feature sets. If the similarity coefficient is greater than a threshold value set at the time of enrollment, the user is accepted otherwise the user is rejected.

APPLICATIONS:

The Signature verification system can be used

- ❖ In any field where conventional signature are being used.
- ❖ In check signing and in business documents.
- ❖ To safeguard identification cards, driver's licenses, passports, travel documents.
- ❖ To strengthen the identification process for electronic commerce applications like Computer Sign-on, data access, credit card transactions etc.

ADVANTAGES:

- ❖ It increases the security and authentication.
- ❖ It is the most widely approved form for authenticating.

DISADVANTAGES:

- ❖ Certain environmental factors and characteristics of signature capture apparatus affect the robustness.
- ❖ Signatures alone are not likely to distinguish individuals reliably from among medium to large size populations.

(ii) VOICE RECOGNITION:

Voice recognition is occasionally confused with speech recognition, a technology which translates what a user is saying (a process unrelated to authentication). Voice recognition technology, by contrast, verifies the identity of the individual who is speaking. The two technologies are often bundled – speech recognition is used to translate the spoken word into an account number, and voice recognition verifies the vocal characteristics against those associated with this account. Voice recognition technology utilizes the distinctive aspects of the voice to verify the identity of individuals.

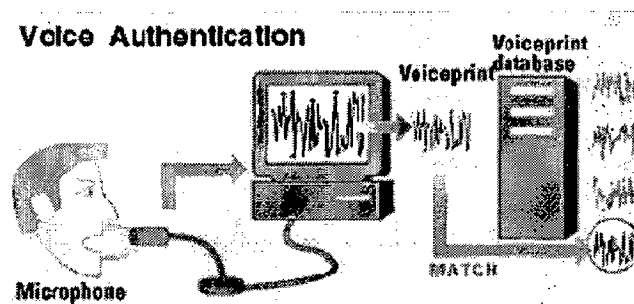


Figure 1.1: Voice Recognition System.

Voice recognition utilizes any audio capture devices like ordinary microphones, including mobile, land telephones and PC microphones. The performance of voice recognition systems can vary according to the quality of the audio signal as well as variation between enrollment and verification devices, so acquisition normally takes place on a device likely to be used for future verification.

During enrollment an individual is prompted to select a pass phrase or to repeat a sequence of numbers. The pass phrases selected should be approximately 1-1.5 seconds

in length as very short pass phrases lack enough identifying data, and long passwords have too much, both resulting in reduced accuracy. The individual is generally prompted to repeat the pass phrase or number set a handful of times, making the enrollment process somewhat longer than most other biometrics. The inflection points of speech, emphasizing the highs and lows specific to the way of user's talking forms the template (or voice print). Once the user is enrolled, at the time of verification the obtained new template is compared with the reference template for verification.

APPLICATIONS:

- ❖ It adds security to automated telephone – based transactions in areas such as financial services and health care.
- ❖ It can be added as additional security to Banking and Accounting business to discuss important matters on telephone.

ADVANTAGES:

- ❖ Low cost is the main advantages of this biometric system.
- ❖ If voice verification is used in conjunction with a Four digit PIN, a 1 in 100 False Acceptance rate (FAR) becomes roughly strengthened to 1 in 10,00,000.

DISADVANTAGES:

- ❖ A person's voice is susceptible to sickness, drugs and emotions.
- ❖ Background noise and nature of acquisition devices affects the accuracy.
- ❖ The size of the voice template (around 5 KB) is large when compared to IRIS (250 byte), Retina (96 bytes) and Hand (9 bytes) scans.

1.3.2. PHYSIOLOGICAL CHARACTERISTICS:

(i) IRIS SCANNING:

Iris recognition leverages the unique features of the human iris to perform identification and, in certain cases, verification.

THE IRIS: According to Webster's New World Dictionary, the iris is "the round pigmented membrane surrounding the pupil of the eye, having muscles that adjust the amount of light entering the eye." *Figure 1.2* shows the image of Human Iris.

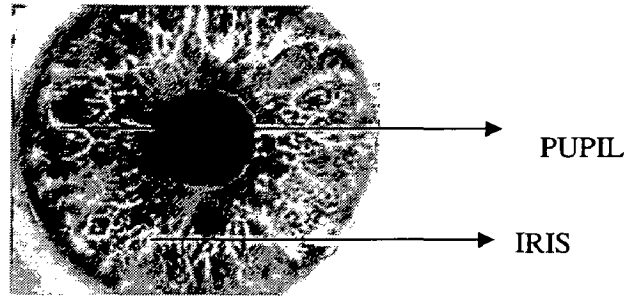


Figure 1.2: Image of Human Iris

Iris recognition is based on visible (via regular and/or infrared light) qualities of the iris. A primary visible characteristic is the trabecular meshwork (permanently formed by the 8th month of gestation), a tissue which gives the appearance of dividing the iris in a radial fashion. Other visible characteristics include rings, furrows, freckles, and the corona, to cite only the more familiar. Although small (11 mm) and sometimes problematic to image, the iris has the great mathematical advantage that its pattern variability among different persons is enormous

Iris Code™ :

Expressed simply, iris recognition technology converts these visible characteristics as a phase sequence into a 512 byte Iris Code™, a template stored for future identification attempts. From the iris (11mm diameter), Dr. Daugman's algorithms provide 3.4 bits of data per square mm. This density of information is such that each iris can be said to have 266 'degrees of freedom', as opposed to 13-60 for traditional biometric technologies. This '266' measurement is cited in most iris recognition literature; after allowing for the algorithm's correlative functions and for characteristics inherent to most human eyes, Dr. Daugman concludes that 173 "independent binary degrees-of-freedom" can be extracted from his algorithm - an exceptionally large number for a biometric. A key differentiator of iris-scan technology is the fact that 512 byte templates are generated for every iris, which facilitates match speed (capable of matching over 500,000 templates per second).

Iris Acquisition:

The first step is location of the iris by a dedicated camera no more than 3 feet from the eye. After the camera situates the eye, the algorithm narrows in from the right

and left of the iris to locate its outer edge. This horizontal approach accounts for obstruction caused by the eyelids. It simultaneously locates the inner edge of the iris (at the pupil), excluding the lower 90° because of inherent moisture and lighting issues.

The monochrome camera uses both visible and infrared light, the latter of which is located in the 700-900nm range (this is in the lower range of IR). Upon location of the iris, an algorithm uses 2-D Gabor wavelets to filter and map segments of the iris into hundreds of vectors (known as phasors).

The wavelets of various sizes assign values drawn from the orientation and spatial frequency of select areas, bluntly referred to as the "what" of the sub-image, along with the position of these areas, bluntly referred to as the "where." The "what" and "where" are used to form the Iris Code. Not the entire iris is used: a portion of the top, as well as 45° of the bottom, is unused to account for eyelids and camera-light reflections as shown in *Figure 1.3* For future identification, the database will not be comparing images of irises, but rather hexadecimal representations of data returned by wavelet filtering and mapping.

Advantages:

- ❖ It is the least intrusive of the eye related biometrics, requiring no intimate contact between user and reader.
- ❖ Iris Scan is highly accurate.
- ❖ It can work in identification mode (due to the data richness), potentially avoiding the need for any token identity claims.

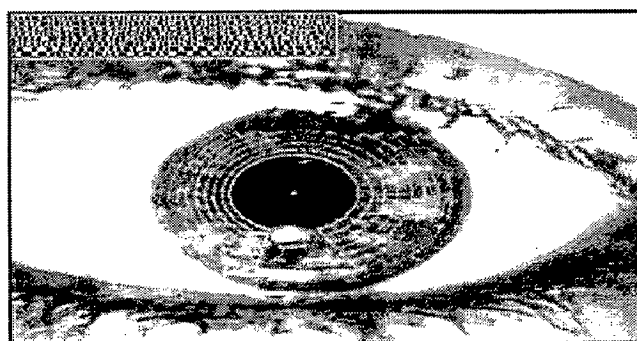


Figure 1.3: Iris pattern with part of Iris eliminated

Disadvantages:

- ❖ **Light sensitivity:** The changes in lighting significantly affect the scan.
- ❖ **Hand geometry:** It is one of the most widely used Biometric system. Every hand is unique. The Hand Geometry scanners take a measurement of the length, width, thickness and surface area of the hand and fingers. These features are distinctive enough to perform verification of a claimed identity.

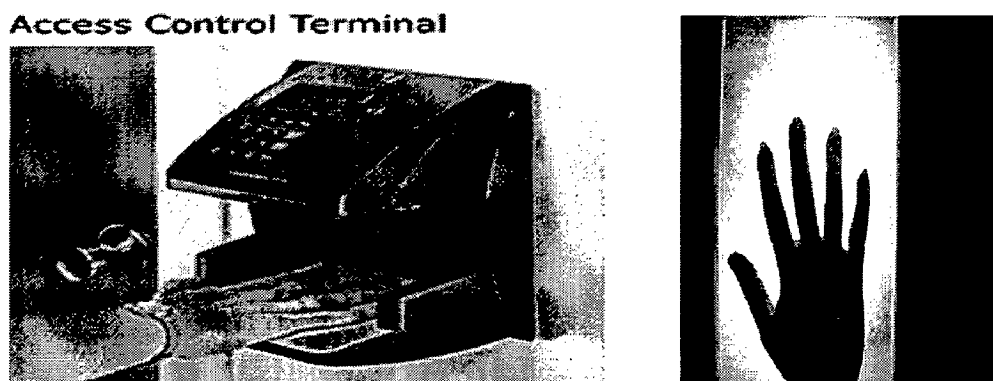


Figure 1.4: RSI Hand Geometry Reader and Image of the Hand

Figure 1.4 shows the RSI's hand geometry reader and the image of the hand obtained. The RSI image acquisition system consists of a light source, a camera, a single mirror and a flat surface (with 5 pegs arranged on it for appropriate placements of user's right hand). RSI device captures two images of the hand. The light source illuminates the hand placed on the flat surface and the camera captures the image. The mirror is used to reflect side view of the hand onto the camera. RSI uses silhouetted images to calculate the length, width, thickness and surface area of the four fingers (the thumb is not used). More than 90 measurements are taken and these features are stored in a 9-byte template. For pattern matching this reference template is compared with acquired template.

ADVANTAGES:

- ❖ The size of the reference template is small (size < 20 bytes).
- ❖ It can handle high volume use and do not require calibration or ambient light adjustments like some other biometrics.

- ❖ Hand Geometry is easy to use, reliable, and less likely to suffer from presentation errors than other biometrics.

DISADVANTAGES:

- ❖ The Hand Geometry system is expensive to purchase.
- ❖ The Image acquisition Device takes up large amount of space

(ii) FACIAL RECOGNITION:

Face has certain peaks and valleys that make up different facial features. These are the features like position, size and shape of the mouth, nose, jaw line, eye brows, cheek etc. Facial recognition makes use of these features to identify an individual. *Figure 1.5* shows the facial features of an individual.

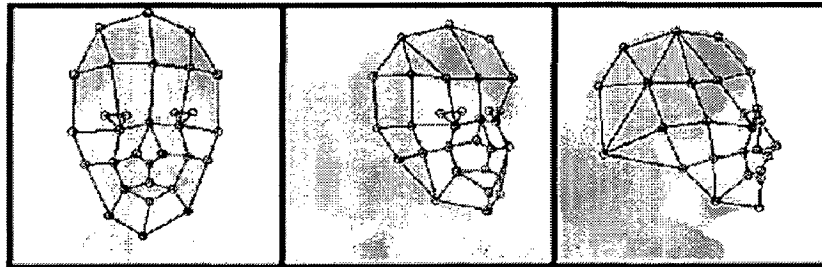


Figure 1.5: Facial Features of an Individual

A static camera or a video camera that generates images of sufficient quality and resolution is used to acquire the facial image. Once the image is obtained these important facial features are extracted and the generated template is compared with stored facial templates. Based on the match between the two templates the individual is accepted or rejected.

APPLICATIONS:

Facial Recognition is widely used in identification, authentication applications, Surveillance and monitoring. Identification & Authentication applications involve verifying identity for access control either physical or computer based. Surveillance applications scan faces in public areas or at check points and compare faces against a watch list data to see if a “bad person” is present. In addition it used to support video

search and indexing application i.e it can be used to search hundreds of hours of news video to find all occurrences of a political figure or known individual. Future applications will make use of Facial recognition in Cell Phones, video conferencing applications, robots, interfacing games and “smart home” applications.

ADVANTAGES:

- ❖ The size of the reference template is small (<100 bytes).
- ❖ It is one of the most passive, natural & non invasive types of Biometrics.

DISADVANTAGES:

- ❖ FAR and FRR are high (around 10^{-2}).

(iii) RETINA SCANNING:

Retina Biometrics distinguishes individuals by using the patterns of veins occurring in the back of the eye.

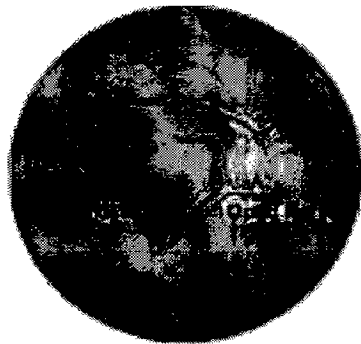


Figure 1.6: Retina

Retina Scanning is accomplished by illuminating the retina with a low-intensity infrared light and imaging the patterns formed by the major blood vessels. The retina’s intricate network of blood vessels as shown in *Figure 1.6* is a physiological characteristic that remains stable throughout the life of a person.

Retina scanners use a low power light source to gently illuminate the Retina. The light source provides some visible light but mostly consists of near infrared light (890 nm wavelength). Infrared light is necessary because retina is transparent to these wavelengths. The scanner captures the entire retinal and subsequent image segmentation and the localization and registration of the portion of the image necessary for the recognition,

locates the optic nerve, and samples an area band around it. This process creates a 96-byte template for each enrolled individual.

Retina-scan has robust matching capabilities and is typically configured to do one-to-many identification against a database of users. While the algorithms themselves are robust, it can be a difficult process to provide sufficient data for matching to take place. In many cases, a user may be falsely rejected because of an inability to provide adequate data to generate a match template.

APPLICATIONS:

Retina scan is generally used

- ❖ As a powerful access control system for standalone, single door applications.
- ❖ As part of a larger networked security applications.

ADVANTAGES:

- ❖ **Resistance to False Matching:** Retinal patterns are highly distinctive traits, sufficient to enable 1: N identification.
- ❖ **Stable Physiological Trait:** Unlike some of the other traits used in physiological biometrics, the retina patterns of an individual remain very stable throughout a person's life.

DISADVANTAGES:

- ❖ **Difficult to Use:** Retina scan is more difficult to use than most other biometric technologies, with enrollment requiring prolonged concentration and effort, and identification requiring a well trained and highly motivated user.
- ❖ User Discomfort with eye related technology.

(iv) FINGER SCAN BIOMETRICS:

It is a physical biometric that analyses the shape and dimensions of one or more fingers to generate the features of a finger. These features are sufficient enough to distinguish the identity of an individual. The Finger Scan Biometrics is quite commonly termed as Fingerprint Biometrics.

FINGERPRINTS:

Fingerprint is a print made by an impression of the ridges in the skin of a finger tip. The basic definitions of various terms related to fingerprints are

- ❖ **Ridges** are the raised markings found across the fingertip.
- ❖ **Valleys** are the corresponding marks found on either side of a finger image ridge.
- ❖ **Ridge ending** is the point at which fingers image ridge ends.
- ❖ **Ridge bifurcation** is the point at which fingers image ridge splits or divides into two ridges.
- ❖ **Minutiae** are the small details found in finger images such as ridge endings or bifurcations.

Fingerprints are the ridge and valley patterns on the tip of the finger and have been used extensively for personal identification of people. *Figure 1.7.* shows the image of a fingerprint and the minutiae in the fingerprint.

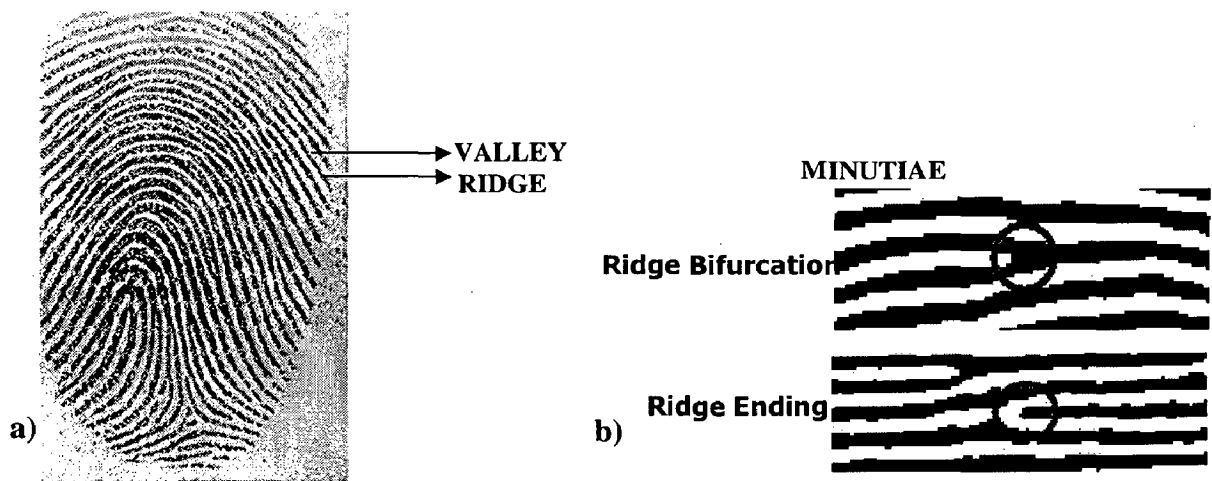


Figure 1.7: a) Image of a fingerprint b) Minutiae in the fingerprint.

1.4. LITERATURE REVIEW:

Fingerprint verification schemes are either based on predominantly local landmarks (e.g., minutiae-based fingerprint matching systems) or exclusively global information. The minutiae-based automatic identification techniques first locate the

minutiae points and then match their relative placement in a given finger and the stored template. The global representation of fingerprints (e.g., whorl, left loop, right loop, arch, and tented arch) is typically used for indexing, and does not offer good individual discrimination. Further, the indexing efficacy of existing global representations is poor due to a small number of categories (typically five) that can be effectively identified automatically and a highly skewed distribution of the population in each category.

Minutiae-based representation does not utilize a significant component of the rich discriminatory information available in the fingerprints. Local ridge structures cannot be completely characterized by minutiae. Further, minutiae-based matching has difficulty in efficiently and robustly matching two fingerprint images containing different numbers of unregistered minutiae points.

1.5. OUTLINE OF THE REPORT:

Chapter 1 gives an introduction to the Biometrics and need for opting the biometrics in security applications. It then gives an idea of the various Biometric techniques available

Chapter 2 provides basic concepts of fingerprint biometrics and presents the details on various types of fingerprint sensors. Then the data acquisition results are discussed.

Chapter 3 is the main part of the report. It explains the overall algorithm implemented. Each part of the algorithm implemented is discussed in detail with results for each stage provided after the description. At the end it concludes the statistical analysis of the entire Online Fingerprint Verification system.

Chapter 4 provides details about implementation of the software and GUI (Graphical User Interface) and finally

Chapter 5 concludes the work and gives the future scope of the work done.

FINGERPRINT BIOMETRICS

2.1. INTRODUCTION:

Fingerprints have been used for verification and identification purposes since the dawn of civilization. It is the oldest and most commonly accepted form of biometrics technology. Ancient kings and queens sealed letters and authenticated them with their fingerprints on hot wax thousands of years ago. Over a hundred years ago, both the United States and Europe began documenting the use of fingerprints for identification and verification purposes.

Amazingly, after all this time, and millions of fingerprints later, no two identical fingerprints have ever been found. Based on this kind of hard physical evidence, it is safe to say that fingerprints are truly a unique human characteristic. No other biometrics technology can boast this level of scientific history and evidentiary support. Accordingly, its advantage over other biometric solutions lies in its historically and scientifically proven accuracy, reliability, convenience, user acceptance and familiarity.

2.2. COMMON TYPES OF FINGERPRINTS:

Fingerprint patterns are divided into three main groups consisting of: Arches, Loops and Whorls. Approximately 5% of all fingerprints are Arches, 30% are Whorls and 65% are Loops. [6]

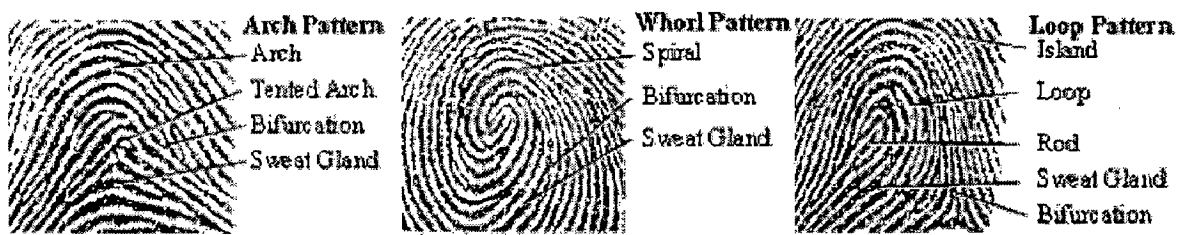


Figure 2.1: Common types of Fingerprints

COMMON LINE TYPES (SHAPES) FOUND IN FINGERPRINTS:

Fingerprint patterns are made up of 'line-types' (shapes) which determine the general classification characteristics of the print (i.e., Arch, Loop or Whorl). The 'Pattern Area', is a term used to describe the center area of a print which contains many of the line-types. This area and its contents determine the classification of the print (i.e., Arch, Loop, Whorl, etc.). The following *Figure 2.2* represents the most common line-types found in fingerprints.



ROD-A Rod generally forms a straight line. It has little to no recurve features and tends to be found in the center of the fingerprint's pattern area.



ELLIPSE-An Ellipse is a circular or oval shaped line-type which is generally found in the center of Whorl patterns.



SPIRAL-A Spiral line-type spirals out from the center of the fingerprint and is generally found in Whorl print patterns.



BIFURCATION-Is the intersection of two or more line-types which converge or diverge.



TENTED ARCH-Resembles a tent. This line-type quickly rises and falls at a steep angle. They tend to be associated with Tented Arch pattern prints.



LOOP-A Loop is a recurve line-type that enters and leaves from the same side of the fingerprint.



ISLAND-An Island is a line-type which stands alone. (i.e., does not touch another line-type and is totally contained in the pattern area of interest.)



SWEAT GLAND-The finger contains many sweat glands. The moisture and oils they produce actually allow the fingerprint to be electronically imaged.

Figure 2.2: Common types of lines found in Fingerprints

FEATURES AVAILABLE FOR BIOMETRIC IDENTIFICATION:

Coarse features (Loops, Archs, Whorls): Coarse features have strong genotypic contributions and are suited for presorting during identification with a very large data base.

Fine features (minutia): The minutiae are predominantly random in nature and cause most of the uniqueness in a fingerprint. Therefore, either directly or indirectly (in picture correlation procedures), almost all fingerprint systems examine minutia.

Pore structure: Pore structure is seldom used, due to large fluctuations in the quality of the scanning procedure.

2.3. ADVANTAGES & DISADVANTAGES OF FINGERPRINT BIOMETRICS:

Advantages:

- ❖ Considerably High Level of Accuracy.
- ❖ Easy to use devices when compared to Iris or Retina Scanners.
- ❖ Ability to enroll multiple fingers.
- ❖ Increased Government and Industry adoption.

Disadvantages:

- ❖ Inability to enroll some users like manual laborers, very old people etc. who have a lower quality fingerprint image.

2.4. FINGERPRINT SENSOR TECHNOLOGIES:

2.4.1. OPTICAL TYPE:

Ink and paper are the tried-and-true way to take fingerprints, but technology has found ways to eliminate smudges and ink stains. Newer 'live-scan' readers use frustrated refraction over a glass prism. The finger is illuminated from one side with a LED while the other side transmits the image through a lens to a CCD (Charge Coupled Device) camera. Old readers were obliged to use a frame grabber to convert the video signal into digital information that could be processed by the computer. [7,8].

Optical sensors are quite common, though they were very expensive in the past, and even now, system cost cannot be extremely low because of the cost and mechanical assembly of the prism, lens and camera. Size cannot be reduced substantially due to

required focal lengths, and very often, there is a large distortion of the image because of the difficulty of focusing an image in such a small space. This distortion can be compensated for by software (if one knows the characteristics of the reader), but still, this distortion may even vary from one reader to another of the same model.

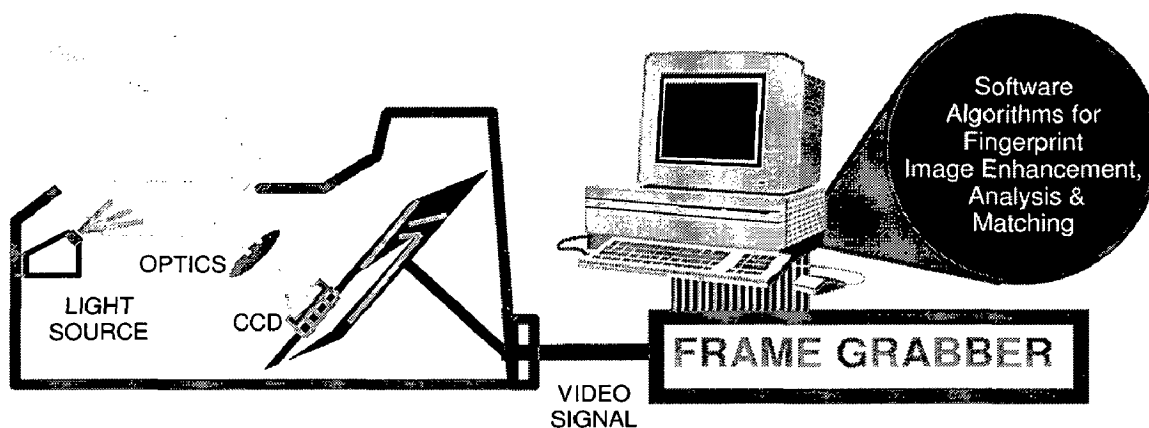


Figure 2.3: Optical Type Sensor

Kinetic Sciences Inc (KSI):

It is one of the vendors which produce Optical Finger Print Sensors. Its model KC-901 is shown in *Figure 2.4*.

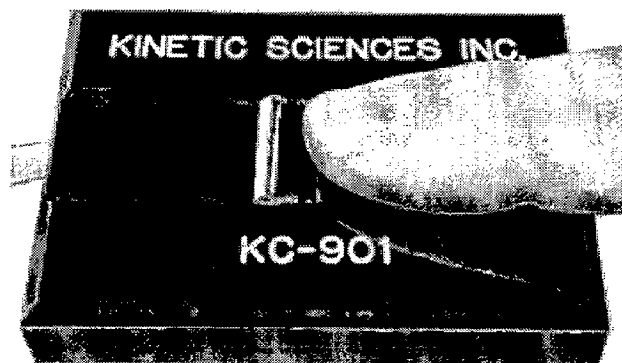


Figure 2.4: KSI's (KC-901) Optical Fingerprint Sensor

The KSI fingerprint sensor [8] is a low cost, compact optical device for capturing high quality images of a fingerprint. The device consists of miniaturized optics, LED illumination, and CMOS sensing and processing. The unit has no moving parts and is designed to easily integrate into any system. A user uses the sensor by simply sliding

their finger over the sensing window anytime while it is illuminated. The raised sensing window allows for low finger pressure. The KC-901 is an external sensor with high speed serial interface for evaluation of the Kinetic Sciences Inc technology.

Sensor Characteristics

- ❖ Low cost
- ❖ Very high optical quality
- ❖ Wet & dry finger tolerant
- ❖ Low finger pressure required
- ❖ Rugged, reliable, ESD safe

Specifications

- ❖ 250, 500, 725 & 900 approximate dpi
- ❖ up to .75" x 1" or longer
- ❖ b/w, 2, 4 or 8-bit images
- ❖ PCB Area: 2.1" x 2.7" (5.3 x 6.8cm)
- ❖ height: 6.3mm internal (including cover), 1.8mm protruding
- ❖ built-in light source (red)
- ❖ expected product life of 10 years

Applications

- ❖ Computer & Network Security
- ❖ E-commerce
- ❖ Database & file security
- ❖ Access control (building, vehicle)
- ❖ Laptop theft prevention
- ❖ Automated teller machine access
- ❖ Home security
- ❖ Point-of-sale terminals
- ❖ Cell-phone access

2.4.2. CAPACITANCE TYPE FINGERPRINT SENSOR:

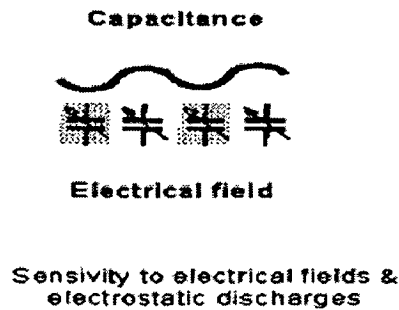


Figure 2.5: Capacitive Sensing Type

This is the most popular effect today. Several companies produced a device based on the measurement of the capacitance between the skin and the pixel. Where there is a ridge or a valley, the distance varies, as does the capacitance. *Figure 2.6* explains the working principle of Capacitive Sensing Fingerprint technology. [9]

Principle:

The finger chip consists of a number of sensor cells. Each sensor cell on the chip registers one pixel and contains an active capacitance feedback circuit whose effective capacitance is modulated by the presence of live skin close to the sensor surface.

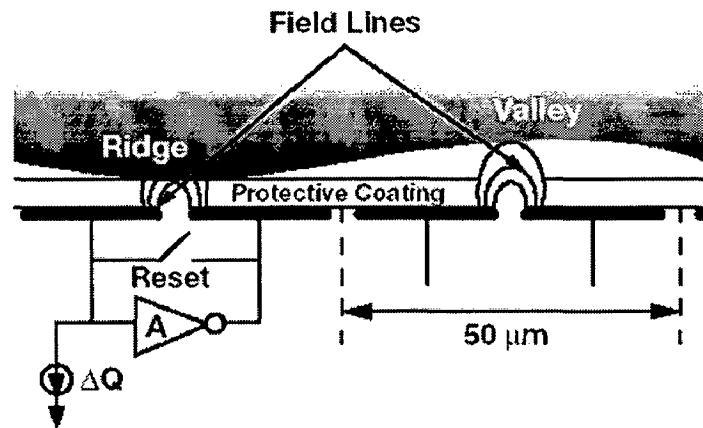


Figure 2.6: Capacitive Sensing Type Fingerprint sensor

The surface of each sensor cell consists of two adjacent metal plates that are separated from the skin and the environment by an ultra hard protective coating. The sensor plates are connected in an active feedback circuit with one plate connected to the input of an

inverting amplifier and the other connected to the amplifier's output to form a charge integrator. Thus, the charge integrator converts the feedback capacitance of the sensor cell to an output voltage that corresponds to the distance between the sensor plates of that cell and the skin above it.

Between the sensor plates is a fringing capacitance whose field lines extend beyond the silicon surface. When live skin comes close to the sensor plates, it interferes with the field lines between the plates, reducing the effective capacitance between them. Therefore, skin at a fingerprint ridge falls on the sensor surface, minimizing feedback capacitance, while skin at a fingerprint valley is off the sensor the surface, maximizing feedback capacitance.

Working: The sensor cell works in two phases: reset phase and sensing phase.

- ❖ **Reset phase:** In this phase the input and output of the inverter are shorted through a reset switch. This short causes the charge integrator output to settle to the logical threshold of the inverter.
- ❖ **Sensor Phase:** In this phase, the reset switch opens and a calibrated charge is applied to the input-side sensor plate. The effect is to change the charge integrator output by an amount proportional to the feedback capacitance between the sensor cells. Because the feedback capacitance of a fingerprint ridge is smaller than that of a fingerprint valley, the output swing for a sensor cell that is under a ridge is greater than the swing for a sensor cell under a fingerprint valley. The entire fingerprint image is captured by a two dimensional array of sensor cells. The array is addressed in a random access mode through row and column decoders. This provides for such advanced functions as “windowing” and sub sampling. Moreover, the output of the sensor array goes through an analog signal-conditioning block that allows for adjustment of the sensor gain and offset before the signal is digitized to an 8-bit word by on an on-chip analog-to-digital converter.

2.4.3. THERMAL TYPE:

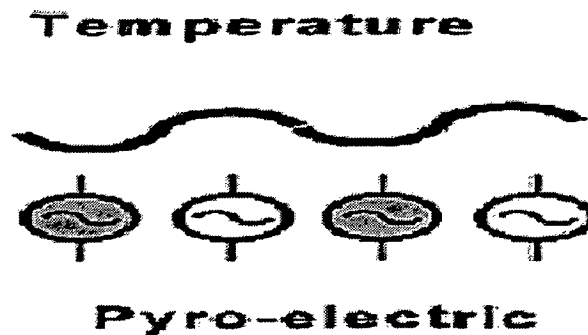


Figure.2.7: Thermal Sensing Type Fingerprint sensor

Pyro-electric material is able to convert changes in temperature (ΔT) into a specific voltage. This effect is quite large, and is used in infrared cameras. This type of sensor does not measure the difference of temperature between the skin in the ridges and valleys, because the difference is negligible. In fact, as the finger is directly placed on the material, the ridge's temperature is what is measured, as it is in contact. The valleys do not make contact, so the temperature of the pyro-electric material under the valleys remains almost unchanged.

Drawback:

A significant drawback of the technique is that the image disappears quickly. When we place a finger on the sensor, there is a big change of temperature, and therefore signal, but after a short period (less than a tenth of a second), the image vanishes. The finger and the chip have reached thermal equilibrium, and as there is no change in temperature, there is no signal.

2.4.4. ACOUSTIC (ULTRASOUND) SENSORS:

Ultrasound technology, though considered perhaps the most accurate of the fingerprint technologies, is not yet widely used. The finger surface on the glass is recorded by very high frequency ultrasound (e.g., 50 MHz). It transmits acoustic waves and measures the distance based on the impedance of the finger, the platen, and air.

Advantages of Ultrasound Technology:

- ❖ Ultrasound is capable of penetrating dirt and residue on the platen and the finger, countering a main drawback to optical technology.
- ❖ Its main advantage is the reading of the derma, the sub-surface of the skin, rather than the surface.

Disadvantages of Ultrasound Technology:

- ❖ Ultra-sound sensing requires quite a big device with mechanical parts, and is quite expensive.
- ❖ It takes a few seconds to grab an image. It is not suited for large production volumes at low cost.

Until ultrasound technology gains more widespread usage, it will be difficult to assess its long-term performance. However, preliminary usage of products from Ultra-Scan Corporation (USC) indicates that this is a technology with significant promise. It combines the strength of optical technology, large platen size and ease of use, with a strength of silicon technology, the ability to overcome sub-optimal reading conditions.

2.5. FINGERPRINT SENSOR USED:

TouchChip™ (Model: TCRU1A) fingerprint sensor is used to acquire the fingerprint of the user. This is developed by STMicroelectronics which is one the leading vendors of Capacitive type fingerprint sensor. Its model **TouchChip™** (TCRU1 A) is as shown in the *Figure 2.8* and has the following characteristics. [7, 9]

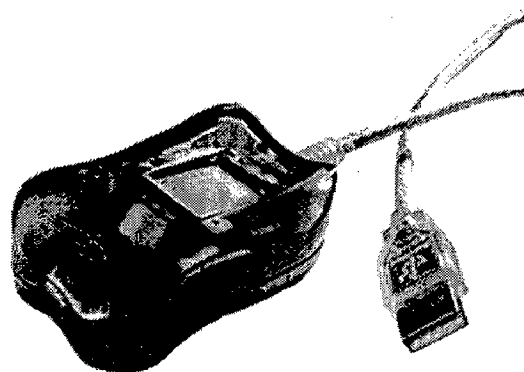


Figure 2.8: Touchchip™ Fingerprint Sensor (TCRU1 A)

Characteristics:

- ❖ This model is a Silicon Finger Print Sensor
- ❖ This is based on CMOS Active Capacitive Pixel Sensing.

Applications:

- ❖ For Desktop security
- ❖ For Network security
- ❖ For Verification and identification systems

Specifications:

Model	:	TCRU1A
Sensor size	:	12.8 X 18 mm
Array size	:	256 X 360 pixels
Array Pitch	:	50 microns
Image Resolution	:	508 DPI
Capture Rate	:	15 frames per second
Package Size	:	27 x 20.4 x 3.5 mm
Cable	:	USB

2.6. DATA ACQUISITION:

TouchChip™ (TCRU1A) sensor is used to acquire the online fingerprint image from the users. A database of fingerprints is created with these fingerprint images of different users obtained from the sensor.

2.6.1. FINGERPRINT IMAGE DETAILS:

The technical details of the image obtained from TouchChip sensor are

Sensor used	:	(TCRU1 A) TouchChip Fingerprint Sensor
Type of the image	:	Bit map image (bmp), RGB color image
Width	:	253 pixels
Height	:	357 pixels
Horizontal Resolution	:	96 dpi (Dots per inch)
Vertical Resolution	:	96 dpi

2.6.2. DATABASE DETAILS:

A database of fingerprints obtained from different users has been created. The database is created for 50 users. Each user is asked to submit 3 fingerprint images of the same fingerprint. The database details are given below

Name of the Database created	:	IITRDB
Number of subjects	:	50
Number of fingerprints per subject	:	3
Total number of fingerprints	:	150

This 'IITRDB' database serves as the live field data and is used to analyze the performance of the overall Fingerprint verification Algorithm implemented.

FINGERPRINT VERIFICATION

3.1. INTRODUCTION:

Traditionally, there are two main types of features in fingerprints:

1. Minute details associated with local ridges and valleys (minutiae), and
2. Global ridge and valley structures which form a special pattern in the central region of the fingerprints.

Based on these features there are two main types of fingerprint verification algorithms.

3.1.1. MINUTIAE BASED:

The minutiae-based algorithm first locates the minutiae points on the fingerprint image. Each minutia is completely characterized by the following parameters: x-coordinate, y-coordinate, and *orientation* (refer to **Figure 3.1.** for their definition). A typical live-scan fingerprint image of good quality, has about 50-100 minutiae. The pattern of the minutiae details of a fingerprint form a valid representation of the fingerprint. This pattern of minutiae details forms the template of the fingerprint and is used for the fingerprint matching. [10, 11]

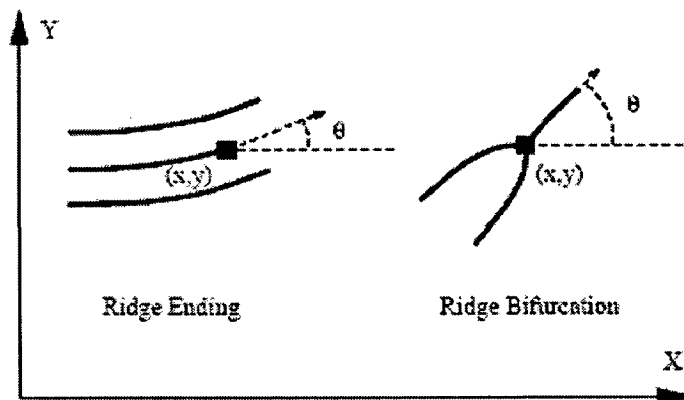
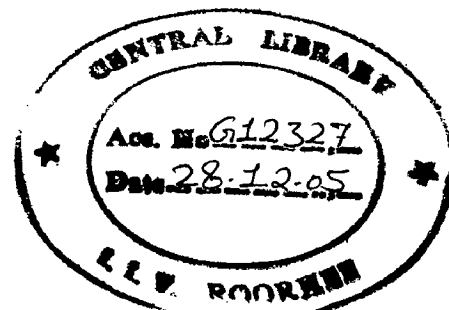


Figure 3.1: Characterization of Minutiae.



3.1.2. FILTER BANK BASED:

In case of filter bank based fingerprint algorithm, a bank of oriented filters (filters oriented in a particular direction) is used to extract the features of fingerprint. Each filtered image has ridge information oriented along the filter direction. For each of these oriented images, variance of pixel intensities, at different parts of the image are noted. These variance values for all the oriented images forms a valid representation of fingerprint. Though the minutiae-based representation is the most popular representation of fingerprints it has some draw backs like

- It doesn't take into account the global information of fingerprint like global pattern of ridges and valleys, inter-ridge distances, and overall patterns of ridge flow.
- If a typical fingerprint contains 46 minutiae, then an automatic fingerprint verification system that makes its decision based on 12 minutiae correspondences is utilizing only a limited amount of information for its verification.

Due to the limited amount of information present in the minutiae representation of fingerprints, it is desirable to use filter bank-based representation of fingerprints for automatic matching which eliminates the above said weaknesses. This filter bank-based representation of fingerprints not only takes into account the local anomalies in the ridge structure (e.g., minutiae), but also, accounts for the global pattern of ridges and valleys, inter-ridge distances, and overall patterns of ridge flow. Further, it is an added advantage to design representations which can be automatically and reliably extracted from the fingerprint and whose extraction will degrade gracefully with deterioration in the quality of the fingerprints.

3.2. FILTER BANK BASED VERIFICATION:

Fingerprints have a well defined local ridge frequency and orientation. If these local frequency and orientation features are captured then these features become quite differentiating features for fingerprints. The main idea of Filter bank based fingerprint representation is to extract these features with the help of a bank of orientation filters. Overall algorithm is shown in *figure 3.2*.

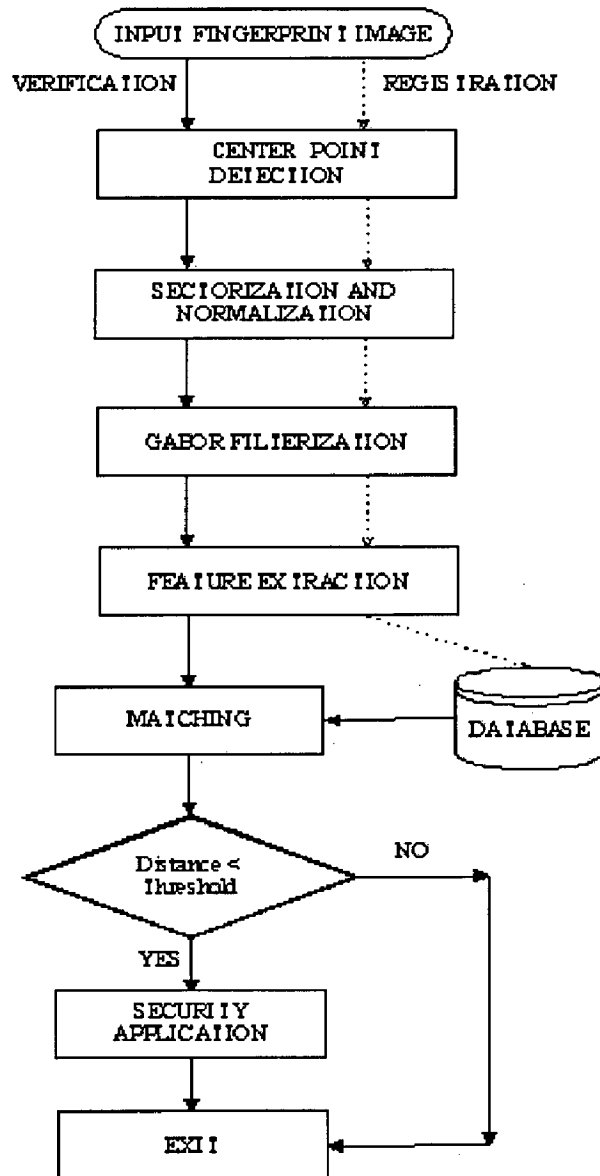


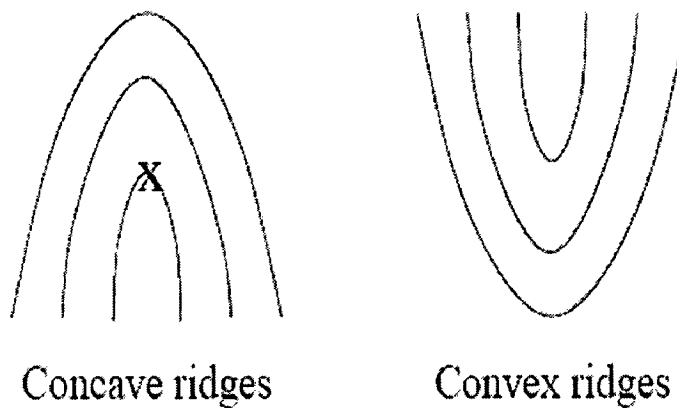
Figure 3.2: Flow chart for filter bank based verification.

In the filtered bank based Algorithm, [12] first the input fingerprint image is acquired from a sensor. The center point (the point of maximum curvature of the concave ridges) is detected on fingerprint which acts the reference for fingerprint feature extraction. The image is divided into sectors around the center point and each sector is normalized separately to a constant mean and variance. This normalized image is given to a bank of Gabor filters (orientation filters) to obtain filtered images along different orientations. These filtered images are again sectorized and the variance of pixel

intensities in each sector in all the filtered images forms the template of fingerprint. This template is stored in the database during the registration. During the verification process when the user gives his fingerprint the same features are extracted and compared with the stored template. Depending on the distance between the two fingerprint features the user is either accepted or rejected.

3.3. CENTER POINT DETECTION:

We define the center point of a fingerprint as the point of maximum curvature of the concave ridges (see *Figure 3.3.*) in the fingerprint image.



*Figure 3.3: Concave and convex ridges in a fingerprint image.
'X' marks the center point.*

3.3.1. ALGORITHM FOR CENTER POINT DETECTION:

The fundamental steps in the center point detection of fingerprint are

- (i) Divide the input image, into non overlapping blocks of size $W \times W$.
- (ii) Compute the gradients $\partial_x(i, j)$ and $\partial_y(i, j)$ at each pixel (i, j) . Any operator can be used depending on the computational requirement. Sobel operator is used to find the gradients of the image.

Masks for Sobel operation:

Mask size : 3 X 3

$$G_x = \begin{array}{|c|c|c|} \hline -1 & -2 & -1 \\ \hline 0 & 0 & 0 \\ \hline 1 & 2 & 1 \\ \hline \end{array}$$

$$G_y = \begin{array}{|c|c|c|} \hline -1 & 0 & 1 \\ \hline -2 & 0 & 2 \\ \hline -1 & 0 & 1 \\ \hline \end{array}$$

Zeros are added around the image so as to maintain the same size of the image after applying the mask.

(iii) Estimate the local orientation of each block centered at pixel (i,j) using the following equations

$$V_x(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u, v)\partial_y(u, v), \quad (3.1)$$

$$V_y(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} (\partial_x^2(u, v) - \partial_y^2(u, v)), \quad (3.2)$$

$$O(i, j) = \frac{1}{2} \tan^{-1} \left(\frac{V_y(i, j)}{V_x(i, j)} \right), \quad (3.3)$$

where $w =$ size of the block ($w=10$)

$O(i,j)$ = Least square estimate of the local ridge orientation at the block centered at pixel(i,j).Mathematically $O(i,j)$ represents the direction that is orthogonal to the dominant direction of the *Fourier Spectrum* of the $W \times W$ (10 X 10) window.

(iv) Smooth the orientation field in a local neighborhood. In order to perform smoothing(Low pass Filtering), orientation image needs to be converted into a *continuous vector field*.

$$\begin{aligned} \Phi_x(i, j) &= \cos(2 * O(i, j)) \\ \Phi_y(i, j) &= \sin(2 * O(i, j)) \end{aligned} \quad (3.4)$$

Where Φ_x = x component of continuous vector field.

Φ_y = y component of continuous vector field.

With this vector Low pass filtering is performed as

$$\Phi'_x(i, j) = \sum_{(u=-w_\Phi/2)}^{(w_\Phi/2)} \sum_{(v=-w_\Phi/2)}^{(w_\Phi/2)} W(u, v) * \Phi_x(i-uw, j-vw) \quad (3.5)$$

$$\Phi'_y(i, j) = \sum_{(u=-w_\Phi/2)}^{(w_\Phi/2)} \sum_{(v=-w_\Phi/2)}^{(w_\Phi/2)} W(u, v) * \Phi_y(i-uw, j-vw) \quad (3.6)$$

where

W is a 2 dimensional Low pass Filter with unit integral

$w_\Phi \times w_\Phi$ is the size of filter

It is to be noted that Smoothing operation is performed at block level.

$$\text{Smoothed orientation field } O'(i, j) = \frac{1}{2} * \tan^{-1} \left(\frac{\Phi'_y(i, j)}{\Phi'_x(i, j)} \right) \quad (3.7)$$

Filter used:

Filter size : 5 X 5 Mean Filter

Filter coefficients:

$$\frac{1}{25} *$$

1	1	1	1	1
1	1	1	1	1
1	1	1	1	1
1	1	1	1	1
1	1	1	1	1

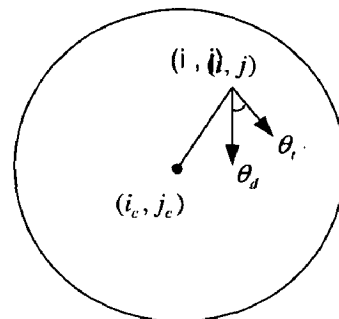
(3.8)

(v) Let D be the smoothed orientation image with d(i,j) representing the local ridge direction at pixel (i,j).

(vi) Initialize the image L with the same size of D. L will be used to indicate the center point.

(vii) As shown in fig for the each pixel (i_c, j_c) in D , define a local region S , centered around (i_c, j_c) . Assign the corresponding pixel in L the value of the following summation. [13]

$$L(i_c, j_c) = \sum_{(i,j) \in S} |\cos(\theta_r(i, j) - \theta_d(i, j))|. \quad (3.9)$$



$\theta_d(i, j)$ represents the local ridge direction of a pixel (i, j) in S .

$\theta_r(i, j)$ represents the direction perpendicular to the line joining (i, j) and (i_c, j_c) .

(viii) If (i_c, j_c) is the center of the ridges curves θ_d , θ_r will be similar at most points within S , thus will produce high value in L .

3.3.2. RESULTS:



Figure 3.4: Center point (marked as X) detected for various fingerprints

3.4. SECTORIZATION AND NORMALIZATION:

3.4.1. INTRODUCTION:

Sectorization is the process of dividing the image into sectors around the center point. Sectorization of the image is mainly carried out for Feature extraction of fingerprint. Before Sectorization center point is moved 50 pixels below the actual center point in order to retain the features corresponding to center point. This new center point is known as pseudo center.

No of circular bands =Ncb = 5

Width of circular band=20 pixels

Radius of central circle=10 pixels

Angle per sector (Aps)= 30⁰

Number of sectors per band (Nspb)= 360⁰/Aps=360⁰/30⁰ = 12

Total no of Sectors =Nspb X Ncb = 12 X 5 = 60

In some fingerprints depending on the effective area of fingerprint selected around the pseudo center point, the image is sectorized into 12 or 24 or 36 or 48 or 60 sectors.

Normalization is the method of restricting the pixel intensities to the required levels. Sector normalization is performed in fingerprints to remove the effects of sensor noise and gray level deformation due to finger pressure differences.

For all pixels in Sector S_i (i ∈ 1, 2 ,3 , Total number of sectors)

Normalized Image is defined as

$$N_i(x, y) = \begin{cases} M_0 + \sqrt{\frac{V_0 (I(x, y) - M_i)^2}{V_i}} & \text{if } I(x, y) > M_i \\ M_0 - \sqrt{\frac{V_0 (I(x, y) - M_i)^2}{V_i}} & \text{Otherwise} \end{cases} \quad (3.10)$$

Where

N_i(x,y) denotes the Normalized gray level at pixel (x,y).

M₀ and V₀ denote the desired mean and variance values respectively.

$I(x,y)$ denote the gray value at pixel (x,y)

M_i and V_i denote the estimated mean and variance of sector S_i respectively.

With this Equation the fingerprint image is normalized in each sector to constant mean and variance.

3.4.2. RESULTS:

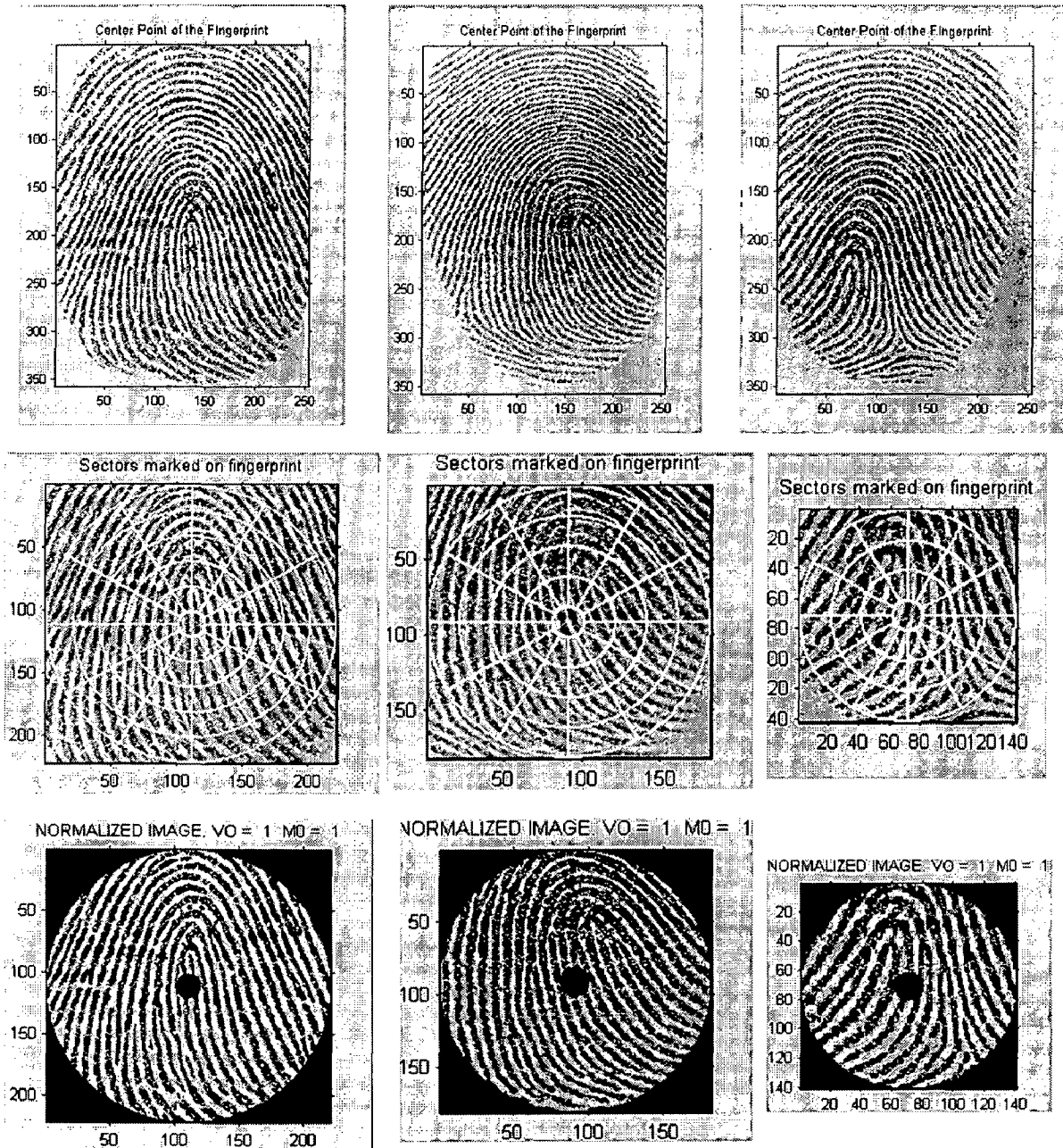


Figure 3.5: Results of the Sectorization and normalization

3.5. FILTERIZATION:

3.5.1. INTRODUCTION:

Fingerprints have a well defined local ridge frequency and orientation. If these local frequency and orientation features are captured then they become quite differentiating features for fingerprints. Gabor Filters on the other hand have a very well defined frequency and orientation (see *Figure 3.6.*).So, a properly tuned Gabor filter removes the noise, preserves the true ridge and valley structures and provides the local information contained in a particular direction in the image.[14,15]

A minutia point can be viewed as an abnormality in locally parallel ridges and this vital information is captured using the Gabor filters. Thus the filter bank based fingerprint verification Algorithm, in addition to the global ridge and valley patterns it also uses the local ridge and valley structures for feature extraction.

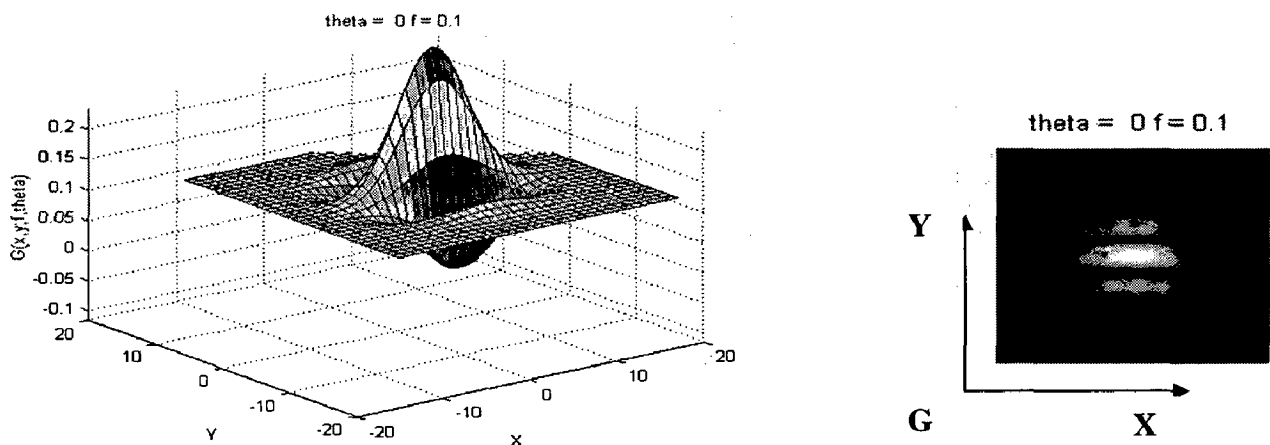


Figure 3.6: a) Gabor filter oriented at 0^0 b) Top view of Gabor filter.

3.5.2. GABOR FILTER ANALYSIS:

A Gabor filter is defined by a sinusoidal plane wave (second term of **Equation (3.11)**) tapered by a Gaussian (the first term in **Equation (3.11)**).Gabor filters have both frequency selective and orientation selective properties and have optimal joint resolution in both spatial and frequency domains. The even symmetric two dimensional Gabor filter in the spatial domain has the general form [16, 17, 18]

$$g(x, y; f, \theta) = e^{-\frac{1}{2} \left(\frac{x_{\theta}^2}{\sigma_x^2} + \frac{y_{\theta}^2}{\sigma_y^2} \right)} \cdot \cos(2\pi f \cdot x_{\theta}) \quad (3.11)$$

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

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

where $g(x, y; f, \theta)$ denotes the Gabor filter value in spatial domain

x & y denote the x and y co ordinates of the Gabor filters

f denotes the frequency of the sinusoidal plane wave in the direction Θ from x-axis.

σ_x and σ_y denote the standard deviations of the Gaussian envelope along x & y-axes separately.

To apply Gabor filter to an image, the four parameters (θ , f , σ_x , σ_y) must be specified. The frequency of the filter is completely determined by the local ridge frequency and the orientation is determined by the local ridge orientation.

The selection of the values σ_x and σ_y involves trade off. The larger the values of σ_x and σ_y , the more robust the filters are to the noise in the fingerprint image, but also are more likely to create spurious ridges and valleys. On the other hand, the smaller the values, the less likely the filters are to introduce spurious ridges and valleys but then they will be less effective in removing the noise. If σ_x and σ_y (standard deviations of the Gaussian envelope) values are too large, the filter is more robust to noise, but is more likely to smooth the image to the extent that the ridge and valley details in the fingerprint are lost. If σ_x and σ_y values are too small, the filter is not effective in removing the noise.

3.5.3. IMPLEMENTATION:

The specifications of the Gabor filters used in this analysis are

- Size of the Gabor filter : **33X33**
- Standard deviations of the Gaussian envelope $\sigma_x = \sigma_y = 4$.
- Orientation θ varying between 0^0 , 30^0 , 60^0 , 90^0 , 120^0 , and 150^0 .
- Frequency of the filter $f = 1/(\text{Inter ridge distance}) = 1/10 = 0.1$.

In our implementation, the filter frequency is set to the average ridge frequency ($1/K$), where K is the average inter-ridge distance. The average inter-ridge distance is approximately 10 pixels in a 500 dpi fingerprint image. If f is too large, spurious ridges are created in the filtered image whereas if f is too small, nearby ridges are merged into one. The values for σ_x and σ_y are each set to 4.0 (about half the average inter-ridge distance).

3.5.4. RESULTS:

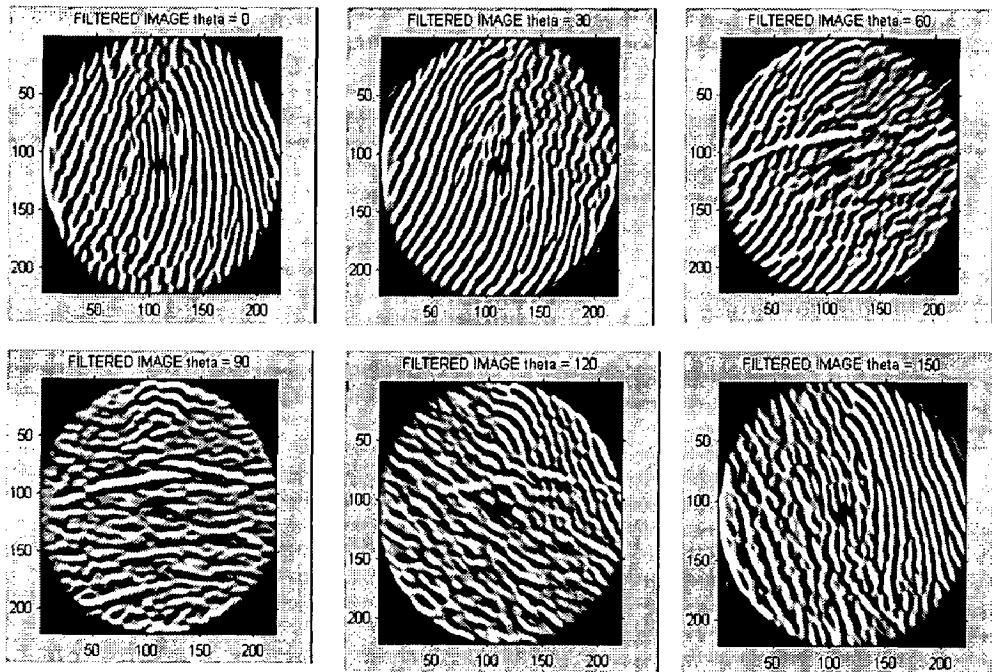


Fig 3.7: Filtered images

The normalized region of interest in a fingerprint image is convolved with each of these six filters to produce a set of six filtered images. A fingerprint convolved with a 0^0 oriented filter accentuates those ridges which are parallel to the 0^0 -axis and smooths the ridges in the other directions. Filters tuned to other directions work in a similar way. These six directional-sensitive filters capture most of the global ridge directionality information as well as the local ridge characteristics present in a fingerprint.

3.6. FEATURE EXTRACTION:

3.6.1. INTRODUCTION:

Feature Extraction is the process of extracting the discriminating features of fingerprint. Variances of each sector in each of the filtered images, forms the feature vector of fingerprint. Variance of a data is defined as the average of the sum of the squares of the deviation from the mean. The equation for variance of n point data is defined as

$$V = \frac{1}{n-1} \left(\sum_{i=1}^n (X_i - \bar{X})^2 \right) \quad (3.12)$$

where,

V denotes the variance of n data points

X_i denotes the value of each element and

\bar{X} denotes the mean of the n data points

3.6.2. FEATURE VECTOR:

Let $F_{i\theta}$ be the θ -direction filtered image for sector S_i . The feature vector $V_{i\theta}$ is defined as

$$V_{i\theta} = \frac{1}{K_i - 1} \left(\sum_{K_i} (F_{i\theta}(x, y) - \bar{X}_{i\theta})^2 \right) \quad (3.13)$$

where $V_{i\theta}$ is the variance of sector S_i corresponding to θ - direction filtered image.

K_i is the number of pixels in sector S_i

$F_{i\theta}(x, y)$ is the θ - direction filtered image for Sector S_i

$\bar{X}_{i\theta}$ is the mean of the pixels of $F_{i\theta}(x, y)$ in sector S_i .

i varies from 1, 2, 3,, 60 (No of sectors per filtered image)

θ varies in between 0^0 , 30^0 , 60^0 , 90^0 , 120^0 , and 150^0 .

Feature vector of the fingerprint represents the group of features which completely represent the fingerprint. The variance of each sector in each of the six filtered images defines the components of the feature vector. This Feature vector is called FingerCode.

3.6.3. IMPLEMENTATION:

In the present analysis,

No of sectors per filtered image = 60

No of variance values for each filtered image = 60

No of filtered images =6

Total number of variance values = $60 \times 6 = 360$.

These 360 variance values represent the feature vector of the fingerprint.

3.6.4. RESULTS:

The 360 dimensional feature vectors for fingerprint image shown as gray level images with six disks, each disk corresponding to one filtered image in *Figure 3.8*.

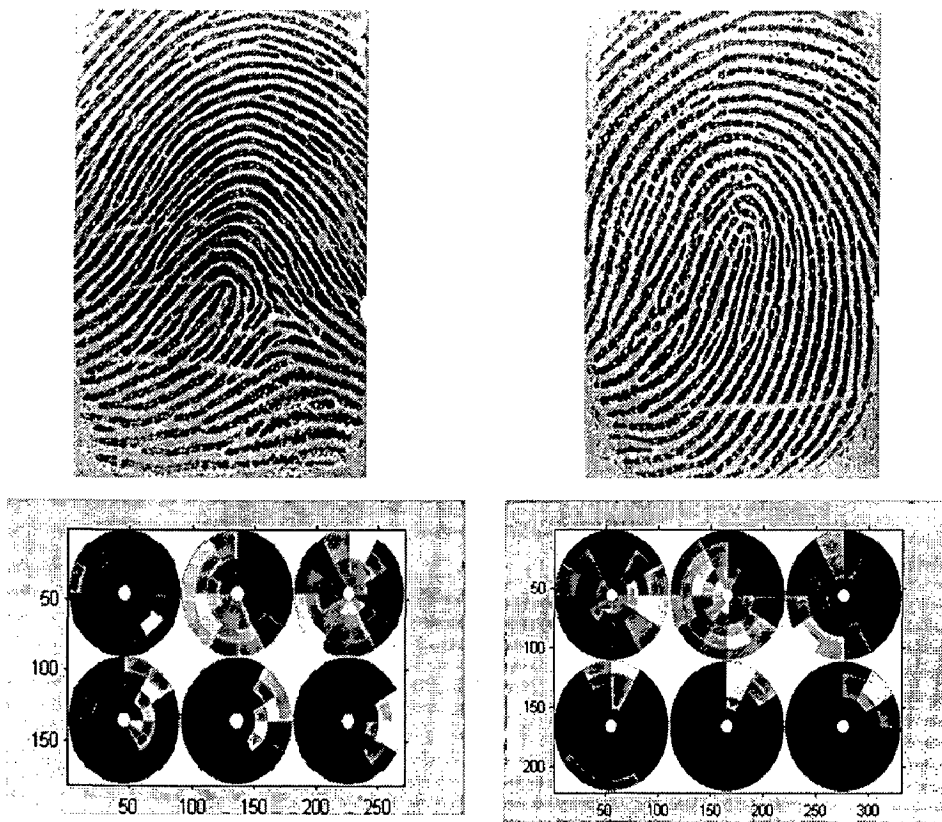


Figure 3.8: Feature vector of the fingerprints.

3.7. FINGERPRINT MATCHING:

3.7.1. INTRODUCTION:

Fingerprint Matching is based on Euclidean distance between the corresponding FingerCodes. The Euclidean distance between the FingerCodes, helps in detecting the genuineness of the user. The distance between the FingerCodes of the same user will not be zero as assumed. Instead there will be certain distance between the fingerprints of the same user. This is due to the small translation in the images, rotation in the images and different pressure differences in the images due to the ineffectiveness of the user in maintaining the same pressure and same location on the fingerprint sensor.

3.7.2. ACCEPT/REJECT DECISION:

The Euclidean distance between two FingerCodes is defined by

$$FpDist = \sum_{\theta=0^{\circ}}^{150^{\circ}} \sum_{i=1}^{60} (FC1_{i\theta} - FC2_{i\theta})^2 \quad (3.14)$$

where FpDist denotes the distance between the two fingerprints

FC1_{iθ} and FC2_{iθ} are the FingerCodes of the Fingerprint 1 and Fingerprint 2

i varies from 1, 2, 3,.....,60(No of sectors per filtered image)

θ varies in between 0°, 30°, 60°, 90°, 120°, and 150°.

Based on the distance between the two fingerprints, the user is either accepted or rejected.

If FpDist < threshold

ACCESS TO SECURITY APPLICATION

Else

REJECT THE USER.

If the distance FpDist is less than predefined threshold then the user is given access to the security application and he is identified as genuine user. On the other case if the distance FpDist is greater than the threshold the user is rejected and is identified as unauthorized user.

3.7.3. RESULTS:

To fix up the threshold for the verification, each of the 3 fingerprints of a user was compared with the rest of the 2 fingerprints of the same user and the distances of each of

these comparisons are recorded. The average of all these distances recorded represents the average distance between the fingerprints of the same user. This process is repeated for all the 50 users. The mean of all the 50 average distances is taken as the threshold for the verification. The threshold thus obtained is **542.43**.

False Acceptance ratio (FAR) is defined as the no of false acceptances to the total number of comparisons made for false acceptances. This ratio indicates the number of times an unauthorized person is given authorized access.

False Reject ratio (FRR) is defined as the number of False rejects to the total number of comparisons made for false rejects. This ratio indicates the number of times an authorized person is rejected as a false user. [19]

Let fp_{i_j} represent the i^{th} fingerprint of j^{th} user and let the database contains 50 users with 3 fingerprint images from each user. Then to find the false acceptance rate

Fp _{1_1} is compared with fp _{1_2} , fp _{2_2} ,fp _{3_2} ,.....,fp _{3_50}	147 comparisons
Fp _{2_1} is compared with fp _{1_2} , fp _{2_2} ,fp _{3_2} ,.....,fp _{3_50}	147 comparisons
Fp _{3_1} is compared with fp _{1_2} , fp _{2_2} ,fp _{3_2} ,.....,fp _{3_50}	147 comparisons
Fp _{1_2} is compared with fp _{1_1} , ..fp _{3_1} ,fp _{1_3} ,.....,fp _{3_50}	147 comparisons
Fp _{3_50} is compared with fp _{1_1} , fp _{2_1} ,fp _{3_1} ,.....,fp _{3_49}	147 comparisons
Total No of comparisons	----- 147 X 150 comparisons -----

FAR =no of false acceptances/Total no of comparisons for false acceptance.

Where Total no of comparisons for false acceptance= 147 X 150 = 22050

No of false accepts indicates the number of times distance between the fingerprints of two different users is less than the threshold.

Similarly

FRR = no of false rejects /Total no of comparisons for false rejection.

Where, Total no of comparisons for false rejection=2X150=300.

No of false rejects indicates the number of times the distance between fingerprints of the same user is greater than the threshold.

Table 3.1. indicates the FAR and FRR values for various thresholds. The plot of FAR vs FRR is displayed in **Figure 3.9**. The overall system developed is sufficiently good enough in verifying the identity of an individual to provide access for secure applications

S.No	Threshold	FAR (%)	FRR (%)
1	300	5.29	73.33
2	542.43	23.65	27.67
3	1000	41.96	14.33
4	1500	74.56	8.67

Table 3.1: FAR and FRR values for various thresholds for IITRDB database.

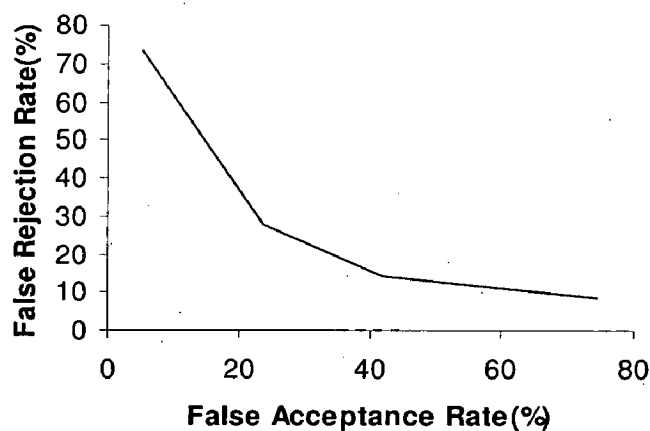


Figure 3.9: Plot of FAR vs FRR for IITRDB database.

IMPLEMENTATION OF SOFTWARE AND GUI

All the algorithms for fingerprint verification have been implemented in MATLAB. This offers flexibility in terms of GUI development and interfacing devices and is also easy to program like C. [20]

There are basically 2 modules that have been developed. The first being the registration module. In this each user is asked to give 3 fingerprints. Relevant features from these and the raw data itself are stored in the database for future retrieval and verification. The interface and procedure for the same is shown in following *figure 4.1* *figure 4.2* and *figure 4.3*.

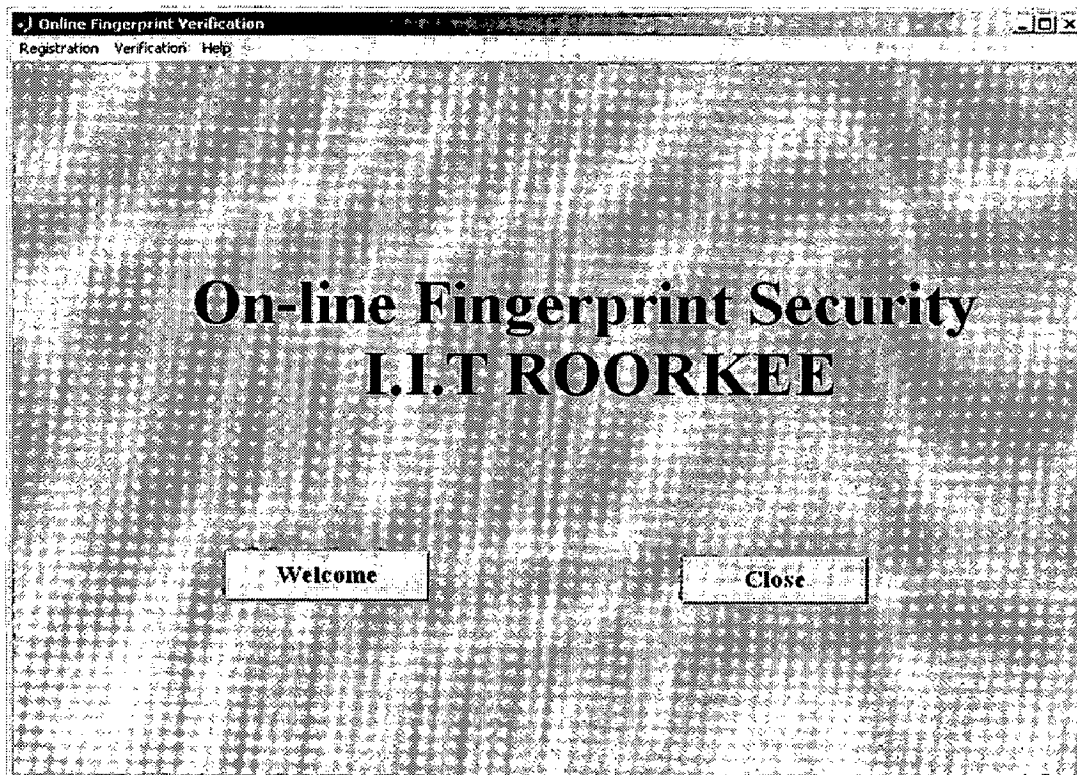


Figure.4.1: Welcome page for the modules.

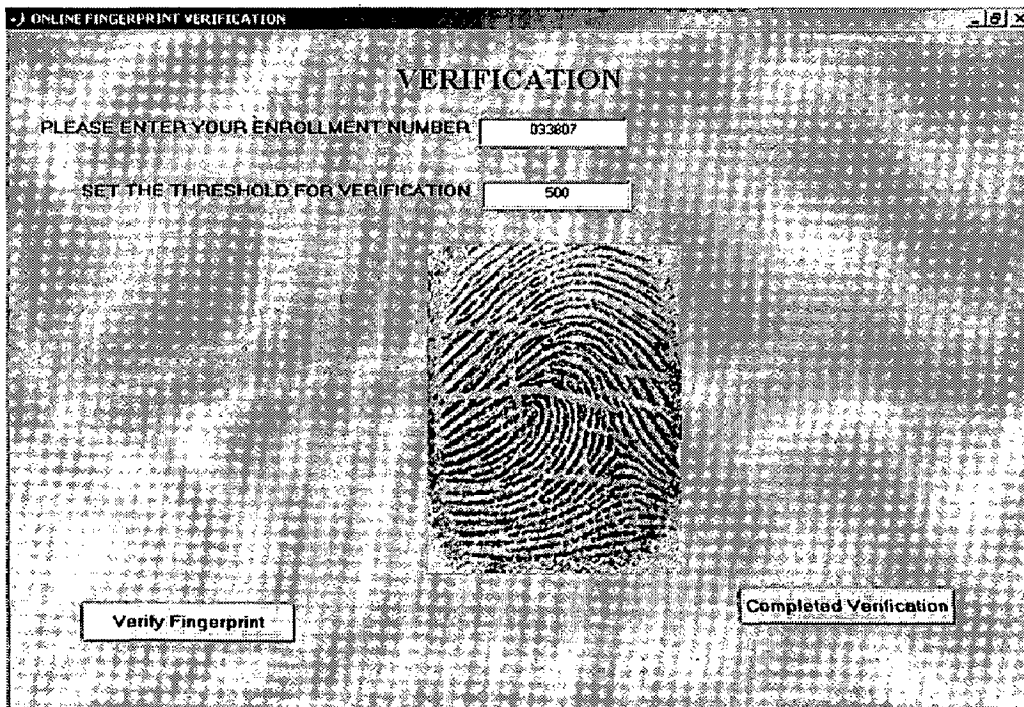
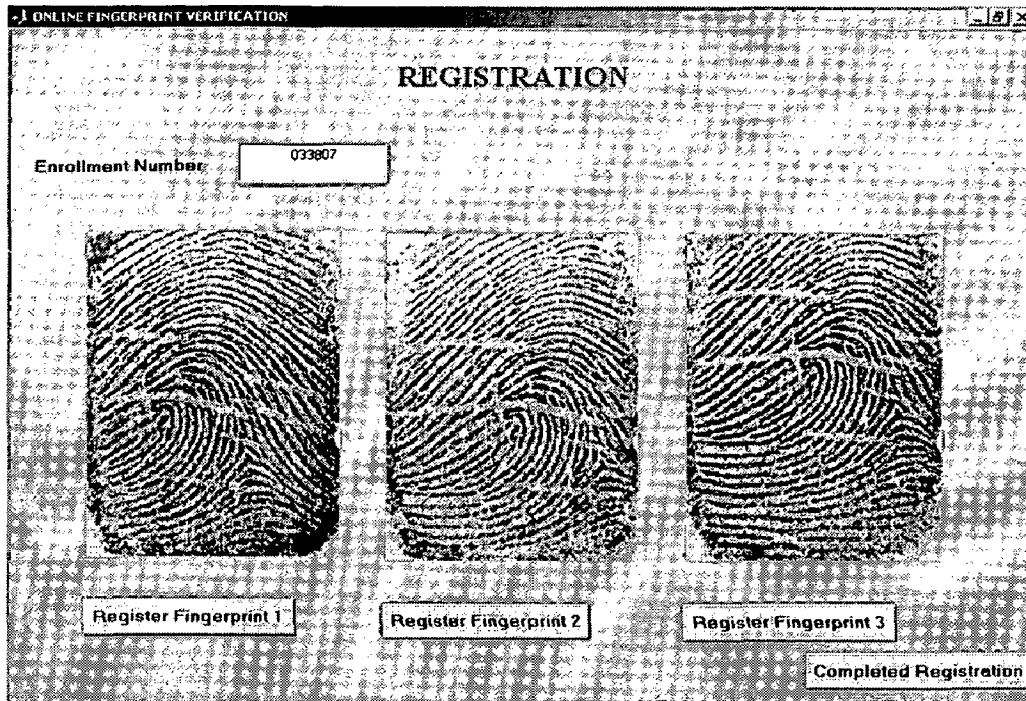


Figure 4.2: Registration and Verification modules

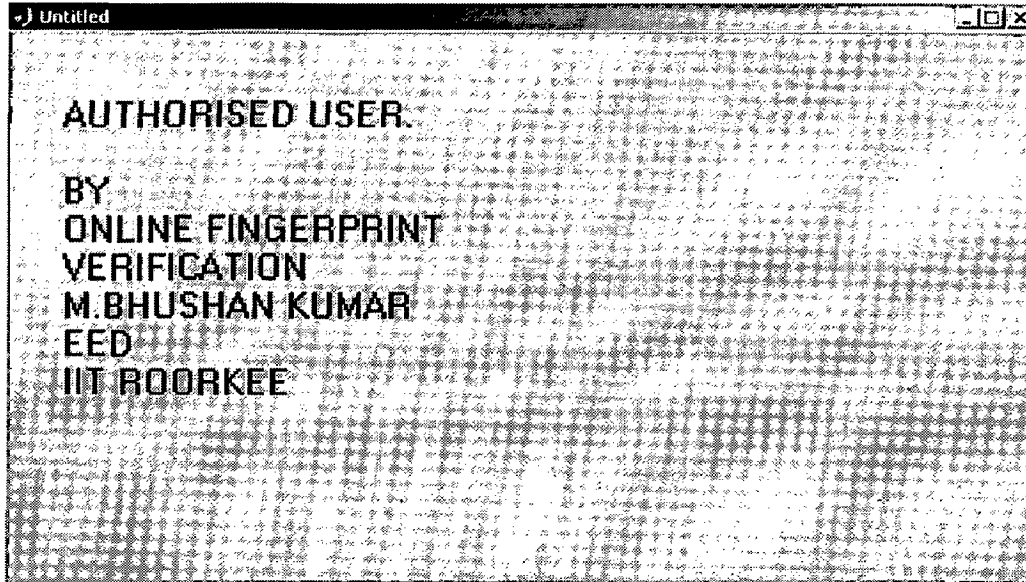


Figure 4.3: Result window after verification

CONCLUSIONS AND FUTURE DIRECTIONS

5.1. CONCLUSIONS:

Fingerprint verification has attained a performance that may be sufficient for several civilian applications, and in the near future we should see fingerprints being increasingly used in authentication systems as the cost of the fingerprint devices reduces further. In this dissertation a fingerprint-based biometric verification system has been developed and successfully tested. An improved filter bank-based fingerprint verification algorithm has been implemented. This implementation has taken into account rotation in fingerprint images. The system is compact and has good discriminatory power compared to minutiae-based finger print verification. Overall performance of the system is tested on a database of 50 students named as IITRDB. Results obtained are FAR (False Acceptance Rate) of 23.65% and FRR (False Rejection Rate) of 27.67% are considerably good enough.

There are still a number of challenges in fingerprint verification. The current verification system still cannot deal with very poor quality fingerprints and large nonlinear distortion. A number of future research directions to improve the filter bank-based system are given in the following section.

5.2. FUTURE DIRECTIONS:

The registration in the Finger Code extraction is based on the detection of the reference point. Even though reference point location is generally accurate, it fails to detect the reference point in very low quality images leading to a rejection of the image in the verification system. A more robust feature extraction algorithm should not rely on a single reference point alone. As a possible solution, multiple reference point candidates can be located and representations corresponding all of these reference points can be stored as multiple templates. At the time of verification, match the input representation with each of the multiple representations and output the maximum matching score.

Use average absolute deviation (AAD) or covariance features to improve the feature vector values. Apply the algorithm on large database like NIST4 or NIST9.

REFERENCES

1. **"Biometrics Introduction"**, Aray Limited, available at <http://www.arayltd.btinternet.co.uk/biolinks.html>
2. A. K. Jain and S. Pankanti, **"Biometrics Systems: Anatomy of Performance"**, IEICE, Special issue on biometrics, Vol. E84-D, No. 7, July 2001.
3. **"A Practical Guide to Biometric Security Technology"** by Simon Liu and Mark Silverman, January/February 2001
www.computer.org/itpro/homepage/Jan_Feb/security3.html
4. Digital Persona, Inc., **Fingerprint-based Biometric Authentication**, available at <http://www.digitalpersona.com/.html>
5. E. Newham, **"The Biometric Report"**. New York: SBJ Services, 1995.
<http://www.sjb.co.uk/.html>
6. **"Biometrics Identity Verification in a Networked World,"** Samir Nanavati, Michael Thieme, Raj Nanavati , Wiley – Dreamtech India Pvt. Ltd. , 2003.
7. **"Silicon fingerprint sensor enables low-cost security,"** Jeanneau, Product Marketing Manager, STMicroelectronics, San Jose, California, available at <http://www.ednitalia.com/story/tech/OEG20020528S0055-R>
8. Kinetic Sciences Inc., **"Fingerprint Sensor Comparisons,"** available at <http://www.kinetic.bc.ca/Biometrics/sensor-comparison.html>
9. **"TouchChip Silicon Fingerprint Sensor,"** STMicroelectronics , available at <http://www.st.com/stonline/products/support/touchip/products/sensor.htm>

10. Lin Hong, **"Automated Personal Identification using Fingerprints"**, Ph.D Thesis, Department of Computer Science, Michigan State University, June 25, 1998.
11. A.K. Jain, Lin Hong and Ruud Bolle, **"On-Line Fingerprint Verification"**, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19, No. 4, April 1997.
12. 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.
13. Lifeng Sha, Feng Zhao, and Xiaoou Tang, **"Improved Fingercodes for filter-bank based fingerprint matching,"** IEEE, Vol: 24, No: 2, pp: 895-898, 2003.
14. Rafael C. Gonzalez and Richard E. Woods, **"Digital Image Processing"**, Pearson Education Asia Pte Ltd., 4th edition, 2000.
15. S. Prabhakar, **"Fingerprint Classification and Matching Using a Filterbank,"** Michigan State University, Ph.D. Thesis, 2001.
16. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, **"Hand Book Of Fingerprint Recognition"**, 2th edition, Springer, 2003.
17. Josed Bigun, **"Speed, frequency, and orientation tuned 3-D Gabor filter banks and their design,"** IEEE, Vol:32, No:6, pp: 732-738, 1994.
18. Chih-Jeen Lee and Sheng-De Wang, **"Fingerprint feature extraction using Gabor filters,"** Electronic letters, Vol. 35, No.4, pp. 288-290, 18th February 1999.

19. Lin Hong, Yifei Wan, and Anil Jain, "**Fingerprint Image Enhancement: Algorithm and Performance Evaluation**," IEEE transactions on Pattern Analysis and Machine Intelligence, Vol. 20, No. 8, pp. 777-789 , August 1998.

20. "**Getting started with MATLAB: A quick introduction for Scientists and Engineers.**" by Rudra Pratap, version 6.5, Oxford University Press, 3rd edition 2003.