CHAPTER 1

INTRODUCTION

Fingerprint is one of the well-known biometric techniques capable of identifying an individual. In the modern electronic era, system security is a major concern as a large amount of data is easily exchanged through computer networks. Obtaining positive identification is a vital element of data security. A fingerprint is the impression made by the papillary ridges on the ends of the fingers and thumbs. Fingerprints afford an infallible means of personal identification because the ridge arrangement on every finger of every human being is unique and does not alter with growth or age. Fingerprint verification is one of the most reliable personal identification systems. However, manual fingerprint verification is so tedious, time consuming, and expensive that it is incapable of meeting today’s increasing performance requirements. An automatic fingerprint identification system is widely needed. It plays a wide and important role in forensic and civilian applications. Minutiae extraction is an important step in fingerprint verification system. Fingerprint recognition is still a challenging and important pattern recognition problem. As fingerprints get increasingly embedded into various systems such as cell phones, it becomes highly important to analyse the impact of biometrics on the overall integrity of the system.

1.1 BIOMETRICS

Biometrics is the science of identifying or verifying the identification of a person based on unique physiological and behavioral characteristics.
Physiological characteristics include fingerprints, retinal pattern, iris and facial appearance. Behavioral characteristics include voice and signature scan.

1.1.1 Benefits of Biometrics

Biometrics is superior to traditional authentication methods owing to the following reasons:

- **Increased Security**

  Biometrics can provide a greater degree of security as these resources are accessible only to authorized users and are kept protected from unauthorized users. Passwords, Personal Identification Numbers (PINs), cards and keys are easily guessed, compromised, lost or stolen. Good and long passwords are also too difficult to remember whereas biometrics data cannot be guessed or stolen in the same fashion as a password or card.

- **Increased Convenience**

  One of the reasons why passwords or PINs are kept simple and are subjected to compromise is that they are easily forgotten. Cards and keys can also be misplaced or lost. But biometrics is difficult, if not impossible to forget, and thus offers much convenience than systems based on remembering multiple passwords or on possessing of an authentication token.

- **Increased Accountability**

  Given the increased awareness of security issues in enterprise and in customer facing applications, the need for strong ability to trace and reporting capabilities has become more important than ever. This reliable capability of audit trail will enhance the level of security and accountability.
- Fraud Detection and Fraud Deterrence

As biometric data are unique to every individual, the opportunity of using fraudulent documents, stolen keys, cards and any other access authentication tokens will be totally minimized. In fact, the United States is beginning to implement biometric technologies on individuals in their database for identifying and tracking people to enhance their security.

Biometrics also has a number of disadvantages. For example, if a password or an ID card is lost, it can be easily replaced. However, once a biometrics card is lost, it is not possible to replace it. Similarly, users can have a different password for each account. Thus if the password for one account is lost, the other accounts are still safe. However, if a biometrics is lost, all biometric-based accounts can be broken-in.

1.2 APPLICATIONS OF BIOMETRICS

Biometric technology is used for many types of applications, ranging from modest (providing time and attendance functionality for a small company) to expansive (ensuring the integrity of a 10 million person voter registration database). Depending on the application, the benefit of using or deploying biometrics may be increased security, increased convenience, reduced fraud, or delivery of enhanced services. Biometrics exists because of the technology’s ability to provide verification and identification in areas such as PC and network access, criminal identification, telephony, physical access and e-commerce. Understanding biometrics according to the use or identification for which a technology is deployed is often referred to as horizontal approach. A horizontal approach underscores the substantial differences between biometric applications and allows for the better
understanding of issues essential to the biometric industry such as security, privacy and accuracy.

The application areas of biometric technology range from electronic banking to web access applications where data security is the central issue.

Traditionally, biometric applications are divided into three categories.

- Applications in which biometrics provides logical access to data or information.
- Applications in which biometrics provides physical access to tangible materials or to controlled areas.
- Applications in which biometrics identifies or verifies the identity of an individual from a database or token.

After considering how biometric applications differ so substantially according to these basic criteria, seven horizontal classifications take shape. These are the different areas where biometrics finds its application.

Criminal identification: Criminal identification is the use of biometric technologies to identify or verify the identity of a suspect, detainee, or individual in a law enforcement application. The primary role of biometrics is to identify an individual in order to proceed with, or halt, a law enforcement process. Few technologies can effectively compete with biometrics in this process; without biometrics, it might be impossible to identify the suspect.

Retail / ATM / Point of sale: Retail / ATM / point of sale is the use of biometrics to identify or verify the identity of individuals conducting in-person transactions for goods or services. Biometrics is used to complement
or replace authentication mechanisms such as presenting cards and photo identification, entering a PIN, or signing one’s name.

E-commerce / telephony: E-commerce/ telephony is the use of biometrics to identify or verify the identity of individuals conducting remote transactions for goods or services. Biometrics is used to complement or replace authentication mechanisms such as passwords, PINs, and challenge-and-response interaction. Although there are some differences between e-commerce and telephony applications, most notably in the acquisition device, the two have more in common than one might realize. Both applications involve remote user authentication, and both often require transactional verification. In addition, both applications normally feature unsupervised enrollment and verification processes. This category becomes more important as biometrics is used more frequently to authorize various types of transactions.

Personal computer/ network access: Personal computer (PC) / network access is the use of biometrics to identify or verify the identity of individuals accessing PCs, networks, applications and other PC resources. Biometrics is used to complement or replace authentication mechanisms such as passwords and tokens. Of the seven horizontal classifications, PC/ network access is closest to traditional logical access. Unlike e-commerce/ telephony, PC/network access authentication is not used to authenticate a specific transaction, but instead to grant access to a resource.

Physical access / time and attendance: Physical access / time and attendance are the use of biometrics to identify or verify the identity of individuals entering or leaving an area, typically a building or room at a given time. Biometrics is used to complement or replace authentication mechanisms such as keys, tokens and badges. Time and attendance are frequently
deployed in conjunction with physical access. While these are two separate applications, physical access/time and attendance are linked because they pertain to restricting, registering, or controlling the presence of an individual within a given space.

Citizen identification: Citizen identification is the use of biometrics to identify or verify the identity of individuals in their interaction with government agencies for the purposes of card issuance, voting, immigration, social services, or employment background checks. Biometrics is used to complement or replace authentication methods such as document provision, signatures, or vouchers. Biometrics may provide unique functionality if it is used to prevent duplicate registration for a public benefit or service.

Surveillance: Surveillance is the use of biometrics to identify or verify the identity of individuals present in a given space or area. Biometrics is used to complement or replace authentication methods such as manual monitoring of cameras. Surveillance differs from physical access/time and attendance in as much as surveillance does not assume user compliance. Surveillance also has dramatically different requirements in terms of accuracy and enrollment and verification processes.

A practical biometric system should have acceptable recognition accuracy and speed with reasonable resource requirements, should be harmless to the users, should be accepted by the intended population and should be sufficiently robust to various fraudulent methods. The main applications of biometric technology have been discussed in the above paragraphs. Its application has gained importance in many areas and research is still going on in this field in order to improve its performance.
1.3 VARIOUS BIOMETRIC TECHNOLOGIES

Biometric technologies automate the process of using a physiological or behavioral characteristic to prove someone’s identity. It is closely connected with problems of information security, including criminology. Since a physiological biometric characteristic tends to have smaller intra class variations, it is more reliable in terms of identification accuracy. Nowadays, nine different biometric techniques exist (Jain et al 2004). This includes face, fingerprint, hand geometry, hand, vein, iris, retinal pattern, signature, voice-print and facial thermogram. Signature and voice print are behavioral biometrics and all others are physiological biometrics. Other biometric technologies include odor, keystroke dynamics, gait and Deoxlyribo Nucleic Acid (DNA). The various biometric technologies are shown in Figure 1.1. The main goal of biometric technology is to reduce the false accept rate; thereby increasing the genuine accept rate and security level. This identification mainly helps in crossing the borders between two countries.
Fingerprint                   Iris                        Face                     Retina

D.N.A

Hand Vein                       Voice          Hand Geometry               Signature

Figure 1.1 Main directions of modern biometric techniques

The modern biometric applications mainly concentrate on the following areas: medicine, law and order, banking and finance, immigration control, visual and voice communications, access control and so on (Nanavati et al 2003). Let us discuss each biometric technique in detail.

1.3.1 Face Recognition

Facial-scan technology utilizes the distinctive features of the human face to verify or identify individuals. Acquisition for biometric identification purpose requires the individual’s face to be presented to a video camera. An
evident deficiency in some current schemes is the ability to fool or confuse some systems with make-up. Face recognition usually refers to static, controlled full frontal portrait recognition. By ‘static’, it is meant that the facial portraits used by the face recognition system are still facial images. By ‘controlled’, we mean that the type of background, illumination, resolution of the acquisition devices and faces etc. are essentially fixed during the acquisition process. Therefore intraclass variations are small. It is a non-intrusive technique. The visible spectrum is inexpensive. It is the only biometric capable of operating without user cooperation. One of the very important steps is to determine the best facial features to discriminate one from another. Problems arise when face recognition needs to be done under varying poses. Accuracy is affected due to change of hairstyle, expression, lighting and wearing of glasses. A face recognition system should not impose any annoying controlled restrictions on how the facial images are acquired. This requires that the system should be able to automatically

a) detect whether there exists a face in the acquired image.

b) locate the face if there is one and

c) recognize the face from a general viewpoint

These issues highlight some of the difficulties in face recognition.

1.3.2 Face Thermogram

Facial Thermogram is unique to each individual but its accuracy is quite questionable. It captures the heat emitted patterns derived from the blood vessels through an infrared camera under the skin. These heat emitted patterns are used to create the biometric template which is then used for matching purposes. It is not vulnerable to disguises. It is independent of ambient light and external changes and even plastic surgery. Identity can be
verified without contact, full camera view and the cooperation of objects. It is superior to face recognition using CCD cameras. It depends heavily on emotion, body temperature etc. and it is view-dependent. Even identical twins possess different facial thermograms. It is non-intrusive. But the cost of infrared camera is high. Finally, it has not been shown to have a permanent biometric characteristic.

1.3.3 Retinal Scan

Retina-scan technology utilizes the distinctive characteristic of the retina. Retina is the surface on the back of the eye that processes light entering through the pupil. It is one of the most well-known biometric technologies, but is also one of the least employed techniques. Retinal recognition creates an “eye signature” from the vascular configuration of the retina, an extremely consistent and reliable attribute with the advantage of being protected inside the eye itself. An image of the retina is captured by having the individual look through a lens at an alignment target. Diseases or injuries that would interfere with the retina are comparatively rare in the general population, so the attribute normally remains both consistent and consistently available. It is noted for its accuracy, long term stability and genetic independence. It is also insensitive to variations in external environment, and it is very difficult to spoof. The main drawback is that it is difficult to use and the sensor costs high. Since the retina is small, internal and difficult to measure without the proprietary hardware and camera systems specifically designed for retina imaging, image acquisition is a very difficult process. There is some user-discomfort with eye-related technology, and there is a possibility of a health threat.
1.3.4 Iris Scan

Iris-scan technology utilizes the distinctive features of the human iris. It has been successfully implemented in ATM’s and kiosks for banking and travel applications. Iris scanning is less intrusive than retinal recognition because the iris is easily visible from several feet away. Responses of the iris to changes in light can provide secondary verification so that the iris presented as a biometric factor is genuine. Though empirical tests with the technology will improve its reliability, it appears quite promising and even practical for many applications, especially two-factor scenarios. While some of the technical issues of iris scanning seem pedestrian, they present implementation challenges. A careful balance of light, focus, resolution and contrast is necessary to extract the attributes or minutiae from the localized image. While the iris seems to be consistent throughout adulthood, it does vary somewhat up to adolescence. It is noted for its accuracy, genetic independence, high processing speed and stability. It also suffers from serious drawbacks which include propensity for false rejection, user-discomfort with eye-based technology and high cost with the acquisition device.

1.3.5 Fingerprint

Finger-scan technology utilizes the distinctive features of the fingerprint. It is the most commonly deployed biometric technology. Fingerprint identification techniques fall into two major categories—Automated Fingerprint Identification Systems (AFIS) and fingerprint recognition systems. AFIS is typically restricted to law-enforcement use. Fingerprint recognition derives a unique template from the attributes of the fingerprint without storing the image itself or even allowing for its reconstruction. Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device.
that also checks for validating attributes such as temperature and pulse (Maltoni et al 2009). Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. Solid state sensors overcome this and other technical hurdles because the coated silicon chip itself is the sensor. Solid state devices use electrical capacitance to sense the ridges of the fingerprint and create a compact digital image, so they are less sensitive to dirt and oil. Fingerprint recognition is generally considered reliable enough for commercial use, and some vendors are already actively marketing readers as part of Local Area Network login schemes. It is a mature and proven core technology capable of high levels of accuracy. It employs ergonomic and easy to use devices. It has the ability to enroll multiple fingers and the sensor cost is also comparatively low. At the same time, some small percentage of users especially manual workers and elderly people do not have clear fingerprints. Fingerprints are unique to an individual and cannot be easily forged. They are permanent and reappear even after cuts or bruises.

1.3.6 Voice Scan

Voice-scan technology utilizes the distinctive aspects of the voice to verify the identity of individuals who are speaking. Voice recognition techniques are generally categorized according to two approaches—Automatic Speaker Verification (ASV) and Automatic Speaker Identification (ASI). Speaker verification uses voice as the authenticating attribute in a two-factor scenario. Speaker identification attempts to use voice to identify who an individual actually is. Voice recognition distinguishes an individual by matching particular voice traits against templates stored in a database. Voice systems must be trained to the individual’s voice at enrollment time, and more than one enrollment session is often necessary. Feature extraction typically measures formants or sound characteristics unique to each person’s vocal
tract. The pattern matching algorithms used in voice recognition are similar to those used in face recognition. Voice-scan technology is text-dependent, meaning that the system cannot verify a speaker speaking random snippets of text. But it is easy to use, non-intrusive and uses existing telephony infrastructure or simple microphones. It is less accurate and is affected by background noise.

1.3.7 Signature Scan

Signature-scan technology utilizes the distinctive aspects of the signature. This technology examines the behavioral components of the signature such as stroke order, speed and pressure as opposed to comparing the visual images of signatures. Signature is a simple, concrete expression of the unique variations in human hand geometry. Forensic experts have developed criteria over the years for verifying the authenticity of a signature. Automating this process allows computer automation to take the place of an expert in looking for unique identifying attributes. In addition to the general shape of the signed name, a signature recognition system can also measure both the pressure and velocity of the point of the stylus across the sensor pad. (Keystroke dynamics is a variation on this technique that measures the typing rates and intervals.) Signatures, however, are difficult to model for variation, and users are unaccustomed to signing on tablets. It is resistant to imposters and non-invasive and the users can change the signature.

1.3.8 Hand Geometry

Hand-scan technology utilizes the height and width of the back of the hand and fingers to verify the identity of individuals. The essence of hand geometry is the comparative dimensions of fingers and the locations of joints. Indentimat, one of the earliest automated biometric systems installed at the
Shearson-Hamill investment bank on Wall Street during the late 60s, used hand geometry and stayed in production for almost twenty years. Some systems perform simple, two-dimensional measurements of the palm of the hand. Others attempt to construct a simple three-dimensional image from which template characteristics are to be extracted. In one of the most popular descendants of the Identimat, a small digital camera captures top and side images of the hand. Reference marks allow calibration of the image to improve the precision of matching. It is a mature technology and non-intrusive. It is used to maintain attendance records in factories. It is resistive to temperature, humidity and other environmental conditions. Its accuracy is low and the sensor costs high. Also, it is difficult to use for some users especially children, arthritis patients and people with missing fingers or large hands.

1.3.9 Hand Vein

Hand-vein technology utilizes the distinctive aspects of the vein patterns at the back of the hand. These patterns are captured by means of an infrared camera. Each individual has different vein patterns but these are not a permanent biometric feature. It is less accurate. Hand vein recognition attempts to distinguish individuals by measuring the differences in subcutaneous features of the hand using infrared imaging. Like face recognition, it must deal with the extra issues of three-dimensional space and the orientation of the hand. Like retinal scanning, it relies on the pattern of the veins in the hand to build a template with which to attempt matches against templates stored in a database. The use of infrared imaging offers some of the same advantages as hand geometry over fingerprint recognition in manufacturing or shop-floor applications where hands may not be clean enough to scan properly using a conventional video or capacitance technique.
In this section, various biometric technologies have been discussed. In the next section, a comparison all the biometric technologies is attempted. Each and every biometric technology is noted for its special features and it is used in specific applications as denoted in Table 1.1.

1.3.10 Comparison of various biometric technologies

All the biometric technologies discussed earlier have their own strengths and weaknesses and each is well-suited for particular applications. There is no single best biometric technology, nor is it likely that any single technology will come to dominate in every area of the biometric industry. Instead, the requirements of a specific application determine which, if any, is the best biometric. Attempting to compare biometric technologies without an application is largely meaningless. One normally chooses a biometric application by considering factors such as reliability, security, performance, cost, user-acceptance etc. (Emilio and Sonia 2008).

In this thesis, fingerprint is chosen as the best biometric for identifying or verifying a person. Among all the biometric techniques, fingerprint-based identification is the earliest method that has been successfully used in numerous applications. It is used for criminal identification, national ID cards, immigration and so on. Biometric technology such as face can lie, but fingerprints do not lie (Jain et al 2004). Also, DNA test can not differentiate between twins, but fingerprints of twins differ. Also, fingerprints cannot be easily forged like ID cards and tokens.
### Table 1.1 Comparisons of biometric technologies.

<table>
<thead>
<tr>
<th>Biometrics</th>
<th>Universality</th>
<th>Uniqueness</th>
<th>Permanence</th>
<th>Collectability</th>
<th>Performance</th>
<th>Acceptability</th>
<th>Circumvention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Keystroke Dynamics</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Hand vein</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Iris</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Retina</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Signature</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td>Voice</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td>Facial</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Thermogram</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
</tbody>
</table>

H=High, M=Medium, L=Low

Table 1: Biometrics Parameters are explained below:

- **Universality**: Each person should have a unique character.
- **Uniqueness**: How well the biometric separates one individual from another.
- **Permanence**: Measures how well a biometric resists aging and other variance over time.
- **Collectability**: Ease of acquisition for measurement
- **Performance**: Accuracy, speed and robustness of technology used.
- **Acceptability**: Degree of approval of a technology.
- **Circumvention**: Ease of use of a substitute.
1.4 PROFOUND STUDY ON FINGERPRINTS

1.4.1 History of Fingerprint Science

Fingerprint is one of the wonders of God’s creation. Fingerprint is a unique one, and even today it is a subject of mystery to the general public. It is not known by whom and when the finger print was first used for identification purposes. But the study of palms and the use of finger prints can be traced back to the beginning of civilization.

Thousands of years before the birth of Christ, finger prints were used on pottery to indicate the maker and the brand of pottery. Slabs of clay with finger prints of 3000 years old were found in the tomb of Egyptian King Tut-en-Khamen. Chinese Emperors used thumb impressions on the documents as a seal. The seals were of clay which had the impression of the thumb on one side and the name of the owner on the other side. Emperor Ts-in She (B.C. 246-210) was the first emperor to use such seals. This shows clearly the importance of finger prints for identification purposes.

In 702 A.D. under the law of Taiho, if a Japanese male preferred divorce charges, he had to imprint the mark of his index finger after his name on the document transcribed by another. It was found in an article written by an Arabian merchant, Soleiman in 851 A.D. that in China, the creditor’s bills were marked along with finger prints of both the creditor and the debtor’s middle and index fingers. Finger prints along with palm prints known as ‘Panja’ were used for some centuries in India. In China during the period of Sung (A.D. 960-1278), finger prints were used to identify the persons involved in sales.
Many scientists involved themselves in the research of fingerprints. What following is a discussion on some of them and their findings (Hem Chandra Bose, 1927).

1.4.1.1 Marcello Malpighi (1628 - 1694)

He was a Professor of Anatomy at the University of Bologna, Italy. He discussed the functions and morphology of the skin. He discovered the nature of the layers of epidermis. One of the layers was named after him as Malpighian layer. He made references about the papillary ridges and the different patterns in fingerprints.

1.4.1.2 Nehemiah Grew, M.D.(1641-1712)

He was a Fellow of the College of Physicians and Surgeons of the Royal Society, England. In 1684 he wrote an article on a philosophical transaction titled “Description and use of pores in the skin of hands and feet”. He mentioned the patterns on the fingers and the thumb with a diagram of a hand.

1.4.1.3 Thomas Bewick (1753 - 1828)

He was an English author and wood engraver. He engraved some of his own finger prints and used them to ornament three of his books along with his signature. This master craftsman was one of the first to recognize the individuality of a finger mark.

1.4.1.4 John Evagelist Purkinji (1787 - 1869)

He was a Professor of Physiology in the University of Breslan in Germany. In 1823, he submitted a thesis on finger prints to the University of
Breslan. In that thesis, he named nine standard types of finger print patterns. They are

i) Arch
ii) Tented Arch
iii) Plain Loop
iv) Irregular Loops
v) Whorls – Almond shaped
vi) Whorls – Spiral shaped
vii) Whorls – Elliptical
viii) Whorls – Circular

He made an attempt to classify them. He also referred to the palm of men and monkeys.

1.4.1.5 Sir Francis Galton(1822 - 1911)

He was born in 1822. He established an anthropological laboratory in London in 1886. He was a famous British Scientist and cousin of another famous scientist Darwin. He was known as Father of Finger Prints Science. To find out the aspect of heredity, he studied the finger prints of the mother, the father and the children in a family. He also studied the finger prints from childhood, boyhood, early man hood, man hood and old age. From these studies, he scientifically established the fundamental rules of finger print science. They are given below.

1. Finger prints never change from birth to death till decomposition sets in.
2. No two finger prints will be identical unless they are taken from the same finger of the same person.

He further studied the finger prints collected in India by Sir William Herschel which were brought by the special Registrar, Ramgati Banargee of Hooghly District in the year 1892. He derived a classification on the basis of finger print patterns Arch, Loop and Whorl. In 1892 he published a book titled as “Finger Prints”. Galton’s system of classification of finger prints was introduced along with Bertilon system in Scotland Yard, London. It was called Dual System.

1.4.1.6 Sir William Herschel(1833 - 1917)

He was the Collector of Hooghly District, West Bengal, and he was the first officer who used finger prints in government offices in India in 1858. He took the finger prints of natives and contractors in India in order to frighten them in the dealings of money. The first print he made was on a contract with a Bengali contractor named Rajyadhar Konai in connection with the supply of blue metal. On the contract form, he took his finger prints along with the palm print of the right hand. This historic contract is still preserved in the British museum. He ordered to use finger print for identification of prisoners from 1858. In the year 1877, he directed all the Registrar of Deeds to take finger prints from all who execute deeds in front of him to prevent false personating. All the pensioners were finger printed at the time of receiving pension in 1880. He submitted a proposal to use finger prints in other provinces of British India. But it was not accepted by the government.

In order to find out the permanency and persistency in ridge characteristics, he imprinted his own finger, palm and sole prints in different
intervals and found that the ridge characteristics and patterns never changed throughout human life.

1.4.1.7 Henry Faulds (1843 - 1930)

An English doctor in Tsukiji Hospital, Tokyo, Japan was interested in the study of finger prints. In 1877 while lecturing the Medical students of Physiology, he explained his study of finger prints on prehistoric pottery made of clay. He made a study on the designs of the palm prints. He studied the finger prints of monkeys also. He suggested that the black ink of a printer could be used for taking finger prints. He was the first man to give the idea of tracing criminals from the crime scene. He wrote about this in an article to the British Magazine “Nature” on 28.10.1880.

He identified two cases. The first one by noticing the greasy prints on a glass tumbler, the criminal was caught and in the second one, finger prints left by a man on a white wall were used as a clue. He suggested the identification of dead bodies from their finger prints. He wrote in an article that the finger prints with blood or impression on clay, glass etc. would lead to scientific identification of criminals. He came to Darjeeling in 1872 as a medical missionary. In 1905 he published a book titled “Guide to Finger Print Identification”.

1.4.1.8 Juan Vucetich (1858 - 1925)

Professor Juan Vucetich derived a classification system independently in finger print identification in Argentina, South America. The methods of his original findings were adopted in most of the Latin speaking countries, and they are still in popular use. Some of Galton’s procedures were incorporated in his system.
1.4.1.9 Azizul Haque (1872 - 1935)

Azizul Haque was born in the district of Khulna, East Pakistan in 1872. In 1892, he joined as a Sub-Inspector of Police in the Bengal Police and worked in Anthropometric Identification Bureau. He helped Sir E.R. Henry to evolve the pigeonhole method of classification. He was the one who derived the arithmetical rule for primary classification. Then the secondary and other classifications were worked out, and Azizul Haque played an important part in this aspect.

1.4.1.10 Rai Bahadur Hemachandra Bose

He was trained by Sir E.R. Henry directly in fingerprint system. During his service in Bengal Finger Print Bureau, he helped to work out lettered classification. In 1926, he published a book titled “Fingerprint Companion”. This book deals with ten digit fingerprint classification and single digit classification method to identify the persons from chance prints and Telegraphic Code for finger impression which can be telegraphed to any distant fingerprint bureau for search and identification of criminals.

1.4.1.11 A.Subramania Iyer

He was an Inspector of Police in Madras State. He went to Kolkata and got himself trained by Sir E.R. Henry. On his return from the training in fingerprint science, he was asked to start a Finger Print Bureau. By his effective action a Finger Print Bureau was opened at Madras in Tamilnadu on 22.8.1895.
1.4.1.12 Sir Edward Richard Henry (1859 - 1931)

He was Inspector General of Police, Lower Province, Bengal, in 1891. He studied the book of Sir Francis Galton and conducted many experiments. He derived a new system of classification. Bengali officers Khan Bahadur Azizul Haque helped him to work out the numerical system, and Rai Bahadur Hemachandra Bose helped him in lettered classification. He requested the British government in 1896 to appoint a committee for adoption of finger print system in the place of Bertilon system, otherwise called Anthropometric System. A committee headed by Mr.C.Strahan, Surveyor General of India and Mr.Alex Pedler, Principal, Presidency College, Kolkata was constituted and this committee examined both the Anthropometric system and E.R.Henry’s system of classification of finger prints and recommended for adoption of finger print system as a means of identification of the habitual criminals in the place of anthropometric system in March 1897. Then a Finger Print Bureau was officially established in Kolkata on 12.6.1897. Finger Print system was approved by the Indian Legislature in 1899 and a special act was passed amending the law of evidence to the extent of declaring relevant the testimony of those who had become proficient in finger print decipherments. In 1900, Sir E.R.Henry published a valuable book entitled “Classification and uses of Finger prints”.

In Scotland Yard, England, Finger Print System was adopted in 1901. In the United States of America, Finger Print System was adopted in 1903. By 1908, the Finger Print System was adopted throughout the world.

1.4.2 Basic principles of Finger Print Science

Basic principles of finger print science were scientifically established by Sir Francis Galton (Francis Galton, 1892). They are
I. Permanency and Persistency: Finger prints never change from birth to death till decomposition sets in.

II. Individuality or Variety: No two finger prints will be identical unless they are taken from the same finger of the same person.

III. Immutability: Simple injuries, age growth, wart and diseases will not change the formation of patterns and ridge characteristics unless dermis is affected.

A detailed discussion of the basic principles of fingerprint is given below.

I. Permanency or Persistency of finger prints

a) The ridges on the friction skin of fingers, palms and soles are developed with fixed and permanent character in one and half months to two months of pregnancy. They are fully formed in the sixth month, i.e. 180 days before childbirth. These formations remain permanent till the skin perishes to decomposition. During the growth of the body, these formations enlarge according to growth. It is like a lace which can be enlarged by stretching (Babler 1991). But it will have the same structure. It can also be compared with a contact photo or an enlargement taken from a photonegative. On comparison no difference in the picture except the size can be found. In childhood, the finger prints and ridge characteristics are small. When the child grows, the finger print pattern and ridge characteristics enlarge according to the growth. But no difference in these stages can be found except the size. This principle can be proved from the following observations.
b) Sir William Herschel, the collector of Hooghly district recorded his finger prints in different intervals of 26th, 44th and 83rd year of his age. In all these stages, the ridge characteristics and their formations remained permanent. No change was noticed.

c) Sir Francis Galton, an Anthropologist and the cousin of scientist Darwin wanted to find out hereditary factors in finger prints. He examined the finger prints of the father, the mother, the son and the grandson of the same family. He also studied the finger prints in childhood, boyhood, manhood and old age. He found that the finger prints are not produced in heredity and the finger prints of an individual remain permanent from birth to the stage of decomposition.

d) For more than a hundred years, finger print bureaus are functioning throughout the world. The finger prints of the same person taken at different intervals are compared till date. They were found to be the same, and they remained permanent.

e) Finger prints of the persons convicted on different dates are received by the Finger Print Bureau for record. Then the search slips on the arrest of the suspected persons are searched in the previous records. If they are ex-convicts, the previous records traced will prove the antecedents. No change is noticed in all these finger prints of the same individual.

f) Finger prints of unidentified dead bodies are received by the finger print bureau for the identification of the person. They will compare it with the finger prints database of the convicts, thumb impressions found in sales deeds, pronotes, receipts or from the records of the
Sub-Registrar office. From this observation, it is confirmed that the finger prints will not change even after death.

On the strength of above findings it may be concluded that finger prints never change from birth to death till decomposition sets in.

II. Individuality of finger prints:

a) Sir William Herschel, the collector of Hooghly district took the finger prints of the contractors, pensioners to avoid false personating. He studied the finger prints of different individuals and found that they were different from one another. So he ordered to take the left thumb impression in the sale deeds at the time of registration from 1877. The left thumb impression will prove the real executor on later days because they cannot be duplicated by other persons.

b) Sir Francis Galton tried to find out the hereditary aspect in finger prints. He compared the finger prints of the individuals in the same family and the finger prints of other persons. He scientifically proved that the finger prints have got individuality. No two persons will have identical finger prints. He proved these facts mathematically through the theory of probability.

c) According to Dr. Robertcliate the differences exist because each person is an incarnation of vital energy. Therefore every person is differentiated from each and every one. This translates into every anatomical organ and physiological functions. Hence the difference exists in the formation of ridges also.
d) In nature also there are no two identical things. Nature never
duplicates. Two leaves, two roses, two of anything in nature may be
found to be similar at a glance. But the microscopic study will
reveal the differences in them. The same rule applies to the ridge
formation in finger prints, palm prints and sole prints.

Therefore, it can be concluded that no two persons will have identical
finger prints in the world including twins, triplets and quintuplets. Even finger
prints taken from different digits of the same individual are not the same; they
are different. So finger prints are God’s seal given to every person on this
earth to keep their individuality.

III. Immutability of finger prints:

There are two layers in human skin called epidermis and dermis (Ji and
Yi 2007). The outer layer of skin is called epidermis, and the inner layer is
called dermis.

Accidental injuries, peeling of skin, warts, creases, burns, skin diseases
will affect the ridges in epidermis temporarily. After some time, the affected
ridges will regain their original shape.

Temporary Scars:

a) A slight cut on a finger made with a razor blade would affect the
epidermis only.
b) After some time the same finger will regain its original position.
c) A piece of epidermis is missing from the finger as a result of a
blister.
d) The same finger regains its original position.
If the wound affects the dermis, there will be a permanent scar. Even then the ridges will appear free from the scar and reveal clear character for comparison and identification.

From the above observations, it may be concluded that fingerprints are infallible throughout human life. It can also be asserted that fingerprint science is most reliable, truthful, unchangeable and very strong in establishing the identity of a person.

1.4.3 Fingerprint Classification

A fingerprint can be identified by its special features such as ridge endings, ridge bifurcation, short ridges and ridge enclosures (Monssens 1971). These ridge features are collectively called minutiae of the fingerprint. It was also reported that for automatic detection of a fingerprint, it suffices to focus on two types of minutiae, namely ridge endings and bifurcation. Ridge endings are nothing but the termination of ridge abruptly, and ridge bifurcation is the point at which a ridge forks into two or more branches.

The central problem in designing a classification algorithm is to determine what features should be used and how categories are defined based on these features (Cheong and Haesun 2005). Figure 1.2 shows the various characteristics of a fingerprint. Two types of fingerprint characteristics are used for identification of individuals. (i) Global features and (ii) Local features.
Figure 1.2 Various characteristics of fingerprints

Fingerprint ridges are not continuous, straight ridges. Instead, they are broken, forked, changed directionally, or interrupted (Kawagoe and Tojo 1984). The points at which ridges end are unique for identifying information. Minutiae points are local characteristic of fingerprints that are mainly used for fingerprint matching.

Figure 1.3 Various minutiae points

Figure 1.3 shows all the local features termed ridge ending, ridge bifurcation, short ridges and ridge enclosures.

Global features are those characteristics that can be seen with the naked eye. Global features include
• Pattern Area

The pattern area is the part of the fingerprint that contains all the global features. Fingerprints can be read and classified based on the information in the pattern area. Certain minutiae points that are used for final identification might be outside the pattern area. One significant difference between Net Eagles’s fingerprint recognition algorithm and those of competing companies is that Net Eagles uses the entire fingerprint for analysis and identification, not just the pattern area, while the other company devices require users to line up their fingerprints on the sensor. Net Eagles acquires a greater amount of information over the entire fingerprint and can obtain enough information to "read" a print even if only part of the print is placed on the sensor.

• Core Point

The Core Point, located at the approximate center of the finger impression, is used as a reference point for reading and classifying the print. It is a point located on or within the innermost sufficiently curved ridges. It is also called inner terminus.

• Type Lines

Type Lines are the two innermost ridges that start parallel, by diverge, and surround or tend to surround the pattern area. When there is a definite break in a type line, the ridge immediately outside that line is considered to be its continuation.

• Delta

Delta is that point of a ridge at, or in front of and nearest to the center of divergence of type lines. It may be a ridge ending, bifurcation point, short
ridge or a dot. The whorls usually have two deltas, the right loops have a delta on the left of the observer, and the left loops to the right of the observer.

Ridge Characteristics

Friction Skin

The fingers, palms and the sole of the foot including toes are covered with a special kind of skin. The skin consists of minute elevated lines which are called ‘Papillary ridges’ or ‘Friction ridges’, and the depressions found in between the elevated ridges, are called ‘furrows’. The ridges are permanent and persistent in nature. Besides the ridges and furrows in the finger, palm and sole prints, some thick white lines can be observed. They are called ‘creases’ which are caused by mere folding of hands and wrinkling of the skin. These creases are not permanent. They often change their directions and dimensions. In the friction skin area, there are neither hairs nor sebaceous glands unlike in the skin covering other parts of the body (Henry E R, 1900). The ridges are studded with microscopic pores which are the mouth of the glands secreting perspiration consisting of oily matter, sweat and other secretions that keep the hand smooth, lubricated and soft. The sensory nerves also formed in the friction skin gives a double sense of touch. The friction skin which is corrugated in nature prevents slipping when in contact with smooth external objects.

Time of appearance of ridges

These ridges can be first seen on the fetus between 6 weeks and two months after impregnation, and they are fully formed in the sixth month.
Ridges

The minute elevated lines corrugated on the friction skin are called ridges. These minute ridges are studded with sweat pores. The ridges are permanent and unchangeable throughout human life until decomposition sets in the skin.

Furrows

The depressions in between the elevated ridges of the friction skin are called furrows.

Creases

In the finger, palm and sole prints some thick white lines can be observed. These are called creases. The creases are caused by mere folding of hands and wrinkling of the skin due to pathological conditions or due to certain occupational conditions. The creases are totally disregarded for the purpose of finger print identification as the creases are not permanent. They often change their directions and dimensions.

Pores

Papillary skin contains countless sweat glands which open through duct to the ridge surface. That is posed on the mouth of the sweat glands which excrete sweat all 24 hours. They are arranged on the summit of the ridge in equal distance. Seat pores are persistent and immutable.

Subsidiary ridges

Subsidiary ridges are not well developed ridges which appear in the depressions in between the well-formed ridges and look like hair in size, short
or broken without any sweat pores. The presence of such ridges depends upon the pressure given while taking the impression. Subsidiary ridges are ignored while counting the ridges. The subsidiary ridges are also called nascent ridges or incipient ridges or counter sunk ridges or hairy ridges or rudiment ridges.

The Finger Print is the actual reproduction of the elevated portions of the ridges of the friction skin surface of the first phalange of the finger.

In an impression taken with black printer’s ink, these ridges are represented as ‘black lines’. The furrows are represented by ‘white lines’ (Jayant et al 2006).

Finger print patterns are divided into four main groups. They are

I. Arch Pattern
II. Loop Pattern
III. Whorl Pattern
IV. Composite Pattern

I. (a) Arch Pattern

In Arch, the ridges run from one side to the other making no backward turn. There is ordinarily no delta. But when there is an appearance of delta, no ridge must intervene between the inner and outer terminus.

(b) Tented Arch Pattern

In the patterns of Arch type, the ridges near the middle may have an upward thrust, arranging themselves as it were on both sides of a spine or axis towards which the adjoining ridges converge. The ridges thus converging give to the pattern of tent in outline. Hence the name ‘Tented Arch’.
II. Loop Pattern

In loops, some of the ridges make backward turn but without twist. There is one delta. There must be at least one ridge count between the inner and outer terminus.

There are two kinds of Loops. They are Ulnar and Radial loops.

(a) Ulnar Loop Pattern:

An ulnar loop is so called because the ridges about the core terminate in the direction of the ulnar bone of the forearm. In other words, the ridges about the core slant towards the right in the case of right hand fingers and towards left in the case of left hand fingers.

(b) Radial Loop Pattern

A radial loop is so called because the ridges about the core terminate in the direction of the radial bone of the forearm, i.e. the ridges slant towards left in the case of right hand fingers and towards right in the left hand fingers.

Loops are further sub-divided according to their appearance. They are listed as

i) Converging Loop Pattern
ii) Nutant or Intended Loop Pattern
iii) Invaded Loop Pattern
iv) Crested Loop Pattern

i) Converging Loop Pattern: A converging loop is defined as one in which there is a visible convergence about the core. More than one ridge must
converge. But they need not necessarily be joining the ridges forming the core. The converging ridges may be on one or both sides of the core.

ii) Nutant or Intended Loop Pattern: When the loop has the appearance of sickle, it is called Nutant or Intended Loop.

iii) Invaded Loop Pattern: This is a loop that presents an appearance as though a series of ridges were swarming over the pattern coming from the side of the delta and threatening to engulf it from above.

iv) Crested Loop Pattern: This is a loop where the ridges swarming over the pattern are stopped along a line which they cannot pass or are swept into the current of normal ridges giving the appearance of crest above the pattern area.

III. Whorl Pattern

In whorls, some of the ridges make a turn through at least one complete circuit. There are two deltas, one on the left and another one on the right. Whorls can be classified according to formation of the core, i.e. Single cored, Double cored, Elliptical and Spiral.

IV. Composite Patterns

A composite pattern means combination of two or more patterns either of the same or different types in one print (Karu and Jain 1996). Composite patterns are sub-divided as follows

1. Central Pocket Loop Pattern
2. Lateral Pocket Loop Pattern
3. Twinned Loop Pattern
4. Accidental Pattern
1. Central Pocket Loop Pattern

   This pattern can be described as an incipient whorl because a few ridges about the core possess features of whorl type, and the remaining ridges confirm the loop type surrounding them as pocket.

   In this pattern, there must not be more than four recurring ridges intervening between the core and the innermost delta.

   It must have two deltas. If an imaginary line is drawn between the two delta points, it would not cut or touch a recurring ridge within the inner pattern area.

2. Lateral Pocket Loop Pattern

   The ridges constituting a loop bend sharply downwards on one side before the curve and thereby forming on the side an interspaced or pocket, ordinarily filled by the ridges of another loop. Such an impression is termed as Lateral Pocket Loop.

   In Lateral Pocket Loop, the ridges containing the point of core have their exit on the same side of the delta.

3. Twinned Loop Pattern

   It consists of two well-defined loops one superincumbent on or surrounding the other. Such an impression is termed as twinned loop. In Twinned Loop, the ridges containing the point of core have their exit on the different sides of the delta.
4. Accidental Pattern

It is comparatively an uncommon type of pattern being one of the more complicated combination of the same or different patterns, i.e. loop by loop, whorl resting on loop, loop resting on whorl, whorl resting on whorl, arch with pocket. It possesses two or more deltas.

In finger prints, the ridges will not run continuously. Breaks and bifurcations can be found in ridge formations. These are called ridge characteristics (Chapel C, 1971). In the finger print work, the ridge characteristics are very important for the positive means of identification. Sir Francis Galton was the first discoverer and described the term ‘minutiae’ for ridge characteristics. They are also known as ‘Galton details’. Several European, American and Indian authors had described different ridge characteristics. Commonly, 12 varieties of ridge characteristics are found with more frequencies.

1. Upward termination
2. Downward termination
3. Upward bifurcation
4. Downward bifurcation
5. Dot
6. Short ridge
7. Enclosure
8. Opposite termination
9. Hook
10. Change over
11. Intersection
12. Deviated break
1.4.4 Applications of fingerprint biometrics

There are several sample applications for fingerprint technology that can be classified into seven main categories

1. International Government

   - National ID programs
   - Passport, Visa and voting programs
   - Driver licenses
   - Background Check
   - Border patrol
   - Prisoner tracking
   - Secure area and building access control

2. Government

   - Building access control
   - Employee background checks
   - Detainee background checks
   - Criminal booking
   - Fraud prevention
   - Visitor management
   - Jail management
   - Computer access control
   - Border and port of entry control

3. Law Enforcement

   - Criminal and civil background checks
   - Verifying an individual’s identity when purchasing a weapon
Capturing prints at pawn shops for tracking the sale of stolen goods
Capturing prints at check-cashing locations for tracking check fraud
Capturing fingerprints from witnesses at a crime scene, or from family members
Capturing prints in court rooms to ensure that the correct individuals are present

4. Education/Child Safety

- Fingerprint and photograph Child ID cards
- Volunteer and employee background checks
- Visitor management of visitors to daycare centers and schools

5. Transportation

- Credentialing transportation workers
- Visitor management
- Mobile ID verification
- Background checks
- Airport and border checks
- Door and secure area access control
- Passport verification

6. Banking/Finance

- Background checks
- Visitor management
- Door and secure area access control
- Check-cashing verification
ATM authentication
Mobile ID verification

7. Health Care

Employee background checks
Doctor and nurse licensing
Patient record access
Pharmacy access control
Hospital visitor management

1.5 MATLAB AND ITS STRENGTHS

The name MATLAB is abbreviated as MATrix LABoratory. In 1970's Cleve Moler developed MATLAB predominantly. MATLAB was written at first to afford trouble-free access to matrix software extended by the LINPACK (linear system package) and EISPACK (Eigen system package) projects. The basic data element of MATLAB is an array which does not need dimensioning. The software package has been commercially available since 1984 known as MATLAB 1.0 and the latest version is MATLAB 8.0. Most of the Universities and international industries consider it as a standard tool. With the help of its powerful built-in routines a very wide variety of computations can be performed. The graphics commands which make the visualization of results at once can also be used easily. Some explicit applications are composed in packages known as toolbox. There are toolboxes for signal processing, symbolic computation, control theory, simulation, optimization, and several other fields of applied science and engineering.

MATLAB may perform as a calculator or as a programming language. Calculation and graphic plotting are merged nicely by this. It is comparatively
easy to learn. It is interpreted (not compiled) and easy to fix errors. MATLAB is optimized to be relatively fast when performing matrix operations. MATLAB does have some object-oriented elements.

The experiments illustrated in the thesis and their corresponding implementations are carried out using MATLAB version 7.12 in windows platform.

1.6 SVM CLASSIFIER AND ITS APPLICATIONS

In the early nineties, Support Vector Machines (SVMs) came into view as optimal margin classifiers in the framework of Vapnik’s statistical learning theory. Because of the improved results of SVM compared with the other techniques, it has been effectively concerned with real-world data analysis problems. By diminishing an empirical risk in a well-posed and reliable way, SVM operates inside the framework of regularization theory. As SVM produces sparse solution to classification and regression problems, it becomes most advantageous. Hence, the progress of SVMs application to problems that engage a large amount of data, such as text processing and bioinformatics tasks has been even. Some of the real-world applications of SVM focused are text categorization, bioinformatics and image recognition.

Many internet search engines use text categorization to go for Web pages associated with user queries. A vector space of dimension identical to the number of diverse words in the glossary is used to signify documents. The very famous and fastest Naive Bayes classifier is four times slower than SVM, and SVM is 35 times quicker than classification trees. In bioinformatics, SVM has been applied newly to tissue classification, protein secondary structure prediction and protein fold prediction, protein subcellular location prediction, gene function prediction etc. The two most significant
problems in image processing are handwritten digit identification and face recognition.

1.7 NEURAL NETWORKS AND THEIR APPLICATIONS

Neural Networks (NNs) are biologically motivated computer programs intended to reproduce the information processing of human brain. NNs congregate their acquaintance by distinguishing the patterns and associations in data and are educated through practice, not as of programming. Hundreds of single units, artificial neurons or processing elements (PE) are linked with coefficients known as weights, which comprise the neural structure and are structured in layers. Connecting neurons in a network constitutes the power of neural computations. Each and every PE encompasses weighted inputs, transfer function and one output. With the transfer functions of its neurons, by the learning rule and by the architecture, the performance of a neural network is strong-minded. Since the weights are the modifiable parameters, a neural network is known as a parameterized system. The activation of the neuron is represented by the weighted sum of the inputs. Transfer function is the way which passed the activation signal of the neuron to construct a single output. The concept of non-linearity is initiated to the network by transfer function. The inter-unit links are optimized at the time of training until the error in predictions is diminished. Hence the particular level of accuracy is attained by the network. The new input data to forecast the output can be given only when the network is trained and tested. There are many types of neural networks and new ones are invented every now and then, but all of them can be portrayed by the transfer functions of their neurons, by the learning rule and by the connection formula.
The applications of neural networks fall within the following wide groups:

- Function approximation, or regression analysis, counting time series prediction, fitness approximation and modeling.

- Classification, together with pattern and sequence recognition, novelty detection and sequential decision-making.

- Data processing contains filtering, clustering, blind source separation and compression.

- Robotics, comprises directing manipulators, computer numerical control.

Application areas consist of system identification and control, sequence recognition, quantum chemistry, pattern recognition, medical diagnosis, financial applications, data mining, game-playing and decision-making, visualization and e-mail spam filtering.

1.8 MOTIVATION AND OBJECTIVE OF THE RESEARCH

The goal of minutiae extraction is to detect and mine the exact and convenient minutiae points. Hence a person can be identified easily and quickly. The four categories of basic algorithm for minutiae detection are direct level minutiae extraction, skeletonization-based minutiae extraction, Machine Learning Method and Binary image-based minutiae extraction. The literature for the last 30 years is full of a large set of proposals which attempt to extract the minutiae points from the fingerprint image based on one of these approaches. However, skeletonization-based minutiae extraction using
crossing number concept is used along with the effective preprocessing and post processing techniques to obtain better results. Regarding gender classification, many more techniques and different types of classifiers already exist. Amongst them Support Vector Machines (SVMs) are identified to be superior for binary classification. With respect to age classification, many techniques are used to classify age from facial images. Fingerprints are very rarely used to classify age. Most of the literatures deal with identifying a person using fingerprints based on minutiae or gender or age and a few proposals consider all the three properties together. Auspiciously, this tendency seems to be identifying the person accurately and able to reduce the number of suspects in a crime scenario when the three belongings of the fingerprints are used all together.

Taking all these considerations into account, the final objective of this work is to propose an algorithm to extract minutiae from the fingerprint images, identification of the gender that fingerprint image possesses and to classify the same to identify the age group of that fingerprint among nine different age groups. The nine various age groups are 1 – 10, 11 – 20, 21 – 30, 31 – 40, 41 – 50, 51 – 60, 61 – 70, 71 – 80 and above 80.