CHAPTER 1
INTRODUCTION

1.1  BIOMETRICS

Today, everyone is using mobile phones for managing their bank account, credit information, trading and online shopping. To access internet safely, highly secured authentication systems are essential. All human beings have their own biometrics which can be changed due to some unavoidable circumstances. Biometrics is a science that describes physical characteristics like fingerprint, palm print, face, ear, toe, hand geometry, iris and behaviour characteristics like gait, speech, voice, signature and chemical characteristics like odour of individuals (Debnath et al 2009 and Maltoni et al 2009). Biometrics has physical and behavioural traits to verify personal identity. A good biometric system should be easily assessable, unique and secure over a period time. It should be accurate, fast, robust, secure and inexpensive as well.

Biometric identification techniques prevent the need to remember a PIN or password which may be forgotten, forged, misplaced, stolen, shared or lost. With increasing usage of biometrics, it is necessary to restrict access to sensitive or personal data. Biometric techniques can potentially prevent unauthorized access to or the fraudulent use of ATM, smart cards, desktop PCs and workstations. More number of biometric technologies have been developed and most of these technologies are successfully deployed in all applications. Each biometric has its own pros and cons and the choice of a particular identifier depends on requirements and demand of the consumer based applications. Biometrics is one of the emerging technologies which are adopted almost in all smart phones. Biometric Industry growth drastically increases every year (Dileep & Yeonseung 2009).
In recent years, performance of the biometric techniques has improved significantly and it has achieved higher accuracy rate in all commercial automatic recognition systems. Enormous opportunities are available in future of biometrics that will shape biometric industry through 2020. Recently, Acuity Market Intelligence has released a report regarding biometric industry revenues that are expected to increase in 2017 in identification and verification services, where the present Compound Annual Growth Rate (CAGR) is 19.69 as shown in Figure 1.1 (Source from reference 2). General incomes for biometrics business sector are anticipated to hit US$12000 millions in 2017.

![Biometric industry revenues expected growth in 2017](image)

**Figure 1.1 Biometric industry revenues expected growth in 2017**

1.2 BIOMETRIC SYSTEM

Biometric system is employed to identify and recognize individuals based on their own characteristics in a systematic manner. Biometrics system has single biometric or multi biometric to recognize the individuals. Based on the applications used in the environment, biometrics system is called verification system or identification system (Maltoni et al 2009).
All Biometric systems consist of three phases such as enrollment, identification and verification (Mary & Dushyant 2010) as shown in Figure 1.2. Enrollment is a process of registering individuals with their biometric sample and personal information.

![Biometric Systems Diagram](image)

**Figure 1.2 Biometric Systems**

After sample acquisition, it is converted into digital values and the quality of sample is checked. Features are extracted from sample in feature extraction module which is turn generates feature set, enrollment template and finally it is stored in the system database. Verification or authentication is a process of confirming a person’s identity by using one to one comparison. During verification process, the scanner or sensor captures the person’s identity, converts it into a sample, extracts the features and the extracted feature set is given to a matcher. The matcher compares it with template available in the system, checks the threshold value for matching and finally produces the result that is either matched or not matched.

Biometric system usually has a threshold value to determine the match score that indicates a match or a non-match. Identification is a process to identify an individual by searching the entire enrollment database. One to
one comparison is established to identify an individual. The claim identity feature set is compared against the templates of all persons. Biometric frameworks can either be operated by light out or semi light out process depending upon the applications. It can be developed either as unimodel or multi model or multiple biometric model based on the need for high level security or accuracy of the system (Dileep & Yeonseung 2009). Biometric system design is a very complicated process due to number of challenges like intra-class variability, inter-class similarity, segmentation, noisy input, scalability and template size.

1.2.1 Comparison Outcomes

When two biometric samples are matched, a similarity or dissimilarity score is obtained. Depending on the system, the score can either be interpreted as a match or a non-match. It also depends on how it compares the matching threshold where the correct matches are called true accepts and the incorrect matches are called false accepts. Accordingly, correct non-matches and incorrect non-matches are known as true rejects and false rejects is given in Table 1.1. Accuracy of biometric systems is measured by comparing the frequency of false accepts with true accepts and they are called False Accept Rate (FAR) and True Accept Rate (TAR). All the biometric systems are generally optimized in minimizing false accept rate and maximizing the true acceptance rate.

<table>
<thead>
<tr>
<th>Match</th>
<th>Non-Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct</td>
<td>True Accept</td>
</tr>
<tr>
<td>Incorrect</td>
<td>False Accept</td>
</tr>
</tbody>
</table>
1.3 APPLICATIONS

The utilization of biometrics has expanded in recent years. Biometrics applications can be limited due to a person's creative imagination ability. Biometric innovation is presently used as a part of each developing areas. Biometrics is commonly applied in our day to day activities. For example in opening the entryway of our home, calculating our financial balance, online shopping, accessing our laptops and smart phones as well as in applying for government and so on. Different types of frameworks are used based on its functions. Depending on advancement of biometrics, its applications can be classified into four kinds namely: forensic, government, business and human health care services.

Forensic Applications

In law enforcement and forensic applications, biometrics has been used for a longer period of time mainly for identification of criminals. Automatic Fingerprint Identification System (AFIS) and Integrated Automatic Fingerprint Identification System (IAFIS) maintained by Federal Bureau of Investigations (FBI) are used for searching the histories of criminals in an automated manner. Some of the typical forensic applications are: Identification of criminals, surveillance, corrections and probation and home arrest.

Government Applications

There are several biometric applications developed and deployed in all government sectors. Government of India has set up a number of expert committee councils to establish standards and guidelines in various e-governance applications of Biometrics areas. These applications are: National Identification Cards, Voter ID and Elections, Aadhar Card, Driving license, Benefits Distribution, Employee access and authentication, Military applications, Air travel, Border crossing, Passports.
Commercial Applications

Biometric identification systems significantly outweigh the benefits derived from customer developed commercial applications. Banking, retail and monetary services offer ample scope for biometric technology innovation. Some applications in this sector are: Account access, ATMs Online banking, Telephony transaction, PC/Network access, Physical access, E-commerce Time and attendance monitoring.

Health Care Applications

Health care applications necessitate in the use of biometrics to distinguish or confirm the identity of people collaborating with a health care entity. The main motivation of using biometrics in health care applications is to prevent fraudulent measures and protect the patient information and identify the diseases. Some applications related to health care are: Access to personal information, Patient identification and Disease Identification.

1.4 BIOMETRICS TECHNOLOGIES

There are different types of biometric technologies available based on physical, behavioural and chemical identification schemes (Debnath et al 2009 and Shyam et al 2011).

Physical Biometrics

Ear

The structure and shape of the ear has been used for identification of an individual.

The ear becomes well formed after initial four months of conception and hence the ear's structure of an individual ought to remain the same all through one’s life time.
**Face Recognition**

Face recognition is perhaps the most friendly and acceptable way to conduct human authentication or recognition of an individual’s identity. These certainties depend basically on their simple collectability and non-intrusiveness property. Most of the people generally accept this biometric characteristic as a legitimate verification technique.

**Fingerprint**

Nowadays, fingerprints are considered as most dependable biometric trademarks for human identification because of their uniqueness and permanence. A fingerprint consists of ridges and valleys in the fingertips’ surface and its development takes place even during the fetal months of a baby.

**Hand Geometry Recognition**

Human verification depending on hand geometry considers various measures in view of hand's shape, size, lengths and widths of the fingers. The major advantage of this kind of human verification strategies depend on its simplicity, straightforwardness and inexpensive detecting devices.

**Iris**

Its visual surface is framed during the fetal period and its arrangement is extended up to the first two years of a baby’s life. The iris composition is extremely hard to be changed surgically.

**Retina**

The pattern of veins underneath the eyeball's back is called retina. It is accepted to be different to every individual and also the most secure biometric system. It can be acquired with low intensity beam or infrared light.
is focused into the eye so that a predetermined piece of the retinal vasculature can be digitized.

**Vein**

Vein is a biometrics that can be used to distinguish people in light of the vein designs in the human finger or palm. Vein patterns are accepted to be distinct for individuals and are invariant to time, even for indistinguishable twins.

**Behavioral Biometrics**

**Gait**

Gait is an emerging behavioural aspect that is used to verify individuals by the way they walk. The attractiveness of this technique relies on its inconspicuous properties, since people are validated at specific separations without any need for technology.

**Keystroke Typing**

Keystroke typing is identified with the way individuals type characters on keyboards. It draws attention as a developing biometric trademark that is supported by studies which exhibit that human repetitive activities are predictable and in this way an individual can be described by their keystroke motion. It calculates the periods between keystrokes whereas the hold times represent to the duration of time between the hit and arrival of a key hold.

**Signature**

The authentication of an individual is done by the analysis of handwriting style in general and signature in particular. Visual comparison takes place between one signature and the other signature and it is captured with the X, Y, T and P coordinates of the signor.
Voice

Voice is a mix of physical and behavioural attributes that are identified with voice sign patterns of a given person. The physical characteristics of voice are identified to the limbs that frame its sound. These characteristics incorporate vocal tracts, mouth, nasal cavities and lips.

Chemical Biometrics

DNA

DNA stands for Deoxyribo Nucleic Acid and it is one of the chemical biometrics and is a molecule in all living organisms. It is composed of nucleotides and genomes. The human genome is more distinctive to each individual.

Odour

Biological organisms are composed by chemical elements where each organism produces a specific odour that becomes a characteristic of that organism and it is used to identify the identity of an individual. An odour can be used as a distinctive characteristic for number of species.

1.4.1 Comparison of Biometric Technologies

Physical, behavioural and chemical characteristics should meet some requirements in order to be used as biometrics methods. Comparison of different types of biometric characteristic is given in Table 1. 2 (Rupinder & Narinder 2014). These requirements are either theoretical or pragmatic.

Theoretical requirements include:

- Uniqueness: No two persons have equivalent characteristics.
- Universality: Each individual should have his/her own biometric characteristic.
- Permanence: These characteristics are last longing and do not undergo sudden changes.
- Collectability: The characteristic should have the ability to be measured quantitatively.

The practical prerequisites are customarily identified with utility of the computational framework as.
- Circumvention: Level of security in the biometric system with given fraudulent attacks.
- Performance: An achievable recognition accuracy and speed that a biometric framework can accomplish.
- Acceptability: An acceptance of users in applying the biometrics system as a part of their day to day lives.

**Table 1.2 Comparison between different biometrics**

<table>
<thead>
<tr>
<th>Biometric</th>
<th>Uniqueness</th>
<th>Universality</th>
<th>Permanence</th>
<th>Collectability</th>
<th>Circumvention</th>
<th>Performance</th>
<th>Acceptability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ear</td>
<td>Average</td>
<td>Average</td>
<td>Good</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
</tr>
<tr>
<td>Face</td>
<td>Low</td>
<td>Good</td>
<td>Average</td>
<td>Good</td>
<td>Good</td>
<td>Poor</td>
<td>Poor</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Good</td>
<td>Average</td>
<td>Good</td>
<td>Average</td>
<td>Average</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Average</td>
<td>Average</td>
<td>Good</td>
<td>Average</td>
<td>Medium</td>
<td>Good</td>
<td>Average</td>
</tr>
<tr>
<td>Iris</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Average</td>
<td>Poor</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Retina</td>
<td>Average</td>
<td>Good</td>
<td>Average</td>
<td>Poor</td>
<td>Poor</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Vein</td>
<td>Average</td>
<td>Good</td>
<td>Average</td>
<td>Poor</td>
<td>Average</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Gait</td>
<td>Average</td>
<td>Poor</td>
<td>Good</td>
<td>Average</td>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
</tr>
<tr>
<td>Keystroke</td>
<td>Poor</td>
<td>Poor</td>
<td>Average</td>
<td>Average</td>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
</tr>
<tr>
<td>Signature</td>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
<td>Good</td>
<td>Good</td>
<td>Poor</td>
<td>Poor</td>
</tr>
<tr>
<td>Voice</td>
<td>Poor</td>
<td>Average</td>
<td>Poor</td>
<td>Average</td>
<td>Good</td>
<td>Poor</td>
<td>Poor</td>
</tr>
<tr>
<td>DNA</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Poor</td>
<td>Poor</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Odor</td>
<td>Good</td>
<td>Good</td>
<td>Poor</td>
<td>Average</td>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
</tr>
</tbody>
</table>

Compared with all biometrics, Fingerprints are the most commonly used biometrics for an individual’s identification and affirmation in biometric recognition. Here, revenue of biometric technologies, fingerprint is found to be first in position as given in Table 1.3 (Source from reference 32).
Table 1.3 Revenue of biometric technologies

<table>
<thead>
<tr>
<th>Biometrics /Revenue</th>
<th>2010 ($millions)</th>
<th>2011 ($millions)</th>
<th>2012 ($millions)</th>
<th>2015 ($millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>2,590.0</td>
<td>2,620.0</td>
<td>2,698.0</td>
<td>6,750.0</td>
</tr>
<tr>
<td>Face, Iris, vein</td>
<td>1,120.0</td>
<td>1,210.0</td>
<td>1,334.8</td>
<td>3,400.0</td>
</tr>
<tr>
<td>Hand, Signatures</td>
<td>300.0</td>
<td>560.0</td>
<td>652.6</td>
<td>460.2</td>
</tr>
<tr>
<td>Others</td>
<td>757.3</td>
<td>1,157.3</td>
<td>1,314.6</td>
<td>1,400.0</td>
</tr>
</tbody>
</table>

1.5 HISTORY OF FINGERPRINT IDENTIFICATION

Fingerprint is a print made by an impression of the friction ridges in the skin of a finger and it is regularly used for biometric identification proof in criminal examinations. Fingerprint Identification is a method of identification that uses impressions made by minute ridge formations, pores or patterns found on the fingertips. The visible human attributes have a tendency to change the fingerprints that are extremely tenacious. Except wounds or surgery that creates profound scarring, the fingerprints do not change during the lifetime of an individual. In earlier days, marking or mutilating was used for criminal ID. Ancient Romans used tattoo needles to distinguish and identity soldiers from their positions. Much earlier, law authorization officers with phenomenal visual memories, purported "cam eyes," that identified captured wrongdoers by sight alone. Photography decreased the weight on memory yet it was not entirely fool proof. Individual appearances can conceivably change.

Around 1870, French anthropologist Alphonse Bertillon concocted a framework to gauge and record the measurements of certain hard parts of the body. These estimations were weakened due to an equation which hypothetically would apply just to one individual and would not change amid his or her grown-up life. Sir Francis Galton, British anthropologist and a
cousin of Charles Darwin suggested his view of fingerprints as a method for identification (ID) in the year 1880's (Lambourne 1997).

In 1900, United Kingdom Home Secretary Office led an investigation on “Identification of Criminals by Measurement and Fingerprints”. Mr. Edward Richard Henry showed up before the Request Board to clarify the framework, “The Classification and Use of Fingerprints”. The panel prescribed reception of fingerprinting as a replacement for the generally erroneous Bertillon arrangement of anthropometric estimation which depended on fingerprints for ID.

The Bertillon system was the most accepted system for a long time. In any case, the anthropometric measurement estimation continued to gain importance. A man named Will West was sentenced to the U.S. Prison at Leavenworth, Kansas. Later it was found that there was a prisoner at the time whose Bertillon estimations were very nearly the same and his name was William West.

Upon examination, there were in reality two men who looked precisely indistinguishable. Their names were William and Will West. Their Bertillon estimations were sufficiently closer to distinguish them as the same individual. Nonetheless, fingerprint comparisons rapidly and effectively distinguished them as two distinctive individuals.

In October 1915, a gathering of twenty two identification personals met and launched the Universal Association for Criminal Identification (UACI). In 1918, the association was renamed International Association for Identification (IAI) because of the volume of non criminal recognizable proof work performed by individuals.
In 1924, Federal Bureau of Investigation (FBI) was established to give archive of fingerprints. It provides a central store house of criminal identification data for law enforcement organizations all through the nation.

By 1946, FBI had prepared 100 million unique finger impression cards in physically looked after documents; and it got increased to 200 million cards in 1971. With the introduction of Automated Fingerprint Identification System (AFIS) innovation, the documents were converted into automated criminal records and were physically kept as common documents.

In the year 1974, United Kingdom’s, Fingerprint Bureau approached unique fingerprint specialists and initiated their nation's first expert fingerprint association and named it the National Society of Fingerprint Officers. This association at first had only UK specialists and it got immediately extended to worldwide and it was renamed The Fingerprint Society in 1977. In the same year, 62nd Annual Conference of the International Association for Identification (IAI) was voted to build the world's first certification programme for fingerprints specialists.

Since 1977, the IAI's Latent Print Certification Board tried a huge number of candidates and occasionally conducted capability tests to all IAI Certified Latent Print Examiners (CLPEs). This tremendous growth of fingerprint identification after 38 years is unbelievable.

In 1992, the Identification Division was re-established as the Criminal Justice Information Services Division (CJIS) which maintains the national repository of criminal history records and data. It also provides ten-print identification services to all federal, state, local criminal justice agencies, authorized employment and licensing agencies. It also ensures quality of all these services.
In 2012, INTERPOL's Automated Fingerprint Identification System storehouse surpasses 1,500,000 sets of fingerprints for critical worldwide criminal records from 190 nations. More than 170 countries have 24 x 7 interface capacity with INTERPOL master unique fingerprint administrations. Today, the biggest AFIS storehouse in America is governed by the Department of Homeland Security's US Visit Program, containing more than 120 million persons' fingerprints. The US Visit Program has been moving from two level fingerprints to ten flat fingerprints. At present, fast catch innovation empowers recording of ten fingerprints within 15 seconds for each person.

In January 2015, the Unique Identification Authority of India (UIDAI) started working for the world's biggest multi-model biometric system, with more than 734 million fingerprints, faces and iris biometric records. India's Unique Identification undertaking program is called Aadhaar. An Aadhaar is a project, with the objective of giving solid national ID to majority of India's 1.2 billion citizens. Fingerprint Identification merges with all other measurable sciences for some reasons. It incorporates different governments sectors in worldwide to give precise ID. No two fingerprints have ever been discovered alike among numerous billions of human beings. Fingerprints are one of the very bases for criminal history establishment and it is the most generally used measurable proof around the world and it continues to be extended for emphatically recognizing persons. Fingerprint identification is one of the oldest biometric sciences. Fingerprint technology has been broadly accepted due to its historical use within the law enforcement community and the presence of AFIS database. It is a basic to precede research on improving the reliability, stability, performance and security of fingerprint recognition systems. Low quality fingerprint image, distortion, partial image problems, large fingerprint databases are all major areas of research that are necessary to enhance the accuracy of current systems.
1.5.1  Fingerprint

Each and every finger has number of ridges and valleys. Fingerprints are unique prototype and are made by friction of ridges and furrows, which appear on the pad of the fingers (Maltoni et al 2009). No two persons have exactly the same arrangement of ridge patterns, and the patterns of any individual remain unchanged throughout life.

1.5.2  Types of fingerprints

Fingerprints are categorized into rolled, plain, latent and overlapped images (Alessandra et al 2013) are shown in Figure 1.3.

**Rolled print**

The rolled print is obtained by rolling the finger from nail to nail either on a paper or in the scanner.

**Plain print**

The plain print is acquired by placing the finger flat on a paper.

![Different fingerprint images](image_url)

**Figure 1.3**  Different fingerprint images a. Rolled Print b. Plain Print c. Latent Image and d. Overlapped Image
**Latent Image**

It is acquired from the surfaces of objects that are partially touched by a person during crime scenes. Latent prints are framed when the body’s natural oils and sweat on the skin are kept onto another surface. It can be found on a variety of surfaces. In crime investigation the suspects are recognized based on the impressions collected from crime scenes.

**Overlapped Image**

A fingerprint image contains either a single fingerprint or a set of non overlapped fingerprints. There are some circumstances where a few fingerprints sit on top of another fingerprints. Overlapped fingerprint is expressed as the ridges and valleys of one finger impression that is merged with same individual or distinctive individual or with background images (Fanglin et al 2011) as shown in Figure 1.3.

**1.5.3 Challenges in latent and overlapped images**

Fingerprints obtained from crime scenes may be of a very bad quality due to presence of some noise. Compared to plain or rolled fingerprints, latent fingerprints are smudgy and unclear and they capture only a small finger area and have a large nonlinear distortion due to pressure discrepancy as well as presence of a complex background. Due to their poor quality and smaller area, latent has a significantly smaller number of features compared to rolled or plain prints (Maltoni et al 2009). In some scenes, due to overlapping and low quality, the fingerprint features may not be accurate, which lead to incorrect identification of person by fingerprint experts. It happens particularly during criminal investigations. There is a chance that the fingerprint experts misjudge in identifying a person. In the low quality and overlapped images, feature extraction, enhancement, classification, segmentation, separation of overlapped images and fingerprint matching is not
applicable, it creates major challenges for designing AFRS for overlapped images (Fanglin et al 2011 and Alessandra et al 2013).

1.6 AUTOMATIC FINGERPRINT RECOGNITION SYSTEM

An Automatic Fingerprint Recognition System (AFRS) is one of the major techniques in the field of biometric research society. AFRS is applied in various commercial applications like government, civilian, financial domains and forensic applications. There are number of complicated issues that need to be addressed to develop the scope of AFRS. General and complicated issues for designing AFRS are non linear distortion (pressure, placement and rotation), low quality image, segmentation, sensor noise, skin conditions (wet, dry, dirty, age), overlap image, inter class similarity, intra class variations and template aging (Anil & Jianjiang 2011). In certain situations, due to overlapping and low quality, the fingerprint features may not be very accurate resulting in mismatch of a person’s identification by fingerprint experts. Determining the distinct features of fingerprints overlapped either with the image of a finger or with the background can be difficult and time consuming process. Due to overlapped fingerprints, recognition may not be possible even if the fingerprint templates for the images are available.

1.7 LITERATURE SURVEY

More related works on overlapped fingerprint image separation in the existing systems (Fan et al 2004), (Singh et al 2008), (Geng et al 2008), (Fanglin et al 2011), (Yuan Shi et al 2011), (Jianjiang et al 2012), (Qijun et al 2012) and (Ning et al 2014) are reviewed and discussed for identifying individuals. Most of the existing fingerprint matching algorithms fail to match the overlapped image in an efficient manner.
A more universal and convenient solution is to develop an image processing algorithm to perform the separation task. Such an algorithm will not only benefit fingerprint recognition systems, but will also simplify manual feature marking as well. An algorithm is developed to separate overlapped fingerprints based on an image enhancement by using a manually marked orientation field (Fan et al 2004). However, it is very tedious and time-consuming for the user to manually mark the orientation field for each component fingerprint in the overlapped fingerprint image. The proposed partition mask method to divide the overlapped fingerprints is focused around a fingerprint image upgrade by using a Gabor filter. It is an extremely monotonous and tedious task for the fingerprint examiners to physically perceive the overlapped fingerprint images. Utilized morphological segment investigation is made (Geng et al 2008) is carried out for a particular fingerprints separation. The trial results demonstrate that their framework can separate just the finger impression segments.

Independent Component Analysis (ICA) for independent covered fingerprints images (Singh et al 2008), without any partition calculation for overlapped fingerprint images. The overlapped fingerprints are separated with the help of fingerprint experts. The orientation fields are marked manually in the overlapped images. Fanglin et al 2011 used relaxation labelling algorithm to separate the images, which acquire manually marked region masks and singular points as input. However it is not applicable for low quality images obtained from uneven surfaces, different pressures and various distortions. Constrained relaxation labelling (Yuan Shi et al 2011) proposed for fingerprint separation where the method is partially automatic.

The robust orientation field estimation algorithm (Jianjiang et al 2012) and (Qijun et al 2012) that it does not work well for presence of singular points such as core and delta in the overlapped region of overlapped
fingerprints. This algorithm cannot address latent images with more than two overlapped fingerprints or latent images with two overlapped fingerprints and structured noise and also not yet fully automatic. The region masks of the two component fingerprints should be marked manually.

The adaptive orientation model (Ning et al 2014) is proposed for overlapped fingerprint separation. This proposed adaptive orientation method is not able to split more than two overlapped fingerprints. There is only one publicly available latent overlapped fingerprints data set currently. Images in this data set are of relatively good quality and no structured noise is presented. This algorithm is not yet fully automatic.

Fingerprint recognition has wider application prospects in all fields which contain identity authentication. The proposed system addresses the design of a new recognition system to overcome the existing limitations in recognizing a person having overlapped and low quality fingerprint images. A typical constraint of all these studies is that no target assessment is performed to figure out whether the overlapped fingerprint separation algorithms have reduced the false recognition and false acceptance rates. In the existing system, there is no algorithm to identify the overlapped images in an automatic manner. An effective methodology is proposed to identify the overlapped images that separate the overlapped fingerprints. In the studies and works made in the existing systems, there is no algorithm to identify and classify the overlapped images in an automatic manner. This proposed system is able to overcome the existing limitations for recognizing the person having overlapped and low quality fingerprint images. The proposed framework used ANFIS classifier for detecting the overlapped images. An effective methodology is proposed to identify the overlapped images and classify them by using the ANFIS classifier. The ANFIS classifier separates them and enhances the matching accuracy of overlapped fingerprints.
1.8 PROBLEM FORMULATION

Automated Fingerprint Recognition Systems have been effectively deployed around the earth for law enforcement, civilian applications and mobile biometrics in smart phones. The fingerprint will ever grow to be emerging and leading biometric trait. Many identity and access based applications will continue to use fingerprint authentication because of its excellent performance, enormous databases and accessibility of the fingerprint devices with lowest cost.

This proposed overlapped fingerprint recognition system framework may help agents in rapidly analyzing and identifying suspects who are found at crime scene. Fingerprint technology shows its worthiness in law authorization offices, by providing help by way of fast and substantial recognizable pieces of proof when individual data is missing or suspicious. The capability of fingerprints for law enforcement has been shown. However its scope for uses seems to be broad and promising.

New research problems have resulted in wider development of fingerprint technology. There are various issues that need to be addressed to develop the scope of Light out Fingerprint Recognition System (LFRS). The latent fingerprint images can be overlapped in crime scenes. During investigations, there are several possibilities for acquiring damaged or overlapped fingerprint images. Individual persons cannot be identified and recognized by using these kinds of overlapped images. The matching accuracy of latent images is critical even if they have manual interference and manual mark-up by latent examiners. Separation of overlapped images and identification of an individual is a very complicated task for fingerprint examiners. The overlapped fingerprint images create a very tedious challenge to the existing fingerprint recognition algorithms.
An AFRS aims to design and develop an algorithm for separating overlapping latent that will serve as an important tool in forensics. The AFRS analyzes and identifies the overlapped images by using an ANFIS Classifier. An Orientation Field Separation (OFS) Algorithm is proposed to identify the regions of overlapped images without any human intervention for overlapped image separation. This work is designed to retrieve fast and accurate data by using one-to-N fingerprint identification for the overlapped images. In the research work carried out, a novel methodology is suggested to separate the overlapped fingerprint automatically and also expand the set of datasets for testing and training process. Extensive experiments are performed on the datasets such as FVC 2006 DB1-A, DB2-A, NIST SD27 and SLF databases.

The experimental results are highly promising and they outperform the previous systems in identifying overlapped images. The AFRS system separates the overlapped fingerprints more accurately and robustly. The achieved results confirm that the proposed AFRS system has higher possibility of overlapped fingerprint detection. The outcome of this work shows that the overlapped fingerprint is separated in a successful manner. The work carried out in this research tries to determine the performance of separation of overlapped fingerprint images in an efficient manner and formulate the identification rate with accurate and fast data retrieval.

1.9 OBJECTIVES

i. The primary objective of this AFRS is to identify and separate overlapped fingerprint images automatically by employing an ANFIS Classifier.

ii. The proposed AFRS can be implemented for public safety, national security, efficiency, privacy, data protection and smooth transition.
iii. A novel OFS algorithm is suggested and implemented to analyze the fingerprints of persons even if it is overlapped so as to provide a secure environment for various online applications where high security is required.

iv. To implement overlapped fingerprint classification in an automatic manner by using neuro-fuzzy system.

v. To train and test the AFRS system so as to make it possible for identifying and recognizing the overlapped fingerprint images.

1.10 DESIGN OF PROPOSED AUTOMATIC FINGERPRINT RECOGNITION SYSTEM

The proposed AFRS design requires five main stages for its implementation. The Block Design for AFRS is shown in Figure 1.4. There are various phases such as fingerprint acquisition, feature evaluation, ANFIS classifier, overlapped fingerprint separation, feature extraction, fingerprint matching and fingerprint recognition.

Fingerprint acquisition phase collects normal and overlapped image datasets from various sources such as Tsinghua University, IIIT, NIST and FVC. The images are preprocessed by employing Gabor filtering.

During feature evaluation phase, features are identified and they can be varied for overlapped and non-overlapped images. Then computing is done for first order features, second order statistical features and third order features for the overlapped and non overlapped images. After calculating the features, the feature vector for overlapped and non-overlapped images is constructed in different directions $0^\circ$, $45^\circ$, $90^\circ$ and $135^\circ$. 
Figure 1.4 Block Design for AFRS

- Input Image (Normal or overlapped image)
  - Image Preprocessing (Gabor Filtering)
  - Feature Evaluation (First order, second order and third order features)
  - ANFIS Classifier
  - Normal image
  - Overlapped image
  - Orientation Field Separation (OFS) Algorithm
  - Orientation Field Reconstruction
  - Feature Extraction (Minutiae and pore Extraction)
  - Fingerprint Matching
  - Fingerprint Recognition

Figure 1.4 Block Design for AFRS
ANFIS Classifier is an adaptive neuro fuzzy classifier which is used to classify the images into two categories which may either be overlapped or normal images. ANFIS Classifier is used to detect the overlapped images when a set of features extracted from the overlapped images were used as inputs. To train the ANFIS classifier, a hybrid learning algorithm (Monireh et al 2012) is used and it combines the least-square estimator and the gradient descent method.

The fourth phase represents the OFS algorithm. An overlapped fingerprint image is partitioned into non-overlapping blocks. The regions of the component fingerprints are identified and the quantity of overlapped area like small, medium and large in the image is calculated. Gaussian high pass filters are used to enhance the overlapped fingerprint images.

Fifth phase feature extraction extracts the features minutiae and pore depending on the quality of the images. The image quality is computed by applying National Fingerprint Image Quality (NFIQ) software.

Sixth phase fingerprints are matched by using minutiae matched and pore matched algorithms and finally it computes the matching score by applying different matching algorithms and compares the results for the algorithms.

1.11 DATASET

In this research work, the normal and overlapped fingerprint images are collected from the Department of Automation, Tsinghua University, Latent fingerprint database and Simultaneous Latent Fingerprint (SLF) databases from Indraprastha Institute of Information Technology (IIIT), Delhi (Sankaran et al 2011). The system also uses NIST SD-27 from the National
Institute of Standards and Technology and FVC 2006 DB1-A, FVC2006 DB2-A databases from the Fingerprint Verification Competition (FVC).

1.12 ORGANIZATION OF THE THESIS

Chapter 1

The First Chapter gives a brief overview of biometrics and applications of biometrics in different fields. This chapter also gives details about fingerprint identification, review works carried out in overlapped fingerprint separation and objectives of the AFRS System. The literature reviews related to overlapped fingerprint separation and recognition were presented to understand their limitations and improvement required to develop the proposed AFRS.

Chapter 2

The Second Chapter deals with image pre-processing by using Gabor filtering and steps included in the assessment of features for normal and overlapped fingerprint images.

Chapter 3

The Third Chapter focuses on fingerprint image classification by using ANFIS Classifier. It systematically analyzes general fingerprint classification system, Fuzzy Inference System, Neural Network, Neural Fuzzy Inference System and ANFIS Classifier. A detailed discussion of the simulation results is presented.

Chapter 4

The Fourth Chapter presents a novel method for overlapped fingerprint separation, reconstruction of the orientation field for separated
Chapter 5

The Fifth Chapter offers feature extraction and matching for fingerprint images. It deals with extraction of features like minutiae and pore based on the quality of the fingerprint images and it applies matching algorithms for fingerprints by using minutiae and pore features and then computes the matching score by using different matching algorithms and combines scores of all algorithms by applying score fusion methods.

Chapter 6

The Sixth Chapter summarizes performance analysis and achieved results of the research work carried out. It compares the results of various proposed algorithms that are discussed with existing methodologies and the evaluation of the proposed algorithms on various databases should be very critical and more challenging. Yet the demand and applications of them are of necessity and will be very beneficial for more accurate and advanced AFIS.

Chapter 7

The conclusion chapter compares the results obtained by using AFRS system with the existing system. The present research work may further be extended in future for inventing a more accurate fingerprint identification and recognition systems. By using the above mentioned methodologies in AFRS system, special applications were developed that will help in communal safety and general security as well as in improving privacy, data protection and smooth transition. Further it discusses the future scope of the work for
improved performance and implementation of AFRS. This chapter presents the summary of the entire thesis.

1.13 SUMMARY

This chapter is discussed which introduction on biometrics, biometric system, applications of biometrics in various fields, various biometric technologies, comparison of different biometric technologies, history of fingerprint identification, problem formulation, objectives of the proposed system and overview of the thesis.