Chapter 1

Introduction

Identification of an individual is essential to check intruders crossing the Indian border for national security and also for most of the applications of day to day transactions. Advancements in digital technology have posed a serious threat to secure authentication of human identity. The traditional methods of personal identification rely on tokens like physical key, identity card, smart card or knowledge based secret password, Personal Identification Number (PIN) [1] etc. The token-based systems are not reliable, since the portable devices used may be lost or stolen and knowledge based systems using password and PIN may be forgotten, easily guessed or even broken by fraudulent attacks. Hence traditional systems are not enough to guarantee the reliable human identification. The biometric traits cannot be lost, stolen and forgotten, since these are parts of the body and behavior of a person. Furthermore, biometric characteristics are unique among individuals and they do not change normally with time.

1.1 Biometric traits

The terms Biometrics and Biometry have been used since early in the twentieth century to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. Biometrics refers to the automatic identification of human beings based on their
physiological and behavioral characteristics [2], which are based on features of human body parts and behavior of a person respectively. The physiological or behavioral characteristics are unique to an individual and an ability to reliably distinguish between an authorized person and an imposter. The biometric characteristics are referred to by different terms such as traits, identifiers or modalities. The physiological traits include face, fingerprint, hand geometry, retina, iris, Deoxyribo Nucleic Acid (DNA), and ear, while the behavioral traits include key stroke identification, voice, signature and gait. The biometric characteristics present some specific properties such as uniqueness and persistency, which makes them suitable for reliable personal identification. The choice of biometrics depends on user acceptance, level of security required, accuracy, and implementation cost and time.

1.1.1 Physiological biometrics

The physiological biometric features are almost constant through out the life time of a person.

(i) **Face:** A face recognition system is used to identify or verify a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing the selected facial features from an image and a facial database. Figure 1.1 shows an example of facial images of a person.
Some facial recognition algorithms identify faces by extracting landmarks or features from an image of the subject’s face. For example, an algorithm may analyze the relative position, size, and/or shape of an eye, nose, cheekbones and jaw. These features are then used to search for other images with matching features [3].

(ii) **Fingerprint**: The fingerprint recognition or fingerprint authentication refers to an automated method of verifying a match between two human fingerprints [4].

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern as shown in Figure 1.2. These include patterns, which are aggregate characteristics of ridges and minutia points, which are unique features found within the patterns.
(iii) **Hand geometry**: The physical characteristics of the users hand and fingers are measured from a three-dimensional perspective as shown in Figure 1.3. Being one of the most established methodologies, it offers a good balance of performance characteristics and is relatively easy to use.

![Hand geometry biometrics](image)

**Figure 1.3: Hand geometry**

The hand geometry biometrics is suitable for larger user databases or users, who may access the system infrequently and may therefore be less disciplined in their approach to the system. The hand geometry readers are deployed in a wide range of scenarios, including time and attendance recording where they have proved extremely popular [5].

(iv) **Retinal scanning**: This is an established technology, where the unique patterns of the retina are scanned by a low intensity light source via an optical coupler. Retinal scanning has proved to be quite accurate in use but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient for spectacle wearers and for those who avoid intimate contact with the
source used for the scan and hence this has a few user acceptance problems although the technology itself can work well [6].

**(v) Iris:** An iris is a colored region between dark pupil and bright sclera. An iris pattern contains many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette [7]. The striated trabecular mesh work of elastic pectinate ligament creates the predominant texture under visible light, whereas in the near infrared wavelengths stromal features dominate the iris pattern. It is the only internal organ, which can be seen outside the body. The probability of uniqueness among all human beings has made iris recognition a reliable and efficient human recognition technique.

The visible portion of the human eye consists of the pupil, the iris, and the sclera. A front view of human eye is shown in Figure 1.4. It controls the amount of the light that reaches the retina. The color of the iris is of little use in recognition, but the texture of the iris is quite complex and unique [8].

![Figure 1.4: A front view of human eye](image)
Among all the biometric techniques, iris recognition has drawn a lot of interest in Pattern Recognition and Machine Learning research area because of the advantages viz., (i) an iris formation starts in the third month of gestation period and is largely complete by the eighth month and then it does not change after two or three years, (ii) the human iris might be as distinct as the finger prints for the different individuals, (iii) the forming of iris depends on the initial environment of the embryo and hence the iris texture pattern does not correlate with genetic determination, (iv) even the left and the right irises of the same person are unique, (v) it is almost impossible to modify the iris structure by surgery, (vi) the iris recognition is non-invasive. (vii) it has about 245 degrees of freedom [9].

**(vi)** DNA Recognition: The human beings have 23 pairs of chromosomes containing their DNA blueprint. One member of each chromosomal pair comes from their mother; the other comes from their father. Every cell in a human body contains a copy of this DNA as shown in Figure 1.5.

![DNA image](image)

Figure 1.5 DNA image

The majority of DNA does not differ from person to person, but 0.1 percent of a person’s entire genome would be unique to each
individual. This represents three million base pairs of DNA [10].

Genes make up 5 percent of the human genome. The other 95 percent are non-coding sequences. In non-coding regions, there are identical repeat sequences of DNA, which can be repeated anywhere from one to thirty times in a row. These regions are called Variable Number Tandem Repeats (VNTRs). The number of tandem repeats at specific places (called loci) on chromosomes varies between individuals. For any given VNTR loci in an individual's DNA, there will be a certain number of repeats. The higher number of loci is analyzed, the smaller the probability to find two unrelated individuals with the same DNA profile.

DNA profiling determines the number of VNTR repeats at a number of distinctive loci, and uses it to create an individual's DNA profile. The main steps to create a DNA profile are: isolate the DNA (from a sample such as blood, saliva, hair, semen, or tissue), cut the DNA up into shorter fragments containing known VNTR areas, sort the DNA fragments by size and compare the DNA fragments in different samples.

(vii) Ear: The ear shape and the structure are distinct. The features of ear are appearance, structure, and morphology of the human ear. The human ear is observed to exhibit variations among individuals as assessed by the curves, surfaces, and geometric measurements pertaining to the visible portion of the ear, commonly referred to as the pinna. The recognition is based on matching between the landmark locations on the ear and salient points on the pinna. The
structure of the ear is stable, despite aging and its growth is linear after the age of four years. The disadvantage is features of an ear are not unique [11].

1.1.2 Behavioral biometrics

Behavioral characteristics are based on behavior of a person and may not be constant over time. It depends on mood, circumstance and the mental status of a person. A brief discussion of behavioral traits such as keystroke dynamics, voice, signature and gait are discussed as follows.

(i) Keystroke Identification: The keystroke dynamics uses the manner and rhythm in which an individual types the characters on a keyboard or keypad as shown in Figure 1.6. The keystroke rhythms of a user are measured to develop a unique biometric template of the users typing pattern for authentication. The raw measurements available from every keyboard can be recorded to determine the time a key is pressed and the time between key up and key down.

![Figure 1.6: Keystroke dynamics](image)

The recorded keystroke timing data is then processed through a unique neural algorithm, which determines a primary pattern for
comparison. Similarly, vibration information may be used to create a
pattern for identification and authentication purposes.

(ii) **Voice Recognition:** The voice is a combination of physical and
behavioral biometric characteristics. The physical features of an
individual’s voice are based on the shape and size of the appendages
(e.g., vocal tract, mouth, nasal cavities, and lips) that are used in the
synthesis of the sound. The physical characteristics of human speech
are invariant for an individual, but the behavioral aspects of speech
change over time due to age, medical condition (such as cold, throat
infection), emotional state, etc. Voice is also not very distinctive and
may not be appropriate for large-scale identification.

The speaker recognition/ voice recognition is the computing
task of validating a user’s claimed identity using characteristics
extracted from their voices. There is a difference between speaker
recognition [12] (recognizing who is speaking) and speech recognition
(recognizing what is being said). These two terms are frequently
confused, as is voice recognition. Voice recognition is combination of
the two.

(iii) **Signature Verification:** The signature is a handwritten
illustration of a person’s authentication depicted through lines and
curves as shown in the Figure 1.7. The signature verification is a
process of discriminating between genuine and forged set of
handwritten signatures and it is a difficult task as the signatures are
a result of the physical and psychological status of an individual.
Signature is preferred among various biometrics as it is widely accepted for identifying an individual in daily routine works such as automated banking transaction, electronic fund transfers, document analysis, and access control. There are two categories in signature verification based on the acquisition of the signature image: On-line and Off-line verification systems. The on-line verification process is conducted using electronic pen with information about velocity, stroke order, acceleration, pen pressure, etc., while an off-line process uses a static two dimensional image of signature. The off-line signature verification problem is more challenging than on-line one, because the valuable information such as the pen’s velocity, pressure and stroke order are not available [13]. The features used in off-line signature verification are signature image area, length to width ratio, geometric centers, angle and distance of a pixel from a reference point and transform domain features.

The challenges in signature recognition are: (i) The segmentation of signature strokes is difficult due to highly stylish and unconventional writing styles. (ii) The nature and the variety of the writing pen may also affect the nature of the signature obtained. (iii) The non-repetitive nature of variation of the signatures, because
of age, illness, geographic location and perhaps to some extent the emotional state of the person.

The forgery is the process of making, adapting, or imitating the signature by an imposter with an intent to deceive. The forged signature images are classified in two groups: (i) random, and (ii) skilled. The random forgeries are formed without any knowledge of the signer’s name and signature’s shape. The skilled forgeries are produced by professional imposter with the knowledge of genuine signature and imitate as closely as possible [14]. The disadvantages of on-line verification are: (i) heavy computational load and (ii) warping forgeries. The disadvantages of off-line verification are: (i) it can be easily forged as compared to on-line signature, and (ii) certain aspects as pen pressure, velocity and stroke order cannot be acquired.

The complete off-line signature verification system is split into four stages: signature database creation, preprocessing, feature extraction and matching. The signature database creation includes capturing the images of signatures. Preprocessing step involves removal of noise and skeletonization for making an acquired signature suitable for feature extraction. Then the preprocessed image is used to extract relevant features that can distinguish signatures of different persons. The extracted features are used to verify a given signature image.

(iv) Gait: Human gait is the manner in which people walk and is one of a few biometric traits that can be used to recognize people at a
distance. The gait is appropriate in surveillance scenarios, where the identity of an individual can be secretly established. It is a spatio-temporal biometric, and not very distinct but satisfactorily distinguish person in low-security application. The biometric may differ over a long period of time due to changes in body weight and major injuries connecting joints and brain [15]. The acquisition of gait is similar to acquiring a facial image. Since video sequence is used to measure several different movements, this method is computationally expensive.

1.2 Biometric System

A biometric system is a real-time identification system, which identifies a person by measuring a particular physiological or behavioral characteristic and later comparing it with database of characteristics belonging to many people. The biometric devices consist of a reader or scanning device to acquire biometric data, and software to identify a person.

The general block diagram of biometric system is shown in Figure 1.8. It consists of three important modules and are enrolment module, test module and classification module.

1.2.1 Enrolment module:

The biometric database is created by capturing biometric samples of many individuals using sensors or scanning devices. The biometric traits are preprocessed to extract features to derive the database feature vectors.
(i) **Database:**

The different kinds of biometric traits can be used in creating database. The popular iris databases publically available for research work are developed by Chinese Academy of Science Institute of Automation (CASIA), UBIRIS developed by Soft Computing and Image Analysis, Portugal. The publically available signature databases are Grupo de Procesado Digital de Senales (GPDS), Ministerio de Ciencia Y Tecnologı´a (MCYT), and Signature Verification Competition 2004 (SVC 2004).

The face biometric databases available for research work are Libor Spacek, AT & T (formerly Olivetti Research Laboratory), Yale, Yale-B, MIT, CMU-PIE (Pose, Illumination and Expression), and Kuwait University face database. The fingerprint biometric databases
available are CASIA-fingerprint version 5.0, Fingerprint Verification Competitions FVC2006, FVC2004, FVC2002, FVC2000 etc.

(ii) **Preprocessing:**

The preprocessing operations include colour to gray scale image conversion, resizing, gray scale to binary image conversion, cropping, histogram equalisation, normalisation, edge detection[16] using canny, sobel, prewitt and robert operators. The thinning of images using skel and spur operators, image enhancement for illumination variation by contrast stretching using histogram equalisation, filtering for noise removal etc. Image segmentation separates the foreground from the background of an image. It makes use of edge detection and transformation operations to segment an image [17].

(iii) **Feature Extraction:**

The significant and distinctive features from both spatial and transform domains are extracted, stored in database along with person’s identity.

(a) **Spatial domain techniques:** The techniques include operations on pixels without applying any transformations.

- Principal Component Analysis (PCA) is used as a mathematical tool in exploratory data analysis and for making predictive models. The PCA involves calculation of eigen value decomposition of a data covariance matrix or singular value decomposition of a data matrix, usually after mean centring of
data for each attribute. The PCA is the simple true eigenvector based multivariate analysis [18].

- Local Binary Pattern (LBP) is a very efficient texture operator, which labels the pixels of an image by thresholding the neighbourhood of each pixel and considers the result as a binary or decimal number. It has discriminative power and computational simplicity. It can be seen as a unifying approach to the traditionally divergent statistical and structural models of texture analysis. Perhaps the most important property of the LBP operator in real-world applications is its robustness to monotonic gray-scale changes caused by illumination variations. The LBP operator labels the pixels of an image by thresholding the 3-by-3 neighbourhood of each pixel with the centre pixel value and considering the result as a binary or decimal number. The binary histogram of the labels computed over an image can be used as a texture descriptor [19].

- Pixel density is the number of black pixels in an image or a cell of specific size in an image and stored as a template in the database for matching purpose.

- Angle measurement: It is the angle subtended by a line joining significant pixels and the reference pixel. The angles are measured and stored in database.

(b) **Transform domain techniques**: The images are transformed from spatial domain to transform domain. The transform domain
techniques include transformation operations like DWT, IWT, DWT and FFT.

- **Discrete Wavelet Transform (DWT):** The wavelet transform represents a signal in terms of mother wavelets using dilation and translation. The wavelets are oscillatory functions having finite duration both in time and frequency, hence represents in both spatial and frequency domains. The features extracted by wavelet transform gives better results in recognition as well as in bifurcating low frequency and high frequency components as approximation band and detailed bands respectively [20].

- **Integer wavelet Transform (IWT):** Lifting is a flexible technique that has been used in several different settings for an easy construction and implementation of traditional wavelets and of second generation wavelets, such as spherical wavelets. Since every wavelet transform can be written using lifting, it follows that an integer version of every wavelet transform can also be built. In each lifting step, the result of the filter is rounded-off right before addition or subtraction. There by the processing speed is increased [21].

- **Directional Filter Bank (DFB):** It is a directionally oriented filter bank with the property that the individual channels may be critically sampled without loss of information. This filter bank decomposes images into directional components, which can be maximally decimated, while still allowing the original image to be exactly reconstructed from its decimated channels. The
filters employed in this new filter bank have wedge-shaped pass band spectral regions. These wedge shaped regions correspond to directional components of the image. To increase the computational efficiency, the filter bank is implemented in a polyphase form. The polyphase filter bank is composed of simple modulators, polyphase filters, adders, delays, up samplers and down samplers. The high efficiency is achieved by exploiting a property of generalized separability. The separable 2-D filter banks in the context of subband image coding involve filtering the horizontal rows of an image and then filtering the columns of the resulting images [22].

- **Fast Fourier Transforms (FFT):** It is an algorithm to compute the Discrete Fourier Transform (DFT) faster by reducing the number of operations. It is applied on spatial domain images to generate the FFT coefficients, which includes features such as real, imaginary, magnitude and phase angle [23].

(iv) **Fusion techniques:** The accuracy and efficiency can be improved by biometric fusion. The spatial domain features can be fused to spatial domain features or transform domain features to generate final feature vector. The researchers have shown that the use of biometric fusion provides better authentication performance. The different levels of fusion are: (1) fusion at the feature extraction level, (2) fusion at the matching score level, (3) fusion at decision level [24].

- **Fusion at the feature extraction level:** Two or more biometric features are fused to get a final feature vector. The features
extracted are independent of each other and are concatenated into a single new vector. The redundant and irrelevant features are removed. From the reported articles of a few researches on feature fusion, it is observed that feature fusion leads to dimensionality problems.

- **Fusion at matching score level:** The matching score obtained from the system indicates the proximity of the feature vector with the template vector. The matching scores obtained from the systems are combined to authenticate the claimed identity.

- **Fusion at the decision level:** The multiple biometric traits and the resulting features are used for classification. A majority vote scheme is used to make final decision.

### 1.2.2 Testing module:

It takes a biometric sample for testing the authenticity of an individual. The sample is preprocessed and features are extracted in the same way as explained in enrolment module.

### 1.2.3 Classification module:

This module includes matching of features and deciding whether test sample is genuine or imposter. The features of test biometric sample are compared with the feature vectors of database using various comparison techniques such as Support Vector Machine (SVM), Neural Networks (NN), Hidden Markov Models (HMM), Time warping, Hamming Distance (HD), Euclidean Distance (ED) etc. Decision-making section compares the matching score against a threshold to establish the user’s identity. The claimed
identity is either accepted or rejected based on the matching score generated in the matching section.

The biometric system can be utilized in two contexts: verification and identification [25]. Verification is a one-to-one match in which the biometric system tries to verify a person’s identity by comparing the distance between test sample and the corresponding sample in the database, with a predefined threshold. If the computed distance is smaller than the predefined threshold, then the subject is accepted as being genuine, else rejected. Identification is a one-to-many match in which the system compares the test sample with all the samples in the database and chooses the sample with the minimum computed distance i.e., greatest similarity as the identified result. If the test sample and the selected database sample are from the same subject, it is a correct match.

### 1.3 The desirable properties of biometric traits

The biometric traits are used for various applications. Each biometric trait has its own advantages and disadvantages. The choice of a biometric trait for a particular application depends on a variety of issues besides its recognition performance. In general many factors are considered for determining the suitability of a biometric trait for a particular application. The human physiological and behavioral biometric traits shall possess the following properties.

1. **Universality:** Each person should have the biometric trait.
2. **Distinctiveness**: The features/patterns of biometric traits should be sufficiently distinct among different persons.

3. **Permanence**: The characteristics of biometrics should be sufficiently invariant over a period of time. A biometric trait that changes over time is not suitable for authentication, because it increases False Rejection Rate (FRR).

4. **Collectability**: The characteristic can be acquired and measured quantitatively without causing inconvenience to individual. The acquired data should be suitable for preprocessing and feature extraction.

5. **Performance**: It refers to an achievable recognition accuracy and speed.

6. **Acceptability**: It indicates the extent to which people are willing to accept the use of a particular biometric trait in their daily lives.

7. **Circumvention**: It reflects how easily the system can be fooled using fraudulent methods.

### 1.4 Advantages of biometric system

The main advantages of selecting biometrics for personal authentication purpose are discussed in this section.

(i) **Security**: The biometric systems offer a higher degree of security than traditional authentication methods (passwords or tokens), since biometric characteristics cannot be guessed or stolen. The efficient passwords are traditionally characterized by a long and alternated sequence of numbers and symbols. Therefore, it is sometimes difficult to remember, on the other hand, tokens may be
stolen or lost. The passwords and tokens can be shared among others, which is threat to the actual used. The biometric characteristics are not shared, hence this shortcoming is almost solved.

**(ii) Accountability:** One important benefit of using biometric-based authentication systems is that they are able to keep track of the user's activities. It is possible to know who has been doing what at a given time.

**(iii) Convenience:** The biometric systems are convenient in environments, where access to privileges is necessary. Traditionally, in many authentication environments, a user may have different tokens or passwords. In these cases, biometrics can be used to simplify the authentication process since the multiple passwords or tokens can be replaced by single biometric characteristics.

**(iv) Scalability:** The biometric systems are easily scalable. The sophisticated biometric characteristics could be used depending on the security level desired. At a bottom level, one could use for example, characteristics that are not very discriminative. If more discriminative properties are desired in the system, biometric characteristics with higher distinctive properties may be used.

### 1.5 Limitations of biometric System

The biometric identification systems have a few limitations. The limitations in off-line signature verification are:

**(i)** Inconsistency in signature.

**(ii)** Forgeries could be easily produced.
(iii) Input to the system is only the 2-dimentional static image, which does not contain information like velocity, pressure, acceleration of pen, and stroke order in the signature.

The limitations in iris recognition are:

(i) Incompatible with law enforcement and immigration authorities.

(ii) Susceptible to poor image quality.

(iii) Difficult to process at a distance larger than a few meters.

(iv) Unwillingness of the people.

(v) For the people affected with diabetes, the eyes get affected resulting in increased FRR.

Apart from the above specific limitations of signature and iris, the general drawbacks are discussed as follows.

The enrolment process, variations in the captured data, passive capture without individuals consent, storage and transmission are general disadvantages of biometrics. Regardless of the method, extracted biometric data is different every time. The exact match between testing data and database cannot be guaranteed, resulting in FAR (False Acceptance Rate) and False Reject Rate (FRR).

The fingerprint of the people working in chemical industries is often affected. The voice of a person changes with age. When the person has flu or throat infection, the voice changes or if there is too much of noise in the environment, then voice biometric may not authenticate correctly. An imposter can circumvent a biometric
system using spoofed traits. Behavioral traits like signature and voice are more susceptible to such attacks than physiological traits.

### 1.6 Applications of Biometrics

The personal identification with high confidence is becoming critical in a number of applications in vastly interconnected society. The automated personal authentication systems based on biometrics have been receiving attention over past decade due to increasing emphasis on security. The biometric recognition is being increasingly incorporated in several different applications and is mainly categorized into three groups:

(i) Commercial applications such as computer network login, electronic data security, e-commerce, internet access, Automated Teller Machine, physical access control, distance learning etc.

(ii) Government applications such as national identity card, driving license, social security, welfare disbursement, border control, passport control etc.

(iii) Forensic applications like corpse identification, criminal investigation, missing children, parenthood determination etc.

(iv) Biometric time clocks or Biometric time and attendance systems, which are being used in various organizations to control employee time keeping.

(v) *Biometric access control systems, providing strong security at entrance of the organization.*
(vi) Wireless biometrics for high end security and providing safer transactions from wireless devices like Personal Digital Assistants (PDA), remote server etc.

(vii) Biometrics airport security devices are also deployed at some of airports to authenticate passengers and employees.

(viii) Biometrics is widely used in many applications such as access control to secure facilities, verification of financial transactions, welfare fraud protection, law enforcement, electronic voting machine, banking system and immigration status checking when entering a country.

(ix) Military force to authenticate refugee.

1.7 Definitions

In this section, definition of a few terms and phrases are given.

1. Image: Image is defined as a two-dimensional light intensity function varying with two spatial coordinates and the value of intensity function is proportional to the brightness value at any point [26].

2. Pixel: A digital image is a matrix of elements, which are intersection of rows and columns. The elements of matrix are pixels and the intensity values vary based on gray scale or color image.

3. Signature: It is a handwritten illustration of a person through lines and curves to authenticate the identity.

4. Random Forgery: It is a signature affixed by an imposter, who does not know the shape and structure of genuine signature.
5. *Skilled forgery:* The signatures affixed by a professional imposter with the knowledge of genuine signature and imitate it as closely as original signature.

6. *Decidability Index:* It is a measure of showing how well the genuine and imposter distributions are separated.

7. *False Acceptance Rate (FAR):* It is the probability that an unauthorized person is incorrectly accepted as authorized person and it is computed using the Equation 1.1.

\[
FAR = \frac{\text{Number of unauthorized persons accepted}}{\text{Total number of unauthorized persons}} \quad \text{(1.1)}
\]

8. *False Rejection Ratio (FRR):* It is the probability that the authorized persons are rejected as unauthorized persons and is computed using the Equation 1.2.

\[
FRR = \frac{\text{Number of authorized persons rejected}}{\text{Total number of persons in database}} \quad \text{(1.2)}
\]

9. *Equal Error Rate (EER):* It is the point of intersection of the FAR and FRR curves on the plot of FAR/FRR against threshold. It can also be defined as error at which both FAR and FRR are equal. A smaller EER indicates a better performance.

10. *Total Success Rate or Correct Recognition Rate (TSR or CRR):* It is the probability that all the persons are correctly authenticated and is computed using the Equation 1.3.

\[
TSR = \frac{\text{Number of persons recognized correctly}}{\text{Total number of persons in database}} \quad \text{(1.3)}
\]

11. *Pixel Density:* It is defined as the number of black pixels pertaining to the image in the cell of specific size.
12. *Geometric Centre of Signature:* The signature image is scanned to count the number of black pixels. The total number of black pixels is divided by two to locate geometric centre.

### 1.8 Motivation

The motivation behind developing the biometric algorithms to authenticate a person is to address the problems in traditional authentication systems. The traditional authentication systems are smart cards, Personal Identification Number (PIN), password, visiting cards, credit cards and debit cards. The traditional identifications can be easily breached and forged. The biometrics are related to body parts and behavior of a person, which cannot be stolen or duplicated, hence biometrics are highly reliable compared to traditional methods. The physiological biometric trait iris is highly reliable compared to other biometric traits; hence it is used in highly protected areas such as military and airports. The behavioral biometric trait signatures are being widely used in daily routine works such as document analysis, accountability, land records, banking, and legal purposes. Hence it is required to develop robust signature identification systems. The requirement of efficient biometric systems is a challenge and has motivated me to work towards developing biometric algorithms with low error rate and high success rate.

### 1.9 Objectives

Authentication of a person using biometrics is more reliable and secure as biometric traits are related to body parts of a person,
compared to traditional methods using smart cards, PIN, passwords etc. The biometric trait signature is widely accepted in day to day activities of a person. The iris biometric is used in highly restricted areas for reliable authentication. Hence the objectives of the research are to develop efficient biometric algorithms with low values of FRR, FAR and EER and also with higher values of TSR for personal identification.

1.10 Organization of the Thesis

The organization of the thesis is as follows. Chapter one presents a brief introduction to biometrics, types of biometrics, and techniques involved in biometric system, desirable properties, advantages, limitations, applications, related definitions and motivation and objectives of the research. The detailed literature survey of existing iris recognition and off-line signature verification using different techniques is given in chapter two. The iris recognition based on DFB, DWT and IWT are discussed in chapter three. In chapter four, fusion of spatial and transform domain features for iris recognition is presented. In chapter five, off-line signature verification using center of gravity and angular features are proposed. The intra-modal score level fusion of two feature sets of signature is presented in chapter six. Finally conclusions, contributions and future work are discussed in chapter seven.