Chapter 1

INTRODUCTION

1.1 Introduction to Biometrics

An accurate authentication of a person is essential in daily routine works such as bank transactions, access to computer, entry to office etc. The recognition of a person from national database of human beings is required for national security. The term Biometric comes from the Greek words *bios* (life) and *metrikos* (measure) [1] that recognizes a human being based on biometric traits derived from a specific physiological or behavioral characteristic of a person. The biometric system [2] is accurate and more reliable compared to conventional security systems such as password, PIN, ID card etc. The conventional security systems can be easily breached since the password may be forgotten and ID card may be stolen or lost. The biometric system uses parts of body and behavior of a person as biometric traits which cannot be stolen or lost, hence biometric system is highly reliable to avoid intruders from neighboring countries. The biometrics is a promising technique to identify a person accurately.

A biometric system can work in the following two modes [3]:

- **Verification mode**: the personal identity is obtained by comparing the captured image with the image of same person present in the database. The system conducts a one-to-one comparison for personal verification.
• Identification mode: the system recognizes a person by searching the templates of all users in the database for a match. The system conducts one-to-many comparison to establish a personal identity.

1.2 Biometric Classification.

The biometric traits are classified into two categories [4] such as (i) Physiological and (ii) Behavioral biometrics as shown in Figure 1.1. The physiological biometric is related to body parts of person which are stable over a period of time that include face, fingerprint, iris etc., and behavioral trait changes with time due to age, health, physiological state, mood, circumstances etc., of a person that includes signature, gait, voice, keystroke, etc.

1.2.1 Physiological Biometrics

(i) Fingerprint

The impression of ridges of any part or the entire finger over any smooth surface is a fingerprint as shown in Figure 1.2. A ridge is a raised portion of the epidermis on the finger and is formed during third to fourth month of fetal development [5]. The ridges on the finger arrange themselves to form a regular pattern which is unique to all fingerprints, even identical twins have different fingerprints and are not inherited. The ridge pattern contains sweat pores that allow sweat and oil to exit from the glands. The Fingerprint ridges expand uniformly in all directions during the growth phase, hence the pattern never changes. When the skin tissue is injured,
the skin that grows back will have the same pattern and cannot be altered and it remains same throughout life.

Fig 1.1: Classification of Biometric Traits.

Fig 1.2: Fingerprint image.
The fingerprints are classified as (i) *Latent fingerprints*: The accidental impressions left by ridge on a surface, regardless of whether it is visible or invisible at the time of deposition. (ii) *Patent fingerprints or Visible fingerprints*: The impressions caused by the transfer of ink materials on the finger onto a surface and fingerprint captured on a scanner. (iii) *Impressed fingerprints*: The impression from a finger deposited on a material that retains the shape of the ridge details. The fingerprint matching approaches are Correlation based, Minutiae-based, Ridge feature based and Pores based approach. The different fingers namely thumb index finger, middle finger, ring finger and little finger have unique fingerprint pattern. Fingerprint recognition is widely used, since capturing the fingerprint image is easy and universally acceptable. The fingerprint is used in all fields such as Forensic, Automobiles, cell phones, property registration, personal computers etc.

(ii) IRIS

The unique and complex texture of an iris begins to form during fetal development and stabilizes in the first two years of life of any individual [6]. The iris of identical twins is different and distinctive. The round contractile membrane of an eye suspended between the cornea and lens which is perforated by the pupil, this membrane is an iris as shown in Figure 1.3. The texture details in the iris image such as cornea, crypts, filaments, flecks, radial furrows, stripes, arching ligaments etc., make an iris pattern unique. These irregularly shaped microstructures are very
randomly distributed patterns which make the human iris as one of the most important and distinct biometric characteristics. The iris is encircled by two concentric circles i.e., inner boundary is between iris and pupil and outer boundary is between iris and sclera.

![Iris Image](image)

**Fig 1.3: Iris image**

The tampering of an iris texture using surgery is extremely difficult as it is invasive and highly sensitive organ of the body. The iris-based recognition systems required considerable user participation and expensive.

**(iii) Deoxyribo Nucleic Acid (DNA)**

The one-dimensional ultimate unique structure of DNA [7] for one’s individuality as shown in Figure 1.4. Naturally identical twins have identical DNA patterns. Presently DNA is used as an evidence for person recognition in forensic applications. The biometric application of DNA is restricted because of the following disadvantages.
(i) **Contamination and sensitivity:** The DNA can be stolen easily from any individual from a single point of blood. That can be subsequently abused for an ulterior purpose.

(ii) **Automatic real-time recognition issues:** The current technology used for DNA matching requires cumbersome chemical methods involving an expert’s skills and is not geared for on-line non-invasive recognition.

(iii) **Privacy issues:** Personal health information of an individual suffering from particular disease can be known from DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination.

![DNA Image](image.png)

Fig 1.4: DNA Image.

(iv) **Face**

The face identification/verification \[8\] is the most effective biometric system used in today’s world and samples of facial images are as shown in Figure 1.5. The applications of facial recognition range from a static, controlled verification to dynamic, uncontrolled face identification in a cluttered background. The face recognition systems are dependent on (i) The location and shape of facial attributes such as the eyes, eyebrows,
nose, lips and chin, (ii) The overall (global) analysis of the image that represents a face as a weighted combination of a number of canonical faces.

(v) **Hand vein infrared thermogram**

The Vein patterns are unique among individuals and invariant to time, even in the case of identical twins, hence it is used to authenticate individuals [9]. An image of the vascular patterns is obtained by using an infrared sensor that captures the hemoglobin in the blood. Traditionally, the de-oxygenated hemoglobin appears as black patterns in the captured image, while the hand or fingers have lighter patterns. It is difficult to capture the hand vein structure, since the veins usually move and they flex as the blood is pumped through the human body. Special devices are used to capture and resize the image. The main disadvantage of this biometric trait is cost.
**Hand and Finger geometry**

The hand geometry recognition systems is the process of recognition of individual based on a series of measurements taken from the particular individual hand, including its palm size, shape, lengths and widths of the fingers [10] as shown in Figure 1.6. The hand and finger geometry pattern are variant during the growing stages of adolescents and are not unique. The environmental factors such as dry weather or individual anomalies like dry skin does not have any negative effects on the verification accuracy of hand geometry based systems. The disadvantages of hand geometry based recognition systems are (i) it cannot be used for systems requiring identification of an individual from a large population (ii) An extraction of hand geometry is difficult if jewelry on fingers and arthritis and (iii) Due to the length of the hand being considerably large, it cannot be embedded in certain devices like laptops.

![Fig 1.6: Hand geometry.](image-url)
1.2.2 Behavioral Biometrics

(i) Signature

It is the person writes his/her name as signature [11] as shown in Figure 1.7. The signature verification system is preferred among various biometric authentication methods as it is widely accepted method for endorsing financial transactions. The pen accelerations that are proportional to the muscle forces exerted by the signer are consistent in a habitual signature. Natural pauses between sections of the name i.e., interruption, reflecting on the sensation of writing on an unfamiliar surface, skipped strokes, for example eliminating a middle initial, replacing a first name with an initial and decorative rubrics like dotting the ‘i’ with a star, underlining the name can affect the repeatability of signature samples. The signature consists of regions of high correlation of unknown duration separated by variable regions of low correlation. A verification strategy is required to separate correlation regions, compare them individually with reference signatures and combine the results in an overall verification decision. The verification system must be able to detect forgeries and at the same time reduce rejection of genuine signatures. Two different types of forgeries considered for a signature verification system are: (i) Random forgeries (ii) Skilled forgeries. The problem of signature verification becomes more difficult for skilled forgeries when compared to random forgeries.
The signature verification system can be classified into On-line and Off-line systems.

(a) **Online verification system:**

The signatures are captured dynamically using a graphic tablet and are stored as a function of time. It avails spatial and temporal characteristics of signatures such as speed, acceleration of the stroke, pen-location and pen-pressure. Online signatures are more unique and difficult to forge since dynamic features are available along with the shape information.

(b) **Offline verification system:**

The signatures are digitized using flatbed scanner and then stored as an image. It uses static features, which are of three types:

(i) **Global features:** provide information about specific cases of the signature shape such as signature area, signature height-to-width ratio, maximum horizontal and vertical histogram, horizontal and vertical center of the signature, horizontal and vertical local maximum numbers of the signature and number of edge points of the signature.

(ii) **Mask features:** provide information about the direction of the signature stroke i.e., skew angle of the signature.

(iii) **Grid features:** are used for finding densities of signature parts. The various approaches for offline signature verification
are based on neural networks, parallel processing, 2-D transform, histograms of directional data or curvature, horizontal and vertical projections of the writing trace of the signature, local geometric information, shape of the signature, the position of feature points located on the skeleton of signature and global shape descriptors. Signature verification is used in bank transaction, electronic fund transfers, document analysis and access control.

(ii) Gait

The gait is the peculiar way one walks and is a complex spatio-temporal biometric [12] shown in Figure 1.8. The gait is used as characteristics to differentiate between individuals and used in low security applications for personal verification system. The gait is a behavioral biometric and change over a span of time due to variations in body such as weight, health issues like paralytic stroke, major injuries due to accidents. Since gait based systems require a video footage of an individual which requires more space in storage system, specifying the different movements of joints, hence these types of systems are not much in use.

Fig 1.8: Image of Gait
(iii) Keystroke

Every individual types on a keyboard is distinct [13] and keystroke is shown in Figure 1.9. It is not unique and can be treated as behavioral biometric, it offers sufficient discriminatory information for personal verification. When closely observed large difference exists between person to person in the way they type on keyboard. More storage is required to create the database, hence it is used in low security applications.

![Fig 1.9: Image of Keystroke.](image)

(iv) Odor

Every individual possesses body odor which is characteristic of its chemical composition [14]. It varies between persons, hence can be treated as biometrics for identification. A whiff of an air surrounding a person is blown over an array of chemical sensors, each sensitive to a certain group of aromatic compounds. A part of an odor emitted by any individual is differentiable to a particular individual. It is very rarely used biometric system since chemical sensors are used.

(v) Voice

It is behavioral biometric and the body parts like mouth, lips, teeth, throat are responsible for voice [15]. It varies with age, health conditions, emotions etc., of person. The voice of person is recorded and stored as
database, speech processing is done to identify a person. Since the process takes more time it is rarely used.

1.3 Biometric systems

The block diagram of the general biometric system used to identify a person is as shown in Figure 1.10. The biometric system has blocks of data acquisition, preprocessing, feature extraction, comparison and decision.

![Block Diagram of Biometric System](image)

Fig 1.10.Block Diagram of Biometric System

1.3.1 Biometric Data acquisition: This step involves in acquiring the biometric data of an individual for identification and verification. Huge numbers of image samples are collected from a different persons at different intervals using sensors. The collected samples are divided into test set and database.

1.3.2 Preprocessing: The principal objective of preprocessing is to obtain a transformed image, which is more suitable than the original image and to enhance the quality. It includes (i) Color Conversion (ii) Resizing of image (iii) Normalization shown in Figure 1.11.
Fig 1.11: Block diagram for Pre-processing.

(i) *Colour Conversion*: It involves, colour to gray scale image conversion and the gray scale image with intensity values between 0 and 255 is obtained from colour image to reduce processing time.

(ii) *Resize*: The original size of an image is increased or decreased based on the requirement by cropping without losing information.

(iii) *Normalization*: The step includes noise removal, rotation, thinning, smoothing etc. The images in database and test set are normalized such that the features extracted from number of samples of single person are almost similar and features are different for different persons. An example for noise removal, smoothing, thinned image and rotated image on signature is shown in Figure 1.12.
1.3.3 Feature Extraction: The features of biometric parameters are extracted from spatial domain or transform domain or combination of both which is considered as hybrid domain.

(i) Spatial domain features:

The intensity values of spatial domain images are considered and the mean, variance and standard deviation are computed to extract features. The techniques such Principle Component Analysis (PCA) [16], Independent Component Analysis (ICA) [17], Singular Value Decomposition (SVD) [18] etc., are used to obtain spatial domain features. The two or more spatial domain features are fused to get final feature. The spatial domain feature extraction and the fusion of two or more spatial domain feature types are shown in Figure 1.13.
(ii) Transform domain features:

The biometric traits in spatial domain are converted into transformation domain i.e., frequency domain. The few transform domain technique are Fast Fourier Transform (FFT) [19], Discrete Cosine Transform (DCT) [20], Discrete Wavelet Transform (DWT) [21], Complex Wavelet Transform (CWT) [22], Dual Tree Complex Wavelet Transform (DTCWT) [23], Kekre Transforms (KT) [24] etc. The transform domain feature extraction and the fusion of two or more transform domain feature types are shown in Figure 1.14.
Fig 1.14: (a) Feature Extraction using Transform Domain. (b) Fusion of Transform Domain features

(iii) Hybrid domain features.

The final features are obtained by combining spatial domain and transform domain features. This technique is considered as hybrid domain technique as shown in Figure 1.15. The image is decomposed into two cells, features are extracted by applying spatial domain on one cell and transform domain technique on another cell and the features obtained are fused to get final feature vector as shown in Figure 1.16.

Fig 1.15: Fusion of Transform domain and Spatial Domain Features
1.3.4 Matching: The features of test biometric is compared with features of database using classifiers such as Euclidean Distance, Hamming distance, Chi Square distance, Support Vector Machine, Random Forest, K-Nearest Neighborhood algorithm, Neural Network etc., to authenticate a person. The block diagram of matching section is shown in Figure 1.17. The results obtained in the classifiers determine whether the individual sample is accepted or rejected by the biometric system.

The block diagram of biometric system with fusion at the matching level is shown in Figure 1.18. The spatial domain and transform domain features of database and test images are extracted. The performance parameters such as FRR, FAR, and TSR are computed separately using
spatial and transform domain features. The performance parameters of spatial and transform domain are fused to obtain better performance parameter values compared to individual domain parameter values.

**Fig 1.18: Fusion at matching level**

### 1.4 Characteristics of Biometrics

The biometrics is accepted in finding the uniqueness of an individual if it satisfies the following parameters.

- **Universality**: The personal feature should be universally acceptable.
- **Distinctiveness**: Any two persons should be sufficiently different in terms of the characteristics.
• **Permanence:** The characteristic should be sufficiently invariant with respect to the matching criterion over a period of time.

• **Collectability:** The characteristics can be measured quantitatively.

• **Performance:** The accuracy and speed of recognition.

• **Acceptability:** It gives an extent to which people are willing to accept the articular biometric identifier or characteristics in their daily transactions.

• **Uniqueness:** It is the property of the biometric how well it separates individuals.

### 1.5 Applications of Biometrics

There is absolute need for security in today's world of intrusion, exponential increase in hacking led to the wide applications of biometrics. Automated personal identification and verification based biometrics are highly attention seeking methods in the past few decades. Biometric system is extensively used in some of the applications are listed below.

- Monitoring of an attendance and timing
- Banking systems
- Boarding pass in airport for personal authentication
- Home security systems
- Electronic voting and automated teller machines
- Military force to authenticate refugee
- Multinational companies to authenticate office employees
- Entry to high security zones like parliamentary house, defence establishments
- Legal documentations like land and business dealings etc.

1.6 Definitions

(i) **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.

(ii) **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.

(iii) **Signature**: It is a handwritten illustration of a person through lines and curves to authenticate an identity.

(iv) **Random Forgery**: It is a signature affixed by an imposter, who does not know the shape and structure of genuine signature.

(v) **Skilled forgery**: The signature affixed by a professional imposter with the knowledge of genuine signature and imitates it as closely as original signature.

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

\[
FAR = \frac{\text{Number of unauthorized persons accepted}}{\text{Total number of unauthorized persons}} \quad \text{.................. (1.1)}
\]
(vii) **False Rejection Ratio (FRR):** It is the probability that the authorized persons are rejected as unauthorized persons and is computed using an Equation 1.2.

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

(viii) **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.

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

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

(x) **Pixel Density:** It is defined as the number of black pixels pertaining to the image in the cell of specific size.

(xi) **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.

(xii) **Signature height:** It is the height of the signature image and is vertically measured.

(xiii) **Signature width:** It is the width of the signature image and is horizontally measured.
(xiv) **Aspect Ratio:** The ratio of signature height to width.

(xv) **Image area:** It is the number of black pixels in the image. In skeletonized signature images, image area represents a measure of the density of pixels in signature traces.

(xvi) **Fingerprint:** Impression of a finger acquired from digital scanners.

**1.7 Motivation.**

The motivation behind developing biometric algorithms is to address the problems in traditional authentication systems. The traditional methods can be easily broken if the password is disclosed and the card is lost. The biometric traits are related to body parts of a person and behaviour, which cannot be stolen or duplicated. The biometric traits such as offline signature identification, fingerprint recognition and face recognition are having potential benefit in routine activities like bank transaction, land record registration, personal identification in public places etc. Hence I have been motivated to develop robust biometric algorithms with low values of FRR, FAR, EER and higher value of TSR.

**1.8 Objectives.**

The authentication of a person using biometrics is more reliable and secure as biometric traits are related to a person compared to traditional methods using smart cards, passwords, PIN etc. The biometric traits viz., face, fingerprint and signature are widely accepted in the society, hence it is required to develop a robust biometric algorithm with low values of FRR, FAR and EER with high values of TSR.
1.9 Organization of the Thesis

The thesis is organized as, chapter one presents a detailed introduction to biometric, biometric system, biometric applications, characteristics of biometrics, motivation and objectives of the research work. The detailed literature survey on existing signature identification, fingerprint verification and face recognition using different techniques is given in chapter two. The spatial domain based signature verification techniques such as global feature along with histogram values and graph matching with cross validation are discussed in chapter three. The fingerprint verification using segmentation and Discrete Cosine Transform (DCT) is presented in chapter four. The fusion of two transforms domain techniques for face recognition is proposed in chapter five. The bimodal biometric i.e., face and finger are fused, is proposed in chapter six and conclusions, contributions and future work are presented in chapter seven.