Chapter 1

INTRODUCTION

1.1 Introduction

The Biometrics is a technology of analyzing features of human body parts to authenticate a person for security purpose and the word is derived from the Greek word [1] *bios* (life) and *metrikos* (measure). The biometric system captures and store biometric information onto the database and compares the test biometric information with the database biometric information. The system has received considerable attention and has been successfully used in many applications. Normally the biometric systems employed in the real-world applications for authentication are unimodal that depends only on single source of biometrics information. Biometric identification is becoming more popular now a day’s, due to the security requirements in the field of information, business, military, e-commerce, internet and electronic transfers. In the mid nineteenth century the police criminal identification division in Paris [2] have developed and practiced the idea of using many features of human body parts and behavioral characteristics to identify criminals. Since then biometric recognition technology emerged rapidly in law enforcement to identify criminals. The personal identification
based on biometrics is essential to create Unique Identification (UID) card, which can be used for voting in electoral system, accessing secured areas, identification to avail government and nongovernment facilities.

Traditional authentication systems such as passwords, employee key, smart cards, Personal Identification Number (PIN), etc., can be easily stolen, forgotten and lost, where as biometrics cannot be stolen, forgotten and lost, hence use of biometrics is more secure compared to traditional methods of identification. A real time biometric system must satisfy the requirements such as recognition accuracy, speed, False Acceptance Rate (FAR), False Rejection Rate (FRR), robust to fraudulent techniques and attacks, harmless to the users and accepted by the intended users.

1.2 Types of Biometrics

The biometrics is widely categorized into physiological and behavioral characteristics [3] used for automated recognition that are based on features of fixed human body parts and behavior of a person respectively. The choice of biometrics depends on user acceptance, level of security required, accuracy, and implementation cost and time.

1.2.1 Physiological Parameters

Physiological characteristics are related to parts of the body such as Fingerprint, Face, Ear, Facial Thermogram, Deoxyribo Nucleic Acid (DNA), Hand and Palm print, Iris and Retinal blood vessel patterns.

(i) Fingerprint: The biometric fingerprint has minutia, pores, valleys and
ridges with almost fixed pattern. Every individual has fingerprints with unique features. Thus fingerprints have been used for identification in forensic investigations and sciences since nineteenth century, criminal investigations, civil and commercial identifications. Fingerprint verification is simple, faster, cheap and reliable to identify the individuals compared to iris, voice, retina, face and other recognition systems. The disadvantages of fingerprint recognition are fingerprint features may not be unique sometimes, universally may not be accepted, injury to finger, fingerprint of the person working in chemical industry may change, database protection and maintenance from fraudulent user.

(ii) *Face*: The person identification mechanisms based on their facial features existing since two to three decades. The Human Visual System (HVS) provides an effective way of recognizing other people’s expressions and facial features. Normally HVS identify people by their faces and sometimes much better than computer based recognition systems. The face recognition system is nonintrusive and most common biometric system used now a days for personal identification.

(iii) *Ear*: The ear shape and the structure are distinct. The features of ear are size of ear and pattern of ear structure. The recognition is based on matching between the landmark locations on the ear and
salient points on the pinna. The disadvantage is features of an ear are not unique.

(iv) **Facial thermogram:** The property of human body heat radiation is considered as feature for recognition and the heat radiation is captured by infrared camera. The application of facial thermogram is limited to covert recognition.

(v) **DNA:** The biometric based on DNA sampling is a form of blood sample and tissue and it is considered as unique feature for recognition. The disadvantage is the patterns of DNA may not be unique for twins and the issues such as contamination, sensitivity, privacy and automatic real-time recognition are not clear.

(vi) **Hand and Palmprint:** The features of person's hand and palm are used to authenticate a person for specific applications. Hand scanner and finger reader recognition system measure and analyze the pattern in the palm and hand such as ridge length, orientation of ridges and valleys. The technique is relatively easy, simple and inexpensive. The disadvantage is hand and palm geometry is not unique and distinctive over the years.

(vii) **Iris:** The human iris is unique compared to other biometrics and iris image can be captured using camera. The iris pattern contains large amount of arbitrariness, becomes unique features and is normally formed between the third and eighth month of growth of a foetal.
The iris pattern remains same throughout the life of an individual.

(viii) *Retinal blood vessel patterns:* The retinal vasculature is characteristic of each individual eye and not easy to change or replicate. The biometric sample acquisition is difficult and usage is limited compared to other biometrics.

**1.2.2 Behavioral Parameters**

The behavioral biometrics is connected to the behavior of a person and investigates gesture of an individual such as Gait, Signature, Keystroke, Voice etc.

(i) *Gait:* The way person walks and a combined spatial 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 fluctuations in body weight and major injuries connecting joints and brain.

(ii) *Signature:* The way person symbols his/her name is acknowledged to be a feature of that person. The signatures have been acknowledged in lawful, business communication and in government as a technique of verification of person. The signature is a behavioral biometric usually changes over a period of time and is inclined by physical and emotional conditions of the person. The automatic signature confirmation system has several applications such as symbol of approval, predominantly in credit cards
validation, bank cheques, land purchases, legal documents and security systems. The disadvantages with this system are signature forgeries such as arbitrary, casual and skilled.

(iii) Keystroke: The pressure applied by a person while typing on a keyboard, in a unique way is referred as keystroke. The keystroke is not always unique to each person but provides sufficient discriminatory information to recognize an individual. It is observed that there exists a deviation in typical typing patterns for some persons. The weakness with the keystrokes of a person using a system could be monitor and imitate.

(iv) Voice: The biometric is a combination of both behavioral and physiological characteristics. The individual’s voice features are based on vocal tract, mouth, nasal cavity and lips. Thus, shape and size of the appendage are used in sound synthesis. The physiological uniqueness of human verbal communication are invariant for a person, but the behavioral element of the communication of a person changes over time due to age, medical conditions and emotional state. The voice is uniquely different including twins and cannot be exactly duplicated. Voice is also not appropriate for exact authentication of an individual because it is not very distinctive. The disadvantage with the voice biometric system is the features of speech may vary due to noise introduce into the system.
1.3 The Biometric System

The biometric system normally operates in two modes such as verification mode and identification mode depends on the application:

- **Verification** - The process of one-to-one comparison to claim an identity of a person. The test image is compared with an image in the stored database.

- **Identification** - The process of one-to-many comparison of the test biometric with biometric database to identify an unknown person. The comparison of the test biometric sample with a template in the
database falls within a predefined threshold then it is succeeded in identifying the individual. The general biometrics system is divided into three sections viz., enrolment section, test section and classification section is shown in Figure 1.1. The biometric database is created and preprocessed on each biometric data to device good quality and appropriate image for further processing. The feature vectors are extracted on each biometric data and are developed on whole biometric database.

1.3.1 Enrolment Section

The biometric database is enrolled and features are extracted in this section. The enrollment stage performs operations such as preprocessing and feature extraction on database biometrics.

1.3.1.1 Biometric Database

The significant section of any biometric system for person identification is the data collection and creation of database. Each component of the database is created by biometrics collected with different image sensors such as mobile cameras, digital cameras, iPods and web cameras at different sessions with at least two weeks time separating each session and at different intensity, angle, expressions and with or without accessories. The database is created with different images on same person and some of the databases are readily available in the internet.
The popular face biometric databases [4] available for research work are Libor Spacek, AT & T (formerly Olivetti Research Laboratory), Oulu Physics, XM2VTS, Yale, Yale-B, MIT, CMU-PIE (Pose, Illumination and Expression), UMIST, Bern University face database, Purdue AR, University of Sterling online database, FERET, Kuwait University face database and AR. The fingerprint biometric databases such as Chinese Academy of Science Institute of Automation (CASIA) developed by Chinese academy institute, SFinGe, FVC2006, FVC2004, FVC2002, FVC2000 etc. The iris biometric databases viz., CASIA v4 and UBIIRIS, the palmprint biometric database such as CASIA palmprint image, Hong Kong Polytechnic University 3D palmprint database etc. The available signature databases are GPDS300 and SVC 2004.

1.3.1.2 Preprocessing

The operations involved in preprocessing are color conversion, image resize to the required size, gray scale image to binary image, image enhancement for illumination variations using Discrete Cosine Transform (DCT). The homomorphic filtering [5] and image enhancement like contrast stretching using histogram techniques such as Histogram Equalization and Histogram Matching [6, 7, 8, 9], expression normalization using higher decomposition of Discrete Wavelet Transform (DWT) [10], pose normalization [11, 12], image restoration using noise models and averaging filters are performed in preprocessing. The edge
detection techniques Sobel operator, Canny operator and Robert operator are used to derive biometric image edge information.

1.3.1.3 Feature Extraction

The features of each biometric are computed to identify a person and are based on spatial and transform domain techniques.

(i) **Spatial Domain Techniques:** The biometric features are directly extracted from spatial domain itself by applying spatial domain techniques on image pixels without converting into frequency domain.

- *The Edge detection techniques:* Normally color image is converted into gray scale image for easy processing and then into binary image for edge detection. The edge detection operators such as Canny, Sobel, Prewitt, Robert etc., are used to obtain edges of an image. The features are extracted by measuring different lengths of edges in an image [13].

- *PCA:* The best eigenvectors of the covariance matrix in a larger dimension data refers to the best low dimensional space and are called as principal components of covariance matrix [14].


- *Line Edge Map [LEM]:* The approach of LEM [16] extracts lines from an image edge map and geometrical feature matching. Edge information is a useful object representation feature i.e., invariance
to illumination changes, low memory requirement and high recognition performance of template matching. LEM integrate the structural information with spatial information of an image by grouping pixels of an image edges in to line segments.

• **3D Morphable Model**: The vector representation of images that is being constructed such that any convex combination of shape and texture vectors of a set of examples describes a realistic image is a morphable model [17].

• **Hidden Markov Model (HMM)**: A discrete HMM [18] models is viewed as a probabilistic model whose states are not explicitly observed. In HMM each state is based on the decision of probability distribution function and symbols are emitted based on the probability of occurrence of that symbol and depends on the previous states.

**(ii) Transform Domain Techniques:**

The biometric traits are converted from spatial domain into transform domain i.e., frequency domain [19].

• **Fast Fourier Transform (FFT)**: The FFT is applied on spatial domain image to obtain FFT coefficients. The features are extracted from FFT [20] coefficients are real part, imaginary part, magnitude value and phase angle. The FFT computation is fast compared to Discrete Fourier Transform (DFT), since the number of
multiplications required to compute N-point DFT are less i.e., only \( \frac{N}{2} \lceil \log_2 N \rceil \) in FFT as against \( N^2 \) in DFT.

- **Discrete Cosine Transform (DCT):** The technique is used for video and image compression. The DCT technique [21, 22] is a linear and invertible frequency domain transform to express pixel intensity values of an image in terms of sum of cosine functions oscillating at different frequencies. The original spatial domain image is converted into the frequency domain using the DCT technique and original image is reconstructed from DCT coefficients by applying inverse DCT technique. The transform domain image represents original image DCT coefficients and reflects in terms of frequencies present in it. The first DCT coefficient has lowest frequency and forms the DC-coefficient and normally carries the significant information of original image. The last DCT coefficient has higher frequencies consists of detailed information of signal and usually generated by noise. The rest of the coefficients carry different frequency components of the original signal varies between very low and very high frequency.

- **Discrete Wavelet Transform (DWT):** The wavelet transform represents a signal in terms of mother wavelets using dilation and translation [23]. The wavelets are oscillatory functions having finite duration both in time and in 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.

- **Complex Wavelet Transform (CWT):** The CWT [24] is a two dimensional wavelet to provide multiresolution and improved transformation of DWT. CWT provides high degree of shift invariance and has more redundancy.

- **Dual Tree Complex Wavelet Transform (DT-CWT):** The decomposition technique DT-CWT eliminates disadvantages of DWT, DCT and Gabor Wavelet Transform, and gives better results in feature extraction [25, 26]. Two wavelet trees are created in parallel forming Hilbert pairs. The two trees of the DT-CWT are the real and imaginary parts of complex wavelet. The Hilbert transform pairs in DT-CWT are called half sample delay condition.

**(iii) Fusion Techniques:**

- The spatial domain features extracted by different techniques are fused to obtain final spatial domain feature vector.

- The transform domain features are extracted using various transformation techniques. The different features are combined to generate final feature vector.
• The spatial and transform domain features are combined to obtain hybrid features with different techniques.
• The different biometric traits such as speech, face, iris and fingerprint features are too fused to identify a person [27].

1.3.2 Test Section

In this section, the one sample of biometric test image is considered to authenticate a person. The preprocessing and feature extraction on test image is similar to that of enrollment section.

1.3.3 Classification Section

The given test biometric data is compared with database biometric to authenticate a person is discussed in this section. The distance formulae such as Euclidean Distance (ED) [28], Hamming distance [29], Chi-square [30] are used for comparisons. The classifiers such as Support Vector Machine (SVM) [31], Artificial Neural Network (ANN) [32] and Random Forest (RF) [33, 34], Multiple Classifier Systems (MCS) [35], Template Matching [36], Graph Matching [37] and Mahanalobis Distance [38] are used for matching.

1.4 Design Issues in Biometric System

The biometric traits can be used as biometric characteristics to authenticate an individual as long as it satisfies the following parameters.
• **Universality**: The human beings must have some common body parts such as face, finger, palm, iris etc.

• **Collectability**: The features of human body parts are acquired and quantitatively measured.

• **Distinctiveness**: The patterns of each biometric trait of any two persons in the world should be distinct and different in terms of both physiological and behavioral characteristics.

• **Permanence**: The physiological and behavioral characteristics of biometric traits should not change over a period of time pertaining to recognition criterion.

• **Acceptability**: In general people need to accept a particular biometric identifier for day-to-day business or any related transactions.

• **Uniqueness**: The biometric characteristic that differentiate effectively between persons.

• **Performance**: The accuracy and speed of recognition determines the performance of the biometric system technique.

### 1.5 Applications of Biometrics System

The biometric need for security systems is going up, hence recognition of human being every day based on fully automated personal identification and authentication has been attracting extensively over the past ten years. Some of the biometric system applications are as listed below.
(i) The biometric systems have wide range of applications in different areas such as human-computer interaction, image processing, film processing, security applications, computer access control, criminal screening and surveillance.

(ii) Banking systems

(iii) Regular attendance monitoring and authentication of the employees using any of the biometric traits.

(iv) Airport checking for personal authentication

(v) Home security applications

(vi) Electronic voting system

(vii) Military force to authenticate refugee

(viii) Using a pre-stored image database, the biometric recognition system is able to verify and authenticate one or more persons in the database.

(ix) Biometric is one of the major research topic in the current fields such as neural networks, man and machine intelligence system, robotics and computational vision, computer graphics, image processing and psychology study.

1.6 Challenges in Face Recognition

The challenging problems in face recognition are wide range of viewpoints, complex outdoor lighting, facial expressions, occlusions, pose variations and aging of subjects. A reliable facial image processing
system performance must be rigorously tested and verified on real-world datasets for face. Thus, rigorous research is needed to solve such outstanding challenging problems and propose advanced solutions and systems for emerging applications of facial image processing and analysis.

1.7 Definitions

1. **Pixels**: Picture Element (pel) is a single point image and is addressable as small screen element. The pixel can be controlled and is represented using dots or squares with its own address. The address is corresponds to its coordinates with a two dimensional grid.

2. **Histogram**: The graphical representation of digital image pixels by showing the number of pixels at each intensity level found in the image is defined as histogram of an image.

3. **Histogram equalization**: The technique which enhances the dynamic range of an image by assigning intensity values of pixels in the input image is referred to as histogram equalization. The image obtained after histogram equalization has pixels with uniform distribution of intensities.

4. **Segmentation**: The image processing technique partitions the image into smaller regions or objects for analysis purpose.
5. **RGB image**: The digital image with M*N*3 array of color pixels and each color pixel has three intensity levels corresponding to the red, green and blue components of an RGB image at each spatial location.

6. **Correlation**: The process in which the value of an output pixel is computed as a weighted sum of neighboring pixels without rotating the matrix of weights is called as correlation.

7. **Neighborhood operation**: The output pixel of an image is computed from a set of neighboring input image pixels. The neighborhood operations are convolution, correlation, dilation and median filtering.

8. **Percentage Increase or Decrease of NCC value**: Difference in Normalized Cross Correlation (NCC) of complement of LOG and NCC of Gaussian to Complement of LOG is given in Equation (1.1)

\[
\% \text{ Increase or Decrease of NCC Value} = \frac{\text{NCC}[\text{LOG}] - \text{NCC}[\text{Gaussian}]}{\text{NCC}[\text{LOG}]} \times 100
\]

9. **Preprocessing**: The face image is preprocessed for resize, color to gray scale conversion, gray to binary conversion, image enhancement, restoration, noise removal and illumination compensation.

10. **Inter-ocular distance**: The distance between the right eye midpoint and left eye midpoint pixels in the face image.

11. **Lips to Nose**: The distance between nose tip to the midpoint of the lips pixel in the face image.
12. *Nose to Eyes:* The distance between Nose tip to the line joining two eyes midpoint of the pixels in the face image.

13. *Lips to Eyes:* The distance between lips midpoint to the line joining two eyes midpoint of the pixels in the face image.

14. *Eccentricity of the face:* The shape of the face containing pixels in the face image.

15. *Ratio of Dimension (D):* The ratio of width to height of the face image.
   The bounding box coordinates of the face image are determined and the width (D_x) and height (D_y) are computed using these coordinates is given in Equation (1.2)
   \[
   D = \frac{D_x}{D_y} \quad \text{........................................................}\ (1.2)
   \]

16. *Width of the lips:* The distance between right endpoint of the lip to the left endpoint of the lip containing pixels in the face image.

17. *Mean:* The pixels mean is the arithmetic average intensity value and computed by adding intensity values and dividing by their total number of pixels and is given in Equation (1.3)
   \[
   \text{Mean} = \frac{\sum_{i=1}^{n} a[i]}{n} \quad \text{........................................................} (1.3)
   \]

18. *Variance:* The average distance between set of data points and their mean value is given in Equation (1.4)
\[
\text{Variance} = \frac{\sum_{i=1}^{n} (a[i] - \text{Mean})^2}{n} \quad \ldots \quad (1.4)
\]

19. **Standard Deviation:** Square root of variance is the Standard Deviation (S.D) is given in Equation (1.5)

\[
\text{S.D} = \sqrt{\text{Variance}} \quad \ldots \quad (1.5)
\]

20. **FPCA:** The technique PCA uses Gram-Schmidt Orthonormalization with reduced computational complexity is referred to as FPCA.

21. **Mean Square Error (MSE):** The measure of distortion in images and is the expected value of the square of the error as given by the Equation (1.6)

\[
\text{MSE} = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{i=1}^{N} (I_o - I_a)^2 \quad \ldots \quad (1.6)
\]

where \( I_o \) and \( I_a \) are original image and approximated or reconstructed image respectively of image size \( N \times N \). Decrease in the value of MSE the will increases in the value of peak signal to noise ratio.

22. **Threshold:** The distance between the test image and the database images are recorded as Error Vector (EV) using distance formula and then the average of EV is considered as the threshold value for recognition declaration.

23. **False Rejection Rate (FRR):** The ratio of the number of false rejections to the number of identification attempts and is given in Equation
24. **False Acceptance Rate (FAR):** The ratio of the number of false acceptances to the number of identification attempts and is given in Equation (1.8)

\[
FAR = \frac{\text{No. of unauthorized test images accepted}}{\text{Total no. of identification attempts}} \quad \text{(1.8)}
\]

25. **Equal Error Rate (EER):** The rate at which both accept and reject errors are equal and it is taken from the region of convergence plot by considering the point where FAR and FRR have the same value. The system with the least EER is most accurate.

26. **Correct Recognition Rate (CRR):** The CRR measures the percentage of match rate regardless of the FRR and is given in Equations (1.9)

\[
CRR = \frac{\text{No. of test images matches correctly}}{\text{Total no. of persons in the database}} \quad \text{(1.9)}
\]

27. **Efficiency (η):** Number of matches and mismatches at EER, is the system overall efficiency.

### 1.8 Motivation

The biometric validation of a person have several advantages compared to the earlier validation systems such as smart cards, PIN, password,
visiting cards, credit cards and debit cards. The biometric identification is based on several parts of human body and behavioral characteristics such as face, fingerprint, iris, retina, palm print, hand geometry, DNA, voice and signature. The face recognition has biggest challenge in designing and implementing as the human face can undergo several transformations such as

(i) The same person may use different face accessories like glasses, earrings, piercings and makeup,
(ii) Many facial expressions like neutral, smile, anger, surprise, fear, disgust, and sadness or doing a grimace,
(iii) Can have/wear mustache and beard,
(iv) Can change hair into long/short/skin/fringe and even dye it and
(v) Face images can be at different ages. These facial changes make the recognition task very difficult, even minor mistakes in design of algorithm leads to wrong person recognition. Hence I have been motivated to design and implement a robust face recognition biometric system with high recognition rate and low FRR and FAR for variations in the face images.

1.9 Organization of the Thesis

The organization of the thesis is as follows. Chapter one presents a detailed introduction to biometric, biometric system, applications of biometrics, design issues related to biometrics and motivation for the
research work. The detailed literature survey on existing face recognition models using different techniques is presented in chapter two. The spatial domain based face recognition techniques such as birth marks or mole presence on face image using complement of Laplacian of Gaussian template and edge information based on Canny edge detection are discussed in chapter three. Transform domain techniques such as Discrete Wavelet Transform and Dual Tree Complex Wavelet Transform are used for feature extraction to achieve high recognition rate on various face databases is presented in chapter four. The technique which uses both transform domain and spatial domain for face recognition is discussed in chapter five. Finally conclusions, contributions and future work are presented in chapter six.