1. Chapter 1

CHAPTER 1

INTRODUCTION

1. INTRODUCTION

In the present world, security is a noteworthy concern. Primary risk the security environments come across is the likelihood of impostors encroaching into the system. To give a protected environment, authentication schemes based on identity cards or passwords are presented.

Recognizing a person naturally by the framework has its own particular applications like, secure access to a computer system, a restricted area, personal identification and video surveillance. The technique of identifying a person is classified into knowledge-based, token-based and biometric-based. Password and Personal Identification Number (PIN) comes under the category of knowledge based system and there are chances that the password and PIN can be duplicated or simulated. Token based systems are those where an authenticated person will have a physical object like ID card or credit card. There are chances that an individual loose the cards. Identifying a person using PIN or a password were used effectively and are still been used. The disadvantage with this system is that PIN or password in general are forgotten or can be hacked. Third category is the biometric systems where the physiological or behavioural characteristic of an individual is captured for identification. This category has many advantages over other authentication techniques where the traditional techniques deal with what one know or possess. Hence the possibility of forgetting the feature or being stolen is ruled out. To solve these concerns that exist with token based or knowledge based system, personal features are considered as a feature which cannot be stolen and hence known by the term biometrics.

1.1 Biometrics

There is an expanded need emerging day by day where clients are compelled to confirm themselves to machines. The most ideal way this should be possible is by utilizing biometric frameworks. In the case of biometric systems, instead of carrying cards or remembering PIN, the cues used in identifying a person are carried in the body. Biometrics is a strategy that alludes to programmed acknowledgment of people in view of their physiological or behavioural qualities. If any of the physiological or behavioural characteristics has following properties it could be a biometrics. The characteristics namely, (i) Universality, this signifies that every person should have the property that is taken into consideration, (ii) Uniqueness, which indicates that the characteristics of the property considered are not common to two persons, (iii) Permanence, the characteristic should be invariant with time, and (iv) Collectability, which indicates that the characteristics can be measured quantitatively is given (Jain et al. 2006). Extensive research is going on in different biometrics but no single biometrics is proved to satisfy the need for all applications. The biometrics that is been researched till date has its own strength and limitations and can be effectively used for specific applications only.

1.1.1 Types of Biometrics

Biometric technology is attracting attention due to the advancement in computation and its ability to deliver accurate results (Akazue and Efozia 2010). Basic classifications of biometrics are namely, (i) Physiological and (ii) Behavioural biometrics. Figure 1.1 gives a classification of biometric system. Traits like fingerprint, palm print, iris, face, retina, ear and DNA can be classified under physiological traits. Signature, voice, keystroke, gait are some of the behavioural cues that can be used as a biometric to identify a person. Choice of biometrics depends on the application. Single biometric has not been in effect to meet the requirement of all the applications. This thesis introduction will briefly describe major physiological traits as; this work is based on physiological traits.

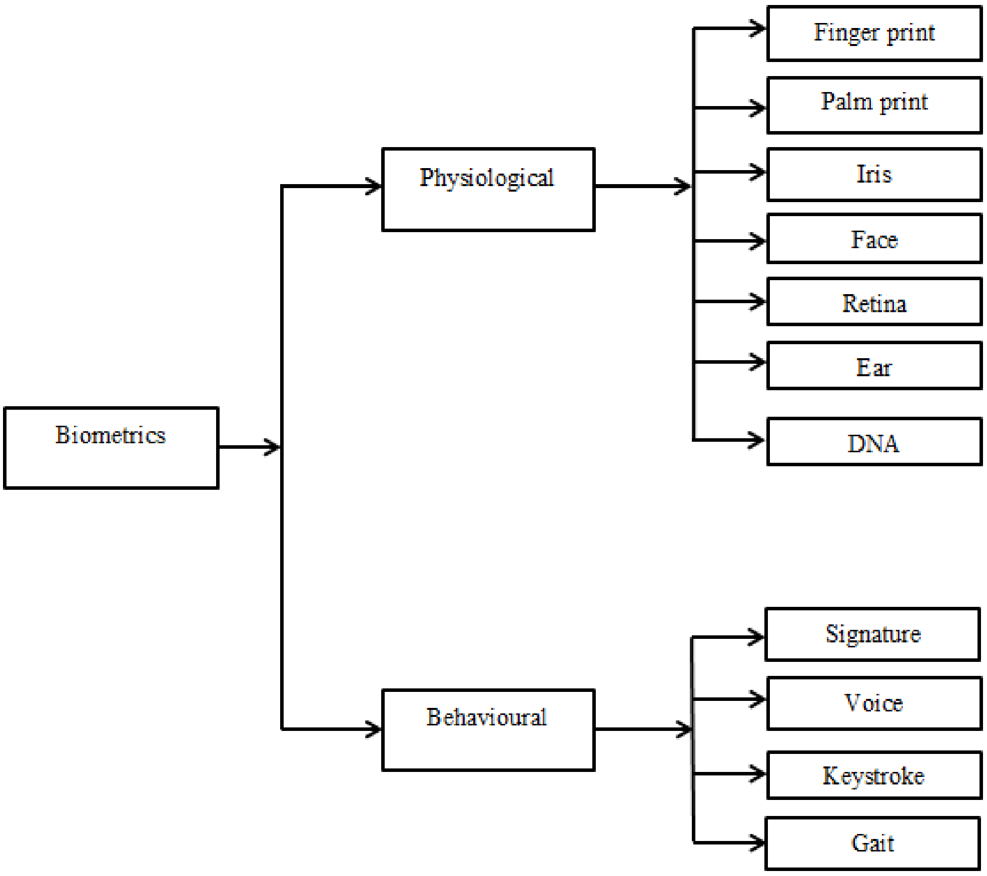

Figure 1.1: Classification of Biometric Systems.

(i) Fingerprint recognition

Finger print impression is being used for numerous hundreds of years. Fingerprint recognition technology is one of the widely used and well known biometric techniques. This biometric is shown to have good matching accuracy. A fingerprint image consists of evenly spaced ridge curves. The spaces that exist between the two ridges are known as the valley. The minute features that are used in identifying the uniqueness of a fingerprint are known as Minutiae. The minutiae of a fingerprint are unique for each person (Jain et al. 1999). There are various methods in which fingerprint matching can be performed like correlation based, minutiae-based and genetic algorithm based. The accuracy of finger print system is well enough for verification and hence been widely used as a biometric for access verification. The disadvantage with fingerprint system is that the computational resources required for this system are large. Adding to this factor, age, environment and occupational reason will also affect the recognition rate of the system (Jain et al. 2004). The finger print consists of different arch, whorl, loops and ridge patterns that are depicted in the Figure 1.2.

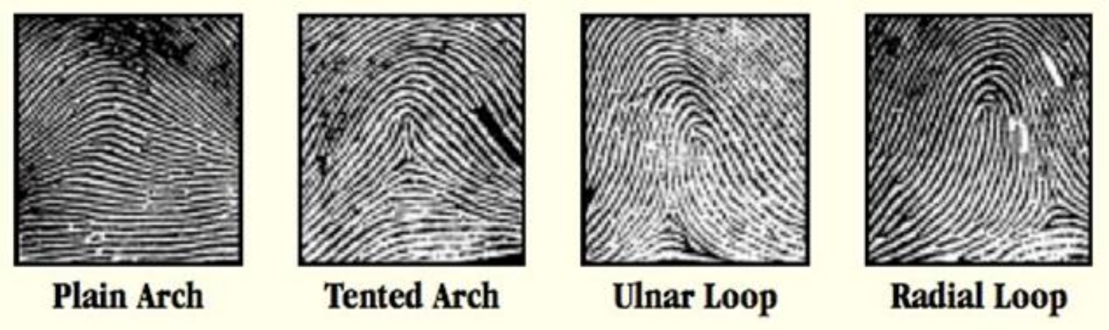

Figure 1.2: Finger Prints with Different Arches (George 2012).

Studies prove that only 5 percentage of the population has arches. The ridges of arch enter from one side and leave out from the other side. Plain arches have a wave like pattern and tented arches will have shark spike at the centre as shown in Figure 1.2. The ridge patterns shown in Figure 1.2 are used in differentiating two images of persons. The different characteristics of fingerprint like Core, Ending Ridge, Short Ridge, Fork or Bifurcation, Delta, Hook, Eye, Dot or Island, Crossover, Bridge, Enclosures and Speciality are used in computing the features of an image (George 2012).

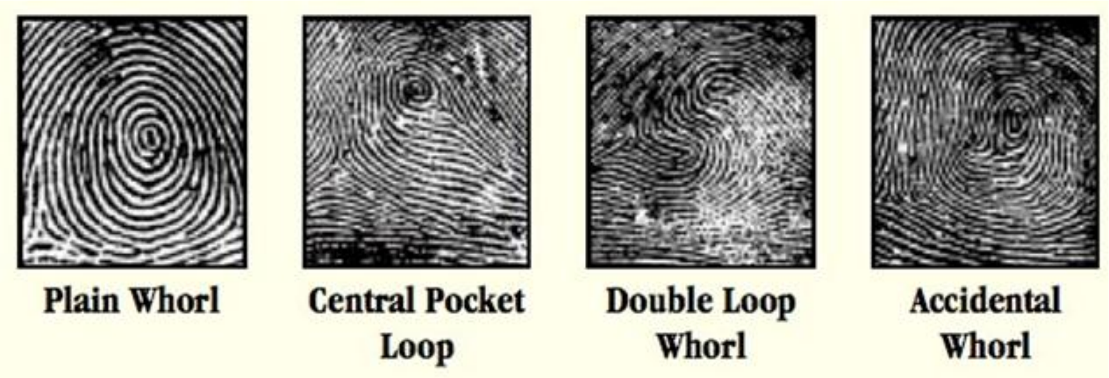

Figure 1.3: Finger Prints with Whorl and Loop (George 2012).

Compared to arches in fingerprints, whorls are seen in about 25-35 % of fingerprint patterns that are encountered. Ridges make a turn through one circuit in the case of whorl. Basically there are four different types of whorl patterns as given in the Figure 1.3. Identifying these features helps in recognition of a finger print.

(ii) Palm print recognition

Palms of human hand contain a specific pattern of ridges and valleys like finger prints but palm prints are more distinctive than finger prints. The inner surface of a palm consists of principal lines and wrinkles. These features as well as ridges, singular points and minutia points present in the palm helps in recognising the identity of a person. A typical palm print system consists of following features namely, (i) Palm print scanner (ii) Pre-processing (iii) Feature extraction (iv) Matching and (v) Database (Kong et al. 2009). A palm print scanner is more bulky and expensive when compared to the finger print sensors (Jain et al. 2004).

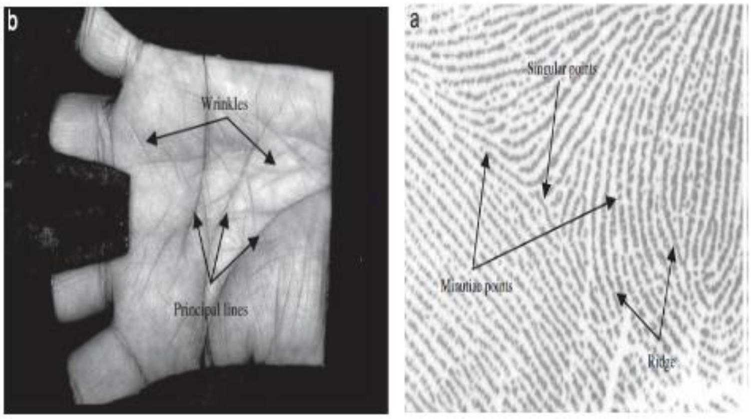

Figure 1.4: Palm Print Recognition with minute and ridges (Jain et al. 2004).

(iii) Iris recognition

On the discussion of the iris recognition biometrics (Srivastava 2013) pointed that damage is minimal in the case of iris recognition compared to other biometrics. Iris is not affected by age factor hence, eyes can be considered as a stable feature on the face when compared with other features on a face. This gives maximum accuracy and less error rate for personal identification in a biometric system. The study carried out by (Zhu et al. 2000) the change in pattern from one person to another differs to an enormous extent. Iris recognition consists of four basic steps: (i) The system captures an image with users eye (ii) Pre-processing is performed to normalize the scale and illumination of iris and perform localisation (iii) Extraction of features representing iris pattern (iv) Matching is performed with the database images. The drawback of this biometric is that the equipment of iris recognition is expensive and user needs an intervention with the system to capture the iris image. Figure 1.5 shows the steps involved in recognising an iris image (George 2012).

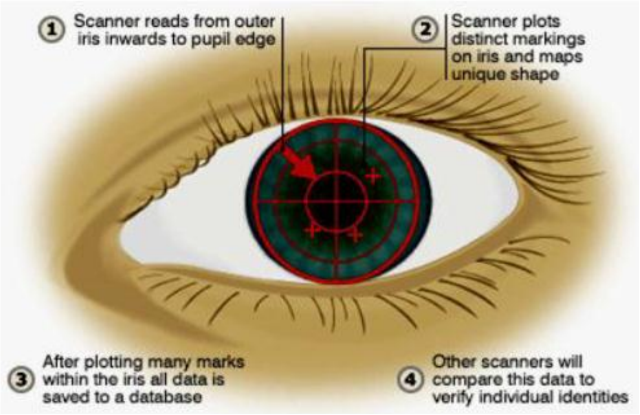
1 Scanner reads from outer iris inwards to pupil edge
2 Scanner plots distinct markings on iris and maps unique shape
3 After plotting many marks within the iris all data is saved to a database
4 Other scanners will compare this data to verify individual identities

Figure 1.5: Iris Recognition (George 2012).

(iv) Retina recognition

Retinal recognition is based on the blood vessel pattern that is found in the retina, back of the eye. These blood vessels provide a unique pattern which cannot be altered by the external factors. This technique has robust matching feature and used to perform one-to-many identification with the data stored in the database. The disadvantage with this technique is that it requires a high quality image, difficult to use and user needs to adjust with the system to a greater extent. To add on to this retinal scanners are very expensive. Highly secure environments use retinal scan systems (Jain et al. 2000).

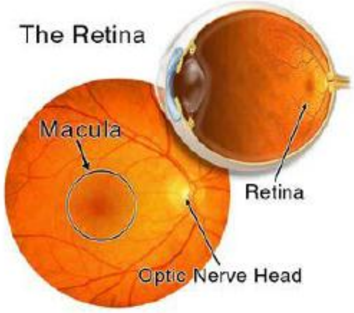

Figure 1.6: Retina Recognition (George 2012).

(v) Face recognition

Face recognition system is one of the most common and widely used biometric systems that are used to make a personal identification. This biometric can be used for identification of the face as well as verification. In this biometric, the characteristic of a person's face is captured through a digital camera. Face recognition can be performed based on the location of the face attribute like eyes, nose, lips etc. or considering face as a whole image. The main advantage with respect to face recognition system is user need not have to intervene with the system. But if faces are captured from two different views, it makes the system difficult to recognise the face. In order for the society to widely accept face recognition system, it should be able to recognise face with varying illumination, faces captured from the different angle and even if it is partially covered (Jain et al. 2000). Face recognition can be performed from a still image face and from a video. Face recognition from the video does not need user cooperation for recognition and can be considered as the only biometric that can be used secretly to watch on suspects. Non-intrusiveness is one of the strongest positive aspects of facial biometric system. This system is gaining popularity and been in use in many law enforcement areas (Akazue and Efozia 2010). Figure 1.7 shows the feature points from a face that can be considered for recognition task. Considering the feature points for recognition is an easy task when the frontal face is captured but this becomes difficult if the face is oriented at different angles.

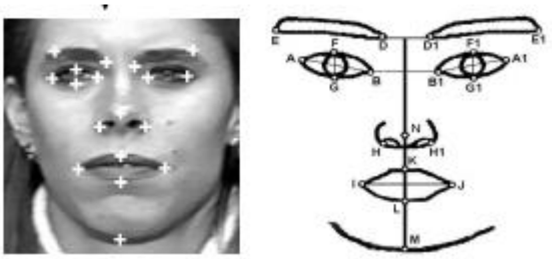

Figure 1.7: Face Recognition (Akazue and Efozia 2010)

(vi) Ear recognition

For ear to be considered as a biometric for recognition, the shape of the ear and the structure of the cartilaginous tissue of the pinna are considered as shown in Figure 1.8 since they are the distinctive features. Ears are used in the forensic field for a quite long time even though they are new to the biometric field. Most of the approaches in recognition have used ear's planar shape into consideration for recognition of an identity. Geometrical properties of the ear curve, number of landmark points is also considered for recognition (Mir et al. 2011). Figure 1.8 shows the features and the patterns of an ear structure that are considered for recognition. These different features can be considered individually or fused for recognition (George 2012).

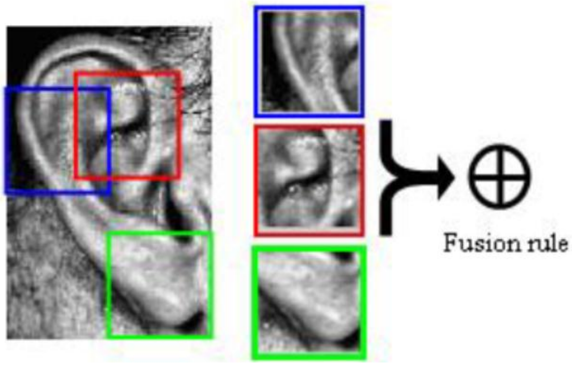

Figure 1.8: Ear Recognition System (George 2012).

(vii) DNA recognition

Deoxyribonucleic acid (DNA) is the unique code to represent one’s individuality. Identical twins share same DNA. DNA recognition is used in forensic applications for a particular person’s identity. DNA sampling requires tissue, blood, saliva or any other body part and is very intrusive. This biometric cannot be considered as a fully automatic biometric technique. Few of the disadvantages of this biometric are namely, (i) It requires complex chemical method with expert skills (ii) Piece of DNA can be stolen from an individual and can be used for interior purposes. Figure 1.9 shows the DNA pattern with the details of the structure.

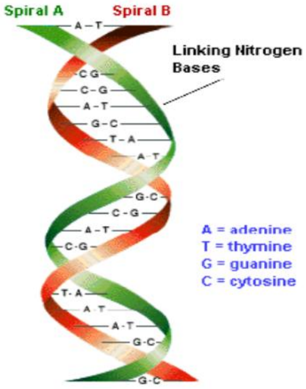

Figure 1.9: DNA Recognition (George 2012).

The above study on different biometric systems, each one with its own advantages and disadvantages led us to the need of understanding the efficiency of each of the biometric system with respect to the functionality of biometrics. Each biometric system or a combination can be used for a specific application based on the need of the application.

1.2 Comparative Study on Biometric Systems

There is no particular biometric that can be utilized in common for each of the applications. Henceforth it is vital to know which one of them will be appropriate for a particular application. With a specific end goal to know this, it is imperative to have a relative study on various biometrics. Table 1.1 provides a comparative study of the mainstream physiological biometrics present based on the characteristics of a biometric system like, Universality, Distinctiveness, Permanence, Collectability, Performance, Acceptability and Circumvention. The biometrics considered for the comparison with respect to the above features are physiological traits like Face, Fingerprint, Iris, Retina, Ear and DNA.

Table 1.1 Comparative Study on Different Biometric System.

Biometric identifier	**Universality**	**Distinctiveness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**circumvention**
Fingerprint	M	H	H	M	H	M	M
Palm print	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Retina	H	H	M	L	H	L	L
Face	H	L	M	H	L	H	H
Ear	M	M	H	M	M	H	M
DNA	H	H	H	L	H	L	L

From the above comparative study it is clear that acceptability of face and ear recognition systems are high compared to other biometric. Universality of face is high compared to ear. Hence in this work, a study is conducted on recognising faces using a face recognition system.

1.3 Face Recognition

Security being the major concern in today's world, face recognition from the video is a most seeking research area. Face recognition is considered to be one of the most successful application on which image analysis is performed (Zhao et al. 2003). With advancements in the research field, this technology is used in electronic devices for security. When a face recognition technology is introduced, it helps in identifying face automatically from an image or video. Face recognition technique can be operated either as (i) Face verification (face authentication) and (ii) Face identification (face recognition). Among the above-mentioned two methods, face verification is when one if the faces is matched against the template face images whose identity is to be checked against, whereas face identification is when the query face is matched with all the images in the database (Jain and Li 2005). Even though face recognition technology is used in all fields as a best biometric for security and research in this field has increased to a greater extent, recognition rate of faces in unconstrained environments where angle at which face is viewed, illumination, expression, occlusion vary considerably.

1.3.1 Face Recognition Approaches

Designing a system that can automatically detect and recognise a face is a tedious task. The procedure of detecting a face can be broadly categorised into (i) Feature-based approach and (ii) Image-based approach (Hjelmasa and Lowb 2001).

(i) Feature-based approach

In feature-based approach the low-level features are taken into consideration. In this method of face detection, the distance, angle formed with respect to a different feature, an area of the visual features are extracted from the frame. Edge, colour, motion detection are the different methods that exist in the case of feature based methods. Moving image contours can also be used to analyse moving motion of the faces and human bodies.

(ii) Image-based approach

Feature-based approaches are limited to head and shoulder or frontal faces alone. In order to overcome this, the procedure of extracting features that help in classifying data into face and non-face classes were looked into. Comparing the information among these classes and data extracted from the input image helps in detecting if a face is present or not in a cluttered background. Window scanning technique is one of the most used methods for detecting face under this category. Appearance based and learning based methods are discussed below among which AdaBoost learning based methods are the most successful ones in terms of accuracy and speed (Jain and Li 2005). Appearance based methods classify scanned sub-window as either a face or non-face. A face/non-face classifier is built to identify the face as pixels in face are highly correlated and non-face has less regularity.

1.4 Face Recognition as a Process

Face recognition system consists of four modules namely (i) Face Detection/Tracking(in the case of videos), (ii) Face Alignment, (iii) Feature Extraction and (iv) Matching of the test image with the image in the database. These modules of face recognition system are depicted in Figure 1.10. As illustrated, the recognition process starts with identifying the face region in the given image. Tracking is performed to locate a human face if the input is a video sequence. There are various methods to detect a human face from the background of a scene. One of the widely used methods is Viola-Jones algorithm that uses AdaBoost technique. Further from the detected frame, face part is detected. The detected face region is aligned and adjusted as a major aspect of pre-processing. Features are extracted from the aligned face image using any of the feature extraction techniques and further matched with the features extracted from the gallery images. Each step in this process is further explained underneath.

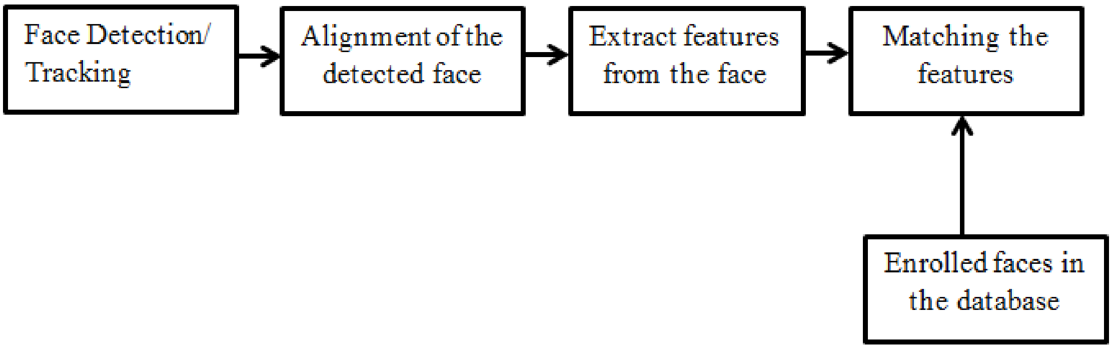
Face Detection/ Tracking
Alignment of the detected face
Extract features from the face
Matching the features
Enrolled faces in the database

Figure 1.10: Processing Diagram for Face Recognition.

1.4.1 Face Detection

Face detection is the very first step in face recognition. The major goal of face detection is to determine if there are any human face in the frame and if present return to the user its location and spatial extent. This method helps in extracting the face image from the background scene. Face tracking from frame to frame is required in the case of face recognition in video. A face is detected from a cluttered background or from a video sequence based on cues like skin colour, the shape of the human face, motion especially in the case of videos, or a combination of above factors (Jain and Li 2005).

1.4.2 Feature Extraction

Feature extraction is the most important step the process of face recognition. Once the face is detected from the video sequence, features are extracted from the face image in order to match the face with the training images stored in the database. The features extracted can fall into two different categories namely, (i) Geometric features and (ii) Appearance features. In the case of geometric feature based approach, facial points from the face are extracted to find the matching. Whereas with respect to appearance-based model, there are various methods that describe the pixel intensity of the face image which is used as a metric for recognition. Most systems that are available today use the combination of appearance and geometric features as explained (Senior and Bolle 2002) in the chapter face recognition and its application. Appearance information is subject to variation in pose, expression and light. Hence geometric parameters are estimated in order to derive a face representation that can handle pose variation and expression change. Further, the appearance plan can be classified into local and global. Global, when the face is represented as a whole face image and local, is when face is represented as a series of small regions.

1.4.3 Classification

Once the face is being processed and the features are being extracted these feature values are transmitted as a facial feature code. To determine similar faces, a similarity measure is defined that will help the system to find the similar face with respect to the sample faces stored in the database. In the case of any biometric system, a particular threshold value must be chosen to find the match between the test image and the gallery images. To find this match, there are different methods used. Few of them are listed below (i) Nearest Neighbour Approach (ii)Support vector machine approach (iii) Mahalanobis approach (iv) Histogram based approach (v)Sparse representation approach.

1.5 Video Based Face Recognition

In general face recognition algorithm consider still face as the input for recognition. With the advance in application and research, face recognition from still face is moving towards video based face recognition. In video based recognition the face in the casing is followed and the face is recognized. Video is an accumulation of still images thus still image based face recognition can also be applied to recognize a face from video. Temporal coherence is a vital element in video and is been widely utilized for tracking faces (Chellappa and Zhou 2005). Video based face recognition can be categorised as: (i) Still image to video recognition, where the probe is a still face image and the gallery consist of video sequences. The input still image is checked if present in the frame sequence. (ii) Video to still image recognition where video is the probe and gallery consist of still images of faces. In this case, from the input video it is checked if the enrolled face is available or not to give access and the third category, (iii) Video to Video recognition. The third category is the video to video face recognition, where both input and the gallery set are video sequences.

1.6 Challenges of Video Based Face Recognition

Video-based face recognition is good at applications like surveillance and verification system for access control. Applying the face recognition system at various applications, the outcome of the recognition result is not always accurate and hence this biometric suffer from various challenges. The major challenges with respect to video based face recognition are described below.

1.6.1 Illumination

(Georghiades et al. 2001) in their work mentioned that the variation due to illumination is much difficult to identify when compared with two different identities. Recognising a face under a specific lighting and stance can be performed dependably given the face has been beforehand seen under comparable circumstances. As it were, these techniques in their unique structure can't extrapolate to novel review conditions. Authors in their work built an illumination cone; the shape and albedo of every face are reproduced utilizing a variation of photometric stereo. Faces enlightened by point light sources at different, obscure positions, are used to gauge its surface geometry and albedo map up to a summed up bas-relief (GBR) transformation. A GBR transformation scales the surface and presents an added substance plane. Further exploitation of the symmetries and similarities in faces are taken into consideration to determine the three parameters indicating the GBR change. Other than pose variation, illumination is the most critical element influencing the recognition rate of faces (Gross and Brajovic 2003). Ambient lighting changes significantly inside and in the middle of days and among indoor and open air situations. Because of the 3D state of the face, an immediate lighting source can cast solid shadows that emphasize or lessen certain facial components. Assessments of face acknowledgment calculations reliably demonstrate that best in class frameworks cannot manage extensive contrasts in brightening conditions between gallery and probe images. Authors in this work proposed a new image pre-processing algorithm that makes up for illumination variation in images. In their work a face image from a solitary brightness image the proposed algorithm first estimates the illumination field and afterward compensates for it to generally recover the scene reflectance.

1.6.2 Pose Variation

Pose variation while capturing frames from video is extremely normal and this property is a troublesome errand in recognising faces. Figure 1.11 gives a look at faces with various poses. As the complete structure of the face is not visible when faces are at different poses, recognition is a difficult task.

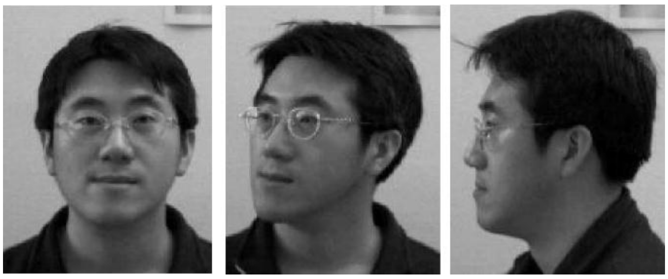

Figure 1.11: Faces with Varying Pose, (Honda/UCSD dataset).

(Abate et al. 2007) carried work on a survey on 2D and 3D face images. They commented that iris recognition is a very accurate biometric but is not accepted as implementation of this biometric is expensive compared to rest. Fingerprints are reliable but not suited for non-community oriented people. Contrasted with the above biometrics face is all around acknowledged and balances security and protection. This work expresses that pose changes in face recognition influences largely on the recognition process. There are a few methodologies that try to fathom this issue and can be classified into multi-view and across pose. Multi-view face recognition is one of the methodologies where the gallery comprises of pictures of each user with various poses. Face recognition across pose algorithms are built to recognise face from a novel viewpoint. (Tan et al. 2006, Huang et al. 2000) carried their work on recognising faces that are with varying poses using the neural network. In their work they considered faces oriented from left 30 degree to right 30 degree for recognition.

1.6.3 Occlusion

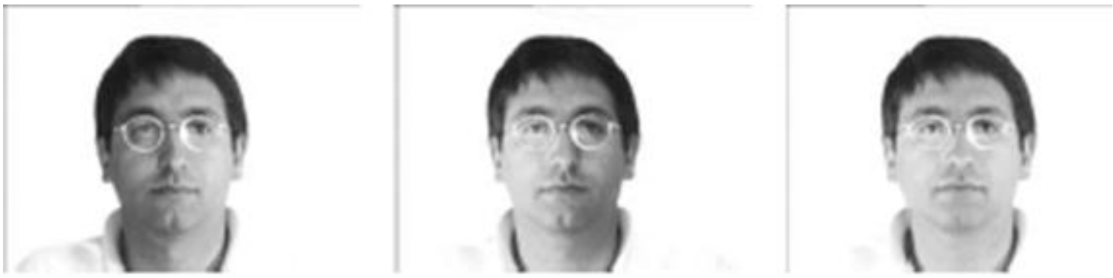

Figure 1.12: Faces with Occlusion due to Glasses (AR dataset).

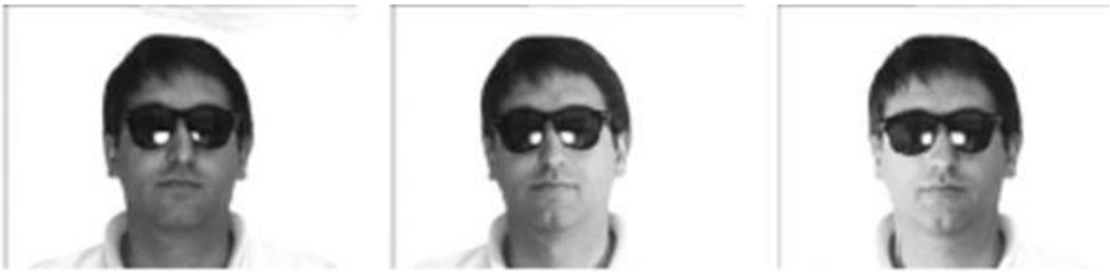

Figure 1.13: Faces with Occlusion due to Sunglasses, (AR dataset).

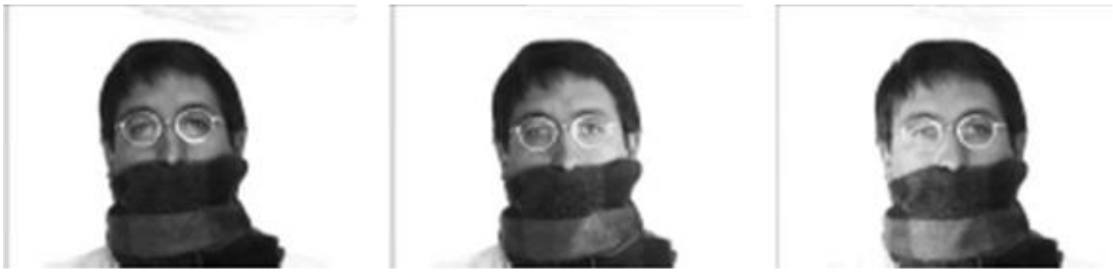

Figure 1.14: Faces with occlusion due to Scarf, (AR dataset).

Occlusion is one of the major drawbacks that affects recognition rate in face recognition technique. Occlusion can occur due to facial accessories or any other object covering your face as the users need not cooperate with the camera when the faces are captured. As the part of the face is covered, the recognition rate reduces drastically when a system is built. Figure 1.12 shows the occlusions on a face that may occur due to the usage of accessory like a glass. This will deteriorate the recognition rate of a face.

1.7 Applications of Biometrics

The various applications of biometrics can be categorised as (i) Commercial application, (ii) Government application and (iii) Forensic applications. Few of the commercial application can be electronic data security, e-commerce, internet access, ATM, physical access control etc. Government applications can be namely Aadhar card, driver's licence, passport control, social security etc. The forensic application can be such as criminal investigation, determining parenthood and finding missing children to name a few (Jain et al. 2004).

1.8 Thesis Organization

Under this section, organization of the thesis is briefed. Chapter one gives a detailed introduction to biometrics, applications of biometrics, design issues related to biometrics. Chapter two presents a comprehensive literature survey on face recognition; video based face recognition, face recognition with a varied pose, partially occluded face recognition, inpainting techniques and exemplar inpainting. A proposed model for recognising faces with varying pose from a video is discussed in Chapter Three. Inpainting is a technique used in recovering the lost part of an image. Exemplar-based inpainting and modified exemplar-based inpainting are discussed in Chapter Four. Chapter Five gives a proposed method to recognise faces that are partially occluded that uses modified exemplar-based inpainting for recovering the lost region. In Chapter six, results obtained and a discussion of the result is carried out. Finally, in Chapter seven conclusions, contributions and future enhancement are presented.