Chapter 3
Biometric Systems and Template Security

This chapter provides a detailed background on biometric systems and biometric template security. This chapter begins with an introduction to biometrics, the features of different biometric modalities, mode of operation, performance measures of biometric systems and limitations of biometric systems. An iris recognition system is implemented and a comparison of feature extraction and classifications are carried out. The chapter concludes with a discussion on template security, different type of method for template security.

3.1 Introduction

Reliable identity establishment is becoming critical issue in a variety of applications including sharing networked computer resources, performing remote financial transactions, border security control and forensic applications. Biometric systems, which are based on the physiological and behavioral characteristics of individuals provide better security and greater convenience than the traditional systems which are either knowledge based (e.g., passwords) or possession based (e.g., ID cards).

In the following sections, a brief introduction to biometric systems and biometric template security is provided

3.2 Biometric Systems

Now-a-day, biometric authentication system or simply biometric system, offers a reliable and user-friendly solution to the problem of identity management by establishing the identity of an individual based on “who the person is”, rather than the knowledge-based i.e. “what the person knows" or token-based i.e. “what the person carries” (Jain *et al*., 1999). The word biometrics is derived from the Greek words *bios* (meaning life) and *metron* (meaning measurement); biometric identifiers are measurements from living human body (Maltoni *et al*., 2009). Biometric system refers to automatically identify or verify an individual's identity based on his physiological characteristics (e.g. fingerprints, face, iris and hand geometry) and behavioral characteristics (e.g. gait, voice and signature) as shown in Figure 3.1. Ancillary characteristics (also known as soft biometric) such as gender, ethnicity, age, eye color, skin color, scars and tattoos also provide some information about the identity of a person. However, soft biometric traits do not provide sufficient evidence to precisely determine the identity (Jain *et al*., 2004a). Biometric traits provide a unique and permanent binding between an individual and his identity. This “binding" cannot be easily lost, forgotten, shared or forged and free from making false repudiation claims. Biometrics offers several advantages over conventional security measures. These include

(i) *Non-repudiation*: A user/perpetrator can claim that his identity was stolen in order deny service or committing the crime pleading. However, biometrics is indefinitely associated with a user and hence it cannot be lent or stolen making such repudiation infeasible.

(ii) *Accuracy and Security*: Conventional identification systems are prone to dictionary and brute force attacks. On the other hand, biometric authentication requires the physical presence of the user and has also been shown to possess a higher bit strength compared to conventional based systems.

(iii) *Screening*: Enrollment of user with multiple identities (e.g. a terrorist using multiple passports to enter a foreign country) cannot be screened in traditional authentication mechanisms and biometrics provides the only available solution.

A biometric system is a pattern recognition problem consisting of acquiring of biometric (row) data, extraction of important features, storing in system database and matching the patterns make decision. A typical biometric system consists of five main modules.

(i) *Sensor modules*: Row biometric data for the target population are collected in this module by using suitable sensor or scanner under appropriate arrangement.

(ii) *Feature extractor module*: A set of salient discriminatory features is extracted from the acquired biometric sample to represent the underlying trait, called the *feature set*. The feature set obtained during enrolment is generally referred as a *template* and stored in the system database for future reference.

(iii) *Matching module*: During authentication, the query feature set is matching with stored template and generate some similarity or distance score.

(iv) *Decision module*: This module gives decision on the identity of the user based on the degree of matching between the query (input) feature set and the store template.

(v) *System database module*: The system database is the depository of biometric templates that stores the extracted feature set from the raw biometric sample.

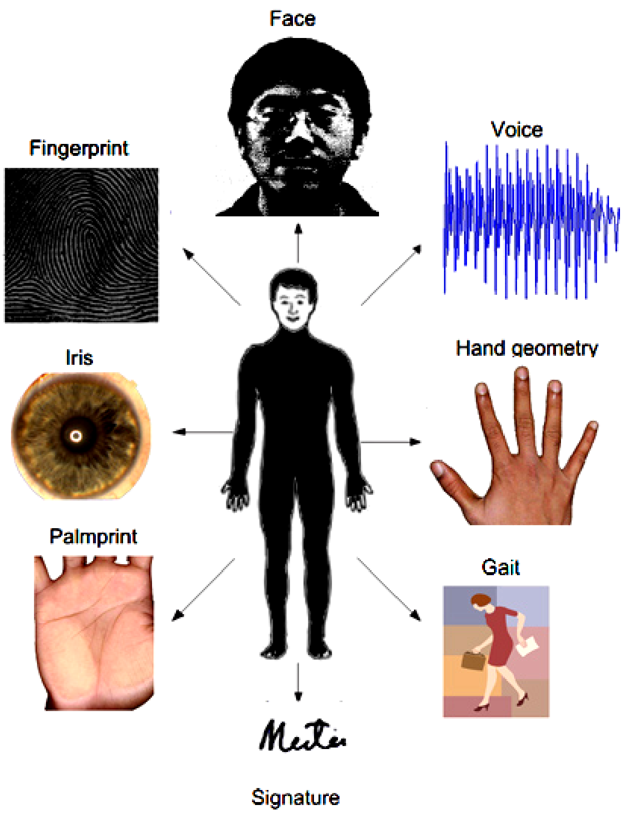


Figure 3.1 Examples of Biometric Traits

3.2.1 Biometric Modalities

However, each biometric has its advantages and disadvantages and selection of a biometric trait for a particular application is based on the following seven properties (Jain *et al*., 1999).

(i) *Universality*: It should be possess in every individual using the system.

(ii) *Uniqueness*: It should be sufficiently distinguishable for every person within a population.

(iii) *Permanence*: It should be sufficiently invariant over a period.

(iv) *Measurability*: It should be a quantitatively measurable characteristic and there should not be any undue inconvenience to the individual while acquiring it.

(v) *Performance*: It should meet an acceptable level of identification accuracy.

(vi) *Acceptability*: people in the target population should willingly accept the system, and

(vii) *Circumvention*: It should be difficult to fool the system by deceptive techniques.

The comparison of characteristics for some commonly used biometrics is shown in Table 3.1.

Table 3.1 Comparisons of Biometric Characteristics (Jain *et al*., 1999)

Biometric Traits	**Universality**	**Uniqueness**	**Permanence**	**Measurability**	**Performance**	**Acceptability**	**Circumvention**
Iris	H	H	H	M	H	L	H
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Signature	L	L	L	H	L	H	L
Hand Geometry	M	M	M	H	M	M	M
Hand Vein	M	M	M	M	M	M	H
Retinal Scan	H	H	M	L	H	L	H
Voice Print	M	L	L	M	L	H	L
Key-strokes	-	-	L	M	L	M	M
Gait	M	M	H	M	M	H	M
Ear	M	M	H	M	M	H	M

Note: H - High; M - Medium; L - Low

The biometric traits can be divided into two major groups: physiological or behavioral. Physiological modalities are those referred to, as the name indicates, a physiological characteristic of the user, such as fingerprint, face, or hand geometry. On the other hand, behavioral modalities are based on the data derived from an action performed by the user. Examples of behavioral modalities are speech, signature recognition and key dynamics. Behavioral modalities are non- invasive and therefore are more accepted by users. However, these techniques are, in general, easier to falsify and imitation becomes a possible attack. A brief note to the most common biometric traits is provided next.

3.2.1.1 Physical Modalities

3.2.1.1.1 *Face*

Face recognition is the most intuitive biometric modality, as it is common methods of recognition that humans use to identify each other in their daily visual interactions. In addition, face image acquisition is nonintrusive. Face recognition (Li and Jain, 2005) is based on the following approaches:

(i) The location and shape of facial attributes, such as the eyes, noses, lips, eyebrows, and chin and their spatial relationships,

(ii) The overall (global) or texture analysis of the face image that represents a face. However, face recognition technique has many challenges e.g. distinction of twins or people with similar faces, effects due to facial expression, variations in the imaging environment, aging, facial pose with respect to the camera, artificial techniques such as make-up or plastic surgery.

3.2.1.1.2 *Fingerprint*

Fingerprint has been used for personal identification for many decades. The fingerprint has many particular properties such as uniqueness, stableness, and inseparability from the host. Moreover, the fingerprints of identical twins as well as the prints on each finger of the same person are different. The matching (i.e., identification) accuracy of fingerprint recognition system is very high (Maltoni *et al*., 2009). It can be represented by a large number of features, including the overall ridge flow pattern, ridge frequency, location and position of singular points, location of minutia points, ridge counts between pairs of minutiae, and location of pores. Fingerprint technology has become one of the most commonly used modality because of its marginal cost. One problem with fingerprint recognition is that they require a huge amount of computational resources at large-scale. Finally, fingerprint may be unsuitable for automatic identification for a small fraction of the population because of genetic factors, aging, environmental or occupational reasons.

3.2.1.1.3 *Hand Geometry*

Hand geometry of a person are based on a number of measurements including its shape, size of palm, and the lengths and widths of the fingers and it can be used as a biometric trait (Zunkel, 1999). The technique is very simple, relatively easy to use, and inexpensive. Environmental factors (e.g., dry weather) or individual anomalies (e.g., dry skin) do not appear to adversely affect the accuracy of hand geometry-based recognition systems. However, the hand geometry is not known to be very distinctive and recognition systems based on this trait cannot be suit for a large population. Furthermore, hand geometry information may be invariant due to the growth period of children. In addition, these system may pose challenges in extracting the correct information due to an individual's jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis). The physical size of a hand geometry-based system is large, and it is not suited to embed in certain devices like laptops.

3.2.1.1.4 *Palmprint*

The palms of the human hands contain pattern of ridges, valleys, principal lines, and wrinkles much like the fingerprints. The area of the palm is much larger than the area of a finger and, is expected to provide a more accurate recognition system than the fingerprints (Zhang *et al*., 2003; Kumar *et al*., 2003). When using a high-resolution palmprint scanner, all the features of the hand such as geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system. However, palmprint scanners need to capture a large area; they are bulkier and more expensive than the fingerprint sensors.

3.2.1.1.5 *Hand Vein*

Thermographic images of veins located in the hand can be employed as a biometric modal. Vein development is a stochastic process carried out during gestation, and just as the fingerprint or iris, it is considered unique for each individual. However, recognition results obtained are far less efficient than expected; this is because the images are highly sensitive to environment variations, especially temperature (Sanchez-Reillo *et al*., 2007).

3.2.1.1.6 *Retina*

This trait is based on the pattern of the veins located at the retina in the eye. It is highly secure and provides better performance results. The retina scanners are relatively costly. While acquire the retina vein pattern, the user need to close to the scanner, invading the user’s intimacy and invasion the eye. Also, scanning the retina can be affected by many factors such as blood pressure illnesses.

3.2.1.1.7 *Ear*

The human ear possesses unique physiological features, and its characteristics do not change significantly during adult ages. Ear biometrics can be used as a supplementary evidence for face recognition systems, because a system designed for face recognition already includes all the necessary hardware for capturing and computing ear biometrics (Burge *et al*., 1998). This approach is developing in the Spanish Police corps.

3.2.1.1.8 *Iris*

Iris has complex and distinctive pattern of a pigmented fibro-vascular tissue known as stroma. Its pattern does not change during the one's lifespan and even the iris patterns of two eyes of same person are different. Due to its characteristics, it is highly suitable for biometric purposes (Daugman, 1993). In the present work, iris pattern is used as one of the biometrics. Hence, a detailed introduction to iris recognition is provided in section 3.3.

3.2.1.2 Behavioral Modalities

3.2.1.2.1 *Voice*

Voice trait is a combination of two biometric features:

(i) Physical features of an individual's voice are based on the shape and size of the appendages (e.g., lips movement, nasal cavities, vocal tracts and mouth) that are used in the synthesis of the sound. These features are invariant for an individual and

(ii) Behavioral characteristics such as word or phoneme pronunciation (e.g., dialect), use of characteristic words or phrases and conversational styles are mostly learned. (Campbell, 1997). The speech changes over time due to age, medical conditions (such as common cold), emotional state, etc. Voice is also less distinctive and may not be appropriate for large-scale applications. A voice recognition system may be implemented as (a) *text-dependent* mode in which recognition is based on the utterance of a fixed predetermined phrase and (b) *text-independent* system recognizes the speaker independent of what she speaks. It is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as back-ground noise.

3.2.1.2.2 *Keystroke*

Keystroke dynamics is a behavioral biometric and it deals with the way a user types on the keyboard, to how the user emphasizes certain keys i.e. the time duration for a certain key is press and the time interval between key strokes (Coltell *et al*., 1999). A person's typing patterns may vary due to changes in emotional state, relative position of the user with respect to the keyboard, change of keyboard used, etc. However, this biometric allows "continuous verification" of a user’s identity over a session after logs in using a stronger biometric such as fingerprint or iris with no additional sensor other than the keyboard.

3.2.1.2.3 *Gait*

Gait refers to the manner in which a person walks. Although this modal is not very distinctive among users, it offers potential to recognize people at a distance without contact with the user or at low resolution, when other biometrics might not be perceivable. This modality, therefore, is very appropriate in surveillance scenarios where the identity of an individual can be surreptitiously established (Nixon *et al*., 1999). However, the gait of an individual is highly affected by several factors including ageing, the choice of footwear, nature of clothing, affliction of the legs, walking surface, etc.

3.2.1.2.4 *Signature*

Signing name has been accepted in government, legal, and commercial transactions as a method of authentication for years. The signature is a behavioral biometric which is characterized by the peaks and inclination of curvature or counting the information contained in a determined window (Ross *et al*., 2006). Signature verification based on above attributes can be classified as Static signature verification. In dynamic signature verification, a number of additional attributes like the inclination of the pen when signing, the pressure exerted, the speed and direction of strokes and the number of stokes etc. are also incorporated. Signature changes over a period of time and is influenced by the physical and emotional conditions of the signatories. Signatures of some people vary substantially. Further, it is relatively easy to reproduce or copy that can fool the signature verification system.

Among biometrics modalities, iris is receiving attention as one of the most accurate and reliable biometric for personal identification because of its characteristics like stability over a person's life, naturally protected, highly complex and distinctive pattern which provides desirable properties of a biometric (i.e., uniqueness, stability, and noninvasiveness) (Lim *et al*., 2001; Daugman, 2004; Ross *et al*., 2006). Hence, performance analysis of the feature reduction methods and pattern classifiers based for iris recognition is discussed in Section 3.3.

3.2.2 Biometric Functionalities

Depending on the mode of operation, a biometric system may operate as verification and identification as shown in Figure 3.2.

3.2.2.1 Verification Mode

In verification scenario, the system answers the question "Are you who you say you are?" i.e. the captured biometric data of a claimed identity is compared with its own biometric template stored in the system (i.e. one-to-one comparison) to determine whether the claim is "genuine" or "impostor". If the matching score is above a predefined threshold (θ), the claim is classified as "genuine". Otherwise, the claim is considered as an "impostor". In short, verification is a two-class classification problem and is generally used for positive recognition.

Formally, the decision function of a biometric system in verification mode can be represented as in Equation (3.1):

$$F(x) = \begin{cases} genuine, & if \quad S \geq \theta \\ imposter, & otherwise \end{cases} \tag{3.1}$$

where, S is the match (similarity) score between query feature set T_Q and stored biometric template T_I corresponding to identity I, given by the expert.

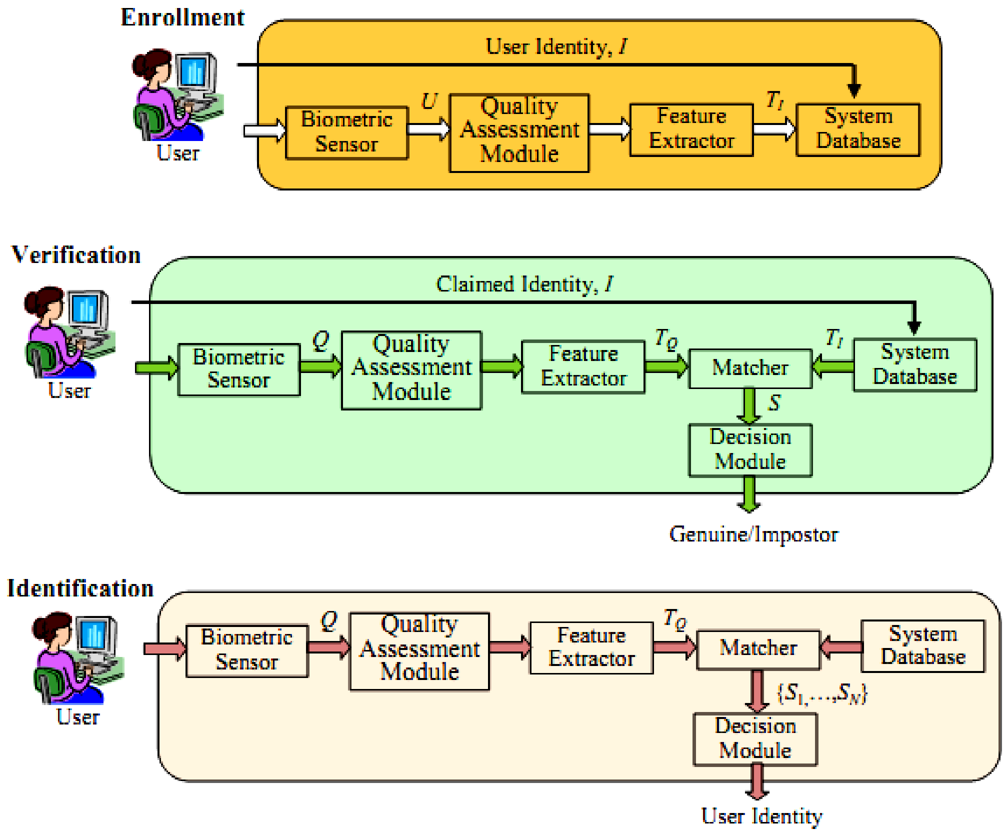


Figure 3.2 Enrollment and Two Modes of Biometric System (Nandakumar, 2008)

In Figure 3.2, U represents the biometric sample collected from sensor. Q is the query biometric sample, T_I and T_Q is the template and query feature sets, respectively, S represents the match score and N is the total number of users enrolled in the system.

3.2.2.2 Identification Mode

In this mode, the user's query biometric is compared with the templates of all the persons enrolled in the system (i.e. one-to-many comparison) to establish an individual's identity. The decision is either the identity of the user having highest matching score between his templates and the query sample or the claimed user is an imposter. Identification is used for negative recognition and therefore used for preventing from multiple identities.

Formally, consider a system with N enrolled user identified by $I_1, I_2, \ldots, I_N$; T_{I_N} be the stored biometric template for Identity I_N; I_{N+1} be the imposter and query feature set T_Q, then the decision rule for identification is given by Equation (3.2).

$$T_Q \in \begin{cases} I_{n_0}, & if \;\; n_0 = \arg\max_n S_n \quad and \quad S_{n_0} \geq \theta \\ I_{N+1}, & otherwise \end{cases} \tag{3.2}$$

where, S_n be the match (similarity) score between T_Q and T_{I_N} and θ is a predefined threshold.

3.2.3 Performance of Biometric Systems

In conventional authentication methods, such as password-based systems, a perfect match between input and stored password is mandatory to validate a user's identity. However, in biometric system, the two sample of the same biometric trait of an individual may varies due to the several factors such as sensing conditions (e.g., sensor noise), variations in illumination (in iris recognition) and improper interaction with the sensor (e.g., occluded iris or face). Thus, the two biometric samples can't match 100% perfect and as a result, the biometric system can never attained 100% accuracy. The variation in the feature sets of a biometric trait for a user is known as *intra-class* variation. On the other hand, extracted features sets of different users may be quite similar (e.g. nearly identical facial appearance among father and son or identical twins, etc.). Such a similarity is known as *inter-class* similarity (Maltoni *et al*., 2009).

Evaluation of a biometric system is based on the three important concepts i.e. (a) types of errors, (b) threshold criterion and (c) evaluation criterion. The types of errors are false acceptance and false rejection. A threshold criterion refers to a strategy to choose a threshold which is necessarily tuned on a development set. An evaluation criterion is used to measure the final performance and is necessarily calculated on an evaluation set.

3.2.3.1 Types of Errors

In biometric, there are two types of matching score: (i) genuine match score is acquired by comparing two samples of the same biometric trait of a user and (ii) the impostor match score is obtained by comparing two biometric samples originating from different users (Jain *et al*., 2008). Similarly, two types of errors will encounter in biometric system, namely, (i) Type I error or false non-match or false rejection and (ii) Type II error or false match or false acceptance. If the intra-class variation is large, the genuine match score will be less than the operating threshold (θ) and this leads to a false rejection (FR) error. A false acceptance (FA) error occurs when the impostor match score is greater than the operating threshold (θ) due to large inter-user similarity. Therefore, the basic accuracy of a biometric system at specified operating threshold (θ), are measured in term of False Non-Match Rate (FNMR) and False Match Rate (FMR). FNMR, also known as False Rejection Rate (FRR), is the fraction of genuine scores less than the threshold and FMR, also known as False Acceptance Rate (FAR), refers to the fraction of impostor scores greater than the threshold (θ).

Let S, $f_{gen}(s)$ and $f_{imp}(s)$ be the matching score, probability density functions of the genuine and that of impostor scores, respectively. Then FAR and FRR of the biometric system can be defined as in Equation (3.3).

$$FAR(\theta) = p(S \geq \theta \mid impostor) = \int_{\theta}^{\infty} f_{imp}(s)ds = \frac{FA(\theta)}{NI}$$

$$FRR(\theta) = p(S < \theta \mid genuine) = \int_{-\infty}^{\theta} f_{gen}(s)ds = \frac{FR(\theta)}{NC} \tag{3.3}$$

where, NI and NC are the total number of impostor and client accesses, respectively. For example, 5% FRR indicates that on average, 5 in 100 genuine attempts are likely to fail. Again, 0.01% FAR indicates that on average, 1 in 10,000 impostor attempts are likely to succeed. If the operating threshold (θ) is decreased, FAR will increase and FRR will decrease and vice versa. The Genuine Accept Rate (GAR) is the fraction of genuine scores exceeding the operating threshold (θ) and is defined by Equation (3.4).

$$GAR(\theta) = p(S \geq \theta \mid genuine) = 1 - FRR(\theta) \tag{3.4}$$

3.2.3.2 Threshold Criterion

To optimize the threshold, a *threshold criterion* is to be defined within a development set. The Weighted Error Rate (WER) and Equal Error Rate (EER) are two commonly used criteria. WER is defined by Equation (3.5).

$$WER(\alpha, \theta) = \alpha FAR(\theta) + (1-\alpha)FRR(\theta) \tag{3.5}$$

where, $\alpha \in [0, 1]$ is the balancing factor of FAR and FRR. EER is a special case of WER at which the costs of FA and FR are equal i.e. the class prior distributions of client and impostor accesses are equal. In this case, $\alpha = 0.5$, then Equation (3.5) can be represented as Equation (3.6).

$$EER(\theta) = \frac{1}{2}(FAR(\theta) + FRR(\theta)). \tag{3.6}$$

The optimal threshold (θ_α*) that minimises WER on a development set can be calculated by Equation (3.7).

$$\theta^* = \arg\min_{\theta} \mid \alpha FAR(\theta) + (1-\alpha)FRR(\theta) \mid = \arg\min_{\theta} WER(\alpha, \theta) \tag{3.7}$$

3.2.3.3 Evaluation Criterion

After chosen the optimal threshold (θ_α*) using WER, the performance of the biometric system is finally measured using Half Total Error Rate (HTER) which is calculated by Equation (3.8).

$$HTER(\theta_\alpha^*) = \frac{FAR(\theta_\alpha^*) + FRR(\theta_\alpha^*)}{2} \tag{3.8}$$

From Equation (3.6) and (3.8), it can concluded that HTER is identical to EER except that HTER is a performance measure calculated on an evaluation set whereas EER is a threshold criterion optimized on a development set. Hence, EER may not be interpreted as a performance measure (in place of HTER) to compare the performance of different systems.

The overall performance of a biometric system can be graphically presented using performance visualizing tool namely Receiver Operating Characteristic (ROC) curve (Fawcett, 2006) and Decision Error Tradeoff (DET) curve (Martin *et al.*, 1997). DET curve is plotted FRR as a function of FAR on a normal deviate scale. The ROC curve is plotted the GAR as a function of FAR on linear, semi-logarithmic or logarithmic scale. Figure 3.3 shows the ROC curve for fingerprint matcher in MCYT database, which plots the GAR against FAR. Equal Error Rate (EER) is the location where FAR equals FRR on a DET or ROC curve. The system having a lower EER value indicates better performance.

In biometric system, two more errors may occur based on biometric sample quality. The proportion of failure to enrollment is referred to as Failure to Enroll Rate (FTER). The proportion of authentication attempts in which the biometric sample cannot be captured is known as Failure to Capture Rate (FTCR) (Jain *et al.*, 2008).

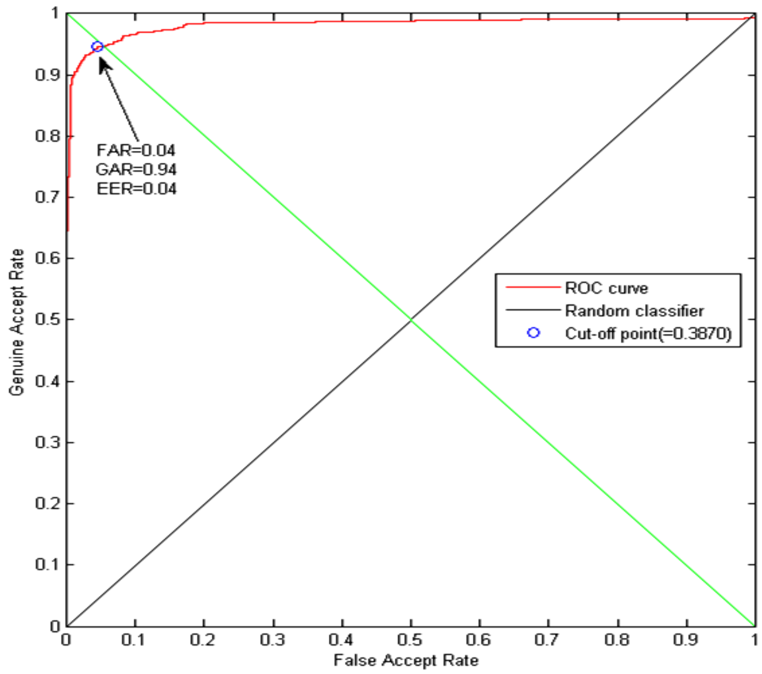


Figure 3.3 ROC for Fingerprint Matcher in MCYT Database

3.2.4 Challenges in Biometric Systems

Though biometric systems have several advantages over conventional password and token-based authentication applications, biometrics is not yet a fully solved problem. Despite the inherent advantages, unibiometric systems also have three main vulnerabilities/limitations based on accuracy, scalability and usability (Jain *et al.*, 2004b). They are listed below.

(i) *Noisy Sensor Data*: During the acquiring biometric data, noise can be produced due to defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor or dirty fingerprint), unfavorable conditions (e.g., poor illumination or failure to focus to capture face and iris images or a voice sample altered by cold).

(ii) *Non-universality*: Universality means that every user should be able to represent the respective biometric trait to the system. But it may not be possible to present meaningful biometric data by every user in the target population. For example, users having long eyelashes and those suffering from eye abnormalities or diseases like glaucoma and cataract etc. cannot provide good quality iris images for iris recognition (BBC *et al.*, 2013).

(iii) *Intra-class Variations*: Biometric samples of an individual may exhibit intra-user variations due to the user's inappropriate interaction with the sensor (e.g., incorrect facial pose or presence of facial hair), variation in the environmental conditions (e.g., illumination changes). Such intra-class variations usually increase False Rejection Rate (FRR) of a biometric system.

(iv) *Inter-user Similarity*: Inter-user similarity refers to the overlapping of biometric feature sets corresponding to multiple user or classes. The lack of uniqueness in the biometric feature set causes the False Matching Rate (FMR) of the system. The size of the target population is to be less than an upper limit.

(v) *Scalability*: Most biometric systems are confined within the assumption that the system should operate with a single technology under same environment and hence little flexible. For example, fingerprints obtained using multiple sensor technologies (e.g. Optical sensors, Solid-state sensors and Ultrasound sensors) cannot be reliably compared due to variations in sensor technology, sensing area, image resolution, distortion effects, etc. (Ross *et al*., 2006).

(vi) *Spoof attacks and Template security*: Spoof attack refers to the deliberate attempt to manipulate one's biometric template in order to avoid recognition, or generate biometric artifacts in order to take someone's identity. For example, spoof fingers have been reported (Nandakumar *et al*., 2007).

3.3 Iris Recognition

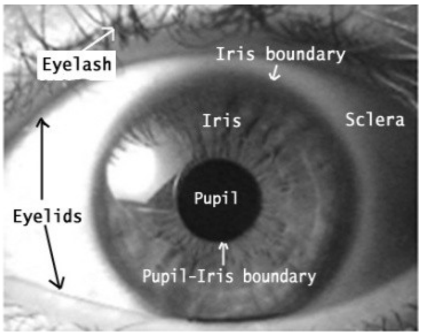
Iris is one of the most accurate and reliable biometric used presently in a biometric system. In the present work, iris pattern is used as one of the biometrics. This section provides the details of an iris recognition system.

The iris is situated in the middle layer of the eye between the lens (inner layer) and the cornea and aqueous humor (outer layer) (UTHSCSA, 2001). It consists of a pigmented fibro-vascular tissue known as stroma that forms a unique structure of valleys and ridges for each person. Due to these situation and anatomy, it provides several important characteristics that make it suitable for biometric purposes (Daugman, 1993):

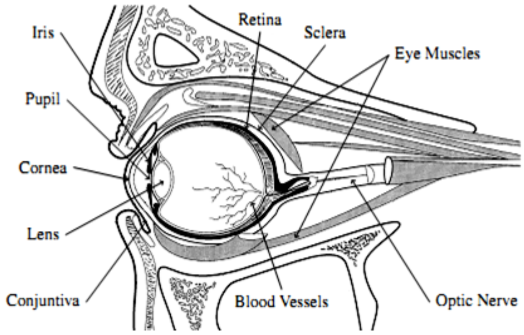
- The iris begins to form in the third month of gestation and its complex pattern is almost completely developed by the eighth month. The formation of iris depends on the initial environment of embryo, so the iris texture patterns don't correlate with genetic determination.
- It has complex and distinctive pattern such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles, and a zigzag collarette.
- The iris structure does not change during the user's lifespan, although its colour does change (Daugman, 2003), so lifetime recognition is possible for each user.
- Iris patterns possess a high degree of randomness i.e. variability of 266 degrees-of-freedom, entropy of 3.2 bits per sq-mm and uniqueness in the order of one in 10^{72} (Daugman, 2003).
- Even iris patterns of the two irises from the same person are different. These make them suitable for large scale identification applications.
- Iris is protected naturally from possible modifications or accidents as it is located between the lens and the cornea and aqueous humour. This protection makes it even more difficult to change the iris structure without risking vision damage, and therefore, avoids potential intruders from modifying iris characteristics to defraud the recognition system (Huang *et al.*, 2002).
- Iris based biometric recognition system is non- invasive to the users, which is of great importance for real-time applications (Mansield *et al.*, 2001).
- The natural dilations and contractions of iris control the light entering into the eye through the pupil. These properties can be used for liveness detection of the iris and can resist spoofing attack.
- The computational time required to perform the identification is relatively low, this makes iris recognition as a successful large scale real-time detection applications.
- The iris degrades rapidly after death. This characteristic provides an extra countermeasure against the use of eyes from a corpse to access systems.

These advantages make iris recognition to be one of the most accurate and reliable biometric for identification. A front-on view and anatomy of the human eye is shown in Figure 3.4.

In literature, many authors proposed different methods for iris recognition. In spite of their specificities, different proposals share a common structure. There are four main stages of the iris recognition system (i) *Image acquisition*, (ii) *Image segmentation,* (iii) *Feature extraction* and (iv) *Matching or Classification*. Each of these stages uses different algorithms.



(a)



(b)

Figure 3.4 Human eye (a) A Front-on View (b) Anatomy of the Human Eye (UTHSCSA, 2001)

Image acquisition deals with capturing sequence of iris images from the subject using cameras and sensors. Occluded by the eyelid and eyelash, lighting, the number of pixels on the iris are factors that affect the image quality (Kevin *et al*., 2008).

Iris segmentation involves various steps such as iris localization, determination of the inner and outer boundary of the iris and the determination of the upper and lower bound of the eyelids and its removal and normalization. The inner boundary is located between the pupil and iris boundary, the outer boundary is located between the iris and sclera boundary. Iris may be captured in different size with varying imaging distance and illumination variations. Multiple eyelashes were detected using the variance of intensity. Specular reflection regions in the eye image were also detected by setting a threshold. The segmented iris may be of different size due to the variations in the pupil and iris size. Therefore, the iris region needs to be normalized to compensate for these variations Daugman (2003) normalized of the iris image using the *rubber sheet* method in which coordinate is transformed from Cartesian to polar. In the *rubber sheet* model, each point on the iris, regardless of its size and papillary dilation, is assigns to a pair of real coordinates (r, θ), where r is on the unit interval [0, 1] and θ is an angle in [0, 2π].

Feature extraction identifies the most prominent features and the features are encoded to a pattern suitable for recognition.

Last module is the *pattern matching or classification* in which results are obtained by comparison of query iris or features with stored templates (Li *et al.*, 2003). The inter-class and intra-class variability are used as metrics for pattern classification problems.

3.3.1 Iris Databases

The biometrics research requires the analysis of human data. Obviously, it may be infeasible to perform the test of algorithms with live data (i.e. captured on-the-fly), due to many factors. Moreover, a common database is needed for fair comparison between recognition methods. Therefore, standard biometric databases become highly significance and essential factor to the development process.

The CASIA-IrisV1 database used in the present experimental work on iris recognition is a collection by the Chinese Academy of Sciences' Institute of Automation for algorithm testing. CASIA iris image database (version 1.0) (CASIA, 2006) includes 108 classes (or eyes) in a total of 756 iris images. Each iris class is composed of 7 samples taken in two sessions, three in the first session and four in the second. Sessions were taken with an interval of one month. Images are 320×280 pixels gray scale taken by a digital optical sensor designed. It is the oldest, the most known and widely used iris database by the majority of the researchers. Hence, we use this database in the present work.

3.3.2 Iris Recognition Steps

The stages of iris recognition for the present work can be summarized as follow: (i) *Iris segmentation*, where the iris is localized and isolated from iris image. (ii) *Feature extraction* – feature extraction methods, namely SVD, PCA, AFE, ICA and DWT are applied to reduce the dimension of Iris Pattern (iii) *Classification* accuracy is obtained by using BPNN and SVM with Gaussian RBF kernel in the experiment. The stages of the iris recognition system are shown in Figure 3.5. The implementation details of the present work are explained in the following sub-sections.

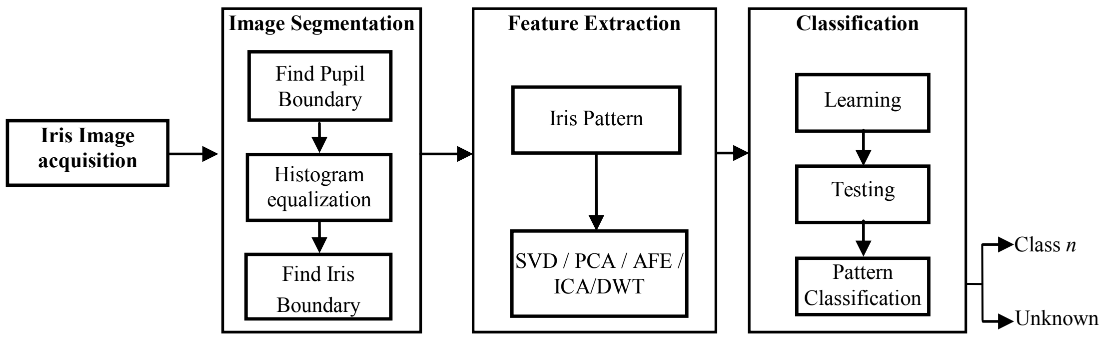


Figure 3.5 Stages of the Iris Recognition System

3.3.2.1 Iris Segmentation

Iris segmentation can be defined as the partitioning of an image into several components. It is an important stage of iris recognition because it is the basis for any further operations i.e. recognition. The main reason for the iris segmentation is twofold:

(i) To isolate only information that distinguishes individuals.

(ii) To reduce the size of pattern vector from iris image to iris patterns.

Iris segmentation is carried out in the following steps (i) Papillary boundary detection (ii) Iris outer edge detection and (iii) Iris pattern normalization. The following algorithm for image segmentation is used in the present work:

3.3.2.1.1 *Papillary Boundary Detection* (Merloti, 2004)

The eye region (containing iris, sclera and eyelids) is taken as input image. The pupil is distinguishable in input image because it has a concentration of pixels with very low level intensity (black or almost black). To find the pupil, a linear threshold (of value 70 in present work) is applied to the image using Equation (3.9)

$$g(x) = \begin{cases} f(x) > 70 : 1 \\ f(x) \leq 70 : 0 \end{cases} \tag{3.9}$$

where, f is the original image and g is the thresholded image.

By applying this, pixels with intensity greater than empirical value of 70 are converted to 1 (black) and others are assigned to 0 (white). Some parts of eyelashes satisfy Equation (3.9), but have a much smaller area than the pupil area. We can remove all small regions other than pupil by applying Equation (3.10).

$$\begin{array}{l} \textit{for each region } R \\ \quad \textit{if } AREA(R) < 2500 \\ \quad\quad \text{set all pixels of } R \text{ to } 0 \end{array} \tag{3.10}$$

Thus, pupil region is obtained. Two imaginary orthogonal lines are drawn passing through the centroid of the pupil region and the first pixel with intensity zero, from the center to the extremities is the boundaries of the binarized pupil. The output of this process is illustrated in Figure 3.6.

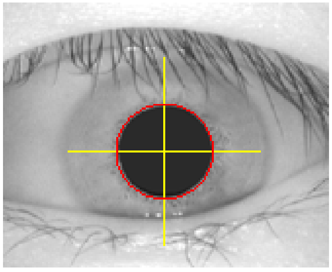


Figure 3.6 Detecting the Papillary Boundary

3.3.2.1.2 *Iris Outer Edge Detection*

The next step of iris segmentation finds the outer contour of the iris i.e. the iris-sclera boundary. The papillary and limbic boundaries of the eye are modeled as two concentric circles by many authors to reduce complexity (Kevin *et al*., 2008). Sometimes the eyelid may occlude part of the iris, as it will occur often with the Asians, and iris boundaries may not be circular. In some cases, the iris center will not match the pupil center and the strips of iris will be of different width around the pupil.

To find iris outer contour, a horizontal imaginary line is drawn across the whole image passing through the center of the pupil that found out by using algorithm in Section 3.3.2.1.1. Starting from the edges of the pupil, the signal composed by pixel intensity from the center of the pupil towards the border is analyzed on both side of pupil and tries to detect abrupt increases of intensity level. Although the edge between the iris disk and the sclera is most of the times smooth, it is known that it always has greater intensity than iris pixels. The difference of pixel intensity between the iris disk and the sclera are intensified by enhancing contrast of the image using histogram equalization (Merloti, 2004). Edge detection of the iris image $I(x, y)$ is described in Algorithm 3.1.

The time complexity is O ($m.n$) for the histogram equalization of an image of size $m \times n$, and O (m) for edge finding. Total time complexity is O ($m.n$). The iris segmented results obtained from an iris image from CASIA-IrisV1 database is shown in Figure 3.7. The algorithm is based on variation of local intensity and computes fast. While testing against iris images from CASIA-IrisV1 database, the algorithm gives a satisfactory result of 723 successes (95.64%) and 33 failure (4.36%) out of 756 images. From the analysis of the failure cases, it is noted that eyelashes were around the iris or the sclera was not as white as expected.

Algorithm 3.1: Iris Outer Edge Detection

Input: Iris Image ($I(x, y)$)

Output: Segmented Iris Image

Step 1: Draw a horizontal imaginary line passing through the center (x_{cp}, y_{cp}) of the pupil. rx is horizontal radius of the pupil.

Step 2: Apply histogram equalization on image $I(x, y)$: $G(x, y) = histeq(I(x, y))$

Step 3: Create vector $V=\{v_1, v_2, \ldots, v_w\}$ that holds pixel intensities of the imaginary row passing through the center of the pupil (x_{cp}, y_{cp}), with w being the width of enhanced image $G(x, y)$

Step 4: Create two vectors $R=\{rx_{cp} + rx, rx_{cp}+rx+1, \ldots, rw\}$ and $L=\{lx_{cp}-rx, lx_{cp}-rx-1, \ldots, r_1\}$ from the row that passes through the center of the pupil (x_{cp}, y_{cp}) of enhanced iris image $G(x, y)$ on right and left side of pupil respectively. Vector R formed by the elements of the y_{cp} line that start at the right fringe of the pupil ($rx_{cp} + rx$) and vector L by that start at the left fringe of the pupil and go all the way to the width (w) of the image.

Step 5: For both vectors R and L:

a) Create the average window vector $AvgW=\{a_1, a_2, \ldots, a_n\}$ where, $n=|L|$ or $n=|R|$. Vector $AvgW$ is subdivided in i windows of size ws. For all windows $i_1^{n/ws}$, elements $a_{i.ws-ws} \ldots a_{i.ws}$ will contain the average of that window.

In our experiments, a window size ws=10 provides satisfactory results.

b) Identify the edge point given side of the iris (vector L or R) as the first increase of values in A_j ($1 \leq j \leq n$) that exceeds a set threshold d. In our experiments, a value of d equal to 18 has shown to identify the correct location of the iris edge.

Step 6: Calculate outer radii of iris IR and IL on both sides. If $IR \leq 80$ or $150 \leq IR$ then $IR = IL$ and vice versa. We make this assumption because the iris images in CASIA-IrisV1 database has iris radius 80 to 150 (Chandra-Murty *et al.*, 2009).

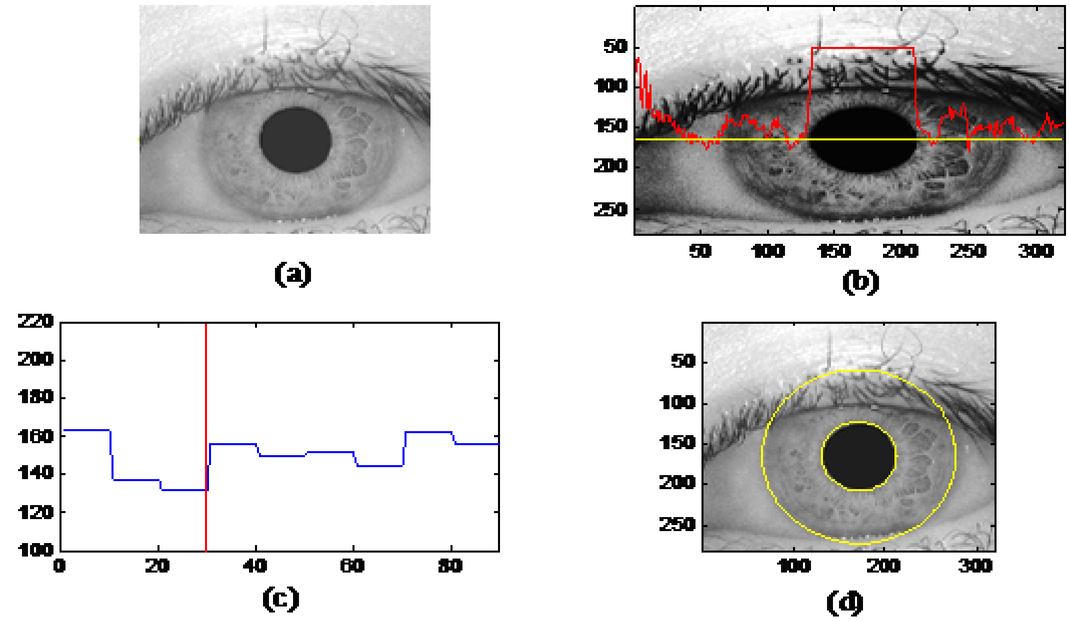


Figure 3.7 Iris Edge Detection (a) Original Image (b) Histogram Equalization Image, Horizontal Line passes through y_{cp} (Center of Pupil) of Image, Zig-zag Line shows Pixel Intensities along Horizontal Line. (c) Averaged Intensities of Pixels along Horizontal Line y_{cp} for Right Side of the Pupil (d) Iris Image with Boundaries

3.3.2.1.3 *Iris Pattern Normalization*

Last step of segmentation is formation of iris pattern by isolating only information that distinguishes individuals and also to reduce the dimensionality of the problem by extracting areas of the iris at the right and left of the pupil. By avoiding the intra-class rotation of iris images, an iris pattern ($m \times n$) is extracted from iris image (320×280) where $m \times n$ is the required dimension of iris pattern. It is a model of normalization. The overall algorithm can be summarized in Algorithm 3.2 (Merloti, 2004).

Present work takes into consideration that areas of the iris at the right and left of the pupil of the extracted data are the ones that is most visible in an iris image. The areas above and below the pupil also contain unique information, but it is very common that they are totally or partially occluded by eyelash or eyelid. This approach reduces removal of occlusion by eyelash or eyelid. Figure 3.8 shows the output of the algorithm.

Algorithm 3.2: Iris Pattern Normalization

Input: Segmented Iris Image

Output: Normalized Iris Pattern

Step 1: Retrieve pupil center and radius; iris endpoints.

Step 2: Calculate rows spacing s = pupil diameter / m.

Step 3: Calculate the first target row index = center of pupil – vertical pupil radius.

Step 4: For each side of the pupil

a) Calculate width of baseline = |iris edge of current side – pupil edge of current side|.

b) Starting from the top of the pupil to the bottom with a spacing of s, perform the following steps for all baselines:

i) By using the equation of circle, find the location of pixel (x, y) that resides in the intersection of current baseline and circle centered at pupil center with radius equal to pupil horizontal radius.

ii) Vector B is appended with $n/2$ pixels that are under the baseline. Pixel intensity is calculated by taking average mask of 3×3 pixels.

iii) Append vector B to iris pattern matrix of respective side of the iris.

Step 5: The two halves of iris pattern matrices are merged side by side into one final iris pattern matrix.

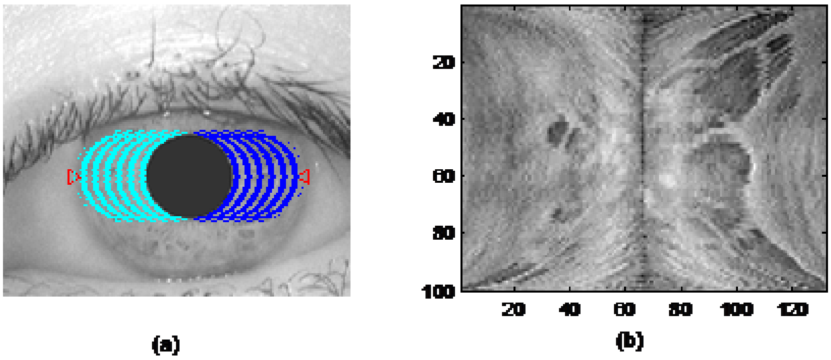


Figure 3.8 Iris Pattern (a) Iris with Iris Pattern (b) Isolated Iris Pattern

3.3.2.2 Feature Extraction

Automatic Pattern Recognition and Classification faces one very difficult problem of dimensionality reduction. Generally sensory systems are constantly capturing a huge amount of information, and if not summarized, it would bottleneck the whole processing capacity i.e. these signal are highly redundant. Mathematical and statistical methods (such as ICA, PCA, Wavelets and Fourier Transforms) may be applied to reduce the dimensionality problem.

Size of iris images in CASIA-IrisV1 database is 320×280 pixels and one image is equivalent to a vector with 89,600 elements. Classification of these vectors needs too high computing power, and still may not guarantee satisfactory results. During iris segmentation, dimension reduction was already achieved by simply isolating the area of the iris image that contains the characteristic information about an individual. For instance, the number of elements in the input vector is decreased from 89,600 (320×280 image) to 1600 (40×40 images), a 98% reduction in size. Still a large percentage of redundant information is contained in iris patterns. The problem of dimensionality reduction is also known as feature extraction. From a set of *n* features, a set of *m* most prominent features that leads to dimension reduction as well as to minimum classification error is selected. Single Value Decomposition (SVD), Principal Component Analysis (PCA), Automatic Feature Extraction (AFE), Independent Component Analysis (ICA) and Discrete Wavelet Transform (DWT) are applied to iris patterns for this purpose.

3.3.2.2.1 *Single Value Decomposition* (SVD)

Single Value Decomposition is a powerful technique in matrix computation and analysis and noise signal filtering etc. The key properties of SVD are its relation to the rank of a matrix and its ability to approximate matrices of a given rank. In the present work, SVD is employed as a noise signal filter to reduce dimension of iris pattern.

The basic operation of SVD relies on the factorization of an $m \times n$ matrix ($m \geq n$) into three other matrices on the form of Equation (3.11) (Akritas *et al.*, 2006):

$$A = USV^T \tag{3.11}$$

where, the superscript "*T*" denotes matrix transpose. *U* is an $m \times m$ orthogonal matrix, *V* is an $n \times n$ orthogonal matrix and *S* is an $m \times n$ diagonal matrix with $s_{ij} = 0$ if $i \neq j$ and $s_{ii} \geq s_{i+1\,i+1}$. The columns of *V* are right singular vectors and the columns of *U* are left singular vectors. Either the singular vectors of the singular values (or both) are called principle components. SVD reduces the dimension of input pattern from $m \times n$ to only a vector of *n* elements. The first *n* elements contain substantial information, and we can crop the vector tail without significant loss of generality. This property is very useful for the present work.

3.3.2.2.2 *Principal Component Analysis* (PCA)

PCA is a useful statistical technique that aims to find a linear orthogonal transformation $v = Wu$ (where, u is the observation vector) such that the maximum amount of variance possible by n linearly transformed components can be retained. Mathematically, the method of studying the eigenvalue decomposition of the covariance matrix is known as Principal Components Analysis (PCA) (Jolliffe, 2002).

Let A be a square symmetric $n \times n$ matrix, and consider its eigenvalue decomposition, then A is decomposed using Equation (3.12).

$$A = P \Lambda P^T = \sum_{i=1}^{n} \lambda_i p_i p_i^T \tag{3.12}$$

where, P is an orthogonal matrix with columns $p_1, p_2, \ldots, p_n$ and Λ is a diagonal matrix with eigenvalues $\lambda_1, \lambda_2, \cdots, \lambda_n$ which are sorted in descending order. p_i is the eigenvector corresponding to eigenvalue λ_i.

A simple approach to PCA is to use singular value decomposition (SVD). Let n m-dimensional vectors X_j is aligned in the data matrix X ($m \times n$) and C is the covariance matrix of X. Then, SVD (C) will be the PCA of X.

3.3.2.2.3 *Automatic Feature Extraction* (AFE)

Automatic Feature Extraction is based on Nyström approximation method. Nyström method is used to approximations based on the numerical integration in integral equations. This method is commonly used with uniform sampling without replacement, though non-uniform distributions have been used to theoretically analyze the Nyström method (Drineas *et al*., 2005). It is used in a variety of large-scale learning applications, in particular in dimensionality reduction and image segmentation.

Consider the eigenfunction problem given by Equation (3.13).

$$\int_D K(t.s)\Phi(s)ds = \lambda \Phi(t), t \in D \tag{3.13}$$

where, $K(t,s)$ is kernel, Φ eigenvector, Let $D = [a, b] \subset \Re$. All points in D are interpolated with the quadrature rule governed by Equation (3.14).

$$\int_a^b y(s)ds = \sum_{j=1}^{n} w_j y(s_j) \tag{3.14}$$

where, $\{w_j\}$ are the weights and $\{s_j\}$ are the quadrature points. Then (3.13) becomes Equation (3.15).

$$\int_D K(t.s)\Phi(s)ds \approx \sum_{j=1}^{n} w_j k(x,s_j)\widetilde{\Phi}(s_j) \tag{3.15}$$

that leads to an eigenvalue problem of the form defined by Equation (3.16).

$$\sum_{j=1}^{n} w_j k(x,s_j)\widetilde{\Phi}(s_j) = \widetilde{\lambda}\widetilde{\Phi}(x) \tag{3.16}$$

The approximate eigenvalue $\widetilde{\lambda}$ and approximate eigenfuction $\widetilde{\Phi}$ for $x = x_i$, $i = 1, 2, \ldots, n$ can be found out with the Nyström method as in Equation (3.17)

$$\sum_{j=1}^{n} w_j k(x,s_j)\widetilde{\Phi}(s_j) = \widetilde{\lambda}\widetilde{\Phi}(x_i) \tag{3.17}$$

that depends on the set $\{x_i\}$ of Nyström points. If $\widetilde{\lambda}_m \neq 0$, the exact eigenvectors $\widetilde{\Phi}_m$ on the Nyström points can be extended to a function $\overline{\Phi}$ given by Equation (3.18)

$$\overline{\Phi}_m(x) = \frac{1}{\lambda_m}\sum_{j=1}^{n} w_j k(x,s_j)\widetilde{\Phi}(s_j) \tag{3.18}$$

The function $\overline{\Phi}_m(x)$ is the Nyström extension of the eigenvector $\widetilde{\Phi}_m$, and can be calculated for a (small) number n of points in the (large) full domain D.

3.3.2.2.4 *Independent Component Analysis* (ICA)

Independent Component Analysis (ICA) is a statistical technique that represents a multidimensional random vector as a linear combination of non-gaussian random variables ("independent components") that are as independent as possible. Alternatively, ICA is a non-gaussian version of factor analysis (Hyvärinen *et al*., 2000). It aims to find a set of independent sources that capture the underlying randomness of the observed signals.

Mathematically, it is convenient to use matrix notation. Let (mixed) random vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_m)$ and likewise random (source) vector $\boldsymbol{s} = (s_1, s_2, \ldots, s_n)$. Let A be a (mixed) matrix with elements a_{ij}, $i = 1, 2, ..., m, j = 1, 2, ..., n$, then, $\boldsymbol{s}$ can be decomposed as Equation (3.19).

$$s = Ax \tag{3.19}$$

where, maximally independent components ($x_1, x_2, \ldots, x_m$) measured by some function F ($s_1, s_2, \ldots, s_n$) of independence. The statistical model in (3.19) is called independent component analysis, or ICA model.

The pre-processing of the input pattern in the present work is based on FastICA (2005). ICA depends on the correlation information between patterns, and to obtain reasonable results, we need to process the full dataset in order to obtain the Separating and the Mixing matrix, as well as the independent components. Also, as reduction is done internally in the algorithm, we need to decide on the final number of dimensions prior to processing. Some special arrangements are also necessary in order to obtain the independent components. For example, given the input image $I_{m\times n}$ and the data set D_l of L cases, the usual way to arrange pixels of this image is to concatenate m rows of n columns into only one row of ($m\times n$) columns. The training set would have in this case L rows and $m\times n$ columns. For supervised learning, there is also one additional column labeling the case, making the total length of the pattern vector as $m\times n+1$. The *FastICA* algorithm requires transposing the data set so it ends up with L columns and $m\times n$ rows.

3.3.2.2.5 *Discrete Wavelet Transform* (DWT)

Wavelet transform can be used to extract features from normalized iris template. In the present work, 'db2' wavelet filter has been used (Matlab 2012). The conceptual process of obtaining the feature vectors using wavelet transform (upto level 3) is shown in Figure 3.9. Here, L and H mean the low-pass and the high-pass filter, respectively, and HH indicates that the high-pass filter is applied to the signals of both axes. In the present work, Wavelet transform is applied up to four levels to the normalized iris template (240×20 pixels) in order to get the 4×17 sub-images.

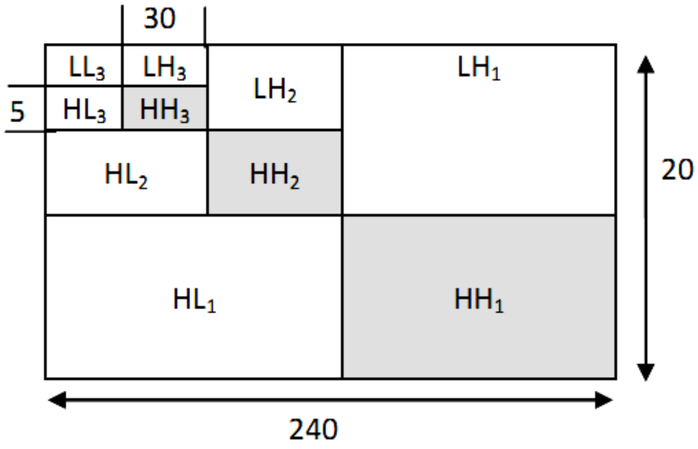


Figure 3.9 Wavelet Decomposition

3.3.2.3 Classification

Pattern classification is the process of assigning a class label to an object, a physical process or an event based on a set of measurements called attributes or features (Heijden *et al.*, 2004). In this work, two classifiers namely Feedforward Backpropagation Neural Network (BPNN) and Support Vector Machines (SVM) with Radial Basis Function (RBF) kernel are employed to classify the *IrisPattern* with different dimensions and a comparative study is made. Brief notes on the two classifiers are given in the following subsections.

3.3.2.3.1 *Backpropagation Neural Network* (BPNN)

Artificial neural networks (ANNs or simply NNs) provide a range of powerful techniques for solving problems in pattern recognition, data analysis and control. The basic computational units of an ANN are known as neurons, nodes that serve as inputs, outputs or internal processing units. These neurons communicate and pass signals among themselves using synapses (like human nerves), which are modulated by weight parameters (Bishop, 2006). Neural network is used to classify the iris pattern obtained after feature extraction of the iris image. The problem in hand is supervised network training and classification. “Feedforward Backpropagation of Error” among several network models is chosen because it is well suit for supervised problems. In this model, input vectors and the corresponding target vectors are used to train a network until it can approximate a function, associate input vectors with specific output vectors, or classify input vectors in an appropriate way as defined by user.

The 3-layer architecture which employed in the present work is shown in Figure 3.10. The input layer contains as much neurons as the dimension of the feature vector that characterizes the iris pattern. As a rule of thumb, number of neurons in the hidden layer should be approximately double of the neurons in the input layer. That usually obtains good classification results. The number of neurons in the output layer is equal to the number of classes to be recognized. For example, if it is to classify iris images into 50 classes, there should have 50 output neurons in the network.

When the network is trained in supervised mode, a target vector is also presented to the network. This target vector T has every element set to zero, except on the position of the target class that will be set to 1. The idea behind this design decision is that for each input pattern X presented to the network, an output vector Y which has number of elements equal to that of output neurons is produced. Each output neuron implements a squashing function that produces a real number in the range [0, 1]. To determine which class is being indicated by the network, we select the maximum number in Y and set it to 1, while setting all other elements to zero. The element set to 1 indicates the classification of that input pattern.

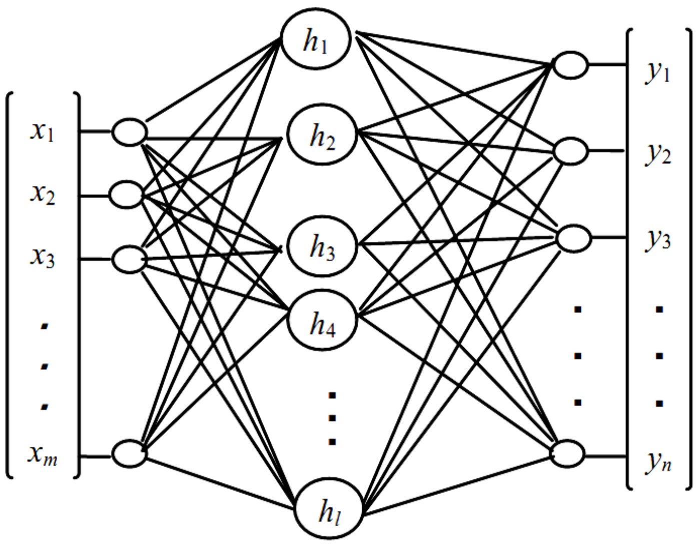


Figure 3.10 BPNN (m ranges from 3 to 40, l ranges from 6 to 80 and n ranges from 3 to 50)

3.3.2.3.2 *Support Vector Machines* (SVM)

The foundations of SVM have been developed by Vapnik in 1995 (Bishop, 2006). SVMs have been proposed for pattern recognition in a wide range of applications by its ability for learning from experimental data, and its effectiveness over some other conventional parametric classifiers. In SVM, the objective function is convex, and so any local solution is also a global optimum although nonlinearly optimize during the training. Basically, SVM is a statistical learning machine based on a structural risk minimization technique and its objective is to minimize the upper bound of the generalization errors consisting of the sum of training errors and a confidence interval (Burges, 1998). The SVM method was originally developed as a linear classifier to find the separating hyperplane with the largest margin. The input (non-linear) space is transformed to a higher dimensional feature space by using a non-linear feature mapping and resulted space is linearly separable by a hyperplane. This extension is performed using a non-linear function base on some kernel. There are three common kernels used for the non-linear feature mapping *viz*. Polynomial, Radial Basis Function, and Sigmoid kernels.

The principle of data separation using SVM is demonstrated on a simplified linear example in Figure 3.11.

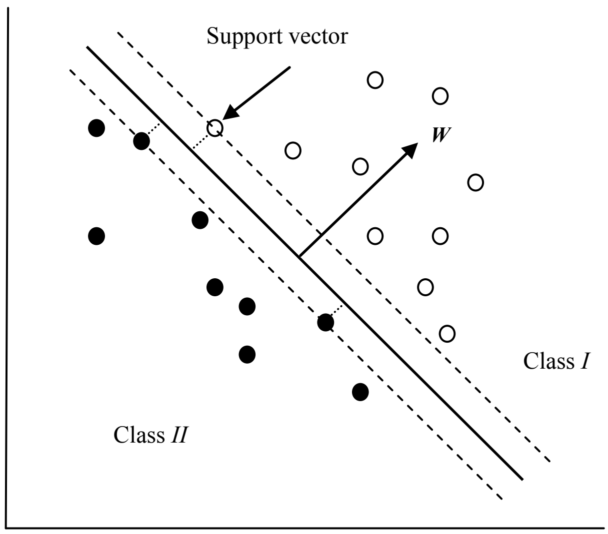


Figure 3.11 Data Separation using SVM

A linear classifier is defined by a hyperplane's normal vector W and an offset b (Müller *et al*., 2001) as given by Equation (3.20).

$$(W.x)+b=0 \tag{3.20}$$

where, $b/|W|$ is the perpendicular distance from the hyperplane to the origin.

The distance of the decision surface (or hyperplane) (solid line in Figure 3.11) from the nearest appearance of the individual data sets should be as large as possible. The dashed lines that are parallel with the hyperplane contain support vectors. The margin is defined as the minimal distance of a sample to the decision surface. The support vectors are given by Equation (3.21).

$$w=\sum_{i=1}^{N} v_i x_i \tag{3.21}$$

For a linearly separable data, a matrix H is created by dot product of input variables as given by Equation (3.22).

$$H_{ij} = y_i y_j k\left(x_i . x_j\right) \tag{3.22}$$

where, $y_i \in \{1, -1\}$; x_i, x_j are data points from the original space and $k(x_i. x_j)$ is an example family of functions called *Kernel Functions*.

The kernel functions can be recast into a higher dimensionality space by some potentially non-linear feature mapping function $x \rightarrow \Phi(x)$. Kernel trick is useful in many classification problems that are not linearly separable in the space of the inputs x, which might be in a higher dimensionality feature space by using a suitable mapping $x \rightarrow \Phi(x)$.

In the present work, Gaussian Radial Basis Function (RBF) kernel is used. RBF kernel is given by Equation (3.23).

$$k(x_i . x_j)=\exp(-|x_i - x_j|^2 /c), \qquad c>0 \tag{3.23}$$

It is important to find optimal parameter c because different parameter setups are suitable for solving different problems. $c > 0$ is the penalty parameter of the error term used in determination of a separating hyperplane with the maximal margin by SVM.

Classification of the test sample **x** is then performed by using Equation (3.24).

$$y = sign\left(\sum_{i=1}^{N} \alpha_i v_i K(x_i, x) + b\right) \tag{3.24}$$

where, N is the training size, v_i is the class label, α_i a Lagrangian multiplier, the elements x_i for which $\alpha_i > 0$ are the support vectors, and $K(x_i, x)$ is the function kernel (i.e. radial basis function for the present work).

3.3.3 Comparison of Features Extraction and Classification Methods

At first stage of the iris recognition, the grayscale intensity based algorithm is applied for localization of irises. Experiments are conducted in MATLAB 7.11 environment. The average time for the detection of inner and outer boundary of the iris images was 0.13s. The accuracy rate was 99.40% for papillary boundary segmentation and 95.64% for iris outer edge segmentation.

In classification stage, the iris patterns are classified using BPNN and SVM with RBF kernel. The network design parameters of BPNN for the present experiment are summarized as:

Training function	: *traingda*
Initial learning rate	: 0.15
Learning rate increment	: 1.05
Epochs	: 50,000
Error goal	: 0.0000000001
Minimum gradient	: 0.0000000001

Iris pattern of 50 persons/classes (i.e. 350 images) from CASIA-IrisV1 database is used in this experiment. Iris pattern is 40×40 pixels with an average mask of 3×3 pixels. The outputs of the neural network are classes of iris patterns. Each class characterizes a person's iris. Five instances of each class is used in training and the remaining two instances of each class form the testing set for testing propose.

The performance of the different reduction methods with different dimensions and different number of classes are analysed using BPNN and SVM with RBF. The recognition method that generates the best classification performance is ranked the best. The best classification accuracy rate (%) of ten times execution is shown in Table 3.2 with four different dimensions (i.e. 3D, 10D, 20D and 40D) with twelve different classes by using both classifiers.

Table 3.2 Comparison of the Classification Rate (%) of BPNN and SVM with RBF

Extraction Methods	**Dimen-sion**	**Classi-fier**	**No. of Class**											
			3	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**20**	**30**	**40**	**50**
SVD	3D	BPNN	100	100	100	91.67	89.58	78.57	66.67	65	45	25	15	17
		SVM	100	87.5	40	33.33	50	43.75	50	55	30	18.33	17.5	21
	10D	BPNN	100	100	100	75	78.5	73.75	68.89	65	52.5	25	15	16
		SVM	100	62.5	40	33.33	28.57	43.75	44.44	45	37.5	30	21.25	21
	20D	BPNN	100	100	100	91.67	78.57	62.5	66.67	60	42.5	16.67	11.25	7
		SVM	100	75	60	41.67	42.86	56.25	48.89	50	40	31.67	20	16
	40D	BPNN	100	100	90	75	78.6	75	77.8	75	50	10	8.7	5
		SVM	83.33	75	60	41.67	57.14	62.5	50	50	43.5	36.67	31.25	26
PCA	3D	BPNN	66.67	75	60	50	50	62.5	61.11	70	22.5	21.67	7.5	15
		SVM	66.67	75	60	50	42.86	50	55.56	45	32.5	28.33	26.25	27
	10D	BPNN	100	100	100	100	92.85	100	88.88	95	90	35	21.2	19
		SVM	100	100	100	100	100	87.5	85.7	85	87.5	81.67	75	67
	20D	BPNN	100	100	100	100	100	100	100	100	90	83	30	24
		SVM	100	100	100	100	100	100	100	100	95	91.67	93.75	90
	40D	BPNN	100	100	100	100	100	100	100	100	97.5	75	22.5	19
		SVM	100	100	100	100	100	100	100	100	100	100	98.75	95
AFE	3D	BPNN	83.3	75	80	66.67	78.57	68.75	55.56	45	40	21.67	12.5	19
		SVM	50	50	40	50	42.86	43.75	44.44	50	25	20	16.25	12
	10D	BPNN	100	100	90	91.67	71.43	68.75	61.11	80	45	20	20	14
		SVM	100	100	90	83.33	71.43	75	88.89	90	52.5	45	52.5	47
	20D	BPNN	66.7	87.5	90	100	88.57	93.75	88.89	90	57.5	23.3	20	18
		SVM	83.33	87.5	90	83.33	85.71	75	77.78	75	70	55	55	62
	40D	BPNN	83.33	100	100	91.67	78.57	81.25	83.33	80	70	63.33	27.5	21
		SVM	100	87.5	80	66.67	71.43	75	77.78	80	77.5	66.67	72.5	74
ICA	3D	BPNN	83	87.5	100	83.33	71.42	81.25	77.77	85	60	40.3	25	20
		SVM	83.33	87.5	60	66.67	57.14	56.32	61.11	60	37.5	33.33	37.5	27
	10D	BPNN	100	100	90	91.67	78.57	81.25	77.78	80	72	75	72.5	62
		SVM	100	75	90	83.33	78.57	81.25	77.78	70	62.5	63.33	60	55
	20D	BPNN	100	100	100	100	92.85	87.5	94.44	95	90	91.67	92.5	91
		SVM	100	100	100	100	100	100	100	100	90	88.33	90	89
	40D	BPNN	100	100	100	100	100	100	100	100	100	96.67	95.75	94
		SVM	100	100	100	100	100	100	100	100	100	**98.33**	**98.75**	**96**
DWT	3D	BPNN	83.33	75.0	60.0	50.0	50.0	25.0	27.78	45.0	27.5	18.33	8.75	10.0
		SVM	66.67	87.5	70.0	41.67	35.71	31.25	38.89	30.0	25.0	20.0	17.5	14.0
	10D	BPNN	100	100	90.0	83.33	71.43	56.25	55.56	65.0	57.50	16.67	17.5	15.0
		SVM	100	100	80	58.33	57.14	50.0	50.0	65.0	42.50	31.67	30.0	27.0
	20D	BPNN	100	87.5	80.0	58.33	57.14	68.75	72.22	70.0	60.0	55.0	37.5	19.0
		SVM	83.33	87.5	80.0	83.33	64.29	68.75	77.78	70.0	57.5	45.0	40.0	33.0
	40D	BPNN	83.0	87.5	100	83.33	57.14	78.57	68.75	55.56	45.0	40.0	43.75	37.0
		SVM	83.33	87.5	80.0	58.33	57.14	62.50	72.22	65.0	55.0	41.67	40.0	40.0

The target classes for classification were varied from 3 to 50. From the experimental result, it is observed that higher the number of classes decreases the correct classification rate in both cases (except some cases). Performance of BPNN with SVD, PCA, AFE and DWT is poor in higher number of classes (i.e. more than 20) therefore these combinations perhaps cannot be applied for classes above 20. And also BPNN shows its highest classification results only with ICA except 3D. On the other hand, SVM with RBF performs better with PCA or ICA (except some cases) than with SVD, AFE or DWT and it also works better than BPNN in higher number of classes. ICA is the best feature extraction method among the four methods for both BPNN and SVM with RBF for the considered dataset.

The time taken in classification (in sec) by the two classifiers with four different extraction methods at different dimensions and classes is shown in Table 3.3. Experimental observations show that BPNN can classify faster with PCA or ICA than with SVD, AFE or DWT. SVM with RBF takes longer time in classification for higher number of classes than at lower number of classes in all extraction methods and can classify faster than BPNN. Figure 3.12 shows classification rate (%) of the five feature extraction methods at 40D and 50 Classes.

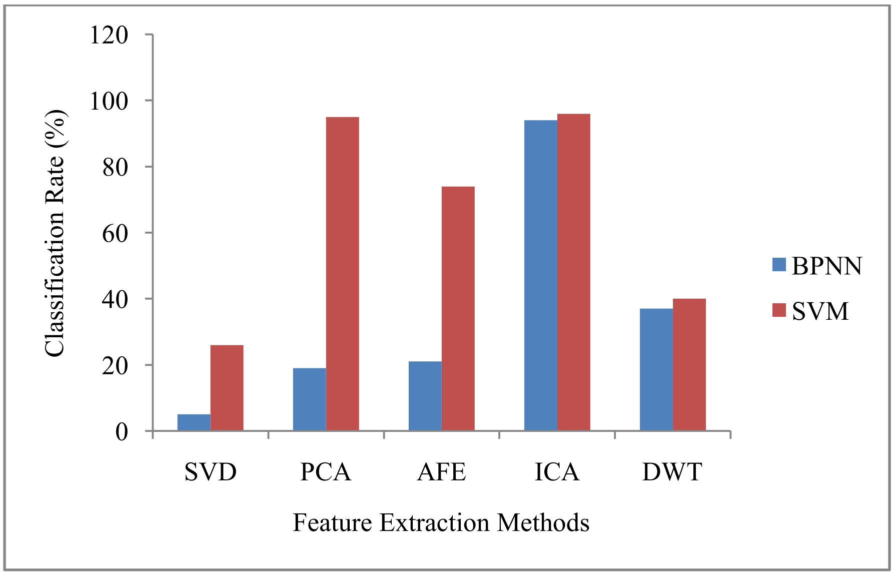


Figure 3.12 Classification Rate (%) of the Feature Extraction Methods at 40D and 50 Classes

Table 3.3 Classification Time Taken (in sec) by BPNN and SVM with RBF

Extraction Methods	**Dimen-sion**	**Classi-fier**	**No. of Class**											
			3	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**20**	**30**	**40**	**50**
SVD	3D	BPNN	16.88	32.21	60.8	83.85	225.4	226.2	401.2	560.9	479.7	13.41	16.49	13.61
		SVM	0.95	1.29	1.42	1.87	2.25	2.64	2.98	3.06	6.68	10.82	15.89	22.0
	10D	BPNN	224.1	28.9	278.6	26.5	211. 7	362.2	412.6	513.8	163.5	258.5	14.8	12.5
		SVM	1.25	1.31	3.86	1.93	2.29	2.68	3	4.79	10.14	15.72	20.14	24.78
	20D	BPNN	276.5	234.9	207	280.1	279. 9	297	291.9	313.5	373.2	11.9	11.03	11.85
		SVM	1.31	1.29	1.98	1.90	2.28	2.65	3.07	3.98	8.71	13.70	19.37	25.45
	40D	BPNN	272.6	280.1	279.3	306	314.5	325.3	322.5	324.9	363.5	123.4	16.73	15.55
		SVM	1.12	2.78	2.14	1.86	2.23	2.67	3.06	4.23	9.31	15.08	21.52	29.14
PCA	3D	BPNN	4.38	3.44	12.33	30.21	47.74	44.82	52.61	102.5	13.20	13.44	15.92	17.60
		SVM	1.26	1.26	2.15	1.92	2.25	2.57	2.96	4.59	9.39	14.67	19.95	23.92
	10D	BPNN	3.29	3.38	5.75	16.33	39.33	45.27	52.72	56.65	321.4	33.50	18.46	23.13
		SVM	1.20	1.26	1.90	1.95	2.31	2.65	3.10	3.90	8.46	13.15	18.51	24.5
	20D	BPNN	3.53	3.59	4.63	5.8	12.05	13.99	14.73	12.61	53.99	52.32	19.66	20.78
		SVM	1.15	1.35	2.06	2.07	2.37	2.78	3.06	4.59	8.61	12.74	16.89	20.84
	40D	BPNN	2.42	3.47	3.34	4.54	8.78	7.39	10.98	10.66	19.06	142.2	30.69	16.03
		SVM	0.95	1.40	1.5	2.17	2.53	2.90	3.29	3.37	7.64	12.98	19.39	28.89
AFE	3D	BPNN	3.2	5.49	210.6	489	494.9	498.4	555.2	512.9	634.7	17.31	15.62	17.26
		SVM	1.18	1.28	1.98	1.93	2.26	2.62	3.07	4.12	8.79	13.71	15.84	19.43
	10D	BPNN	2.31	2.78	7.49	52.36	92.65	216.9	95.26	203.7	28.16	25.63	15.56	26.52
		SVM	1.01	1.34	1.60	1.96	2.34	2.76	3.09	3.31	7	11.34	15.95	22.43
	20D	BPNN	3.34	5.19	17.63	22.88	43.37	58.89	58.06	56.52	431	8.85	14.4	16.14
		SVM	1.03	1.37	1.70	1.97	2.29	2.72	3.14	3.59	8.36	12.91	19.09	23.84
	40D	BPNN	2.40	2.90	9.59	13.06	29.14	26.73	26.73	25.41	237.2	540.7	19.62	15.74
		SVM	2.53	1.34	1.76	2.09	2.45	2.87	3.31	3.43	7.54	12.95	19	26.87
ICA	3D	BPNN	2.08	3.58	4.24	5.06	25.58	25.38	37.64	142.4	575.7	10.12	12.08	22.71
		SVM	0.89	1.32	1.51	1.93	2.26	2.70	3.11	3.14	6.84	11.25	16.26	22.14
	10D	BPNN	2.63	2.19	3.07	2.76	10.26	13.25	15.87	16.83	31.43	66.8	82.47	21.3
		SVM	1.25	1.34	2.08	2.0	2.37	2.72	3.078	4.17	8.34	12.53	16.22	20.45
	20D	BPNN	2.22	2.25	2.78	2.92	4.25	6.13	6.01	6.89	10.17	17.41	24.74	36.12
		SVM	1.22	1.26	2.29	2.0	2.36	2.73	3.09	4.12	8.72	13.89	19.51	25.5
	40D	BPNN	1.98	2.17	2.14	2.20	2.39	2.61	2.86	2.94	5.45	8.81	14.09	24.24
		SVM	1.29	1.34	2.22	2.01	2.44	2.75	3.11	4.33	8.99	14.92	23.15	28.70
DWT	3D	BPNN	0.020	**0.017**	**0.016**	**0.018**	**0.017**	**0.020**	**0.017**	0.023	**0.019**	**0.019**	0.020	0.020
		SVM	0.406	0.537	0.665	0.95	0.926	1.072	1.255	1.473	3.11	4.797	6.847	8.848
	10D	BPNN	**0.018**	0.018	0.016	0.017	0.023	0.017	**0.017**	0.020	0.024	0.021	0.022	0.020
		SVM	0.397	0.543	0.726	0.785	0.932	1.095	1.284	1.505	3.17	4.934	6.941	9.5
	20D	BPNN	0.019	0.019	0.022	0.024	0.0195	0.024	0.024	0.023	0.022	0.021	0.026	**0.019**
		SVM	0.391	0.59	0.712	0.931	1.034	1.147	1.327	1.445	3.353	5.068	7.287	9.475
	40D	BPNN	0.024	0.023	0.021	0.020	0.019	0.024	0.018	**0.019**	0.019	0.022	**0.019**	0.026
		SVM	0.421	0.541	0.695	0.902	0.991	1.22	1.434	1.454	3.529	5.865	8.714	11.58

3.4 Biometric Template Security

Security deals with freedom from risk or danger. In computer system, security is the ability of a system to protect system resources and information with respect to confidentiality and integrity. Since biometrics system uses individual's behavioral and biological characteristics for recognition, this system is relatively more convenient to users and higher in security aspect. However, a stronger lock does not necessarily mean higher security because many possible means may still be available to break into the facility, e.g. break the door or windows, make a large hole in the wall, or kidnap the owner at gunpoint. Thus, irrespective of the installed security system, no system is absolutely secure or foolproof.

In literature, vulnerabilities in biometric system are taken into account from different viewpoints. Ratha *et al*. (2001b) and Bolle *et al*. (2002) have identified a number of *points of attack* based to the system architectural. Jain *et al*. (2008a) used a compact *fishbone* model to summarize the biometric system vulnerabilities (Figure 3.13). This model captures the relationship between causes and effects of failures. According to this model, the main causes for biometric system failure are:

(i) *Intrinsic*: The inherent limitation in information content, and the representation/matching schemes may lead to erroneous acceptance of an intruder

(ii) *Non-secure infrastructure*: System functionality can be disabled by a denial-of-service attack

(iii) *Administrative abuse*: The integrity of the system can be abused by compromising the administrative capability and

(iv) *Biometric overtness*: If the biometric system is not capable of liveliness of biometric trait, an artificial spoofed trait could make fool the system.

The two effects of biometric system failure are:

(i) *Denial-of-service*: It refers to the scenario where an authorized user is prevented in assessing the entitled service(s). It can be result from sabotage the infrastructure by an adversary; intrinsic failures like false reject, failure to capture and failure to acquire; administrative abuse such as modification of templates or the operating parameters (e.g. matching threshold) of the biometric system.

(ii) *Intrusion*: It refers to an unauthorized user gaining illegitimate access to the system. As a result, the hacker may allow access, and modify privileged data (e.g., unauthorized access to personal information) and security threats (e.g. terrorists crossing borders).

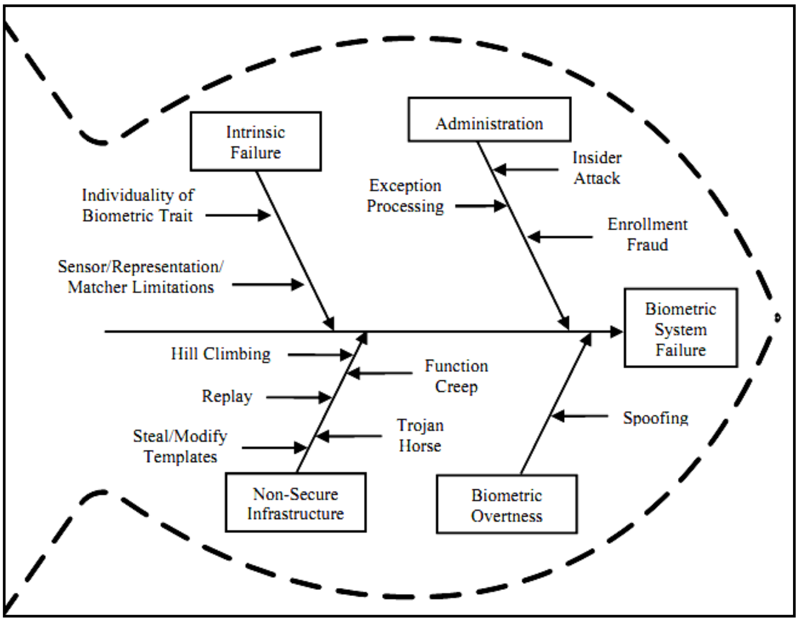


Figure 3.13 *Fishbone* Model of Biometric System (Jain *et al*., 2008a)

Intrinsic failures are also known as zero-effort attack and can occur even when there is no explicit effort by an adversary to circumvent the system. So this type of failure poses a serious threat if the false accept and false reject probabilities are high. Adversary attacks are characterized by an impostor intentionally stages to impersonate an authorized user and probably more dangerous than the zero-effort attacks. An adversary success depends on the loopholes in the system design and the availability of adequate computational and other resources to the adversary.

Security of the stored biometric template in biometric system database is one of the most important issues. Stolen biometric templates can be used to compromise the security of the system in the following different ways:

(i) A template can be replaced by an impostors' template to gain unauthorized access.

(ii) The stolen template can be replayed to the matcher to gain unauthorized access.

(iii) A physical spoof can be created from the template (Adler, 2003) to gain unauthorized access to the system (as well as other systems which use the same biometric trait) and

(iv) The Stolen templates can be used for cross-matching across different application databases to covertly track a person without his/her consent.

Unlike passwords, it is impossible for a genuine user to revoke his biometric identifiers and switch to another set of uncompromised identifiers. Due to this irretrievable nature of biometric data, an attack against the stored templates constitutes a major security and privacy peril in a biometric system. If the biometric identity of a person is compromised once, his right to privacy and secrecy is lost throughout his life. Hence, strategies to protect biometric template and to ensure an individual's privacy are urgently needed.

An ideal biometric template protection technique should possess the following properties (Maltoni *et al*., 2009):

(i) *Diversity*: The secure template must not allow cross-matching across different databases/applications, thereby ensuring the user's privacy.

(ii) *Revocability*: It should be straightforward to revoke a compromised template and reissue a new template based on the same biometric data.

(iii) *Security*: It must be computationally infeasible to reproduce the original template from the protected template. This property prevents an imposter from creating a physical spoof of the biometric trait from a stolen template.

(iv) *Performance*: The biometric template protection scheme should not substantially degrade the system recognition performance (FAR and FRR) of the biometric system.

From the practical point of view, it is hard to design a biometric template protection scheme that satisfies simultaneously all the above requirements which is to be an ideal. It becomes a major challenge in a biometric system. Due to the intra-variance nature of biometric sample, it is impossible to employ standard encryption techniques like RSA, AES as encryption/decryption tool in biometric domain.

The template protection schemes available in literature can be classified into four categories, *viz*. (i) *Biometric cryptosystem* (ii) *Feature transformation* (iii) *Data Hiding* and (iv) *Hybrid* approach (Figure 3.14).

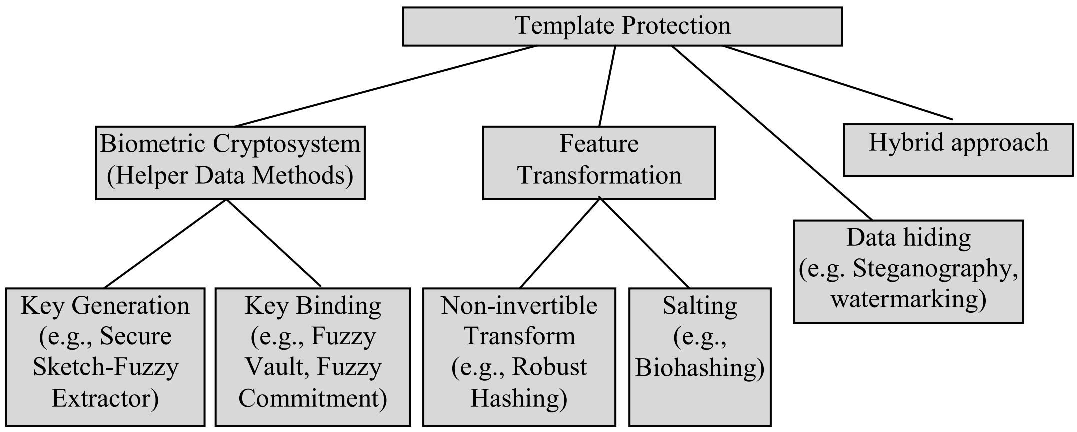


Figure 3.14 Classification of Template Protection Schemes (adopted form Jain *et al*., 2008a)

3.4.1 Biometric Cryptosystems

Biometric cryptosystems is a technique in which either securing a cryptographic key using biometric features or directly generating a cryptographic key from biometric features (Soutar *et al*., 1998a, b, Uludag *et al*., 2004). It can also be used as a template protection scheme. In these approaches, some public information (which is known as *helper data*) about the biometric template is stored and hence, this technique is also known as *helper data-based* methods (Jain *et al*., 2008a). Key matching is performed indirectly by verifying the validity of the extracted key and the output of an authentication process is either a key or a failure message. Some Error correction coding techniques are typically used to handle intra-user variations. Since the verification of keys represents a biometric comparison in encrypted domain, biometric cryptosystems can be employed as a means of biometric template protection, in addition to providing biometric-dependent key-release. Based on how helper data are derived, biometric cryptosystems are classified as *key-binding* or *key-generation* systems. Both schemes are illustrated in Figure 3.15.

3.4.1.1 Key-binding Scheme

In this scheme, the helper data are obtained by binding biometric template with a key (which is independent of the biometric template). As a result of the binding process a fusion of the secret key and the biometric template is stored as helper data. During authentication, the key is regenerated from the helper data with the help of an appropriate key retrieval algorithm (Jain *et al*., 2008a). Given only the helper data, it is computationally hard to recover either the key or the original template. Matching in a key binding system involves recovery of the key from the helper data using the query biometric features. Fuzzy vault (Juels and Sudan, 2002), fuzzy commitment (Juels and Wattenberg, 1999) and shielding functions (Tuyls *et al*., 2005) are common examples of key binding biometric cryptosystems. The biometric templates security schemes proposed in (Li *et al*., 2010) also fall under this category.

3.4.1.2 Key-generation Schemes

In this scheme, the helper data is generated only from the biometric template and the cryptographic key is directly generated from the helper data and the query biometric features (Jain *et al*., 2008a). Dodis *et al*. (2006) introduced the concepts of fuzzy extractor and secure sketch in the context of helper data-based key-generation. A fuzzy extractor consistently generates a uniformly random string from a biometric input while stored helper data assist the reconstruction. In contrast, in a secure sketch, the original biometric template is recovered from helper data.

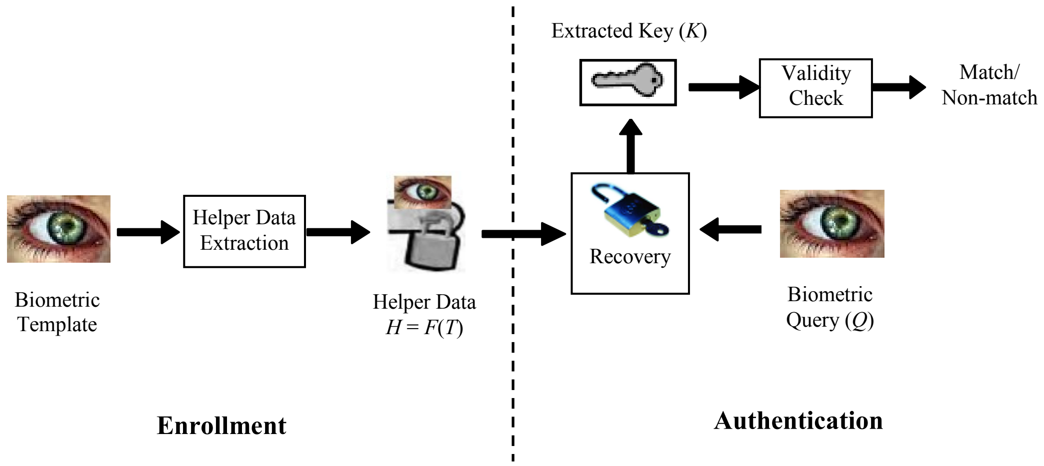


Figure 3.15 Key Generation Biometric Cryptosystem (adopted from Jain *et al*., 2008a)

3.4.2 Feature Transformations

In these approaches, the biometric template (*T*) is transformed into a protected template with the help of a transformation function (*F*) and only the protected template (*F*(*T*, *K*)) is stored in the database as shown in Figure 3.16.

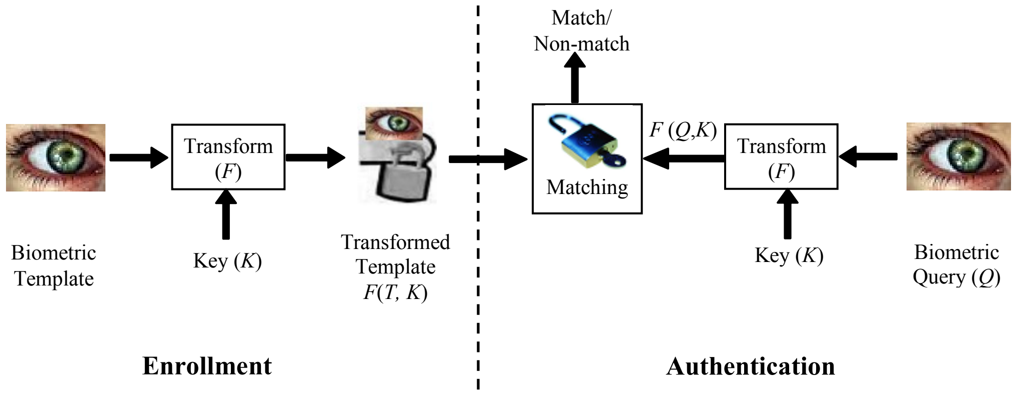


Figure 3.16 Feature Transformation Approach (adopted from Jain *et al*., 2008a)

The transformation function (*F*) is characterized by certain parameters typically derived from a random key (*K*) or a password. During authentication, the query features (*Q*) is transformed by applying the same transformation function and the transformed query (*F*(*Q*,*K*)) is directly matched against the stored template (*F*(*T*,*K*)). Depending on the characteristics of the transformation function (*F*), the approaches can be further divided into two categories as (i) *salting* and (ii) *non-invertible* transforms. In salting transforms, *F* is invertible, i.e., if an intruder gains access to the key and the transformed template, the original biometric template (or a close approximation of it) can be recovered. Hence, the security of the salting scheme is based on the secrecy of the key or password. Examples of salting approach have been proposed for face (Wang and Plataniotis, 2007) and iris (Zuo *et al*., 2008) modalities.

In non-invertible schemes, the transformation (*F*) is typically a one-way direction function (i.e. hashing function) and it is computationally hard to invert a transformed template even if the key is known. Hence, the biometric template is secured. However, transformed biometric templates are difficult to align in order to perform a proper comparison and as result, loss system accuracy. Non-invertible transformation functions have been proposed for iris (Rathgeb *et al*., 2013), fingerprint (Ratha *et al*., 2007) and face (Martin *et al*., 2009) modalities.

3.4.3 Data Hiding

In biometric cryptosystem and feature transformation, a transformation function is employed to transform the biometric template for its security. Steganography and watermarking can be employed on biometric template security. These techniques allow embedding large amounts of biometric information within a carriage image. In biometric watermarking, a certain amount of biometric information referred to as watermark, is embedded into the cover image with or without a secret key, such that the contents of the cover image are not altered. The aim of watermarking is to employ biometric templates as "message" to be embedded in classical robust watermarking applications like copyright protection, to detect the fake biometric trait or non-liveness. In literature, some of these methods performed watermarking in the spatial domain (Gunsel *et al.*, 2002; Jain *et al.*, 2002b, 2003b) while other methods embed the biometric watermark in the frequency domain (Ratha *et al.*, 2000, Vatsa *et al.*, 2004).

3.4.4 Hybrid Approaches

Hybrid approaches are combination of two or more template protection techniques to obtain better performance (e.g., salting followed by key-binding). Feng *et al.* (2008) designed face template protection based on cancelable transformation and applied MD5 to protect transformed biometric, but there is limited intra-class variation and noise after cancelable transformation, so they replaced MD5 with Fuzzy Commitment to modify the hybrid approach (Feng *et al.*, 2010). Another approach is found in Nandakumar *et al.* (2007). The critical issues of hybrid approaches are complexity and possible mutual interference among multiple methods

The template protection schemes are summarized in Table 3.4 including their advantages and limitations (Jain *et al.*, 2008a). In the table, T represents the biometric template, Q represents the query and K is the key used to protect the template. In salting and non-invertible feature transform, F represents the transformation function and M represents the matcher that operates in the transformed domain. In biometric cryptosystems, F is the helper data extraction scheme and M is the error correction scheme that allows reconstruction of the key K.

Table 3.4 Comparisons of Different Template Protection Schemes (Extension of Jain *et al.*, 2008a)

Approach	**Key-binding biometric cryptosystem**	**Key-generating biometric cryptosystem**	**Salting**	**Non-invertible transform**	**Data hiding**
What imparts security to the template?	Level of security depends on the amount of information revealed by the helper data H	Level of security depends on the amount of information revealed by the helper data H	Secrecy of key K	Non-invertibility of the transformation function F	Cover object, Key K (if any)
What entities are stored?	Public domain: Helper Data H=F(T;K)	Public domain: Helper Data H=F(T)	Public domain: Transformed template F(T;K) Secret: Key K	Public domain: Transformed template F(T;K), key K	Public domain: Stegotext (stego-data, stego-object) Secret: Key K
How are intrauser variations handled?	Error correction and user specific quantization K=M(F(T;K);Q)	Error correction and user specific quantization K=M(F(T);Q)	Quantization and matching in transformed domain M(F(T;K);F(Q;K))	Matching in transformed domain M(F(T;K);F(Q;K))	Not required
Advantages	• Tolerant to intra-user variations. • error correcting capability	• Direct key generates from biometrics in turn appealing template protection approach • Appropriate with cryptographic applications.	• Low false accept rates; • Multiple templates of same biometric by using different keys (diversity). • The compromised template can be replaced (revocability)	• Better template security. • Diversity through application-specific F. • Revocability through user-specific F.	• Hide the very existence of the message. • Breaking of a stegenosystems has two stages (i) watermarking detection (ii) read, modify or remove the hidden message. • No transformation applied to the template and hence no effect to the system performance.
Limitations	• May reduce the system performance. • Lack diversity and revocability • Designing of helper data is hard.	• Difficult to generate key with high stability and entropy.	• Template security is depended on user key. • System performance may reduced due to domain transform	• The tradeoff between discriminability and non-invertibility of F. • System performance may be reduced.	• Insecure if steganography/ watermarking is detected.

3.5 Chapter Summary

Biometric system is an automation tool for personal recognition and has many advantages over the classical password or token systems. In this chapter, the details of biometric systems including functionalities, performances measures etc. are discussed along with the limitations. A comparative study of features extraction and classification is also presented and it is found out that ICA is the best feature extraction methods among the five methods employed in the experimentation. The security of stored biometric templates in a biometric system is also a big challenge. Any leakage in biometric template may lose all the privacy of individual as well as the security of the system. Advantages and limitations of biometric template security techniques are discussed.

In the next chapter, design issues of multibiometric systems and proposed design methodology of the thesis are presented.