Chapter 1

Introduction
This chapter provides a general introduction and overview of the biometric. It emphasizes the research objectives, challenges in face recognition and research motivation.

1.1 Biometrics

Biometrics refers to the measurement and analysis of physical or behavioral traits of human beings. More often than not, such an analysis is directed towards the goal of verifying or determining personal identity. Although, identity can be established using means such as PINS or passwords, such clues can be forgotten, stolen, and passed on to others fairly easily. Thus having the secret code/PIN cannot safely be used to validate the identity of the person [1].

Biometrics can be defined as a set of distinctive, permanent and universal features recognized from human physiological or behavioural characteristics. As such, biometrics systems are commonly classified into two categories: physiological biometrics and behavioural biometrics. Physiological biometrics, which include finger-scan, iris-scan, retina-scan, hand-scan, and facial-scan use measurements from the human body. Behavioural biometrics such as signature or keystroke dynamics use measurements based on human actions [2].

Biometric can be defined as technique of studying physical characteristics of a person such as finger prints, hand geometry, eye structure etc to establish his or her identity. This science is primarily implemented to identify individuals. Biometrics-based personal identification techniques that use physiological or behavioral characteristics are becoming increasingly popular compared to traditional token-based or knowledge based techniques such as identification cards (ID), passwords, etc. One of the main reasons for this popularity is the ability of the biometrics technology to differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of an authorized person. Among various commercially available
biometric techniques such as face, voice, fingerprint, iris, etc., retina-based techniques are the most extensively studied and gives accurate result [3].

1.2 Generic Biometric System Process

The biometrics technologies can be used to identify {identification: who am I?} or to verify {verification or authentication: am I whom I claim to be?} an individual. The biometric identification determines who a person is. It involves measuring individual's characteristics and mapping it with users profile stored in the database. The main purpose of positive identification is to prevent multiple users from claiming a single identity. In positive identification method, the user normally claims an identity by giving a name or an ID number, and then submits a biometric measure. Once submitted, it's matched with the previously submitted measure to verify that the current enrolled user is under the claimed identity. These tasks can be achieved through many non-biometric alternatives in such applications as ID cards, PINs and passwords. Depending on the situation or the environment where it's installed, positive identification biometric method can be made voluntary and those not wishing to use biometrics can verify identity in other ways. It is often used in determining the identity of a suspect from crime scene information. There are two types of identification: positive and negative. Positive identification expects a match between the biometric presented and the template, it is designed to make sure that the person is in the database. While the negative identification is set up to ensure that the person is not in the database, more so, it can take the form of watch list where a match triggers a notice to the appropriate authority for action.

The main function of negative identification in an organization is to prevent claims of multiple identities by a single user. In negative identification, the user who enrolls for biometric authentication claims that he or she have not been previously enrolled and submits a biometric measure, which is compared to all others in the system database. If the user's claim of non-enrolment is verified, that means a match is not found. At the moment there are no reliable non-biometric alternatives in such applications, hence the use of biometrics in negative identification applications must be mandatory in places where it's important. The biometrics verification or authentication method requires less processing power and time. It is often used for accessing places or information, depending on the application domain; a biometric
can either be an online or an offline system. To verify an individual's identity a 1:1 check is made between the biometric data and the biometric template obtained during enrolment (see Figure 1.1 for diagrammatic illustration).

![Figure 1.1: Generic biometric system process](image)

For any biometric system to be effective the data should be stored securely and not be vulnerable to theft, abuse or tampering. The data should also be free of errors to prevent false positive and negative results, and the user must be confident that the system is reliable and secure [4].

### 1.3 Biometrics Techniques

A number of biometric characteristics exist and are in use in various applications (see figure 1.2). Each biometric has its strengths and weaknesses, and the choice depends on the application.

There are various biometric identity verification techniques which have surfaced from time to time, including ear lobe recognition and scent recognition. Almost any anatomical feature or behavioural trait might be deemed a candidate for an operable biometric. However, we have to place such ideas in context and align them with the perceived requirement. If this requirement is to have a method by which we might verify an individual identity with a reasonable degree of confidence, then the existing biometric methodologies provide us with the means to do this in a variety of ways, thus facilitating a broad range of applications. Perhaps, in time, other techniques will be developed which might supplant some of the existing methodologies. For now, we might usefully turn our attention towards a better use of existing techniques within contemporary applications, and the provision of a better understanding of the future alignment with societal expectations.
No single biometric is expected to effectively meet the requirements of all the applications. In other words, no biometric is “optimal.” The match between a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the biometric characteristic [5]. A brief introduction to the commonly used biometrics is given below.

1.3.1 DNA

Deoxyribonucleic acid (DNA) Biometrics could be the most exact form of identifying any given individual. Every human being has its own individual map for every cell made, and this map, or ‘blueprint’ as it more often is called, can be found in everybody cell. Because DNA is the structure that defines who we are physically and intellectually, unless an individual is an identical twin, it is not likely that any other person will have the same exact set of genes. It is, however, currently used mostly in the context of forensic applications for person recognition.

DNA can be collected from any number of sources: blood, hair, finger nails, mouth swabs, blood stains, saliva, straws, and any number of other sources that has been attached to the body at some time. DNA matching has become a popular use in criminal trials. The main problems surrounding DNA biometrics is that it is not a quick process to identify someone by their DNA. The process is also a very costly one [6-8].
1.3.2 Ear

One other possible biometric source is the ear. Iannarelli performed important early research on a manual approach to using the ear for human identification [9]. Recent works that explore computer vision techniques for ear biometrics include those of Burge and Burger [10] and Hurley et al. [11]. It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual [12].

1.3.3 Face

Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The applications of facial recognition range from a static, controlled “mug-shot” verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport). The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. While the verification performance of the face recognition systems that are commercially available is reasonable, they impose a number of restrictions on how the facial images are obtained, sometimes requiring a fixed and simple background or special illumination.

These systems also have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. It is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence. In order for a facial recognition system to work well in practice, it should automatically: 1) detect whether a face is present in the acquired image; 2) locate the face if there is one; and 3) recognize the face from a general viewpoint (i.e., from any pose) [13-14].
1.3.4 Facial, hand, and hand vein infrared thermogram

The pattern of heat radiated by human body is a characteristic of an individual and can be captured by an infrared camera in an unobtrusive way much like a regular (visible spectrum) photograph. The technology could be used for covert recognition. A thermogram-based system does not require contact and is noninvasive, but image acquisition is challenging in uncontrolled environments, where heat emanating surfaces (e.g., room heaters and vehicle exhaust pipes) are present in the vicinity of the body [15]. A related technology using near infrared imaging is used to scan the back of a clenched fist to determine hand vein structure. Infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of the thermograms [16].

1.3.5 Fingerprint

Fingerprints are graphical patterns of ridges and valleys on the surface of fingertips. One kind of widely-used features is called minutiae, which is usually defined as the ridge ending and the ridge bifurcation. Various methods based on the minutiae-based fingerprint representation were proposed. Despite its simplicity and efficiency in storage, minutiae-based representation has its drawbacks in practical usage. First, as a kind of local features, the minutiae is difficult to be extracted robustly due to various factors such as large displacement, different pressure, noise, etc., especially on the fingerprints with poor quality or collected on the spot [17-18].

1.3.6 Gait

The genesis of the idea of being able to recognize from gait can be traced back to Cutting and Kozlowski’s perception experiments based on light point displays [19]. They showed that it is possible to identify a person from the manner of walking, i.e., gait. The first effort toward recognition from gait in computer vision was probably done by Niyogi and Adelson in the early 1990s [20].

Gait is the peculiar way one walks and is a complex spatio-temporal biometric. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications [21]. Gait is a behavioral biometric and may not remain invariant, especially over a long period of
time, due to fluctuations in body weight, major injuries involving joints or brain, or due to inebriety.

Acquisition of gait is similar to acquiring a facial picture and, hence, may be an acceptable biometric. Since gait-based systems use the video-sequence footage of a walking person to measure several different movements of each articulate joint, it is input intensive and computationally expensive [22-23].

1.3.7 Hand and finger geometry

Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. Commercial hand geometry-based verification systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems. The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Further, hand geometry information may not be invariant during the growth period of children. In addition, an individual’s jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices like laptops [24]. There are verification systems available that are based on measurements of only a few fingers (typically, index and middle) instead of the entire hand [25]. These devices are smaller than those used for hand geometry, but still much larger than those used in some other biometrics (e.g., fingerprint, face, voice).

1.3.8 Iris

Iris recognition is generally considered to be one of the most effective biometric modalities for biometric identification. Iris is a good biometric because (1) the iris is rich in texture and that texture has many degrees of freedom; (2) the iris is both protected and accessible; (3) the iris texture is thought to be stable throughout most of a person’s life, barring catastrophic injury, or illness; (4) the fraction of a the
population that cannot present an iris due to injury or congenital defect such as aniridia is small; (5) the iris can be easily accessed in a non-contact manner from moderate distances [26-29].

1.3.9 Keystroke

The keystroke patterns produced during typing have been shown to be unique biometric signatures [30]. Therefore, these patterns can be used as digital signatures to verify the identity of computer users remotely over the Internet or locally at a specific workstation [31]. In particular, keystroke recognition can enhance the username and password security model by monitoring the way that these strings are typed. No additional hardware is required since all computers are already equipped with a keyboard. This idea has many computer-based applications, especially for online banking, e-mail, and user account protection, just to name a few [32]. This model can also simplify security requirements by allowing users to reuse the same login information for multiple accounts [33].

Keystroke identification examines the timing pattern that is produced as a typist presses the different keys on the keyboard. From this typing pattern, there are several unique features that can be extracted. One such characteristic (feature) is the key hold-down time (KD), which is the amount of time that a particular key is held down. Another feature is the keystroke latency (KL), which is the time between pressing two consecutive keys; we shall refer to this feature as the down–down keystroke latency (DDKL). These two features have been used in previous research with good results [34-35].

1.3.10 Odor

The body odor biometrics is based on the fact that virtually each human smell is unique [36]. The smell is captured by sensors that are capable to obtain the odor from non-intrusive parts of the body such as the back of the hand. Methods of capturing a person’s smell are being explored by Mastiff Electronic Systems. Each human smell is made up of chemicals known as volatiles. They are extracted by the system and converted into a template. The use of body odor sensors brings up the privacy issue as the body odor carries a significant amount of sensitive personal
information. It is possible to diagnose some diseases or activities in the last hours by analyzing the body odor [37].

1.3.11 Palmprint

The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palmprints are expected to be even more distinctive than the fingerprints. Since palmprint scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors [38]. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper. Finally, when using a high-resolution palmprint scanner, all the features of the palm such as hand 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 [39].

1.3.12 Retinal scans

The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature [40]. The image acquisition requires a person to peep into an eye-piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. The image acquisition involves cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on the part of the user. All these factors adversely affect the public acceptability of retinal biometric [41].

1.3.13 Signature

The way a person signs his or her name is known to be a characteristic of that individual [42]. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of verification [43]. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the system [44].
1.3.14 Voice

The principle of speaker verification is to analyze the voice of the user in order to store a voiceprint that is later used for identification/verification. The aim of speech recognition is to find what principle has been told while the aim of the speaker verification is who told that. Speaker verification focuses on the vocal characteristics that produce speech and not on the sound or the pronunciation of the speech itself.

The vocal characteristics depend on the dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanisms of the human body. These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions (such as a common cold), and emotional state, etc.

A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel [45].

1.4 Comparison of Various Biometrics Techniques

A brief comparison of the above biometric techniques based is provided in Table 1.1. The applicability of a specific biometric technique depends heavily on the requirements of the application domain [46].

<table>
<thead>
<tr>
<th>Rank</th>
<th>Accuracy</th>
<th>Convenience</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DNA</td>
<td>Voice</td>
<td>Voice</td>
</tr>
<tr>
<td>2</td>
<td>Iris</td>
<td>Face</td>
<td>Signature</td>
</tr>
<tr>
<td>3</td>
<td>Retina</td>
<td>Signature</td>
<td>Finger</td>
</tr>
<tr>
<td>4</td>
<td>Finger</td>
<td>Finger</td>
<td>Face</td>
</tr>
<tr>
<td>5</td>
<td>Face</td>
<td>Iris</td>
<td>Iris</td>
</tr>
<tr>
<td>6</td>
<td>Signature</td>
<td>Retina</td>
<td>Retina</td>
</tr>
<tr>
<td>7</td>
<td>Voice</td>
<td>DNA</td>
<td>DNA</td>
</tr>
</tbody>
</table>

No single technique can outperform all the others in all operational environments. In this sense, each biometric technique is admissible and there is no optimal biometric characteristic. For example, it is well known that both the fingerprint-based and iris-based techniques are more accurate than the voice-based
technique. However, in a tele-banking application, the voice-based technique may be preferred since it can be integrated seamlessly into the existing telephone system.

### 1.5 Attributes of Biometrics

Typically, we can identify the following attributes of a biometric system: uniqueness, universality, permanence, measurability, user friendliness, acceptability, and circumvention.

*Uniqueness* refers to the fact that a feature must be unique: an identical feature should not appear in two different people.

*Universality* means that the feature type is present/occurs in as many people as possible. Unfortunately we cannot assume that all people, for example, have all fingers or have one/two of the two irises not damaged.

The *Permanence* property is related to the requirement that the feature not change over time, or at least that it vary very slowly.

*Measurability* concerns the possibility to measure the feature with relatively simple technical instruments.

*User friendliness* requires that the measure should be easy and comfortable to be done.

*Acceptability* refers to the people’s acceptance of the measure in daily lives.

*Circumvention* concerns the toughness to deceive the system by fraudulent methods.

All these attributes must be taken into account designing a biometric system [47].

### 1.6 Objectives

Given an image, recognize the faces that are currently seen. The same face can be seen incredibly different in different images due to differences in viewpoint, illumination etc. A robust recognizer must develop invariant recognition (translation, size and rotation).
The goal of this research work is to develop feature extraction technique to assess its feasibility for security system analysis using the FACE94 face database and other database also.

In theory, security systems involving face recognition would be impossible to hack, as the identification process involves unique identification methods, and thus only authorized users will be accepted. This mechanism would be convenient, with no need to remember passwords or personal identification numbers.

1.7 Challenges in Face Recognition

Face recognition is one of the most relevant applications of image analysis. It’s a true challenge to build an automated system which equals human ability to recognize faces. Although humans are quite good identifying known faces, we are not very skilled when we must deal with a large amount of unknown faces. The computers, with an almost limitless memory and computational speed, should overcome human’s limitations [48]. Some challenges in face recognition are discussed below:

- **Pose variation**: The ideal scenario for face detection would be one in which only frontal images were involved. But, as stated, this is very unlikely in general uncontrolled conditions. Moreover, the performance of face detection algorithms drops severely when there are large pose variations. It’s a major research issue. Pose variation can happen due to subject’s movements or camera’s angle.
- **Feature occlusion**: The presence of elements like beards, glasses or hats introduces high variability. Faces can also be partially covered by objects or other faces.
- **Facial expression**: Facial features also vary greatly because of different facial gestures, imaging conditions, different cameras and ambiental conditions can affect the quality of an image, affecting the appearance of a face.

1.8 Motivation of the Research

A comprehensive review of current literature reveals that there are many possible techniques of feature extraction for faces which can be used for face recognition analysis. Face recognition is necessary for the community. Some groups are working in this area internationally. This work is motivated to build a feature
extraction with various subjects. This work is carried out with the following objectives:

1. To propose methods for machine based face recognition analysis as human eye does.

2. To evolve method of analyzing the faces and to analyze their performance.

3. To improve the performance of face recognition.

4. To provide automatic face recognition system

5. To provide quantitative information of faces.

1.9 Organization of Thesis

Chapter ONE begins with Introduction of Biometric. This research work is related with Face Recognition. Comparison of Face biometric is outlined with other biometrics. Chapter TWO is Literature Survey, which give in detail concept of the traditional Face Recognition techniques. In this chapter brief information of LDA and PCA is also provided. The fundamentals of Pattern Recognition are given in this chapter. Chapter THREE is the Development of the System which covers the proposed feature extraction technique for Face Recognition. Along with this, brief information of pattern classifier is also specified. Chapter FOUR deals with the Performance Analysis in which the results in the form tables are given for techniques of feature extraction. It also details the images used during experimentation. Thesis ends in Chapter FIVE with Conclusions and Future Scope of the work.
REFERENCES


[37] Website: http://www2.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf


[44] Website:
http://www.springer.com/978-0-85729-466-1


[46] Website:
www.scribd.com/doc/3834277/Biometrics


[48] Website: