1.1 Introduction

The exploration of new human-computer interfaces has become a growing field in computer science, which aims to create more natural, intuitive, unobtrusive and efficient interfaces. This objective has become more relevant with the introduction of intelligent machines. These are increasingly more popular in the roles when interpretation of the user’s attractive states is required. Such interfaces can adapt and respond to the users, need better and can benefit from the knowledge of human-human communication.

A wide variety of applications require reliable verification schemes to confirm the identity of an individual requesting their service. Examples of such applications include; secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust verification schemes, these systems are vulnerable to the wiles of an imposter [18], [29], [59].

Traditionally, the identification or the verification of an individual’s claimed identity involved the use of a password, personal identification number (PIN) or cryptographic key (“something you know”). The possession of an identity (ID)
card, smart card or token (“something you have”). However, there are a num-
ber of problems associated with these security measures. For example, passwords 
and PINs can be forgotten, shared with others, and lost or stolen, which could 
compromise the integrity of the system. In contrast, biometric trait is part of an 
individual, as such it offers the third element of proof of identity, i.e. (“some-
thing you are”). Consequently, biometric traits are thought to have a number 
of advantages over the aforementioned security measures: they cannot be lost or 
forgotten, they are difficult to copy, forge or share and they require the individual 
to be present at the time of identification. The use of biometrics also makes it 
difficult for an individual to repudiate having accessed a physical location or a 
computer system, or having conducted a particular transaction.

In fact, biometric traits are often portrayed as the ultimate form of identifi-
cation or verification, and are being promoted in many quarters as a means of 
heightened security, efficiency and convenience and have been proposed as the 
solution to issues of identity theft and benefit fraud. It is envisaged that biomet-
ric systems will be faster and more convenient to use, cheaper to implement and 
manage and more secure than traditional identification and verification methods. 
Nonetheless, biometrics also have their limitations, for example, passwords, PINs 
and ID cards can all be re-issued relatively easily if they become compromised, 
which is not the case for an individual’s fingerprint or iris image.

1.2 History of Biometrics

The term biometric comes from the Greek words bios (life) and metrikos (mea-
sure) [18]. Biometric refers to the automatic recognition of individuals based on 
their physiological and behavioral characteristics.

There are evidences of biometric uses on human history [5] as early as pre-
historical age. Estimated 31000 years old caves are adorned with pre-historical
pictures apparently signed by fingerprints stamps of authors. Another evidence is the use of fingerprints by Babylonian at 500 B.C. They used to record business transactions on clay tables.

The first reported use of biometrics was related by Portuguese explorer João de Barros in the 14th century. He described the practice of Chinese merchants used to settle business transaction. Chinese parents also used fingerprints and footprint to differentiate children from one another.

The first real biometric system was created in 1870 by French anthropologist Alphonse Bertillion and turned biometrics a distinguished field of study. He developed an identification system (Bertillonage) based on detailed records of the body’s measurement, physical description and photographs. Despite their imprecise measures and difficulty to apply methodology, the Bertillonage was an important advance on criminal and people identification. It began to fail when it was discovered that many people share the same anthropologic measures. The first classification method for fingerprints was developed in 1892 by Sir. Francis Galton. The features used by Galton’s method were the minutiae that are still used nowadays.

Some years later in 1896, Sir Edward Henry General Inspector of the Bengal police, began to use Galton’s method to replace the anthropometrics system for identification of criminals. Henry created a method to classify and store fingerprint that lets a quick searching of records. Later, that method was introduced by Henry in London for the first British fingerprint file. In brief Table 1.1 shows the biometrics history outline time upto 2000 as reported by [2].
<table>
<thead>
<tr>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1858</td>
<td>First systematic capture of hand image for identification was recorded</td>
</tr>
<tr>
<td>1870</td>
<td>Bertillon developed anthropommetrics to identify individuals</td>
</tr>
<tr>
<td>1892</td>
<td>Galton developed a classification system for fingerprint</td>
</tr>
<tr>
<td>1894</td>
<td>The tragedy of Puddnhead Wilson was published</td>
</tr>
<tr>
<td>1896</td>
<td>Hennery developed a fingerprint classification system</td>
</tr>
<tr>
<td>1903</td>
<td>New York state prisons started using fingerprints</td>
</tr>
<tr>
<td>1903</td>
<td>Bertillon system collapsed</td>
</tr>
<tr>
<td>1936</td>
<td>Concept of using the iris pattern for identification was proposed</td>
</tr>
<tr>
<td>1960s</td>
<td>Face recognition became semi-automated</td>
</tr>
<tr>
<td>1960</td>
<td>First modal of acoustic speech production was created</td>
</tr>
<tr>
<td>1963</td>
<td>Hughes research paper on fingerprint automation published</td>
</tr>
<tr>
<td>1965</td>
<td>Automated signature recognition research started</td>
</tr>
<tr>
<td>1969</td>
<td>FBI pushed to make fingerprint recognition an automated process</td>
</tr>
<tr>
<td>1970s</td>
<td>Face recognition has taken another steps towards automation</td>
</tr>
<tr>
<td>1970</td>
<td>Behavioural component of speech were first modelled</td>
</tr>
<tr>
<td>1974</td>
<td>First commercial hand geometry systems became available</td>
</tr>
<tr>
<td>1975</td>
<td>FBI fund development of sensors and minutiae extraction technology</td>
</tr>
<tr>
<td>1976</td>
<td>First prototype systems for speaker recognition was developed</td>
</tr>
<tr>
<td>1977</td>
<td>Patent is awarded for acquisition of dynamic signature information</td>
</tr>
<tr>
<td>1980s</td>
<td>NIST Speech Group was established</td>
</tr>
<tr>
<td>1985</td>
<td>Concept that no two irides are alike was proposed</td>
</tr>
<tr>
<td>1986</td>
<td>Exchanging of fingerprint minutiae data standard was published</td>
</tr>
<tr>
<td>1987</td>
<td>Patent stating that the iris can be used for identification was awarded</td>
</tr>
<tr>
<td>1988</td>
<td>First semi-automated facial recognition system was deployed</td>
</tr>
<tr>
<td>1991</td>
<td>Face detection was pioneered, making real time face recognition possible</td>
</tr>
<tr>
<td>1992</td>
<td>Biometric consortium was established within US Government</td>
</tr>
<tr>
<td>1994</td>
<td>First iris recognition algorithm was pointed</td>
</tr>
<tr>
<td>1995</td>
<td>Iris prototype became available as a commercial product</td>
</tr>
<tr>
<td>1996</td>
<td>Hand geometry was implemented at the Olympic Games</td>
</tr>
<tr>
<td>1997</td>
<td>First commercial, biometric interoperability standard was published</td>
</tr>
<tr>
<td>1998</td>
<td>FBI launched CODIS (DNA forensic database)</td>
</tr>
<tr>
<td>2000</td>
<td>First research paper describing the use of vascular patterns for recognition was published</td>
</tr>
</tbody>
</table>
1.3 Biometric System

Biometrics systems are commonly classified into two categories: physiological biometrics and behavioral biometrics. Physiological biometrics (fingerprint, iris, retina, hand geometry, face, etc.) use measurements from the human body. Behavioral biometrics (signature, keystrokes, voice, etc.) use dynamics measurements based on human actions [46], [54], [59]. These systems are based on pattern recognition methodology, which follows the acquisition of the biometric data by building a biometric feature set, and comparing versus a pre-stored template pattern.

1.3.1 Generic Biometric System

A simple biometric system has a sensor module, a feature extraction module and a matching module. Figure 1.1 shows a simple biometric system. Sensor module (Image acquisition): a suitable sensor to acquire the raw biometric data of an individual to be stored in the database. Feature extraction module: a suitable algorithm for feature extraction. It may also require enhancement algorithm to improve the quality of acquired image. Database module: which acts as a respiratory of biometric information? “People have to enroll before they can use biometric systems”. Enrolment involves a copy of a person’s biometric feature being taken, converted into a digital format and stored on an electronic database. Matching module: The extracted features are compared with the stored templates to generate match score.

The performance of a biometric system is largely affected by the reliability of the sensor used and the degrees of freedom offered by the features extracted from the sensed signal [54].
Figure 1.1: Generic Biometrics System

Figure 1.2 shows an example of a biometric system of a fingerprint character. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user’s print with those in the template.

Figure 1.2: an Example of a Biometric System of a Fingerprint Character

1.4 Characteristics of Biometric.

The following are the biometrics characteristics [29], [51].

- **Universality**: Every person should have the biometric characteristic.

- **Uniqueness**: No two persons should be the same in terms of the biometric characteristic.
• **Permanence:** The biometric characteristic should be invariant over time.

• **Collectability:** The biometric characteristic should be measurable with some (practical) sensing device.

• **Acceptability:** The particular user population and the public in general should have no (strong) objections to the measuring/collection of the biometric characteristic.

• **Performance:** Refers to the level of accuracy and speed of recognition of the system given the operational and environmental factors involved.

• **Resistance to Circumvention:** Refers to the degree of difficulty required to defeat or bypass the system.

### 1.5 Popular Biometric Characteristics (Modalities)

There are two types of biometrics modalities, physiological and behavioural biometrics modalities. Figure [1.3](#) shows some of the popular biometrics modalities.

#### 1.5.1 Physical biometrics modalities

Following are the physical biometrics modalities/characteristics:

- **Face**

  Facial attributes are probably the most common biometric features used by humans to recognize one another. Face verification involves extracting a feature set from a two-dimensional image of the user’s face and matching it with the template stored in a database. 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.

- **Fingerprint**
  Humans have used fingerprints for personal identification for many decades. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. It has been empirically determined that the fingerprints of identical twins are different. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points.

- **Iris**
  The iris begins to form in the third month of gestation and the structures creating its pattern are largely completed by the eight month. The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The complex iris texture carries very distinctive information useful for personal recognition of high accuracy and speed. Each Iris is believed to be distinctive. It is possible to detect artificial irises (contact lenses).
• **Retina**
Retinal recognition creates an “eye signature” from the vascular configuration of the retina which is supposed to be a characteristic of each individual and each eye, respectively. Since it is protected in an eye itself, and since it is not easy to change or replicate the retinal vasculature, so it is one of the most secure biometric. Image acquisition requires a person to look through a lens at an alignment target; therefore it implies cooperation of the subject.

• **Facial Thermography**
Thermography recognition measures the amount of thermal radiation (heat) emitted from an individual’s face. It is claimed that a face thermography is unique to each individual and is not vulnerable to disguises. Face thermography is a non-intrusive biometric technique which can verify an identity without contact. An infrared camera can capture the face thermography in the absence of light.

• **Vein Pattern Recognition**
In vein pattern recognition systems a high resolution camera and infrared light are used to capture the pattern and structure of blood vessels visible on the back of an individual’s hand or finger. The algorithm registers the vascular pattern characteristics (e.g. blood vessel branching points, vessel thickness and branching angles) and stores these as a template for comparison with subsequent samples from the enrolled individual. Vein pattern recognition systems are increasingly being used in order to access ATM cash dispensers and banking services, and for physical access to hospitals and universities as well as for residential access, particularly in Japan.

• **Ear**
It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. Matching the distance of salient points on the pinna from a landmark location of the ear is the suggested method of recognition in this case. This method is not very distinctive.
A sensor (e.g. a camera) collects a side profile image of the user’s head, from which the system automatically locates the ear and isolates it from the surrounding hair, regions of the face, and the user’s clothes. The algorithm uses a combination of colour and depth analysis to first localize the ear pit, then generates an outline of the visible ear region.

- **DNA**

DNA stands for Deoxyribonucleic Acid and is a molecule that contains biological instructions of the living organisms. The DNA is composed of chemical building blocks called nucleotides. A sequence of DNA that contains information for producing a protein is known as gene, whereas the whole DNA instructions of the organisms are called genome.

The human genome is shared about 99.5% to 99.9% across the human beings, however, even the small percentages of difference are of the order of millions of base pairs. The human genome is unique to each individual; however this affirmation is not valid for identical twins since they share the same DNA patterns. The low degree of popularity of this biometric characteristic is based on three factors: (1) privacy concerns, some additional information of the individual could be obtained such as diseases, (2) real-time authentication capabilities, this technique involves high computational resources and is difficult to be automatized since it requires some chemical processes, and (3) access availability, it is easy to steal a piece of DNA from an individual and this information could be therefore used for fraudulent purposes.
1.5.2 Behavioral biometrics modalities

Following are the behavioral biometrics modalities/characteristics:

- **Dynamic Signature**
  The way in which an individual signs his/her name is considered to be characteristic of that person and as such could provide a feasible mode of biometric recognition. Dynamic signature recognition is an automated method of examining an individual’s signature. These systems assess specific features of the signature writing process, including the speed, direction and pressure of writing, the time the stylus (e.g. a pen) is in and out of contact with the surface (e.g. paper), the total time taken to write the signature and where the stylus is raised and lowered on the surface.

- **Voice**
  Voice is a combination of physical and behavioral biometric characteristics. The physical features of an individual’s voice are based on the shape and size of the, vocal tracts, mouth, nasal cavities, and lips that are used in the synthesis of the sound. Feature extraction typically measures formants or sound characteristics unique to each person’s vocal tract.

- **Keystroke**
  It has been suggested that individuals have a characteristic way of typing on a keyboard, which is sufficient for use in biometric recognition systems. This technology can assess an individual’s keystroke dynamics (e.g. speed and pressure), the total typing time for a specific password and the time taken between hitting certain keys. Keystroke dynamic systems are moderately resistant to circumvention, but they are usually used for low security applications, e.g. for controlling and monitoring access to computer systems and networks.
• **Gait**

Gait refers to the manner in which a person walks, and is one of the few biometric traits that can be used to recognize people at a distance. Therefore, this trait is very appropriate in surveillance scenarios where the identity of an individual can be surreptitiously established.

• **Odor**

Each object spreads around an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. This would be done with an array of chemical sensors, each sensitive to a certain group of compounds. Deodorants and perfumes could lower the distinctiveness.

Since odor is emitted from pores all over an individual’s body, these systems operate by circulating air around the body part being analyzed (e.g. the back of the hand, the arm or the neck) and over an array of chemical sensors. Each of these sensors is sensitive and receptive to certain groups of aromatic compounds of the individual’s smell, which are extracted and classified into a template.

Table 1.2 shows a comparison among biometrics characteristics/ modalities.

Figure 1.4 graphically shows the revenues of biometric by technology in the year 2010.
<table>
<thead>
<tr>
<th>Biometric Characteristic</th>
<th>Universality</th>
<th>Unicity</th>
<th>Permanence</th>
<th>Collectability</th>
<th>Performance</th>
<th>Acceptability</th>
<th>Circumvention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Iris</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Retinal Scan</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Signature</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Voice</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Thermogram</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
1.6 Functionalities of a Biometric System

A biometric system may operate either in the Verification or Identification modes [10], [54]. But people have to enroll before they can use a biometric system. Enrollment involves a copy of a person’s biometric feature being taken, converted into a digital format and stored on an electronic database as shown in Figure 1.5.
**Verification:** an attempt is made to verify the claimed identity of unknown individual. In this mode; biometric system performs a one-to-one comparison of a submitted biometric characteristic (sample) set against a specified stored biometric references, and returns the comparison score and decision. “Is this person who he claims to be?” as shown in Figure 1.6

![Figure 1.6: The Verification Process](image here)

**Identification:** an attempt is made to establish the identity of an individual. In this mode; biometric system performs a one-to-many comparison/search process in which a biometric characteristic set against all or part of the database to find biometric references with a specified degree of similarity. “Who is this person?” as shown in Figure 1.7

![Figure 1.7: The Identification Process](image here)
1.7 Types of Biometrics

There are two types of biometrics unimodal and multibiometrics.

1.7.1 Unimodal

The unimodal relies on the evidence of a single source of information for authentication (e.g., single fingerprint, face). These systems have to contend with a variety of problems such as [29], [36], [53], [54]:

1. **Noise in sensed data;** a fingerprint image with a scar, accumulation of dirt on a fingerprint sensor, defective, or improperly maintained sensors. In such a case, fingerprint or voice authentication seems not to be a good means for personal identity authenticating. In a system using speech some factors such as, ambient noise, changes in behavioral attributes of the voice, voice sample altered by cold, and voice change due to aging, will affect the system’s performance.

2. **Intra-class variations;** these variations are typically caused by a user who is incorrectly interacting with the sensor such as a variations in facial expression, pose and lighting, will limit the system’s performance.

3. **Inter-class similarities;** in a biometric system comprising of a large number of users, there may be inter-class similarities (overlap) in the feature space of multiple users.

4. **Non-universality;** the biometric system may not be able to acquire meaningful biometric data from a subset of users. For example, fingerprint biometric system, may extract incorrect minutiae features from the fingerprints of certain individuals, due to the poor quality of the ridges.

5. **Spoof attacks;** this type of attack is especially relevant when using behavioural characteristics.
1.7.2 Multibiometrics:

The term multibiometrics denotes the fusion of different types of information \[10\] (e.g., fingerprint and face of the same person, or fingerprints from two different fingers of a person). Since different biometric traits such as the iris and the fingerprint can be considered independent of each other, the combination of them means that more information is used, which is theoretically helpful to improve the performance of biometric systems. Indeed, higher accuracy, which may be considered one of the essential goals of biometric technology, is also the primal reason of the appeal of multibiometric systems. Figure 1.8 shows the different types of multibiometrics.

![Figure 1.8: Different Types of Multibiometrics](image)

Multibiometrics has addressed some issues related to unimodal such as \[30], \[51\]:

- Non-universality or insufficient population coverage (reduce failure to enroll rate which increases population coverage).

- It becomes increasingly difficult for an impostor to spoof multiple biometric traits of a legitimately enrolled individual.
• Multibiometric systems also effectively address the problem of noisy data (illness affecting voice, scar affecting fingerprint).

The multi-biometric system will provide strong feasibility and reliability, also multibiometric systems can offer substantial improvement in the matching accuracy of a biometric system depending upon the information being combined and the fusion methodology adopted [59].

• **Multi-sensor:** Multiple sensors can be used to collect the same biometric.

• **Multi-modal:** Multiple biometric modalities can be collected from the same individual, e.g. fingerprint and iris, which requires different sensors.

• **Multi-instance:** Multiple units of the same biometric are collected, e.g. fingerprints from two or more fingers.

• **Multi-sample:** Multiple readings of the same biometric are collected during the enrolment and/or recognition phases, e.g. a number of fingerprint readings are taken from the same finger.

• **Multi-algorithms:** Multiple algorithms for feature extraction and matching are used on the same biometric sample.

One of the most fundamental issues in an information fusion system is to determine the type of information that should be consolidated by the fusion module [52].

1.8 Related Work

E.J.C. Kelkboom et al. [32] have shown that it is possible to apply multi-sample fusion with the Helper-Data Systems (HDS) system at feature, score, and decision levels. Even the HDS system inherently has only a decision as the output; the authors adapted the system accordingly in order to have a score as output for the score-level fusion. As a distance score the number of bits the error correcting
codes (ECC) has to correct. Furthermore, applying fusion with template protection at feature or decision level is straightforward and conventional. However, fusion at score level is different due to the use of an ECC, which has a limited error correcting capability.

Consequently, for each template protection system there is only a valid score when there is a match. Given the biometric database and feature extraction algorithms there are no significant differences between the best performances (ROC curves) obtained at feature, score, and decision levels.

Kalyan V. et al. [64] have presented an evolutionary approach to the sensor management of a biometric security system that improves robustness. Multiple biometrics is fused at the decision level. The decision fusion rules are adapted to meet the varying system needs by particle swarm optimization, an evolutionary algorithm. This work focuses on the details of a new sensor management algorithm and demonstrates its effectiveness. The evolutionary nature of adaptive, multimodal biometric management algorithm AMBM allows it to react in pseudo-real-time to change security needs as well as user needs. Error weights are modified to reflect the security and user needs of the system.

F. Alonso-Fernandez et al. [9] have compared a fusion scheme based on calibrated scores with simple fusion rules. The aim is to compare the performance of multi-modal fusion algorithms when query biometric signals are originated from different biometric devices. In the proposed fusion strategy, the device used in the access estimated, then a different linear logistic regression classifier adapted to each device. Since linear logistic regression classifiers produce log-likelihood-ratios, output scores produced by the different devices are then easily combined. Authors demonstrate the effectiveness of the proposed approach by comparing it to a set of simple fusion rules with standard Max-Min normalization. Reported results show that the proposed fusion approach outperforms all the simple fusion rules, with the advantage that scores after logistic regression are mapped to an
R. Connaughton et al. [14] have compared three commercially available iris sensors and three iris matching systems. The authors have investigated the impact of cross-sensor matching on system performance in comparison with single-sensor performance. The sensors are evaluated using three different - iris matching - algorithms, and conclusions are drawn regarding the interaction between the sensors and the matching algorithm in both the cross-sensor and single-sensor scenarios. Finally, the relative performances of the three sensors are compared. The results are used to investigate the robustness of each sensor to the changes in the environment as well as difference in dilation ratio between image pairs. The authors analyze the relationship between single and cross-sensor performance for these sensors, and observe the role of the matching algorithm on relative sensor performance.

Kalian V. et al. [63] have accomplished optimization of sensor thresholds and fusion rule for heterogeneous and correlated sensor suite through a particle swarm optimization (PSO) algorithm. Different correlation structures are assumed and the effect of correlation on the choice of final fusion rule and thresholds is analyzed. The Bahadur-Lazarfeld used to adopt expansion estimation of the error probabilities. The evaluation of multivariate integral is done numerically. PSO based optimization achieved significantly better performance as a function of correlation between the sensors and a priori of hypotheses. The results demonstrate PSO as a strong computational paradigm to optimize the distributed detection network in presence of correlation.

K.I. Chang et al. [13] have examined the value of multi-modal biometrics with 2D intensity and 3D shape of face recognition using a single and a multiple probe study. In the results, each modality of facial data has roughly similar value as an appearance based biometric. The combined data from 2D and 3D modalities has
given a significant improved results over either individual modality. In general, the results appear to support the conclusion that the path to higher accuracy and robustness in biometrics involves use of multiple biometrics rather than the best possible sensor and algorithm for a single biometric.

Chunxiao Ren et al. [49] have presented a novel method of score level fusion using multiple enrolled impressions to achieve higher verification accuracy of existing fingerprint systems. The main idea of the method is to build a representation of the biometric reference as a polyhedron by taking into account the matching results of multiple enrolled impressions. According to the authors the verification step consists in measuring a distance between the centroid of the polyhedron and the acquired image. This novel method outperforms the traditional uni-matcher based scheme over a wide range of FAR and FRR values.

Andreas Uhl and Peter Wild [61] have introduced a multi-instance fingerprint and eigenfinger-based biometric system and verified by experiment, that a combination of matching scores can increase performance significantly, and thus tolerate the application of common flatbed scanners for fingerprint and eigenfinger processing. The authors examined the performance of (weighted) score combination methods based on Min-Max normalized scores in the given context of cross-feature and intra-feature multiple-instance fusion. Simple Sum turned out to be best-suited for the separate combination of minutiae and eigenfinger. Product combination delivered lowest error rates EER, ZeroFMR and ZeroFNMR in the total combination scenario. Weights obtained by exhaustive search could not be successfully applied to unseen objects for Max, Median, and Min. Solely Weighted sum or product yields constantly better results also on unseen objects.

Jie Zou et al. [72] have conducted a comprehensive comparative study at each step of the local matching process. The experimental conclusions include: 1) Gabor features are effective local feature representations and are robust to illu-
mination changes; 2) the configuration of facial components does contain rich discriminative information and comparing corresponding local regions utilizes shape features more effectively than comparing corresponding facial components; 3) combining local regions with Borda count classifier combination method alleviates the curse of dimensionality. Without training, illumination compensation and without any parameter tuning, it achieves superior performance on every category of the FERET test: near perfect classification accuracy on pictures taken on the same day regardless of indoor illumination variations and significantly better than any other reported performance on pictures taken several days to more than a year apart.

H. Fronthaler et al. [23] have presented a study of the orientation tensor of fingerprint images to quantify signal impairments like noise, lack of structure, blur, with the help of symmetry descriptors. Especially favourable in Biometrics, strongly reduced reference, but not less information is sufficient for the approach. In this study, several trained and non-trained score level fusion schemes are investigated. The authors elaborated on the benefits of adapting multi-algorithm fusion schemes as a reaction to the signal quality. As to adaptive fusion the authors introduced a non-trained cascaded scheme to dynamically switch on experts in case of uncertainty (low quality), assuming time is the most limited resource. Bayes-based supervisors for continuous fusion implemented to point out another aspect of multi-algorithm fusion. The experiment that quality adaptive fusion and training yields the best recognition rates when combining differently skilled experts.

X. Tan and B. Triggs [58] have investigated the benefits of combining two of the most successful feature sets for robust face recognition under uncontrolled lighting: Gabor wavelets and LBP features. It is found that these features are more complementary than might have been expected, with the combination having only around 2/3 of the errors of either feature set alone. The method was tested in a novel
face recognition pipeline that includes: robust photometric image normalization; separate feature extraction, PCA-based dimensionality reduction and scalar variance normalization of each modality; feature concatenation; Kernel DCA based extraction of discriminant nonlinear features; and finally cosine-distance based nearest neighbour classification in the KDCA reduced subspace. The proposed face recognition method is scalable to large numbers of individuals and easy to extend to additional feature sets.

I. G. Damousis and S. Argyropoulos [15] have developed four machine learning algorithms for the fusion of several biometric modalities in order to detect the most efficient one. The algorithms were Gaussian Mixture Models, an Artificial Neural Network, a Fuzzy Expert System, and Support Vector Machines. The algorithms were trained and tested using a well-known biometric database which contains samples of face and speech and similarity scores of five face and three speech biometric experts. The fusion results were compared against existing fusion techniques and also against each other, showing that the fusion schemes presented in this paper produce better biometric accuracy from conventional methods. From the four algorithms, the most efficient one proved to be the support vector machines-based one offering significant performance enhancement over unimodal biometrics.

C. Wang and S. Mahadevan [65] have introduced a novel approach (discriminative projections) to jointly learn data dependent label and locality preserving projections. The new approach is able to construct discriminative features to map high dimensional data instances to a new lower dimensional space, preserving both manifold topology and class separability. Leveraging the flexibility of labels, discriminative projections goes beyond LDA and LPP in that it can project similar classes to similar locations. The authors approach is a semi-supervised approach making use of both labeled and unlabeled data. It is general, since it can handle both two class and multiple class problems.
G.L. Marcialis and F. Roli [40] have presented some preliminary experiments on the score level fusion of fingerprint and face matchers under stress conditions. This term, means that the subjects cooperation degree of the training set was notably different than that of the test set. Reported results showed that fusion allowed to definitely improving the system reliability, by significantly reducing the gap between expected and real performance. In particular, the most effective fusion rules appeared to be the weighted average and product based on integral parameters, namely, the Total Error Rate.

A. Baig et al. [11] have presented a proof of concept for a single matcher based multimodal biometric identification framework. The framework is verified by utilizing fingerprint and iris modalities. The proposed framework is low cost with a small memory footprint and easier hardware implementation. It is interesting to note that the flexibility and openness of this framework, which allows for easy interchangeability of various feature extractors and matcher helps to spawns the plug and play nature of the system. This approach also has an additional advantage in that it is easier to implement, with low memory footprint and cost. One of the major impacts of applying this framework is on system design in that it forces the designer to think about fusion from the start and pay special attention to the design of the feature extractors.

K. Kryszczuk et al. [34] have presented a framework for a multimodal classification system using Bayesian networks for modeling decision reliability measures for each modality classifier. The reliability measures are explicitly involved in the final multimodal decision rule to resolve disagreement between the classifiers in favour of the more reliable modality. Within this framework, authors introduced the use of automatic signal-domain quality measures which play an important role in the rectification of unimodal classifier errors. Authors have shown that the majority of erroneous decisions of unimodal classifiers can be rectified by the use
of the decision reliability measures. The results of the reported experiments show that, depending on the application and system utilization scenario, the overall accuracy of the system can be significantly improved. It is worth noticing that under current multimodal decision scheme the system is forced to take the decision of the expert who reports higher reliability.

R. Giot et al. [25] have presented a low cost and usable multimodal system based on keystroke dynamics and 2D face recognition. Different fusion methods have been tested on a chimerical database containing two kinds of biometric templates for 100 users (keystroke dynamics and face). Authors have proposed two new fusion functions parametrized genetic algorithm and one built with genetic programming. By fusing biometric systems of the same modality, better performances in the case of keystroke dynamics have obtained, but not with face recognition where the performance of the combined methods was too different. Using the fusion with the whole set of methods really improves the results by reducing EER.

1.9 Consideration for biometrics design and implementation

The following are few out of many considerations have been mentioned here.

1. Scale

- The best choice of biometrics.
- The factors which contribute in developing a person’s biometric.
- The biometric technology to be selected.
- The factors which cause biometric system to fail.
- Identification or Verification to be used.
2. **Accuracy**

- Interaction of the user with the system.
- Biometrics reliability/accuracy.
- Guarantee of matching provided by biometric.
- The accuracy measurement.

3. **Security**

- The possibility of solving the security problems by biometrics.
- The intrusive of biometrics.
- the possibility of stealing a biometric.

4. **Privacy**

- Private information (ethnicity, medical information, etc.) which could be reveal by biometrics.
- The individual’s civil liberties and privacy which could be invade by biometrics.
1.10 Outline of the Thesis

The subsequent chapters in the thesis have been divided into five main chapters: An entire chapter will be devoted to describe methodologies used in this study. Three chapters each are dedicated for representing the contributions of the work in issues of evaluation of multi-instance, evaluation of multi-algorithm and evaluation of multi-modal, respectively and finally a chapter for presenting the robustness analysis.

Chapter 1; presented a brief introduction of biometrics and multibiometric systems. Further, it also presented the discussion about functionalities of a biometric system, literature review and Consideration for biometrics design and implementation.

In Chapter 2; a brief description of the tools and techniques that have been used in this work. Feature extraction techniques such as Appearance based, Kernel based and Texture based are discussed. In appearance based methods PCA, LDA, and LPP techniques are analyzed. In kernel based methods KPCA, KLPP, KDA and KICA are analyzed. In texture based method LBPV, Gabor, Log-Gabor and LPQ methods are analyzed. It also described different levels of fusion and their strategies and statistical measures of performance, fusion rules and the concept of performance measures used throughout the thesis.

In Chapter 3; performance evaluation of multi-instance system. Performance of a single instance system. Performance of two and three instances at different level of fusion (feature, score, and decision). Comparison analysis of the three levels of fusion.

In Chapter 4; performance evaluation of multi-algorithm system. Performance of a single algorithm system. Performance of two and three algorithms at
different level of fusion (feature, score, and decision). Comparison analysis of the three levels of fusion.

In **Chapter 5**; performance evaluation of multi-modal system. Performance of a single modality system. Performance of two and three modalities at different level of fusion (feature, score, and decision). Performance of a three instances at different level of fusion (feature, score, and decision). Comparison analysis of the three levels of fusion.

**Chapter 6**; describes the conclusion arrived at in the study. After presenting concluding remarks, several possible future avenues that researchers can pursue based on this research are indicated.