CHAPTER 1

INTRODUCTION

In the early years of the 21st century, we find ourselves continually moving further away from the necessity of physical human interaction playing a major part of menial everyday tasks. Striding ever closer to an automated society, we interact more frequently with mechanical agents, anonymous users and the electronic information sources of the World Wide Web (WWW), than with our human counterparts. It is therefore ironic that identity has become such an important issue now-a-days. It would seem that in an age where fraud is costing the public billions of pounds every year and even the most powerful nations are powerless against a few extremists with a flight ticket, it is not who we are that is important, but rather, that we are who we claim to be. For these reasons, biometric authentication has already begun a rapid growth in a wide range of market sectors and will undoubtedly continue to do so, until biometric scans are as commonplace as swiping a credit card or scrawling a signature.

1.1 BIOMETRICS

Authentication may be defined as providing the right person with the right privileges and the right access at the right time. In general, there are three approaches to authentication. In order of least secure and least convenient to most secure and most convenient, they are:
- Something you have - card, token, key.
- Something you know- Personal Identification Number (PIN), password.
- Something you are - a biometric.

Any combination of these approaches further heightens security. Requiring all three for an application provides the highest form of security.

Biometrics is a method to automatically verify or identify individuals using their physiological or behavioral characteristics (Huang 1999). Biometric technologies include (Huang 1998):

- Facial Recognition
- Iris Identification
- Retinal Verification
- Speaker / Voice Recognition
- Fingerprint Classification
- Hand/Finger Geometry
- Dynamic Signature Verification
- Keystroke Dynamics

Biometric authentication has been widely regarded as the most foolproof - or at least the hardest to forge or spoof. The increasing use of biometric technologies in high-security applications and beyond has stressed the requirement for highly dependable face recognition systems. Among the bioinformatics technologies face recognition approach has some additional advantages like easy to use, natural, and non-intrusive. This tends researchers to do further work. Out of six biometric attributes considered by Hietmeyer (2000), facial features scored the highest compatibility in a Machine Readable Travel Documents (MRTD) system based on a number of evaluation factors,
such as enrollment, renewal, machine requirements, and public perception. Although progress in face recognition has been encouraging, the task has also turned out to be a difficult endeavor, especially for uncontrolled tasks where viewpoint, illumination, expression, occlusion, accessories, and so on vary considerably.

Face recognition (Shakhnarovich 2002) has been described as the Holy Grail of biometric identification systems due to a number of significant advantages over other methods of identification. However, with the current state of the art, these advantages do not include operating performance in terms of recognition accuracy. When compared with other identification technologies, face recognition cannot compete with the low error rates achieved using iris or fingerprint systems. However, no other biometric technology can match face recognition for its convenience of identification at-a-glance or the advantages offered in being analogous to our own method of identification. Also the importance of face recognition rises from the fact that a face recognition system does not require the cooperation of the individual while the other systems need such cooperation.

1.2 FACE RECOGNITION SYSTEM

The automatic face recognition has been started since 1960. First automatic face recognition system was developed by Kanade (1973). The performance of face recognition systems is being improved significantly but still the problem is not accurately solved. Strictly, the term biometrics describes the quantifiable characteristics used in measuring features of biological organisms. However, now-a-days this term is often used to describe the variation in biological characteristics of humans in order to differentiate them. Some such measurements are now finding use in automated security and surveillance systems, which employ biometrics to verify an individual’s identity against some claimed person at a secure site access terminal or
searching a database of known subjects to identify an individual from some previously, captured biometric data. Interest in biometrics has grown rapidly as the technology has become more readily available and error rates have decreased.

In this thesis, we define recognition in the context of biometric systems, as the capability to perform verification and identification. Verification is the process of comparing one biometric pattern with another biometric pattern of the same subject resulting in either a rejection or acceptance decision. Whereas identification is the process of comparing one biometric pattern with a set of two or more biometric patterns in a given database in order to determine the most likely match.

With the advancements in technology, the need for passwords, swipe cards and pin numbers is slowly being replaced by uniquely identifying biometrics. Although public acceptance and the general understanding of the capabilities of this new technology hinder the switch from legacy systems, there are still great incentives to use biometrics:

- **Increased security:** Swipe cards and PIN numbers can easily be obtained by potential intruders, whereas acquiring a subject’s biometric requires specialist knowledge and equipment, and in most cases would not be possible without alerting the subject’s attention.

- **Reduced fraud:** It becomes extremely difficult for somebody to willingly give up his or her biometric data and hence sharing identities is virtually impossible. In addition, since it becomes necessary to expose one’s own biometric data (i.e. our own face), potential fraudsters are reluctant to attempt false verification.
- **Cost reduction**: By replacing plastic swipe cards, all cost associated with producing, distributing and replacing a lost card is completely eliminated.

In addition to the advantages mentioned above, once a biometric identification system is in place, other advantages begin to emerge. For example, there are known cases of large corporations discovering several of their employees were in fact the same person, having managed to obtain numerous identities on the company payroll system. This is something easily identifiable and avoidable when many employees appear to have the same facial biometric. Without the biometric system in place, any intentional misleading could have been difficult to prove, putting the incident down to a clerical error, but the ability to view the same face logged in as multiple people is extremely convincing evidence.

These incentives have lead to the emerge of several biometric options over the last few years. The most common being fingerprint, face and iris recognition but other examples include the retina, voice, skin texture, ear shape, gait (walking stride), hand geometry, vein pattern, thermal signature and hand-written signature. Each has its own advantages and may be particularly suited towards specific applications. For example, fingerprint scanners are small, light and relatively cheap, allowing for integration into a wide range of mobile devices. The iris pattern is so complex and diverse that a false match is unlikely to occur even between millions of subjects whereas the less accurate thermal signature can be taken in the dark from a distance.

Face recognition, although not necessarily suitable for all applications, exhibits several key advantages over the other biometrics, which we now discuss in detail:
Non-intrusive: While most biometrics require some degree of user interaction in order to acquire biometric data, such as looking into an eye scanner or placing a finger on a fingerprint reader, accurate face recognition can be performed by simply glancing at a camera from a distance. This non-contact biometric acquisition is highly desirable when subjects being scanned are customers, who may have some reluctance due to the big-brother stigma or associated criminality-surrounding acquisition of personal data and therefore the whole process needs to be kept as convenient as possible. This capability can be taken a step further, using strategic camera placement to perform recognition even without the subject’s knowledge. An obvious example would be Closed Circuit Television (CCTV) cameras monitoring an area for known criminals or tracking a suspected terrorist from one location to another.

Public acceptance: It has become apparent that face recognition systems generally receive a higher level of public acceptance than most other biometrics. This is perhaps partly due to the non-intrusive nature of face recognition, but may also be the result of greater understanding and empathy of how the technology is capable of recognizing a face. Another factor is that other biometric systems, say fingerprints are closely associated with the detection of criminals. Moreover, a more committed action on behalf of the subject is highly required such as leaning into an eye scanner (e.g. Iris recognition) or making contact with some other scanning device (e.g. fingerprint recognition). Whatever the reason may be, people have now become accustomed to their facial image being required by numerous organizations and few people now object
to looking at a camera for the purpose of biometric recognition. With many obvious benefits of integrating biometrics into governmental organizations, public acceptance is an important factor if these systems are to be implemented nationwide.

- **Existing databases:** One key hold-up for any large organization considering implementation of a biometric system is the amount of time required in collection of a biometric database. Consider a police force using an iris recognition system. It would take a number of years before the database was of sufficient size to be useful in identifying suspects. Whereas large databases of high quality face images are already in place, so the benefits of installing a face recognition system are gained immediately after installation.

- **Analogy to human perception:** Perhaps the greatest advantage is that the biometric data required for face recognition is easily recognizable by humans. This allows for an additional level of backup, should the system fail. A human reviewing the same biometric source (the reference image and live query image) can always manually check any identification or verification result. Whereas any decision made by other biometric recognition systems, such as iris or fingerprint, would require an expert to provide any reliable confirmation. A second product of this duality with the human method of recognition is that the biometric data can be distributed to other organizations (from a police department to the airport authorities for example) and still be useful even if the other organizations do not have a face recognition system in operation.
A complete biometric face recognition system encompasses three main procedures. The preliminary step of face detection (Hsu 2002) which may include some feature localization is often necessary if no manual (human) intervention is to be employed. This involves the extraction of a face image from a larger scene. Many methods have been applied to this problem such as template-based techniques, motion detection, skin tone segmentation, Principal Component Analysis (PCA), and classification by Neural Networks (NN). All of which present the difficult task of classifying “non-face” images from those areas of a complex scene that do contain a face. This procedure is greatly aided if the conditions under which image acquisition is performed can be controlled. Therefore, it is not surprising that many algorithms currently available are only applicable to specific situations. Assumptions are made regarding the orientation and size of the face in the image, lighting conditions, background and subject co-operation.

The next procedure is that of searching and matching, often termed identification. This step takes the probe image extracted from the scene during the face detection step, and compares it with a database of known people (previously enrolled), searching for the closest matching images, thus identifying the most likely matching people. An important point regarding this process is that it does not produce a definitive ‘yes’ or ‘no’ decision as to whether any two images are of the same person or not. Instead the process simply indicates which images match the probe image more closely than the others do.

The final procedure is verification. This describes the process by which two face images are compared, producing a ‘yes’ or ‘no’ decision as to whether the images are of the same person. This process requires a query image (usually the live captured image) and a single pre-selected gallery image (also referred to as the target image). This pre-selection can take place
in a number of ways: a swipe card or pin number indicating the appropriate gallery image; an automated identification procedure as described above, selecting the most likely match from an image set; a manually selected image offered as a potential match. The two images in question are then compared producing a “same person” or “different people” classification. This decision is often made by application of a threshold to a similarity (or dissimilarity) score, such as that produced in the identification process. By adjusting this threshold value, one can change the balance between the number of false acceptances and false rejections.

1.3 ISSUES IN AUTOMATED FACE RECOGNITION SYSTEM

The problem of face recognition can be stated as follows: Given still images or video of a scene, identifying one or more persons in the scene by using a stored database of faces (Chellappa 1995). This issue is basically considered as a classification problem. Training the face recognition system with images from the known individuals and classifying the newly coming test images into one of the classes is the main aspect of the face recognition systems. The topic seems to be easy for a human, where limited memory can be a main problem; whereas the problems in machine recognition are manifold. Some of the possible problems for a machine face recognition system are:

- **Large Variability in Facial Appearance:** Whereas shape and reflectance are intrinsic properties of a face object, the appearance of a face is also subject to several other factors, including the facial pose (or equivalently, camera viewpoint), illumination, facial expression. In addition to these, various imaging parameters, such as aperture, exposure time, lens
aberrations, and sensor spectral response also increase intra-subject variations.

- **Facial expression change**: A smiling face, a crying face, a face with closed eyes, even a small nuance in the facial expression can affect facial recognition system significantly.

- **Illumination change**: The direction where the individual in the image has been illuminated greatly effects face recognition rate. A study on illumination effects on face recognition showed that lighting the face bottom up makes face recognition a hard task (Zhao et al 2000, 2003).

- **Aging**: Images taken some time apart varying from 5 minutes to 5 years changes the system accuracy seriously.

- **Rotation**: Rotation of the individual’s head clockwise or counter clockwise (even if the image stays frontal with respect to the camera) affects the performance of the system.

- **Size of the image**: A test image of size 20x20 may be hard to classify if original class of the image was 100x100.

- **Frontal vs. Profile**: The angle in which the photo of the individual was taken with respect to the camera changes the system accuracy.

### 1.4 LIMITATIONS OF FACE RECOGNITION SYSTEMS

Much research has been done on face recognition using global and local features over the last decade. By using global feature preservation approaches like PCA and Linear Discriminant Analysis (LDA), one can effectively preserve only the overall structure of face space, that are devoid of
the lack of local features which may play a major role in some applications. On the other hand, a local feature preservation approach namely Locality Preserving Projections (LPP) preserves local information and obtains a face subspace that best detects the essential face manifold structure; however, it also suffers loss in global features which could be important in some of the applications.

Face recognition approaches considering large variations in the visual stimulus due to illumination conditions, viewing directions or poses, facial expressions, aging, and disguises such as facial hair, glasses, or cosmetics have been done earlier. However, in reality the noises that may embed into an image document during scanning, printing or image capturing process will affect the performance of face recognition approaches. Although different filtering algorithms are available for noise reduction, applying a particular filtering technique that is sensitive to one type of noise to an image which has been degraded by another type of noise, leads to unfavorable results. In turn, these conditions stress the importance of the design of robust face recognition approaches that retain recognition rates even under different types of noisy conditions. Moreover, in reality, many face recognition approaches exist and produce good results for noiseless environments but not with various noises.

In the face recognition applications, classification is generally achieved by finding the minimum distance or maximum variance among the training and testing feature set either using neural networks or other conventional approaches. This often leads to wrong classification when presenting untrained or unknown image for recognition since the classification process locates at least one matching cluster that has minimum distance or maximum variance among the existing clusters. But for the
security related applications, these new facial image should be reported as untrained image and the necessary action has to be taken accordingly.

1.5 RESEARCH CONTRIBUTIONS

This thesis aims to cover a wide range of face recognition approaches, including the technical background, ideas, concepts and some of the more practical issues involved. The emphasis will be on research into methods of improving existing systems, while introducing new approaches and investigating unexplored areas of research. Although the focus will tend towards the theoretical, we will prototype the algorithms as verification and identification applications applied to real-world data. We will also touch upon some of the more practical implementation issues that arise when using such systems in the real world, highlighting any additional work or technology that must be realized before a final application is implemented. The ultimate aim will be to produce a fully functional face recognition engine (providing the core verification and identification functions), which is not impaired by some of the shortcomings of existing face recognition systems.

In essence, the thesis summarizes the facial image recognition based on a combined approach of preserving global and local features, and issues related to optimize face recognition. The main objective of the thesis is to design, analyze, and study the following new approaches to address the most important challenges and to optimize the face recognition systems. The objectives are

1. To design and study a new approach for face recognition system that uses a combination of global and local features to get the advantages of global features and local features preservation approaches.
2. To design and analyze the robustness of the proposed face recognition system under various noisy environments such as Gaussian noise, speckle noise, salt and pepper noise and quantization noise in terms of percentage of correct classification.

3. To design and study the use of correlation based similarity measurement technique for improved recognition results in the face recognition applications. Also to compare the performance of this technique in various feature spaces.

4. To design and analyze the two new techniques for adaptive face recognition which identifies and reports the untrained image as new image when presenting untrained image to the face recognition system.

1.6 ORGANIZATION OF THE THESIS

The thesis is organized in seven chapters.

Chapter 1: The ‘Introduction’ gives a brief account of the Face Recognition System and the various considerations needed. The importance and the need of new approaches for face recognition have been discussed. The challenges and issues in the implementation of new approach for face recognition are discussed. The main objective of the thesis, research contribution, and thesis organization are also given.

Chapter 2: In ‘Literature Survey’, a detailed collection of literature on face recognition methods is presented. It provides a literature review to have the necessary background knowledge for a general understanding of the challenges, issues and limitations of the appearance based face recognition systems. This chapter outlines the research works already carried out by
different researchers so far related to this objective. It also details the various feature based and appearance based approaches such as Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), Locality Preserving Projections (LPP) and other approaches applied to the face recognition problem.

**Chapter 3:** A new combined approach for recognizing faces which preserve both global and local information has been introduced in this chapter. This approach combines the global feature extraction approach LDA and local feature extraction approach LPP to achieve a high quality feature set called Combined Global and Local Preserving Features (CGLPF) for facial image representation and recognition.

**Chapter 4:** In this chapter, numerous experiments have been conducted to analyze the robustness of the proposed Combined Global and Local Preserving Features (CGLPF) approach along with other existing conventional approaches under different types of noises such as Gaussian noise, speckle noise, salt and pepper noise and quantization noise and the results are compared with that of other traditionally employed approaches.

**Chapter 5:** It describes the improvements carried out in the CGLPF based face recognition in order to reach the maximum results. A correlation based face matching is employed in the combined global and local preserving feature space for this purpose. Also the comparison has been performed to show the performance of this approach in various feature spaces.

**Chapter 6:** In face recognition applications, the normal classification process often leads to wrong classification when presenting untrained or unknown image for recognition since the classification process locates at least one matching cluster that has minimum distance or maximum variance among the existing clusters. But for the security related applications,
these new facial image should be reported as untrained image and the necessary action has to be taken accordingly. In this chapter, the two new techniques based on minimum matching distances of wrong classifications and technique based on within-class and between-class distances are proposed for this purpose.

Chapter 7: It summarizes the outcome of this research work and possible future research directions. The work concludes with the effectiveness of the combined approach for facial image recognition that combines the global and local features preservation approach. It explores the robustness of this approach in various noisy environments. The performance of the combined feature space for adaptive face recognition in real-time environment is also given.