CHAPTER 1

INTRODUCTION

1.1 OVERVIEW OF BIOMETRIC SYSTEM

Biometrics is a term that encompasses the application of modern statistical methods to the measurements of biological objects (Zhao et al., 2000). Hence, biometric recognition refers to the use of distinctive physiological and behavioral characteristics (e.g. face, fingerprint, hand geometry, iris, gait, and signature), called biometric identifiers or simply biometrics, for automatically recognizing a person. This has been used in several domains, such as person authorization examination in e-Banking and e-Commerce transactions or within the framework of access controls for secure areas.

Biometric-based techniques have emerged as the most promising option for recognizing individuals in recent years since, instead of authenticating people and granting them access to physical and virtual domains based on passwords, PINs, smart cards, plastic cards, tokens, keys and so forth, these methods examine an individual’s physiological and/or behavioral characteristics in order to determine and/or ascertain his identity. Passwords and PINs are hard to remember and can be stolen or guessed; cards, tokens, keys and the like can be misplaced, forgotten, purloined or duplicated; magnetic cards can become corrupted and unreadable. However, an individual’s biological trait cannot be misplaced, forgotten, stolen or forged. Biometric-based technologies include identification based on physiological
characteristics (such as face, fingerprints, finger geometry, hand geometry, hand veins, palm, iris, retina, ear and voice) and behavioral traits (such as gait, signature and keystroke dynamics) (Jain et al., 1999).

Ideally the biometric characteristics used should have the following properties:

**Robustness:** This means that the biometric should be sufficiently invariant (Permanence) over a period of time and thus maintain a low intra-class variability.

**Distinctiveness:** This indicates that biometric identifiers should differentiate (Uniqueness) any two persons and thus have large inter-class variant.

**Availability:** Ideally, a biometric identifier should be possessed by every person (Universality).

**Accessibility:** The characteristic should be easy to acquire (Collectability).

A biometric system is essentially a pattern-recognition system. Such a system involves three aspects: data acquisition and preprocessing, data representation, and decision making. It can thus compare a specific set of physiological or behavioral characteristics extracted from a person with a template/model acquired beforehand, and recognize the individual. The digital representation recorded in a database as a description of a physical trait is defined as a template and is obtained by feature extraction algorithms. Among the different traits, the motivations behind using face and fingerprint for person authentication are manifold. In order to explain the impetus behind the use of any biometric system, some important applications are described in the following section.
1.1.1 Applications of Biometrics

Biometrics has been widely used in forensic applications such as criminal identification and prison security. It also has a strong potential to be widely adopted in civilian applications such as e-Banking, e-Commerce, and access control. Due to the huge increase in the use of electronic transactions, e-Banking and e-Commerce are becoming the most important emerging application of biometrics. Credit card and smart card security, ATM security, check cashing and fund transfers; online transactions and web access are some of the examples of the applications. The token-based authentication used in physical access control is gradually replaced by biometric systems. Similarly, knowledge-based authentication (e.g. password) for remote login and data access applications are substituted by biometrics. Other biometric applications include welfare disbursement, immigration checkpoints, national ID, voter and driver registration, and time and attendance.

1.1.2 Reason for Selecting Face Recognition Over Other Biometrics

- It is non intrusive and requires no physical interaction on behalf of the user. Almost all the technologies require some voluntary action by the user, i.e., the user needs to place his hand on a hand-rest for fingerprinting or hand geometry detection and has to stand in a fixed position in front of a camera for iris or retina identification. However, face recognition can be done passively without any explicit action or participation on the part of the user since face images can be acquired from a distance by a camera. This is particularly beneficial for security and surveillance purposes.

- It is accurate and allows for high enrollment and verification rates.
It does not require an expert to interpret the comparisons.

It can use a person's existing hardware infrastructure; existing cameras and image capture devices can work with no problem.

One can use existing images without having to re-enroll every user (E.g.: passports, ID cards, driver's licenses etc.)

It is only biometric that enables performing passive identification in one to many environments (e.g.: identifying a terrorist in a busy airport terminal).

In some cases one may also want to look at deploying multilayered biometric. Example of multi layered biometric would be the use of both finger print scans and facial scans in one unified access control devices.

Furthermore, data acquisition in general is fraught with problems for other biometrics: techniques that rely on hands and fingers can be rendered useless if the epidermis tissue is damaged in some way (i.e., bruised or cracked). Iris and retina identification requires expensive equipments and are much too sensitive to any body motion. Voice recognition is susceptible to background noises in public places and auditory fluctuations on a phone line or tape recording. Signatures can be modified or forged. However, facial images can be easily obtained with a couple of inexpensive fixed cameras. Good face recognition algorithms and appropriate preprocessing of the images can compensate for noise and slight variations in orientation, scale and illumination. Finally, technologies that require multiple individuals to use the same equipment to capture biological characteristics
potentially expose the user to the transmission of germs and impurities from other users. However, face recognition is totally non-intrusive and does not carry any such health risks.

1.2 FACE RECOGNITION SYSTEM

Face recognition is a necessary aspect of our social interactions. Fortunately the faculty of recognizing faces is very robust and is performed with ease by humans. The vast majority of humans can effortlessly overcome difficulties in the face recognition process such as different illumination conditions, faces with occluded details, different facial expressions or even inverted faces. This ability has induced scientists to argue that the human brain contains a processing region committed to the recognition of faces.

The face is our primary focus of attention in social life, playing an important role in conveying identity and emotions. We can recognize a number of faces learnt throughout our lifespan and identify faces at a glance even after years of separation. This skill is quite robust despite large variations in visual stimulus due to changing conditions, aging and distractions such as beard, glasses or changes in hairstyle.

Computational models of face recognition are interesting because they can contribute not only to theoretical knowledge but also to practical applications. Computers that detect and recognize faces could be applied to a wide variety of tasks including criminal identification, security system, image and film processing, identity verification, tagging purposes and human-computer interaction. Unfortunately, development of computational model of face detection and
recognition is quite difficult because faces are complex, multidimensional and meaningful visual stimuli. Face detection is used in many places nowadays especially the websites hosting images like Picasa, photo bucket and face book. The automatical tagging feature adds a new dimension to sharing pictures among the people who are in the picture and also gives the idea to other people about who the person is in the image. In our research, we have studied and implemented a effective face detection algorithm which takes human skin colour into account.

1.2.1 Generic Face Recognition System

The input of a face recognition system is always an image or video stream. The output is an identification or verification of the subject or subjects that appear in the image or video. Some approaches (Zhao et al., 2003) define a face recognition system as a three step process - see Figure 1.1. From this point of view, the face detection and feature extraction phases could run simultaneously.

![Face Detection Diagram](attachment:face_detection_diagram.png)

**Figure 1.1 Generic face recognition system**

Face detection is defined as the process of extracting faces from scenes. So, the system positively identifies a certain image region as a face. This procedure has many applications like face tracking, and pose estimation or compression. The next step, feature extraction involves obtaining relevant facial features from the data. These features could be certain face regions, variations, angles or measures, which can be human relevant (e.g. eyes spacing) or not. This phase has other applications
like facial feature tracking or emotion recognition. Finally, the system recognize the face. In an identification task, the system would report an identity from a database. This phase involves a comparison method, a classification algorithm and an accuracy measure. It uses methods common to many others which also do some classification process like sound engineering, data mining etc. These phases can be merged, or new ones could be added. Therefore, many different engineering approaches to a face recognition problem could be found. Face detection and recognition could be performed in tandem, or proceed to an expression analysis before normalizing the face (Turk., 2001).

The objective of this thesis is to develop a method of face recognition that is fast, robust, reasonably simple and accurate with a relatively simple and easy to understand algorithms and techniques. The examples provided in this thesis are real-time and taken from standard databases.

1.3 NEED FOR THE PRESENT STUDY

The necessity for personal identification in the fields of private and security systems has made face recognition one of the main fields among other biometric technologies. The importance of face recognition arises from the fact that a face recognition system does not require the cooperation of the individual while the other systems need that.

Traditionally, computer vision systems have been used in specific tasks, such as performing tedious and repetitive visual tasks of assembly line inspection. Current development in this area has moved toward more generalized vision applications such as face recognition, video coding techniques, biometrics,
surveillance, man-machine interaction, animation and database indexing and many other applications that have face detection as the primary building block of their systems. Many of the current face recognition systems assume the availability of frontal faces. In reality this assumption may not hold due to the nature of face appearance and environment conditions. The exclusion of background in these images is necessary for reliable face classification. However, in realistic application scenarios, a face could occur in a complex background and in many different positions and sizes. Recognition systems that are built on the standard face images are likely to mistake areas of the background as faces. In order to rectify the problem, a visual processor is needed to localize and extract the face region from the background. Face detection is one of the visual tasks that humans can do effortlessly. However, in computer vision terms, this task is not easy. A general statement of the problem can be defined as follows: Given an image or a video sequence, detect and localize an unknown number (if any) of faces. The solution to this problem involves segmentation, extraction and verification of faces and possibly facial features from an uncontrolled background. An ideal face detector should achieve this aim despite illumination, rotation, different facial expressions, orientations and camera distance from the object. In the last two decades considerable progress has been made to increase the accuracy of the face detectors while many different methods have been introduced in this area.

1.4 SCOPE AND OBJECTIVE OF THE PRESENT STUDY

There is a wide range of commercial applications today in which an automatic face recognition system seems appropriate and essential. As a result, research in this field of image analysis has been intensified. For example one still needs today a password to access a computer, a pin in order to use an ATM
machine, and quite a few others passwords to be allowed entry to the Internet. In addition a very exciting application that is steadily advancing is the creation of “smart rooms”, i.e. rooms that have embedded in them cameras, microphones and other sensors and use their inputs to recognize the identity of the persons in the room and try to interpret their gestures in order to assist them. Ideally smart rooms will assume the roles of invisible servants. Even though several biometric methods for identification, such as fingerprint analysis, have proved to be quite effective, nevertheless they need the cooperation of the individual. On the other hand a face recognition system can be effective without the participant’s collaboration.

The objectives which make facial feature detection a difficult task are common to many computer vision problems, especially general object recognition. Objectives which are met in the proposed work are listed as follows:

- To identify the human faces which vary substantially between individuals
- To identify the human faces even with different expression variations
- To identify human faces both in plane and out of plane rotation of the head causes major changes in visual appearance
- To identify human faces with different lighting conditions
- To identify human faces with occlusion (i.e.,) Facial hair or glasses can cause the facial features to be obscured.
- To identify human faces with minimum false acceptance and rejection rate.
- To identify human faces in minimum recognition time
1.5 CHALLENGES OF THE PRESENT STUDY

The challenges which make facial feature detection a difficult task are common to many computer vision problems, especially general object recognition. Some face specific problems are as follows:-

Identity variation: Human faces vary substantially between individuals

Expression variation: A human face is capable of a great deal of variety, e.g. when blinking or opening the mouth

Head rotation: Both in plane and out of plane rotation of the head causes major changes in visual appearance

Lighting variation: The lighting of a face causes non-linear effects on the value of image pixels

Scale variation: The face can appear at a wide range of sizes

Occlusion: Facial hair or glasses can cause obscurity in facial features.

False positives: Background regions of the image may resemble human faces and may lead to false detections

Speed Constraints: Face detection is usually followed by further processing, e.g. face recognition, so should ideally be an efficient real-time algorithm.

Any one of the above problems may cause failure of a face detector or facial feature finding algorithm. In general, the difficulty in face and feature detection depends largely on the data set used and the extent to which these variations are controlled. A general statement of the problem of machine recognition
of faces can be formulated as follows: Given still or video images of a scene, identify or verify one or more persons in the scene using a stored database of faces. In identification problems, the input to the system is an unknown face, and the system reports back the determined identity from a database of known individuals, whereas in verification problems, the system needs to confirm or reject the claimed identity of the input face.

The solution to the problem involves segmentation of faces (face detection) from cluttered scenes, feature extraction from the face regions, recognition or verification. Robust and reliable face representation is crucial for the effective performance of face recognition system and still a challenging problem.

1.6 APPLICATIONS OF FACE RECOGNITION SYSTEM

1.6.1 Law Enforcement and Justice Solutions

➢ Today's law enforcement agencies are looking for innovative technologies to help them stay one step ahead of the world's ever-advancing criminals.

➢ As such, Face Recognition System (FRS) is committed to developing technologies that can facilitate the jobs of the law enforcement officer. This includes acclaimed Computerized Arrest and Booking System (CABS) and the childbase protection, a software solution for global law enforcement agencies to help protect and recover missing and sexually exploited children, particularly as it relates to child pornography.
1.6.2 CABS

➢ Store all offence-related data in one easy-to-use system -- data is entered once and only once.

➢ Integrate with any database -- including other detachments and other applications (RMS, CAD, Jail Management systems, and "most-wanted" databases).

➢ Link victims to offenders -- to aid in criminal analysis and investigations

➢ Capture and store digital images of the offender -- encode all mug shots, marks, tattoos, and scars

➢ Perform rapid and accurate searches -- on all data and image fields for crime statistics and reporting

➢ Produce digital lineups -- using any stored image in minutes

➢ Identify previous offenders -- pre-integrated with advanced biometric face recognition software.

1.6.3 Childbase Protection

Childbase is an application that helps protect and recover missing and sexually-exploited children, particularly those children victimized through child abuse images.
1.6.4 Identification Solutions

With regard to primary identification documents, (Passports, Driver's licenses, and ID Cards), the use of face recognition for identification programs has several advantages over other biometric technologies.

➢ Leverage your existing identification infrastructure. This includes, use of existing photo databases and the existing enrollment technology (e.g. cameras and capture stations); and

➢ Increase the public's cooperation by using a process (taking a picture of one's face) that is already accepted and expected;

➢ Integrate with terrorist watch lists, including regional, national, and international "most-wanted" databases.

1.6.5 Homeland Defense

➢ Since the terrorist events of September 11, 2001, the world has paid greater attention to the idea of Homeland Defense, and both governments and private industries alike are committed to the cause of national defense.

➢ This includes everything from preventing terrorists from boarding an aircraft, to protecting critical infrastructure from attack or tampering (e.g. Dams, bridges, water reservoirs, energy plants, etc.), to the identification of known terrorists.
1.6.6 Airport Security

➢ Airport and other transportation terminal security is not a new thing. People have long had to pass through metal detectors before they boarded a plane, been subject to questioning by security personnel, and restricted from entering "secure" areas. What has changed is the vigilance with which these security efforts are being applied.

➢ The use of biometric identification, can enhance security efforts already underway at most airports and other major transportation hubs (seaports, train stations, etc.).

➢ This includes the identification of known terrorists before they get onto an aircraft or into a secure location.

1.6.7 Immigration

➢ Most countries do not want to be perceived as being a "weak link" when it comes to accepting immigrants and refugees, particularly if that individual uses the new country as a staging ground for multinational criminal and terrorist activities. Consequently, governments around the world are examining their immigration policies and procedures on an on-going basis.

➢ Biometric technology, particularly face recognition software, can enhance the effectiveness of immigration and customs personnel. After all, to the human eye, it is often difficult to determine a person's identity by looking at a photo, especially if the person has
aged, is of a different ethnic background, has altered their hair style, 
shaved their beard, etc. FRS does not have this difficulty.

1.6.8 Access Control

➢ The use of biometric technology, particularly face recognition 
software (either independently or as one part of a multi-layered 
bio metric solution), can enhance security efforts considerably.

➢ Biometric identification ensures that a person is one they claim to be, 
eliminating any worry of someone using illicitly obtained keys or 
access cards.

1.6.9 Financial Services

➢ The financial services industry revolves around the concept of 
security. Yet for the most part, security within the industry is limited 
to a simple Personal Identification Number (PIN) or a password.

➢ Biometrics, particularly face recognition software, can improve the 
security of the financial services industry, saving the institution time 
and money both through a reduction in cases of fraud and the 
administration expenses of dealing with forgotten passwords.

➢ Furthermore, biometric-based access control units can safeguard 
vaults, teller areas, and safety deposit boxes for protection against 
theft.
The use of biometrics can also ensure that information remains confidential while deterring identity theft, particularly as it relates to ATM terminals and card-not-present e-commerce transactions.

1.6.10 Scene Analysis and Surveillance Solutions

- This includes the ability to extract, categorize, and search non-facial imagery. For example, within the ambit of the law enforcement application it allows one to capture, archive, and retrieve such identifying characteristics as tattoos, marks, or scars.

- It can also analyze scenes from either streaming or archived video, "looking" for out-of-the-ordinary occurrences, the presence of certain vehicles, specific faces, etc.

- This is beneficial and can save significant time and money to those individuals who spend hours, days, or weeks monitoring video streams (i.e. Examining a bank's security in a criminal investigation).

The scheme of research is presented in Figure 1.2.
A NOVEL APPROACH TO FACE RECOGNITION SYSTEM

Experiments
- Feature Extraction
  - GLCM
  - CCM
  - LTP
  - WI.D
- Face Recognition Techniques
  - PCA
  - KPCA
  - PM
- Gender & Expression Identification
  - PNN
  - SVM

Observation
- Computerized Face Recognition with Gender & Expression Identification
- Observations with different threshold values
- Recognition time
- FAR & FRR

Analysis
- Performance Analysis
  - Recognition time Analysis
  - Analysis of False acceptance & False rejection rate
  - Analysis of results using proposed algorithms

Results and Discussions
- Effect of GLCM & CCM with PCA & KPCA in enhancing recognition accuracy
- Comparisons of results with existing techniques
- Effect of threshold values on output responses

Conclusion
- Conclusions

Figure 1.2 The Scheme of Research
1.7 ORGANISATION OF THESIS

The thesis is divided into two main parts. The first part deals with the designing of face recognition systems with different combinations of algorithms. The second part of the thesis presents the results and discussions of the output responses with respect to different algorithms used and also evaluate the performance of the recognition system by calculating the performance indicators such as recognition time, accuracy and false acceptance and rejection rate.

Chapter 1 gives a brief description of basic knowledge about the biometric recognition and also outlines the most important technique in biometric called face recognition system. The main objectives of the present study, scope and outline of the thesis are elaborated in this chapter.

Chapter 2 is dedicated to the state-of-art of current knowledge about face recognition. The literatures about the face authentication/verification and recognition are reviewed. Knowledge of the face recognition and available techniques for evaluating the performance of recognition systems are discussed.

In Chapter 3 the proposed work is described. A discussion of the techniques and the databases used for face authentication and verification systems are presented. These results include recognition time and false acceptance and rejection rate.

Chapter 4 is dedicated to the design of a face recognition system using the combinations of gray level co-occurrence matrix, colour covariance matrix, principal component analysis and kernel principal component analysis. The analysis
of performance evaluations is carried out to make the system work at the highest accuracy level.

Chapter 5 deals with a face recognition system along with additional features like gender identification and expression identification is presented.

Chapter 6 presents the results and discussions of the output responses with respect to different algorithms used and also evaluate the performance of the recognition system by calculating the performance indicators such as recognition time, accuracy and false acceptance and rejection rate.

Chapter 7 deals with the conclusion of the thesis and suggestions for future study of the work also highlighted.