University of Southern Queensland

Faculty of Engineering & Surveying

Biometric Analysis for Remote Examination System

A dissertation submitted by

J. Hockey

in fulfilment of the requirements of

ENG4112 Research Project

toward the degree of

Bachelor of Electrical and Electronic Engineering

Submitted: October, 2011

Abstract

Tertiary study is considered by many to be a necessary step in not only increasing knowledge, but also for employability and receiving promotions. Accessing Universities, particularly through on campus study can be problematic for those working full time or raising a family. The University of Southern Queensland promotes external studies and although they provide for the most part flexibility examinations are rigid. The ability to complete exams remotely may be an ideal solution; however security and exam integrity must be maintained. This dissertation considers the possibility of using biometric verification as a way of ensuring security.

While many biometric techniques are considered only facial recognition adheres to all of the specifications of a remote examination system. Over the past twenty years facial verification has been a subject of interest, particularly in the area of security. Numerous algorithms have been proposed, stemming primarily from linear and multi-linear algebra.

The Eigenface algorithm based on Principal Component Analysis was implemented to determine if accuracy rates required by a remote examination system could be achieved. The tests were conducted on the XM2VTS database as well as a small test database composed of images similar to those expected during a remote examination.

The algorithm was implemented using MATLAB and results show that Eigenfaces was able to achieve results of 78.8% accuracy, with an imposter error as low as 19.36%. The tests conducted also conclude that pre-processing techniques, in particular face detection and cropping will increase verification rates of the algorithm.

Facial verification is considered to be a feasible method of ensuring security and maintain examination integrity for a remote system.

University of Southern Queensland

Faculty of Engineering and Surveying

ENG4111/2 *Research Project*

Limitations of Use

The Council of the University of Southern Queensland, its Faculty of Engineering and Surveying, and the staff of the University of Southern Queensland, do not accept any responsibility for the truth, accuracy or completeness of material contained within or associated with this dissertation.

Persons using all or any part of this material do so at their own risk, and not at the risk of the Council of the University of Southern Queensland, its Faculty of Engineering and Surveying or the staff of the University of Southern Queensland.

This dissertation reports an educational exercise and has no purpose or validity beyond this exercise. The sole purpose of the course pair entitled \Research Project" is to contribute to the overall education within the student's chosen degree program. This document, the associated hardware, software, drawings, and other material set out in the associated appendices should not be used for any other purpose: if they are so used, it is entirely at the risk of the user.

Prof F Bullen

Dean

Faculty of Engineering and Surveying

Certification of Dissertation

I certify that the ideas, designs and experimental work, results, analyses and conclusions set out in this dissertation are entirely my own effort, except where otherwise indicated and acknowledged.

I further certify that the work is original and has not been previously submitted for assessment in any other course or institution, except where specifically stated.

JOSHUA HOCKEY

0050086081

_____

Signature

_____

Date

Acknowledgements

I would like to acknowledge the help I received throughout the course of preparing and completing this dissertation. I am appreciative of the support my supervisor, Associate Professor John Leis, has offered; firstly for suggesting the project and secondly for helping with the initial formulation of the project. To my lovely wife Kara, and my two wonderful children, Noah and Savannah, for supporting me through my final year. To my mother, Lorraine Hockey, and father, Bruce Hockey, for suggestions and contributions to the project.

J. Hockey

University of Southern Queensland
October *2011*

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Universities are tertiary institutes which provide higher level education and qualifications to those who are able to successfully complete all of the requirements for a particular degree. The most certain way to determine if the student has satisfied the competency requirements for a given profession is to test the students understanding and knowledge of each course by way of mid-semester and end of semester exams. Exams are completed under strict supervision, and rigid guidelines are adhered to at approved examination centres. The students undertaking the exams are carefully monitored to ensure that they complete the exam questions independently. After all, tertiary institutions have an ethical responsibility to the community to ensure that their graduates have indeed satisfactorily completed all requirements and have obtained the necessary knowledge for a professional qualification.

While final semester exams have been completed in the same manner for many years the question is being posed:

"Is it possible to provide greater flexibility in examination procedures while maintaining integrity?"

Biometrics has been suggested as a possible solution to one part of a very complex situation. In particular a suitable biometric method must be found which is able to meet the security requirements and physical requirements of a remote examination system. If a suitable method can be implemented it may provide greater flexibility for students studying externally.

1.1 Aims and Objectives of the Project

This project was designed to conduct research into the feasibility of implementing remote examinations for distance education students at the University of Southern Queensland (USQ). The purpose is twofold, firstly to conduct an analysis of the current methods used by USQ and the system requirements that would be necessary in a remote examination system; secondly to conduct research into a biometric technique which would be suitable for a remote examination system and to implement and test a suitable algorithm.

The goals of the project are to:

1. Research background information on biometric analysis options.
2. Analyse current USQ examination requirements and provide system specifications that would need to be implemented for a remote examination system.
3. Research current algorithms for a chosen biometric system and determine their suitability within the context of a remote identification system.
4. Implement a biometric analysis algorithms using MATLAB
5. Evaluate the raw algorithm by developing a test database which includes biometric information of a subject gathered under various conditions, similar to those expected during a remote examination.
6. Determine to what extent the use of appropriate pre-processing techniques can improve the effectiveness of the algorithm evaluated in 5.

Full details of the project specifications are provided in Appendix A.

1.2 Outline of the Dissertation

Chapter 2 provides background information on the current USQ examination procedures and requirements. It also provides an outline of the system requirements necessary for a remote examination system to be successful.

Chapter 3 details the necessity for a remote verification system to firstly be able to ensure that the correct student is undertaking the exam. There are three methods that are outlined which include knowledge verification, possession verification and biometric verification. Each is addressed in turn to determine the most suitable way of achieving security within a remote examination system. Finally the specifications for a biometric verification technique are discussed in the context of a remote exam.

Chapter 4 introduces both biometric authentication terminology and biometric authentication techniques. The terminology is discussed in detail to give an understanding of the field of biometrics and the requirements of a system to be successful. The biometric techniques are divided into active and passive techniques and are discussed within the context of the specifications for a remote verification system.

Chapter 5 discusses the many facial recognition techniques which have been implemented and tested. The algorithms are discussed in a mathematical context aiming to understand how a facial recognition problem can be solved by a computer. The facial recognition problem is essentially about pattern recognition and hence finding a way to encode and compare images. The effectiveness of each algorithm is considered by its ability to fulfil the requirements of the remote verification system.

Chapter 6 discusses the various databases which will be used to test the facial verification algorithm. It discusses in depth the creation of the XM2VTS database and the protocols used during testing. A brief description is given outlining the

difference between the test databases and real world application of the remote verification system.

Chapter 7 introduces the use of MATLAB for the implementation of the Eigen face algorithm. The primary focus is to discuss how the algorithm was implemented and the scripts that are involved with running the algorithm. This includes the pre-processing techniques used in order to enhance the accuracy of the algorithm. It also provides the methodology used during testing.

Chapter 8 discusses the results which were obtained during the testing phase for both databases.

Chapter 9 looks at the challenges for a facial recognition system in a real world application. It discusses the need for enrolment, as well as the necessity to deal with problems associated with lighting, pose, expression, alignment of the face, time variation and detecting fake faces.

Chapter 10 concludes the dissertation by looking at the achievements, project limitations and future work required.

Chapter 2

Background Information

2.1 Introduction

Higher-level education is valuable for career development, however, studying is not always practical for daily life. The underlying philosophy of The University of Southern Queensland (USQ) flexible learning is ‘life happens’ and that it should not impact on the opportunity for one to study at a tertiary level. For this reason USQ prides itself on the flexibility with which its courses can be taken and completed.

USQ was the pioneer in Australia for distance education and for the past 40 years has provided this mode of study to students around the world. (Currently, there are over 18 000 students undertaking studies through the distance education program from 80 countries, accounting for 75% of students enrolled at USQ. Whether due to work or family commitments, living remotely/internationally or simply due to the comfort and flexibility of studying from home, distance education has become the study method of choice (USQ, 2011)

Therefore catering for students studying by distance and developing new ways of making their studies flexible is a priority for USQ.

There are, however, two study requirements that students are unable to undertake in the comfort of their home, residential schools and examinations (USQ, 2011). Residential schools are intensive courses that are completed during USQ holiday periods and give external students the opportunity to engage with lecturers face-to-face. These classes are held at a USQ campus and require students to travel to attend. Examinations are held at the end of each semester and require that all students attend a formal examination centre. Exam centres have been set up by the University across Australia and in many countries overseas. If you live within 100km of an examination centre University policy states that you must complete your exams at that centre (USQ, 2011). Although students are encouraged to attend residential schools, many faculties do not require compulsory attendance in order to successfully complete the degree. Therefore for many students the only inflexible aspect to their studies is undertaking examinations and determining a more flexible mode for completing examinations would be extremely beneficial for distance students.

2.2 Current Examination Modes

According to the current USQ policies and procedures for completing examinations there are three exam modes, four exam types and three forms that exam questions can take. This information is provided in Table 2.0: Exam Modes, Types and Forms.

Table 2.0: Exam Modes, Types and Forms

Modes	• Closed • Restricted • Open
Types	• Home or online • Formal • Practical/ Clinical • Oral Exams
Forms	• Multiple Choice • Math based Questions • Written Questions

The mode and format of the examination is dependent on which particular course is being undertaken. Closed examinations are those where the candidate is restricted to bringing only writing instruments into the examination room. Restricted exams allow candidates to bring other equipment that is specified in the examination paper (i.e. calculator). Open exams are those where candidates can bring any written material into the examination room. All three examination modes require that students at no time have access to any electronic device, except a calculator where specified.

All formal examination writing is to be completed on official University examination booklets provided by USQ. All booklets, whether used or unused, must be returned to the examination supervisor at the end of the examination period. The examination booklets completed by external students are collected at each recognised exam centre and mailed to USQ for marking.

Students are required to bring a valid form of photo identification (ID) with them when sitting an examination. This is the primary means of security, ensuring that the correct person is undertaking the exam. The photo ID must remain on the table throughout the entire examination period. The supervisor is required to

match the ID photo and student name with the student taking the examination. If these items match it is concluded that the correct person is undertaking the exam. If the supervisor believes that either of these areas has not been satisfied then the examination paper may be revoked.

University policy states that examinations must be produced and printed five weeks before the start of the exam period for external courses. During this five week period exams are kept under security to ensure that the integrity of the examination is maintained. All students completing a course must complete the examination at the same time to ensure that information cannot be passed on to other students

2.3 Remote Examination

The 2020 vision of USQ as stated on their website is ‘to be recognised as a world leader in open and flexible higher education’ (USQ, 2011). While flexibility enables a greater number of students to participate in courses offered by USQ, it is imperative that quality is not jeopardised in granting ease of access. This is particularly true in the case of allowing students the flexibility to complete their examination remotely. The following sections outline the major issues associated with each mode of formal examinations, open, restricted and closed, as well as outlining potential security threats. Each examination mode has its own set of rules that must be adhered to and followed; they act as the foundation for the needs of a remote examination system. There are, however, some common rules that must be followed regardless of examination form. These are presented in Table 2.1: Common guidelines for all examinations

Table 2.1: Common Guidelines for all Examinations

Exam Form	Examination Guidelines
Open Closed Restricted	• Only the student whose name is on the examination booklet can complete the exam • No Collaborating with other students • No electronic device can be accessed by any student in an exam • 10 minutes perusal time • No writing on exam booklet during perusal time • Writing on the exam sheet is permitted during perusal • All exams shall be 2 hours in length • Students must leave photographic evidence on display throughout the test • All students enrolled in the course will complete the exam at the same time • Students will not take more than two examinations per day • Adjustments to exam policies can made for students with disabilities • Examination may be discontinued if a student fails to comply with a supervisors instructions • Students may leave the examination room for a toilet break if they are accompanied by a supervisor • Students must not leave an examination room once they have entered, without being accompanied by a supervisor • Students must remain silent once they have entered the examination room

2.4 Open Examinations

Open examinations are the most flexible of the three types of examinations as they allow students access to hard copy materials used and gathered throughout the semester. Table 2.2: Open Examination Procedures outlines further the rules which govern this type of examination.

Table 2.2: Open Examination Procedures

Exam Form	Examination Guidelines
Open	• Access to printed or written material • Access to a calculator

Information on open examinations can be found at < http://www.usq.edu.au/learningcentre/alsonline/assessment/exam/openexam>

2.5 Closed or restricted examinations

Restricted exams allow students to have access to instruments that are deemed necessary to successfully complete the examination; these are specified by the lecturer of the course. In particular the use of a pre-approved calculator is permitted throughout the exam. The calculator will be checked by the supervisor and the make and model placed on the top of the examination booklet.

Closed examinations only allow students to bring writing and drawing materials into the examination room. Students are not permitted the use of a calculator or other instruments to successfully complete these exams.

2.6 Penalties

The penalties for not adhering to the above rules vary depending on the severity of the misconduct. For instance if a student brings a calculator that is not approved into a restricted examination the calculator may be removed from the student or the batteries taken out to ensure that previous programming has been reset. If students write on their examination booklets before the end of the perusal time the booklet may be removed and replaced with another. These are minor

breaches to examination regulations and are punished accordingly. If the student is found to be collaborating with others during an examination, the student will be dismissed from the exam room and their booklet revoked. They will also be issued with a fail grade for that course. If the University considers the breach to

be serious academic misconduct they may discontinue their program and stop them from participating in any further higher education programs.

2.7 System Requirements for a Remote Examination System

Humans are very good at monitoring and processing multiple amounts of data as well as differentiating between many types of inputs. They have an innate ability to recognise and identify people with an extremely high level of certainty. This is evidenced by their ability to understand and recognise body language, determine behaviours and motives behind lip and eye movement as well as the ability to enforce instructions. Humans can easily alter the implementation of rules based on circumstances and an interpretation of what the instruction intended to achieve. One human is able to monitor many subjects while ensuring a high level of accuracy. Thus, humans are the most reliable source of accuracy when monitoring important activities, such as in examinations where instructions need to be implemented dogmatically. Humans are able to enforce the examination guidelines outlined in section 2.3 – 2.5, thus the integrity of the exam is maintained and therefore the correct scores are given to students based on their understanding of the content.

The guidelines state that only the student whose name appears on the examination paper is able to complete it. Humans possess very complicated yet reliable recognition capability that allows them to match faces. By ensuring that students have a current USQ student identification card, supervisors are able to conclude if the correct person is taking the exam. Likewise student collaboration, use of correct equipment and monitoring toilet breaks can all be accomplished effortlessly by a human supervisor.

In order to be effective the remote examination system must be able to undertake all responsibilities a human supervisor is able perform, as well as being able to enforce the guidelines and rules of the examination with a high degree of certainty.

The following sections outline the overall system requirements in order for the remote examination system to be successful. This is not a discussion of solutions to each of the problems, but rather an evaluation of considerations for determining if a remote examination system is plausible.

2.7.1 Student Verification

As mentioned previously verification is the foundation that all other security protocols are built on. This section is explored further in Section 3.

2.7.2 Means of completing an Exam

Currently, students are required to complete their end of semester exams by hand in written form, however this poses a problem when students are completing their exams remotely. In particular, how is the strict time limit adhered to if students are writing on a sheet of paper which they must subsequently mail to USQ? For this reason it is proposed that students complete their examinations online via computer. While this may provide the ability to the University to monitor student access simultaneously, other problems are created which include:

- How do students submit rough workings?
- How do students enter formulae for mathematics?
- Will examinations need to be changed to cater for such problems?
- Will this affect the integrity of the exam?

Although these problems must be addressed the problem of security is of primary importance when completing an examination via an internet connected personal computer.

2.7.3 Monitoring access to materials

It is a requirement of examinations that no electronic devices are accessed during examination periods. Obviously this is contradicted if students are being asked to complete their exams on a personal computer with access to the internet.

Therefore, the system must be able to ensure that during closed examinations, students are unable to use internet, phones, other sources of information stored on a hard drive including books or study guides. The system must be able to monitor these sufficiently to ensure exam integrity.

2.7.4 Monitoring collaboration

Collaboration with other people during examinations is strictly forbidden by USQ. This problem is multidimensional and encompasses many mediums for student collaboration. During an examination the system must prohibit students from talking to others, ensure that multiple students are not sitting in the same room, as well as ensuring that the exam cannot be copied and emailed to students who have not yet completed the exam.

The system must also monitor students' right to have a toilet break if they desire during an examination. Presently, supervisors will accompany students to the toilet and back to the examination room. Will this be possible during a remote examination, or are students forced to remain at their personal computer? What are the ethical issues surrounding such a delicate problem?

These considerations must be satisfied if a remote system is to be implemented.

2.7.5 Revoking exams if failure to comply with Instructions

A human supervisor is able to make complex decisions based on multiple inputs and circumstances to determine if a student has breached University policy and as such should have their examinations revoked. To fulfil this criterion considerations include:

1. Does the system lock people out from completing an examination if the computer system says that they fail to comply?
2. What if the system isn't perfect? How many chances are given?
3. Are there different levels of failure to comply?

The disciplinary action taken can be determined only by the degree of certainty provided by the system.

2.7.6 One Exam per Day

Presently, students are only allowed to complete one examination per day. At the USQ examination centre the examinations are held at 8:30am and 2:30pm. This ensures that a minimum time period of eighteen hours has elapsed before students complete another examination. Therefore procedures need be put in place that prevents students from completing more than one examination within a minimum of eighteen hours.

2.7.7 CMA

The considerations discussed, paint a bleak picture for the possibility of remote examinations. However, it should be noted that there are already assessments provided by USQ that require computer access and submission. These assignments are known as Computer Managed Assessment and often do not carry many marks, due to the lack of security. Implementing a biometric verification system for CMA would be an appropriate first step for creating flexible exams. This may be implemented in a course such as Electronic Measurement (ELE 3506) where the final assignment is a 24 hour CMA worth 50% of the course marks. Ensuring that the correct student completes this assessment is crucial and at the moment is not monitored sufficiently.

2.8 Chapter Summary

Many USQ students study their degrees via flexible learning pathways. They are an integral part of the university and as a result USQ constantly reviews methods of teaching to improve their distance education. Although studying externally provides a degree of freedom there are still areas that require students to travel and complete assessment at appointed time. This is true particularly of final semester exams where students must complete the exam at the allotted time and at an exam official centre.

Examinations come in many forms and require students to prove their knowledge whilst complying with the guidelines set out for the particular exam. At the present time human supervisors are used to ensure that the student completing the examination is the correct individual and that all students comply with the guidelines. Human supervisors are competent to complete these tasks efficiently with a high degree of certainty.

In order to provide a greater level of flexibility for external students, a remote examination system is being investigated. The system must be able to accurately and reliably monitor all of the examination requirements to ensure rules are being followed. There are many considerations and complications surrounding a remote examination system that need to be resolved.. Identifying problems is rather straightforward, however resolving these is a lot more complicated. Primarily, the system needs to be able to correctly verify student identity when undertaking examinations.

Chapter 3

Ensuring Correct Student Completion of Exam

3.1 Introduction

Chapter 2 gives a wide-ranging list of requirements that need to be addressed in order to be confident that completing examinations remotely would not affect their integrity. Some items build on the foundations laid by others and although the secondary could be carried out independently, they would be unnecessary if the foundation item failed. As an example, in an open examination students are able to access any written material they deem helpful. The system could test to see if this requirement is fulfilled and if so the student is allowed to continue their examination. However, if the system was to first check the identity of the student and is unable to verify their identity the examination can be revoked. This would eliminate the need to ensure that the items accessible during the examination were within the specification set out for the exam.

Essentially ensuring that the correct person completes the examination is a matter of security. It is often said that security is composed of three elements: knowledge, possession and biometric verification. Therefore the remainder of this dissertation will focus on how this security can be achieved.

3.2 Current Exam Security

At the present time security for entrance into an examination is based on possession and biometric verification and is monitored by human supervisors.

3.3 Knowledge Verification

Knowledge-centred security systems are based on the concept that a certain phrase or code can only be possessed by one who has clearance to access. The system depends on the assumption that the phrase remains a secret and is not discovered by a foreign entity. For many years multi-user computer systems have employed knowledge based security as the primary means of identifying correct user access. For the purpose of a remote examination system knowledge verification alone will not give a high level of confidence that the person attempting the examination is indeed the correct person, due to its inherent flaws. However since the examination will be accessed through the UConnect web interface, which requires students to enter their username and password, knowledge verification will be the first level of verification.

3.4 Possession Verification

Possession verification is based on the concept that personnel carry an item which identifies them as authorized personnel. This may be in the form of a stamp, wristband, tattoo or clothing to show that one belongs to a certain club. The most common item for possession verification is that of a key, an item that is not easily replicated yet must be possessed in order to gain entry into an area, such as a house. While possession verification has its uses, it relies on the assumption that

only authorized persons will have physical access to the device needed to gain access (2006). The major problem is that of transferability; the ability for the possession to be taken or given to another. For the purposes of a remote examination where certainty for verification is desired, possession based verification does not provide a high enough level of security.

3.5 Biometric Verification

Biometric verification uses inherently linked information to determine if the person trying to gain access is authorized. The information is intrinsically linked to the individual and is not able to be taken or given to another. The information may be based on deoxyribonucleic acid DNA, facial features, hand characteristics or iris characteristics which are all unique attributes to each individual. Due to the uniqueness of the information required to gain access, it would appear that biometric verification would be one hundred per cent accurate. While the information is unique, the problem occurs with the ability to read the information.

Take for example the nature of twins; although they have unique attributes (i.e. different facial features) to distinguish between them, security may be compromised depending on the ability of the person trying to tell them apart. For this reason the greatest disadvantage to biometric authentication is reader inaccuracy (Vielhauer 2006). Inaccuracy leads to falsely accepting intruders and falsely rejecting authentic users. Although problems can occur with biometric verification, this system provides the greatest level of certainty and security for authenticating access.

3.6 Biometrics for remote examinations

In order for biometrics to be reliably and seamlessly used for remote examinations, certain constraints must be placed on the system, ensuring that the form of biometrics used satisfies the required specifications.

For effective use the specifications required by the biometric technique include:

- Non-invasive
- Does not disrupt examination flow
- Operates in semi-real-time
- Common Acquisition Equipment
- Operates remotely and
- Ethical Operation

3.6.1 Biometric Specifications

Each biometric identification system has its own unique specification based on the requirements and implementation of the system. In this case the biometric verification system will be used in a remote examination system and as such has specific requirements as discussed in section 3.6.

3.6.1.1 Non-Invasive

The biometric technique used in a remote verification system should not require the student to remove bodily elements (such as hair), discharge bodily fluids (e.g. saliva) or use forced bodily entrance (e.g. blood sample). The acquisition device should not require the encapsulation of any body part, nor require the student to remove any piece of clothing that would be deemed to be invasive or inappropriate.

3.6.1.2 Does not disrupt examination flow

Once the examination commences, the biometric system should not distract the student from their task. The technique should be capable of continually

performing verification of the student throughout the examination without the need for the student to perform any specific movements, actions or speaking that would cause them to lose concentration or hinder them momentarily from completing the exam.

3.6.1.3 Operates in semi-real-time

Although the technique does not require instantaneous data processing as is required in real-time systems, the system should be capable of performing multiple biometric verification analysis throughout the examination period.

3.6.1.4 Common Acquisition Equipment

As the system is being used for students, the data acquisition equipment should not be costly specialised equipment that may be difficult to acquire. The hardware requirements of the system should be equipment that is accessible to all students regardless of class or location of study.

3.6.1.5 Operates remotely

The system should not require students to implement difficult installation procedures on local equipment; rather the system should be able to be accessed via an online portal.

3.7 Chapter Summary

The primary concern in implementing a remote examination system is ensuring that the correct student completes the exam. In an automated system there are three primary security means, knowledge, possession and biometric. While knowledge and possession systems are easily implemented and provide a base level of security, the ‘key’ for securing the system is easily transferable and therefore unacceptable as a standalone mechanism for a remote examination system. Biometric verification has been considered the most appropriate and secure means of ensuring accurate student verification for completing remote examinations. The primary benefit of biometric verification is the relative difficulty with which the ‘key’ for accessing the system can be transferred to a third party. Biometrics includes any information that is inherent to an individual and as such many biometric techniques are available for consideration. In order to set up a framework with which to measure biometric techniques against, various criteria for a remote examination were established. The specifications included: non-invasive, non-disruptive, operates in semi-real time, uses common acquisition equipment and can be operated remotely. When considering a biometric verification technique each of these criteria must be fulfilled.

Chapter 4

Biometric Authentication Methods

4.1 Introduction

Biometric authentication methods are placed into two broad categories:

1. Biological Construction and;
2. Learned characteristics.

Biological construction can be thought of primarily as physical makeup. These include DNA, fingerprints, hand prints and iris. They are traits that each individual is born with and cannot be altered or changed but are inherent to one's genetic makeup. Learned characteristics are those that an individual attains as they develop; these are characteristics such as gestures, actions or speech tones unique to an individual (Vielhauer 2006).

Although these classifications describe what ‘type’ of biometric authentication method is used, in practice it is often easier to categorise methods by the ‘way’ the biometric information is extracted and read. For this reason the methods will be classified as either ‘active authentication’ or ‘passive authentication’. As the names suggest active refers to the need for the subject to perform an action in order to read and analyse the biometric information, whereas passive can be performed with minimal effort required from the subject.

The following sections will look at the current methods used in biometric authentication and will compare them with the needs and requirements for the remote examination system.

4.2 Biometric Authentication Terminology

Before the methods of biometric authentication can be examined, it is important to understand how such systems are judged and the elements that are necessary to make them operational. These include: enrolment, authentication, variability, discrimination, ascertainability, data acquisition and performance.

4.2.1 Enrolment

In order for biometric analysis to take place the subject must be ‘enrolled’ in the system. A sample of the subject’s biometrics are recorded and stored, essentially registering them into the system, allowing for later comparison. If a subject is not enrolled, then a biometric analysis of that subject will return void since no match will be found within the system.

4.2.2 Authentication

Authentication occurs when the biometric analysis returns a positive result and is often broken into two categories, identification and verification.

Identification is used to determine who a person is or which person out of a group of people the biometric information belongs to. It essentially asks the questions:

"Who am I?"

The identification system can then answer the question:

"You are (someone)".

Identification is deemed to be a closed system, as all the identities of all people in the group are known. It is a matter of comparing the image against all images in the database and determining which image is the closest match. In a perfect system the result would always return the correct response; however due to many variables the estimate of the system may be incorrect. Therefore the performance measure of an identification system is determined simply by its error rate, E_{ID}:

$$E_{ID} = n_{err}/n_{tot}$$

where n_{err} is the number of trials that produce errors and n_{tot} is the total number of trials.

Verification on the other hand attempts to determine if the person (client) is who they claim to be. It asks the question:

"Am I who I say I am?"

There are only two possible ways the system can answer:

"Yes" or "No"

The person presents themselves to the system along with their claimed identity. The facial verification system compares the information input with that of the information within the database. The system then responds based on whether the result is within the tolerance or not. This lends itself to two error statistics:

1. False Rejections rate (E_{FR})
2. False Acceptance rate (E_{FA})

False Rejection rate (E_{FR}) is the probability that the system will not accept a person who has authentication rights. False Acceptance rate (E_{FA}) is the

probability that the system will allow access to someone who does not have permission. The error rates are calculated as:

$$E_{FR} = n_{false}/n_{tot}$$

where n_{false} is the number of false trial returns and n_{tot} is the total number of trials. Likewise E_{FA} is determined by:

$$E_{FA} = n_{FA}/n_{imposter}$$

where n_{FA} is the number of trials that returned false acceptance and $n_{imposter}$ is the number of imposter images presented to the system (Weaver 2006).

In a remote verification system the concern is only with recognising that the client is who they say they are.

4.2.3 Discrimination

Not all biometric systems are equal. While some are able to tell the difference (discriminate) between all subjects others may produce false discrimination; this is referred to as discriminatory power. It is a mark of the uniqueness of the biometric information gathered and used for comparison.

This adds further complexity to an already complex problem. While authentication is concerned with the accuracy and precision of the algorithms, discrimination is a measure of how different the biometric information is between subjects.

Authentication and discrimination are not independent concepts but rather they work in tandem. If discriminatory power is low the authentication must be exceptional to minimise errors and vice versa.

4.2.4 Variability

Humans are unable to avoid the effects of time, variability refers to how biometric information changes with time. Take for example facial recognition, babies faces are almost constantly changing as they develop and grow to puberty. Therefore

facial recognition performed on a baby enrolled six months earlier may not return a positive result due to the high level of variability. In contrast the facial features of young adults and middle aged persons do not change rapidly and therefore perform better with time.

4.2.5 Ascertainability

Ascertainability refers to the ease with which biometric traits can be gathered. As an example, handwriting biometrics requires the subject to complete a written test which can then be taken for analysis, making it difficult to ascertain. Facial biometrics on the other hand can be captured with simple devices, without the knowledge of the subject, making it easy to ascertain.

4.2.6 Data acquisition and Performance

Data acquisition follows from ascertainability and refers to the transformation of the raw biometric trait into information that can be used for further digital processing. Performance is a time based characteristic that takes into account the time taken to acquire information, pre-processing and processing time. Performance is essentially a measure of how quickly the biometric method can return a result.

4.2.7 Biometric Elements required for a remote System

Each of these elements needs to be taken into account when determining what biometric system will be most useful in the given situation. Every biometric system has its strengths and weaknesses which need to be weighed against the goals and objectives of the system required. This in turn will determine which biometric elements will be weighted as more necessary. The elements listed above have been compared to the requirements described in section 3.5 and have been listed in order of priority in Table 4.1.

Table 4.1: Biometric Element Priorities for Remote System

Priority	Requirement	Element
1	Information easily stored in a database	Enrolment*
2	Non-invasive and does not affect exam flow	Ascertainability
3	Identify the Student	Authentication
4	Semi real-time capabilities	Data acquisition and Performance
5	Ability to determine between similar students	Discrimination
6	Re-enrolment can easily take place	Variability

*Note: Enrolment has been listed as priority 1, since all methods require enrolment.

Each of the following biometric methods will be measured against the information provided in Table 4.1 to determine their suitability for the remote examination biometric authentication system.

4.3 Active Biometric Authentication

Although it could be assumed that active biometric methods would not fulfil the requirements of being non-invasive and non-disruptive, they have been investigated to ensure that a suitable option was not overlooked due to poor assumptions. The active methods that are currently being used in biometric authentication are deoxyribonucleic acid (DNA), voice, handwriting, keystroke and gait biometrics.

4.3.1 DNA

DNA biometric analysis requires the physical removal of bodily material that can subsequently be analysed for genetic information. For the most part genetic DNA coding is considered to be unique to every individual, the exception being for identical twins (Anil K et al. 1999). Bodily materials that contain DNA include saliva, blood, body tissue and hair follicles. The common use for DNA biometrics

at present is in crime scene forensics. Other areas of use have not been heavily investigated due to three primary issues.

1. DNA material is easily stolen: DNA material, in the form of hair, can be taken unsuspectingly or intentionally given to another with minimum effort. Although the accuracy of DNA biometrics may be high, security is low.
2. Difficulties in automation: The current technology for gathering and interpreting information requires expert analysis through cumbersome chemical procedures.
3. Privacy: DNA analysis gives access to one's genetic susceptibilities which could be used to discriminate against individuals or for other forms of abuse. (Anil K et al. 1999)

This method is not viable for remote examination purposes due to its complex nature as well as its inherent ethical issues.

Table 4.2: Pros and Cons of DNA Biometrics

Pros	Cons
• Unique information	• Biometric Information easy stolen • Automation not currently possible • Ethical issues • Requires expert analysis

4.3.2 Voice Biometrics

Fascination with speech and the desire to artificially create the human voice dates back to the 18th century. Speech synthesis, the synthesis of the human voice soon developed into speech recognition; the ability for human voice to be translated to words. Once this was achieved in the early 1990's the focus turned to speaker verification, focusing primarily on attributes such as whether the speaker was male or female, child or adult, as well as determining a person's mood, emotional state and even their language, whether formal or informal. The discovery that the

voice is unique to individuals led to the focus of speaker verification and voice identification (Klevans 1997).

Voice verification consists primarily of two aspects: feature extraction and pattern recognition. The purpose of feature extraction is to determine the characteristic traits of the speech signal. The voice is recorded through use of a microphone and is processed by a computer. Pattern recognition determines within probabilistic limits, how closely the sample features match a sample on file (Klevans 1997).

The first type of voice recognition was ‘voiceprint analysis’. This method creates a speech spectrogram- a graphical representation of the voice. Time is displayed on the “x” axis, frequency on the “y” axis and the spectral energy is displayed as shades at any point. The information is then compared to determine if the speakers are indeed the same person (Ramli et al. 2007). Other methods of analysis include frequency representation using Fast Fourier transform and LPC coefficients.

Table 4.3: Pros and Cons of Voice Recognition

Pros	Cons
• Unique Information • Able to determine other significant factors other than just identity	• Information is difficult to gather • Requires cooperation from user • Requires large samples for good verification

4.3.3 Handwriting Biometrics

Biometric methods such as retina, fingerprint or hand geometry employ physiological characteristics to determine identity (Giroux et al. 2009) Handwriting and keystroke biometrics are dynamic inputs that are based on behavioural characteristics. Yong, Tan and Wang (Yong et al. 2000) note that the current application of handwriting biometrics is used in verification. In this circumstance the written text is known, as in signature verification, and the enrolee’s written text is compared and evaluated. However it has been noted that each individual has specific handwriting and texture. Ttherefore it is possible to

also determine the identity of a person based on a piece of writing where the text is unknown.

Baker, Said and Tan (1998) have shown that due to the textural differences in handwriting, texture analysis techniques can be used for verification. From a sample of handwriting the writing is scanned using extra heavy lighting and divided into sample blocks. Some of the blocks are used as training samples while the others are used as test samples. Features are extracted from the handwriting images using various filtering techniques. Baker, Said and Tan (1998) found that Garbor filtering produced accuracies as high as 95.4%. Handwriting biometric techniques are in their elemental stages of development in comparison to other biometric techniques.

Table 4.4: Pros and Cons for Handwriting Biometrics

Pros	Cons
• Has had successful results	• Does not operate in real time • Requires either a scanner or special computer equipment to capture handwriting • Requires large amounts of samples for enrolment and testing

4.3.4 Gait Biometrics

Gait biometrics is the procedure by which an individual is identified by means of their walking patterns (Bazin & Nixon 2005).

Goffredo, et al., (2010) documents that gait biometrics is “completely unobtrusive without any subject cooperation or contact for data acquisition”. Despite this method of identification being unobtrusive, examinations are static and do not require students to walk while exams are completed. For this reason gait biometrics will only be discussed briefly.

The research is divided into two areas, three dimensional (3-D) and two dimensional (2-D) approaches. 3-D approaches determine the identity by looking at the movement of the limb in space. The information is gathered via several cameras and the images are subsequently reconstructed into a 3-D image. 2-D gait biometrics only requires one camera, which is usually placed to capture the lateral view and extracts only explicit features describing the gait. Each method is well documented and has their individual benefits: 2-D has simplicity and speed, 3-D robustness and accuracy (Bazin & Nixon 2005).

Table 4.5: Pros and Cons for Gait Biometrics

Pros	Cons
• Completely unobtrusive	• Requires students to walk • Requires several cameras • Implemented in 2D or 3D

4.3.5 Keystroke Biometrics

Keystroke biometrics aim to use the uniqueness of an individual's typing characteristics for identity authentication. It is believed that the dynamic physiological behaviours of individuals differ sufficiently to allow for an increase to traditional password security (Peacock et al. 2004). The concept of identifying personnel through keystroke biometrics did not occur with the advent of the personal computer or the type writer but stems back to the early 19th century. At this time telegraph operators were able to identify one another by listening to the distinctive tapping of their colleagues Morse code (Leggett et al. 1991).

The attractive feature of keystroke biometrics for increased security is its transparency. Since users are already required to input username and password details to log on, gathering keystroke information can happen simultaneously. There are many methods that have been proposed; however they essentially rely on gathering timing information as the keys are pressed. This information is then used in conjunction with the password to determine user verification.

Peacock et al (2004) shows that research suggests that the average failure rate of one third of keystroke authentication systems is around 2%. This is considered to be acceptable for this type of system. Enrolling is difficult as it requires the user to enter keystrokes in order to train the system which can require as many as 5,000 keystrokes. Depending on the quality of the users input it is possible that failure to enrol may occur.

Table 4.6: Pros and Cons for Keystroke biometrics

Pros	Cons
• Can use log on information to determine identify • Does not require any other hardware (cost effective) • Transparent • Average failure rate for 1/3 of systems is 2%	• Requires large amounts of samples for training and testing • Failure to enrol is possible

4.4 Passive Biometric Authentication

Passive systems require little or no action from the user in order to gather biometric information. This does not mean that the method of gathering information is not invasive or disruptive to a user, which is one of the requirements for the system. The passive methods that will be examined include: finger print, hand/ palm print, iris and retinal, ear and facial biometrics.

4.4.1 Finger Print Biometrics

It is well documented that the graphical ridges that are present on human fingers are unique and can be used for identification purposes (Jain & Lin 1996). This is most commonly seen in investigations of criminal activities. Fingerprint identification is usually performed manually, requiring a professional fingerprint expert to match prints gathered at the crime scene with one kept on file. This work is time consuming and expensive and does not meet the performance

requirements of the 21st century (Jain & Lin 1996). Automating the processing requires transforming the fingerprint into a digital form that can then be used in a verification system. Many scanners on the market today provide excellent digital fingerprint images; however the scanner is only a way of enrolling subjects and gathering biometric information.

Extraction of the details from the fingerprint and analysis still needs to be performed before authentication takes place. There are two broad ways this can be performed: minutiae-based approach or image based approach. (Sanjekar & Dhabe 2010)

Fingerprint technology has the advantage of requiring a small storage space for the biometric template, for a large database this can be significant.However it is noted that matching minutia patterns can be computationally expensive (Arivazhagan et al. 2007). Image based approaches endeavour to extract the information from the raw data to limit unnecessary pre-processing, therefore making it more efficient. Jain, et al., (1996) note that on average verification from a user input takes eight seconds to complete.

The effectiveness of automated fingerprint authentication is well documented and provides a successful way to determine user verification.

Table 4.7: Fingerprint verification pros and cons

Pros	**Cons**
• Small storage space • Quick processing time • High Discrimination	• Requires additional hardware • Disruptive

4.4.2 Hand/ Palm Biometrics

Hand based authentication systems use the geometric features of the hand and palm to verify users. While each human hand varies in finger length, width, thickness, curvatures and the relative locations of these, it is not as discriminative as fingerprint or iris (Amayeh et al. 2007). Since the system is not highly discriminative, it is better used in applications for verification rather than identification. The system requires a hand geometry scanner which uses a charge coupled device (CCD) camera, infrared LED's with mirrors to capture a silhouette of the hand. The hand scanner reads the shape of the hand while the mirrors allow the width of the hand to be captured. The process does not capture any surface details as a fingerprint scanner would but rather a black and white image of the shape of the hand (Singh et al. 2009). The system requires about one minute for enrolment and is able to give verification within 6-10 seconds. The system is robust, only requiring users to ensure that their fingers remained spread during the image acquisition resulting in 99.75% correct recognition if twenty-eight dimensions were used (Parashar et al. 2008). The major disadvantage is the large size of the capturing device.

Table 4.8: Pros and Cons for Hand/ Palm Biometrics

Pros	Cons
• High Level of verification • Quick enrolment time • Quick processing time • Isn't adversely affected by environment • Small storage requirements	• Large device size • Only useful for verification • Lower discrimination power than other methods

4.4.3 Iris Biometrics

Iris and retinal biometrics are two distinct areas of research which have no correlation to each other apart from the fact they both concern the eye. Therefore they will be discussed separately giving due credit to each as a way of identifying a person through the unique characteristics of different parts of the same eye.

Iris recognition uses the highly differentiated detail of the coloured area of the human eye to distinguish one individual from another (Rejman-Greene 2002). It is not only the uniqueness of the iris that makes this technique possible but also the inability to change the iris (Yu et al. 2008). Research shows that iris recognition can have accuracy as high as 99.946%, with statistics concluding it has the lowest error rate in all biometrics (Lin & Lu 2010). The technique requires capturing an iris image either through still or video camera and then pre-processing the image so that other parts of the eye such as eyelid and eyelashes are removed. Before information extraction can begin the pupil is found and boundary points added to the inner iris so that normalisation of the iris can take place. After iris normalisation the extraction and coding of information occurs by implementing complex algorithms and transforms.

Table 4.9: Pros and Cons of iris biometrics

Pros	Cons
• Highest accuracy out of all biometrics • Human iris are unique • Human iris are stable of the duration of an individual's life • Iris information is inherent and cannot be altered • Data is acquired with still or video camera • Robust algorithms	• Complex algorithms • Computational heavy • Small Iris • Small distances for gathering information • Requires cooperation

Although the algorithms are difficult, the means of finding the iris and normalising is simple due to the inherent nature of the eye (iris is on a white background with a dark pupil as its centre). This eliminates some of the obstacles caused by variation in lighting. The main disadvantage is the size of the iris and therefore taking measurements at a distance can be problematic. The maximum reported distance for successful iris recognition is 46cm (Burge & Burger 2000).

4.4.4 Retinal Biometrics

Retinal biometrics requires capturing a picture of the eye while being illuminated with an infrared light. The photograph produced shows the blood vessel on the back end of the eye ball. These patterns are unique and can be processed and compared to enrolment photos to determine the individual's identity (Rejman-Greene 2002). The technique requires large equipment which is costly and is therefore not suitable for a large scale automated system.

4.4.5 Ear Biometrics

It cannot be proven that each individual has unique ears; however Burge and Burger (2000) hypothesise that this may be the case. Through studies completed by Lannarelli, cited in Burge and Burger (Burge & Burger 2000), which examined over 10,000 ears and a second study that compared ears in fraternal and identical twins, they believe their hypothesis was supported. Ear biometrics has become a popular research area of passive biometrics due to the fact that ears do not change radically over time. In effect this area is an extension to facial biometrics where many problems occur due to expression, cosmetics, hair styles, growth of facial hair as well as external difficulties such as variation in lighting (Burge & Burger 2000). Ear biometrics is not affected as dramatically as facial biometrics, the one exception being hair style.

The recognition system requires ear detection, feature extraction and verification. The process allows for the image to be captured in 2-D; however this causes problems with ear extraction pre-processing and rotation. The strict range of motion for right ear recognition is a right rotation of 20 degrees and left rotation of 10 degrees (Yuan & Mu 2007). The use of 3-D ear biometrics has become an area of recent interest and research. A benefit of ear recognition is the increased distance at which recognition can take place. In research conducted by Yan and Bowyer (n.d) subjects sat 1.5m away from the data acquisition device.

There are many ways of extracting information from the ear including feature points, using curved segments to form Voronoi diagrams, treating the ear as an array to form a Gaussian force field or using the long axis as the basis for curve fitting of the outer ear contour.

Table 4.10: Pros and Cons of Ear Biometrics

Pros	Cons
• Greater distance for data acquisition • Different algorithms and data extraction methods • Excludes problems occurred in facial recognition	• Ears may not be unique • Ears may be completely covered • Small degree of freedom for data acquisition

4.4.6 Facial Biometrics

Facial recognition has been extensively researched and documented, attributed mostly to availability and ease with which the raw biometric data can be gathered. It is possible for the information to be gathered with readily available and inexpensive equipment such as a webcam (Abdel-Ghaffar et al. 2008). While other methods are intrusive or require active input, facial recognition is passive and non-intrusive (Cavalcanti & Filho 2003). There are multiple algorithms that are well documented, which can be implemented in either 2D or 3D (Harguess & Aggarwal 2009). It has also been noted that due to the symmetrical nature of the

human face it is possible to use techniques such as ‘average half face’ to limit the amount of information that is needed to be stored. Research shows that it is possible for face recognition to produce 100% accuracy (Ramesha et al. 2009).

A downfall to this technique is that there are many issues that automated face recognition biometrics needs to overcome including illumination, background, scale, and change in skin colour (i.e. skin irritations, warm or cold, blemishes, and makeup), growth or removal of hair, pose and expression and self-occlusion (Guodong et al. 2010). Despite these complications, facial recognition has received much attention and many of these problems have been solved.

Table 4.11: Pros and Cons of Facial Biometrics

Pros	Cons

• 100% Accuracy Possible
• Well documented
• Low cost and readily available equipment (webcam)
• Passive and unobtrusive
	• Many Problems:
	  o Illumination
	  o Background
	  o Scale
	  o Change in skin colour
	  o Hair growth/ removal
	  o Expression
	  o Self-occlusion
	• Biometric Information can be completely obstructed

4.5 Appropriate Biometrics for Remote Examination System

Through a process of elimination the most suitable technique can be selected for the remote examination system.

Table 4.12 shows the requirements that each biometric system fulfils. It can be noted that the only technique which fulfils all criteria is facial biometric.. Though many problems have been listed for facial recognition it provides the most robust system and fulfils the criterion of being non-invasive, semi-real-time capabilities, easy ascertainable information, low cost and non-disruptive.

Table 4.12: Comparison between Biometric Systems and the requirements of the remote examination system

	Requirement				
Type of Biometric System	*Non-Invasive*	*Non-Disruptive*	*Real-time capabilities*	*Common Acquisition Equipment*	*Remote Operation*
DNA					
Voice	•		•	•	•
Handwriting	•				
Gait	•			•	•
Keystroke	•		•	•	•
Fingerprint	•				•
Hand Geometry	•				
Iris	•			•	
Retinal					
Ear	•		•	•	•
Facial	•	•	•	•	•

4.6 Chapter Summary

Chapter 4 introduces the concepts of biometrics including the terminology and current methods used for identity verification. The terminology is considered such that each term is considered with respect to the needs of the remote verification system. Enrolment is the fundamental requirement of all biometric systems and was therefore assigned the greatest priority. The remote examination system must also be able to ascertain biometric information without being invasive and limiting examination flow as well as correctly authenticating students. These were considered of greater importance than the performance and discrimination of the system and therefore carried greater weighting in the decision. Variability is considered less important as re-enrolment can easily take place throughout a semester.

The current biometric methods were considered in two broad categories: active and passive. Active methods contained those which require the subject to ‘do something’ in order to ascertain the biometric information. Examples of these include handwriting, keystroke and gait biometrics. These methods often require subject cooperation. Passive methods on the other hand do not require any specific action but are able to ascertain the information with limited cooperation from the subject. The pros and cons of each system were considered and compared with the requirements defined in Chapter 3. From the research conducted it was determined that facial recognition was the most appropriate biometric technique for a remote examination system.

Chapter 5

Facial Recognition Algorithms

5.1 Introduction

There are many papers which compare thoroughly the accuracy of facial recognition algorithms and how to overcome inherent problems. The purpose of this project is not to implement and test different algorithms but rather document the current algorithms and find one that will be suitable to serve as a platform for a remote, real time system.

The algorithms which will be looked at include video based, Principal Component Analysis, Independent Component Analysis, Linear Discriminate Analysis (Fisherfaces), 3D Models, Gabor Wavelets, Tensorfaces and Hidden Markov Model

5.2 Video Based Algorithms

Facial recognition can be performed on either static images or time-varying images (video). In recent years video based face recognition systems have received great attention. This may be due to the desire for heightened security in public places, such as airports, particularly in light of the events of 9/11. Harguess, et al., (2009) believe that while this may be the primary reason, the other is that video can provide many frames of a subject's face instead of only a few.

In the past there have been problems associated with video based recognition. Two of the major problems are discussed by Zhao, et al., (2003):

1. Problems associated with real-time systems. Taping may occur outside which increases the amount of uncontrollable variables such as rain, fog, low light etc. Video increases the likelihood of pose variation and occlusion.
2. Video quality is low; therefore, facial images are small. Small faces cannot be used for facial recognition since they do not contain enough distinguishable information.

With the increase in technology over the past ten years resolution is no longer considered to be a primary concern for video based face recognition. However studies conducted by Changbo, et al., (2009) recognise that the un-resolved challenging problems are still illumination, pose and occlusion.

Although Zhou, et al., (2003) recognise the complexities surrounding video based systems they also highlight the areas that make video systems superior to static face recognition systems. These include:

- Abundance of image data. Many frames per second can be captured with video cameras; therefore good frames can be selected to perform analysis.
- Video allows tracking of objects i.e. it is possible to track the face and determine optimal frontal position of the face. This accounts for head rotation and other such phenomena.

- Real-time. Images can be collected through surveillance cameras without the need for subject cooperation. This provides a myriad of applications.

It is important to highlight the ability for video systems to provide:

1. Head Detection and
2. Head Tracking

This concept helps to ensure that a face is present in the frame and that the head is positioned in such a way that facial recognition can be performed. Many researchers have used simple geometric shapes to model the head such as cylinders, ellipsoid or other 3D shapes (Wooju & Daijin 2007). These techniques provide simple head detection and head tracking techniques.

5.3 Principal Component Analysis/ EigenFaces

The current standard for facial recognition algorithms, against which all other algorithms are compared, is Principal Component Analysis (PCA). When this technique is used for the expressed purpose of facial recognition it is often given the term ‘eigenfaces’, as it produces eigenvectors of face images (Moon & Phillips 2001).

This technique was made popular by Turk and Pentland (1991) due to its ease of implementation and the performance levels achieved. Although primary research has been in the area of face recognition, PCA has also been used for face detection. The amount of information stored in an image can be substantial and require large computational efforts to perform even the crudest of facial recognition techniques such as ‘correlation’, a simple pixel by pixel comparison technique. Understanding the need to minimise computational complexity and a desire to extract only relevant information and encode it as efficiently as possible, Turk and Pentland (1991) implemented the technique of PCA. PCA statistically minimises the dimensionality of a data set while retaining important variations within the set. An image that is described by *n* by *m* pixels is interpreted as a point $\mathbb{R}^{nxm}$. In essence it produces the optimal linear least-squares decomposition of a set of images in N-1 dimensional space, thus producing a set of eigenvectors

(e_1,…., e_{N-1}) and eigenvalues (λ_1, …, λ_{N-1}). The eigenvectors are normalised so as to be orthonormal and the eigenvalues ordered such that $\lambda_i > \lambda_{i+1}$ (Moon & Phillips 2001).

Mathematically the goal of PCA is to find the eigenvectors of the covariance matrix of the set of facial images. The eigenvectors are ordered such that they account for the degree of variation within the image set. They are essentially the features of each individual image that characterise the variation between the images. From the variations captured in each eigenvector it is possible to use a linear combination of any of the derived eigenvectors to exactly represent any facial image within the set of images. However since the variation within a training set may be very large, eigenvectors accounting for minuté differences between images, most of which do not increase the accuracy of the recognition process, can be discarded. For this reason it is possible to use only the eigenvectors within a set of images that account for the most significant variations. This reduces computational complex while maintaining the ability to represent each facial image accurately. The eigenvectors or 'eigenfaces' that are chosen span an M-dimensional subspace, termed "face space", of all possible images.

Using 8-bit grayscale images taking a two-dimensional array form I(x,y), an image may be viewed as a vector of dimensions N^2, such that a typical image of 256 by 256 can be described as a vector of 65, 536, or equivalently a point in 65,536 dimensional space. All images within the set are subsequently mapped to this space as a collection of points. As mentioned previously, this allows for the vectors that describe the greatest variations to be found from within the entire image space.

If the training set of images is described by Γ_1, Γ_2, Γ_3,….., Γ_M where M is the number of eigenvectors in the set , then the average face of the set can be defined by:

$$\psi = \frac{1}{M}\sum_{n=1}^{M}\Gamma_n \tag{5.1}$$

The amount that each facial image differs from the average is given by the vector $\phi_i = \Gamma_i - \psi$. In order to best describe the distribution of data PCA is performed on the set in order to find a set of orthonormal vectors, $\mathbf{u}_n$. The k^{th} vector of the set $\mathbf{u}_k$ should be chosen such that

$$\lambda_k = \frac{1}{M}\sum_{n=1}^{M}(\boldsymbol{u_k^T\phi}_n)^2 \tag{5.2}$$

is a maximum, subject to

$$\begin{aligned}&\boldsymbol{u}_l^T\boldsymbol{u}_k = \delta_{lk}\\&= \begin{cases}1, & if\ l=k\\0, & otherwise\end{cases}\end{aligned} \tag{5.3}$$

The eigenvectors and eigenvalues of the covariance matrix,

$$\begin{aligned}C &= \frac{1}{M}\sum_{n=1}^{M}\boldsymbol{\phi}_n\boldsymbol{\phi}_n^T\\&= AA^T\end{aligned} \tag{5.4}$$

where $A = [\boldsymbol{\Phi_1}\ \ \boldsymbol{\Phi_2}\ \ \ldots.\ \ \boldsymbol{\Phi_M}]$, are therefore obtained as $\mathbf{u}_k$ and the scalars λ_k respectively.

It may be noted that the covariance matrix in this circumstance will be N^2 by N^2 which will be impossibly large to compute. In order to reduce the order of complexity the dimensional eigenvectors should be solved by first solving the eigenvectors of a much smaller M by M matrix.

This is shown in the following example where an eigenvector $\mathbf{v}_i$ of A^TA is described such that

$$A^TA\boldsymbol{v_i} = \mu_i\boldsymbol{v_i} \tag{5.5}$$

If each side is pre-multiplied by A then

$$AA^TA\boldsymbol{v_i} = \mu_iA\boldsymbol{v_i} \tag{5.6}$$

From equation 5.4 it is known that $C = AA^T$; therefore it is possible to construct an M by M matrix $L = A^TA$ where $L_{mn}=\boldsymbol{\phi}_m^T\boldsymbol{\phi}_n$ and hence find the M eigenvectors, $\mathbf{v}_l$, of L. The eigenvectors found using this analysis determine the linear combination used to form the eigenfaces $\mathbf{u}_l$.

$$\boldsymbol{u}_l = \sum_{k=1}^{M} \boldsymbol{v}_{lk}\boldsymbol{\phi}_k, \quad l=1, \ldots, M \tag{5.7}$$

The eigenface produced is stored as a combination of all face images within the training set and is essentially used as a template to judge unknown facial images against.

5.3.1 Classifying the images

Regardless of the method used to compress the image data set, the recognition task itself is essentially a pattern recognition task between the known image/s and the unknown image.

In this framework, a face image can be presented to the system and compared with the template image that has been stored for an individual. If the comparison value is below a predefined threshold, the identity of the person is confirmed. This is the desired goal for a remote examination verification system.

In order for a comparison to be made, the presented face is first transformed into its eigenface components by:

$$\omega_k = \boldsymbol{u}_k^T(\boldsymbol{\Gamma} - \boldsymbol{\psi}) \text{ for k =1, . . ., M'} \tag{5.8}$$

where ω_k is the test image projected into the eigenspace, $\boldsymbol{u}_k^T$ is the top M' eigenvectors in the training set and $\boldsymbol{\psi}$ is the mean.

The outcome is a point by point image multiplication and summation of the single image, which in turn produces a vector $\Omega^T = [\omega_1, \omega_2, \ldots, \omega_{M'}]$ which describes

the combination that is required from the training set in order to accurately represent the presented face.

The weighted vector described above is then used as a reference to determine how close the presented face image is to an image within the set of training images. Mathematically this is achieved by determining the face class that minimises the Euclidian distance.

The Euclidian distance is often used since it is computationally light, while providing a simple and effective classification. The Euclidian distance is described by:

$$\epsilon_k^2 = \|(\boldsymbol{\Omega} - \boldsymbol{\Omega}_k)\|^2 \quad (5.9)$$

where $\boldsymbol{\Omega}_k$is the vector describing the kth face class. As such the scalar distance can be calculated by a summation of all distance:

$$\epsilon = \sqrt{\sum_{i=0}^{k} (\boldsymbol{\Omega} - \boldsymbol{\Omega}_k)^2} \quad (5.20)$$

The presented test image is compared to every projected image in the set and the image that produces the minimum score is chosen. Using this method there will be four possible outcomes which include:

1. Near face space and near face class,
2. Near face space but not near face class
3. Distant from face space and no near known face class
4. Distance from face space and near a face class

If an image is described by category 1 then the person's identity is known. Category 2 describes a presented image that is a face but is not part of the training. Category 3 and 4 describe images that do not resemble faces and therefore are not close to the face space.

The Eigenface algorithm is particularly useful for recognition of a user. However in the case of the remote examination system it is not recognition that is the desired result but rather verification, determining if the person is who they claim to be. In this instance the eigenface algorithm can be implemented as described previously with the only change being that the training set only includes images of the one individual rather than many.

Multiple images of the one individual in the training set allows for slight variations that may occur in any image due to expression, lighting, skin colour or other factors. The comparison algorithm and Euclidian distance is calculated in the same manner as in a recognition process. The conclusion should be therefore that, any face that is not part of the training set will be recognised as an imposter, while a face image that is the 'same' as any image in the training set will be verified.

5.4 Independent Component Analysis

Independent component analysis (ICA) is a derived or expanded method built on the weaknesses of its counterpart, PCA. Therefore in considering ICA it is prudent to compare its strengths to the possible downfalls of PCA.

While PCA only considers 2nd order moments, or lower-order statistics, ICA is able to identify the independent source components from their linear mixtures, therefore accounting for higher order statistics (Comon 1994).

Liu and Wechsler (1999) suggest that ICA is able to produce a greater or truer representation of the data since it aims to provide an independent rather than an uncorrelated image. It is known that PCA is indifferent to the role of variation and therefore weights them equally. This may potentially lead to a poor classification if the face classes are not separated by the mean-difference but by the covariant-difference.

Bartlett, Movellan et al (2002) note four distinct advantages that ICA has over PCA which include:

1. ICA provides a better probabilistic model of the data
2. ICA uniquely identifies the mixing matrix
3. The reconstruction of the data may be better than PCA in the presence of noise
4. ICA is sensitive to higher-order statistics in the data, not just the covariance matrix.

The overall difference can be understood by recognising that the ICA of a random vector (i.e. a facial image) searches for a linear transformation which statistically minimises the dependence between components, while PCA only includes/derives the most expressive features, some of which may be irrelevant to facial recognition.

Over the past 20 years many methods for performing ICA have been considered, particularly in fields relating to signal processing. These methods have been well documented by researchers such as Bell and Sejnowski (1995), Jutten and Herault (1991), Comon (1994) and Cickocki, et al., (1994). Although Bartlett, et al., (1998) and Bartlett, et al., (2002) propose methods of ICA directly related to the field of face recognition, for the purpose of this dissertation only the method described by Liu and Wechsler (1999) will be considered.

5.4.1 How ICA works

An image may be represented as a random vector taking the form

$$\boldsymbol{X} \in \mathbb{R}^N \tag{5.31}$$

where N is the dimensionality of the image space. The vector is formed by concatenating the rows or the columns of the image. If $\sum_X \in \mathbb{R}^{N \times N}$ and E is defined as an expectation operator then it is possible to define the covariance matrix of $\boldsymbol{X}$ as:

$$\sum\nolimits_X = E\{[X - E(X)][X - E(X)]^T\} \tag{5.42}$$

It is possible to transform equation 5.12 into

$$\sum_X = F\Delta F^T \quad (5.53)$$

since ICA of $\boldsymbol{X}$ will factorise the covariant matrix.

In equation 5.13 Δ represents the diagonal real positive, while F transforms the original data $\boldsymbol{X}$ into Z. Therefore the final form is given by:

$$X = FZ \quad (5.64)$$

In this form the new component data stored in Z are independent.

The ICA transform F described above consists of three operations which each play a part in transforming the data into independent components. The three operations are whitening, rotation and normalisation developed by Comon (1994).

5.4.2 Whitening

Since the covariance matrix $\sum_X$ is constructed of both an orthonormal eigenvector matrix

$$\Phi = [\phi_1, \phi_2, \ldots, \phi_N] \quad (5.75)$$

and a diagonal eigenvalue matrix

$$\Lambda = diag\{\lambda_1, \lambda_2, \ldots, \lambda_N\} \quad (5.86)$$

The covariance matrix can therefore be written as:

$$\sum_X = \Phi\Lambda\Phi^T \quad (5.97)$$

The goal of the whitening function is to produce a unit covariant matrix from the original random vector $\boldsymbol{X}$. By solving the eigenvalue equation 5.17 Φ and Λ are derived such that

$$X = \Phi\Lambda^{1/2}U \quad (5.108)$$

where U is a unit covariance matrix. This can then be rearranged to determine the unit covariance matrix by multiplying both sides by $\Lambda^{-1/2}$ and Φ^T to give:

$$U = \Lambda^{-1/2}\Phi^T X \quad (5.119)$$

From this form of the equation 5.19 it can be noted that $\Lambda^{-1/2}$is mathematically equivalent to $\frac{1}{\sqrt{\Lambda}}$ and hence the eigenvalues appear in the denominator. In the usual case of eigenvalues they are sorted such that $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$ where λ_N is significantly small in comparison to λ_1 and often represents noise. As with PCA the trailing eigenvalues can be discarded without losing vital data. In fact removing these values helps to avoid misleading variations due to noise (Liu & Wechsler 1999). This allows the leading eigenvectors to define a matrix

$$P \ \epsilon \ \mathbb{R}^{N\times m} \quad (5.20)$$

where $P = [\Phi_1, \Phi_2, \dots, \Phi_m]$

A similar form is derived for the first eigenvalue

$$\Lambda_1 \ \epsilon \ \mathbb{R}^{m\times m} \quad (5.21)$$

where Λ_1 is a diagonal matrix taking the form

$$\Lambda_1 = diag\{\lambda_1, \lambda_2, \dots, \lambda_m\} \quad (5.22)$$

From equation 5.19 the appropriate substitutions can be made such that

$$V = \Lambda_1{}^{-1/2} P^T X \quad (5.23)$$

This details the whitening transform from the high-dimensional space to the low-dimensional space. This process reduces complexity while maintaining data integrity.

Mathematically the transformation from high-dimensional space to low-dimensional space has been completed. However the question in practice remains, "what should the dimensionality of *m* be?" The optimal solution is not easily found but can be decided by considering the two fold purpose for dimensionality reduction and finding that the intersect produces maximums. The generalised purpose is to:

1. Lose as little representation of the original data as possible
2. Discard the trailing eigenvalues

Therefore the balance is to maintain essential spectral energy of the raw data while not allowing the trailing eigenvalues to be small.

5.5 Fisherfaces

In 1936 Robert Fisher developed a linear discriminant analysis for the purpose of taxonomic classification (Fisher 1936). It has since been used as a classical method for pattern recognition and adapted somewhat for specific use in facial recognition. The term ‘fisherface’ is the term often used for this method of face recognition as it is a combination of both fisher linear discriminant analysis (FLD) and eigenfaces (PCA).

Belhumeur et al (1997) show that unlike eigenfaces, fisherfaces have qualities such that they are insensitive to extreme variations in lighting and facial expression. In this sense, lighting is described as the number of sources as well as both intensity and direction.

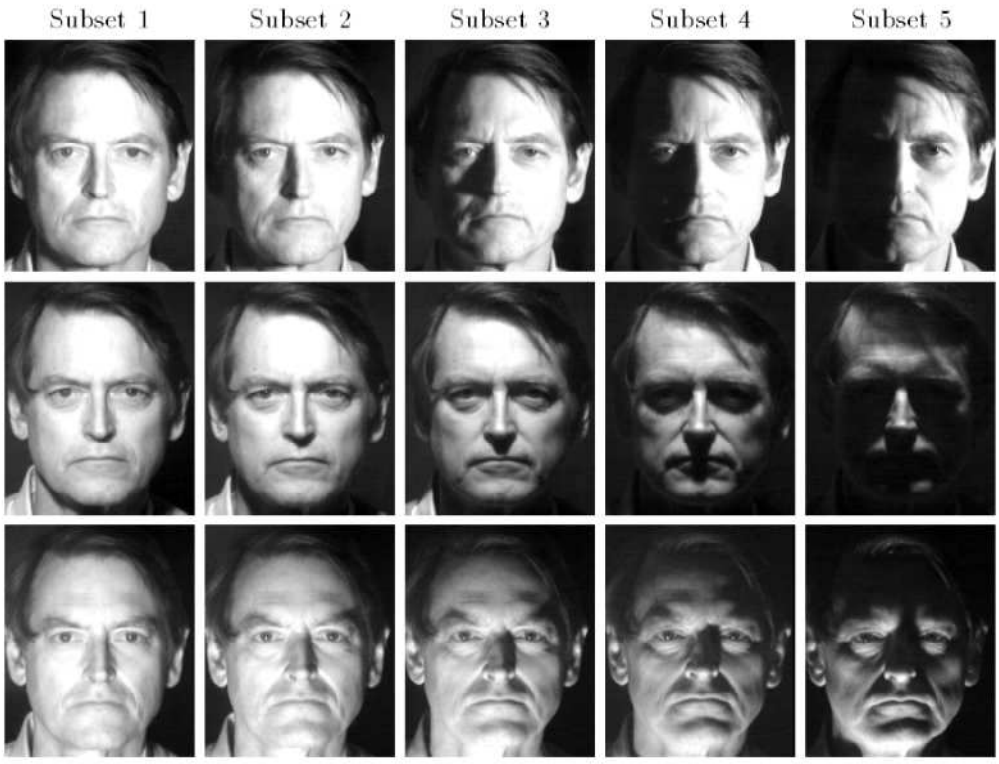

Figure 5.1: The same person seen under varying lighting conditions. (Cited in Belhumeur et al. 1997)

By beginning with the two underlying principles of fisherfaces, the first from PCA and the other from FLD, the combination of techniques can be understood as complementing one another.

It is known that PCA projects face images from a high-dimensional image space to an image space that is lower. However as a by-product of this action the total scatter across all classes is maximised; in doing so unwanted variations due to light and facial expression are retained. It has been noted by Moses,et al., (1994) that "the variations between the images of the same face due to illumination and viewing direction are almost always larger than image variations due to change in face identity". This phenomenon increases the chances for the eigenface algorithm to increase false rejection and false acceptance rates.

In comparison, fisher linear discriminant analysis tries to "shape" a scatter in such a way that a more reliable classification can be made. By using PCA as a pre-processing step within the FLD framework the null space of a training set can be discarded while maintaining the between-class scatter (Juwei et al. 2003). In essence the algorithm selects W such that it maximises the ratio of the between-class scatter to that of within-class scatter.

Linear Discriminant Analysis (LDA) in general attempts to group images into separate classes. The images are projected from N-dimensional space to $C - 1$ dimensional space (where C is the number of classes). This effectively minimises the variation in the between class scatter as it groups images that are similar. Therefore images of the same face, but varying expression will be grouped together as one class, while a different subject face image will be grouped as a separate class. In order to achieve this, two matrices are defined: between-class scatter and within-class scatter.

The between class scatter matrix is defined as:

$$S_B = \sum_{i=1}^{c} |X_i| (\mu_i - \mu) (\mu_i - \mu)^T \qquad (5.24)$$

And the within class scatter matrix is defined as:

$$S_W = \sum_{i=1}^{c} \sum_{x_k \epsilon X_i} (x_k - \mu_i)(x_k - \mu_i)^T \quad (5.25)$$

where μ_i is the mean image of class X_i and $|X_i|$ is the number of samples in class X_i

Once these matrices are determined, the eigenvectors, U, and the eigenvalues, λ, can be found

$$S_B U = \lambda_i S_W U \text{ eq 11} \quad (5.26)$$

As with Eigenfaces the eigenvectors are sorted in descending order and the top eigenvectors are kept. These form the basis vectors that define the subspace.

In a general Linear Discriminant Analysis (LDA) the optimal linear discriminant transform is found by:

$$V_{opt} = argmax \frac{|U^T S_B U|}{|U^T S_W U|} \quad (5.27)$$

where U is a set of generalised eigenvectors. However in this solution V_{opt} is generally singular since the rank of S_W is less than the difference between the number of training images and the number of classes. However because FLD uses PCA as a pre-processor to using LDA, this problem is avoided since the projection is made onto a low-dimensional image space. By using PCA first equation, 5.27, can now be re-written in its general form as:

$$V_{fld} = argmax \frac{\left|U^T V_{pca}^T S_B V_{pca} U\right|}{\left|U^T V_{pca}^T S_W V_{pca} U\right|} \quad (5.28)$$

Therefore

$$W_{FLD} = argmax \frac{\left|W^T W_{PCA}^T S_B W_{PCA} W\right|}{\left|W^T W_{PCA}^T S_W W_{PCA} W\right|} \quad (5.29)$$

and

$$W_{PCA} = argmax|W^T S_T W| \quad (5.30)$$

The matrix W can now be found such that it maximises the ratio of between-class scatter to that of within-class scatter. This is achieved by multiplying W_{FLD} and W_{PCA}:

$$W_{opt} = W_{FLD} W_{PCA} \quad (5.31)$$

therefore,

$$W_{opt} = argmax \frac{|W^T S_B W|}{|W^T S_W W|} = [w_1, w_2, \dots, w_m] \quad (5.32)$$

The images are projected onto vectors $[w_1, w_2, \dots, w_m]$ corresponding to the columns ofW_{opt}. The extracted information, which is examples of features for each face image, can be used directly for classification. The recognition process uses the same technique as that performed for Eigenfaces, Euclidian distance.

The difference between PCA and FLD is shown in Figure 5.2

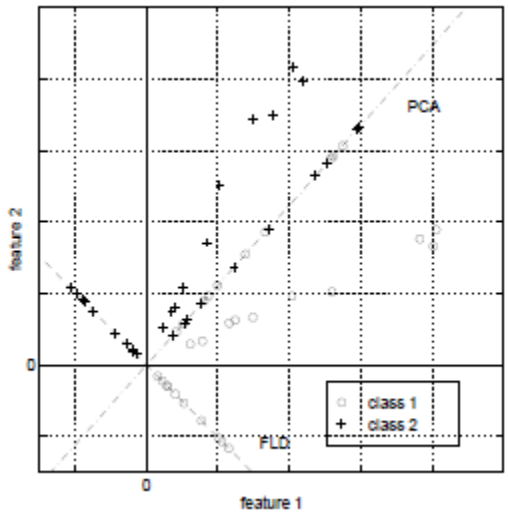

Figure 5.2: Graph showing Fisher's Linear Discriminant (FLD) compared to Principal Component Analysis (PCA) for a 2 class problem where data for each class lies near a linear subspace

Fisherfaces has become a popular technique for overcoming problems associated with lighting and expressions by incorporating the benefits presented by PCA and LDA. Juwei, et al., (2003) mention the problem associated with this technique, particularly the use of PCA, as a pre-processing tool to bring the projections from a high-dimension space to a low-dimension space. It is believed that using this technique causes the loss of significant discriminatory data vitally useful in the facial recognition process.

Researchers such as Qian, Haiyuan and Yachida (1995) have discussed other techniques that relieve LDA of the need for pre-processing with PCA. The proposed method is one of Direct Linear Discriminatory Analysis (D-LDA) where the data captured in high-dimensional space in processed directly without the need to transform to a low-dimensional space. This technique allows for discriminatory data available only in high-dimensional space to be preserved.

5.6 3D Models

3-Dimensional (3D) methods are yet another class of techniques used to overcome problems associated with the complex problem of performing automated facial recognition. 2-Dimensional (2D) methods (simple image based methods) tend to have decreasing accuracy when adverse conditions such as differing illumination, head orientation, facial expression and makeup are encountered. These problems are associated directly with the amount of information available from a 2D portrait of a subject. It is this concept that lead researches to believe that 3D techniques could be the answer; since 3D information is viewpoint and lighting-condition independent (Bronstein et al. 2003).

According to Bronstein, et al., (2004) 3D recognition is able to offer a dramatic increase in recognition under varying conditions due to the inherent differences between the information that is captured in 3D as opposed to 2D. Bronstein, et al., (2004) note “three-dimensional facial geometry represents the internal anatomical structure of the face rather than its external appearance influenced by environmental factors”..

In their paper ‘Three-Dimensional Face Recognition’, they illustrate the ability to use a subject’s facial structure and through the use of texture mapping create an image of two different individuals. Figure 5.3 shows this concept visually.

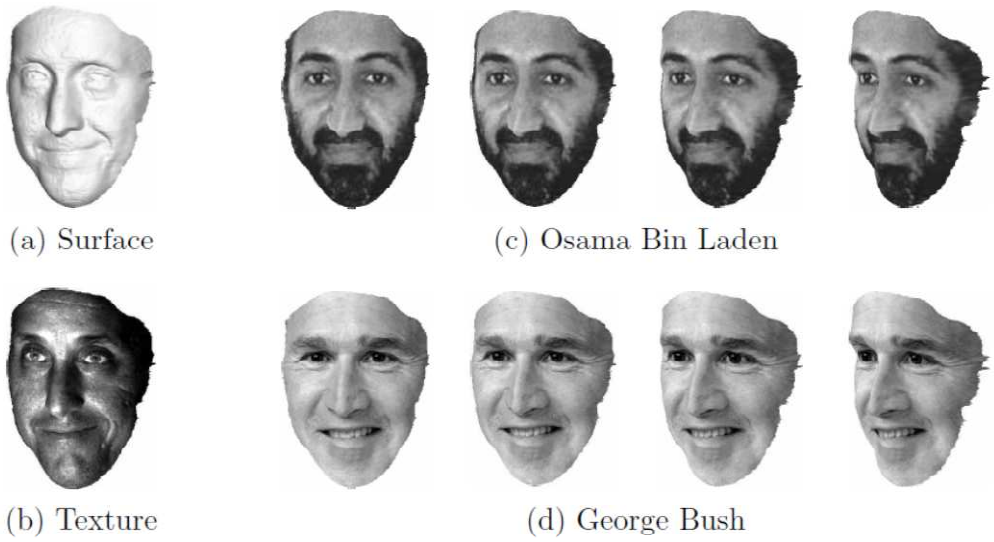

Figure 5.3: Texture mapping on the same facial structure to change the appearance of the 2D facial image to make the same face look like George Bush or Osama Bin Laden. (Cited in Bronstein et al. 2004)

Using the human recognition system these images are easily labelled as George Bush and Osama Bin Laden.However the true identity and 3D geometry of the original subject have been completely lost. This shows the intrinsic weakness with 2D approaches as they only compare surface texture which can easily be changed or varied by the addition of makeup to a subject’s face. 3D recognition which uses the structure of the face for recognition presents additional information which is very useful in the recognition process.

The drawback of such a technique is the need for additional equipment to capture the structural information of a subject’s face. While 2D systems require only a conventional camera for face recognition, 3D face recognition requires a depth of range camera or 3D scanner.

One of the requirements of the remote verification system is that it must use equipment that is readily available and cost effective for students. For this reason a 3D recognition system of this type will not be explored further.

It is however possible to construct a geometric 3D representation of a subject through the use of multiple 2D images. While this technique does not capture all structural features of a subject's face, it does allow for some depth perception and matching to take place.

In 1995 Gaile Gordon performed tests using a 3D model constructed from two images, a frontal image and a profile image. The system block diagram of the method is shown in Figure 5.4

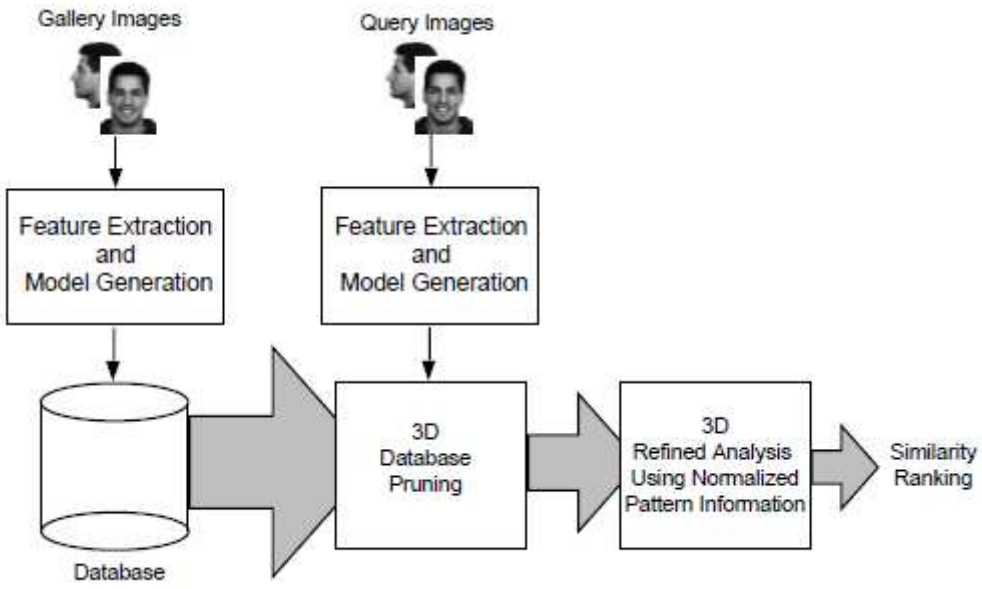

Figure 5.4: Implementation of frontal and profile view into a 3D system. (Cited in Gordon 1995)

Using this system for facial recognition Gordon found that the system was able to produce 98% accurate results, which was an increase of between 33 to 45 per cent over purely image based systems (Gordon 1995). The success of this system is based on the fact that information such as nose length and other characteristic features can be determined and used, since both the profile and frontal images are present.

In order to create a 3D representation, multiple photos must first be obtained from multiple directions. Once the raw images have been obtained the initial pre-processing step is to morph the images, by rotating the images up, down, left and right as well as using common fiducial points on the face, thus ensuring that the images are aligned. This concept is shown in Figure 5.5.

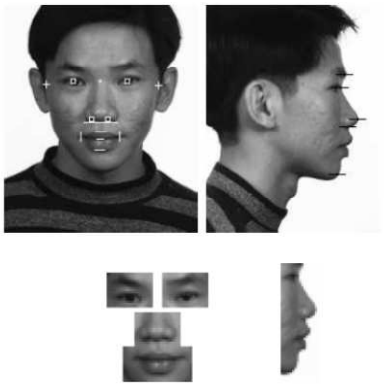

Figure 5.5: Fiducial points used to align images for 3D reconstruction. (Cited in Gordon 1995)

The purpose of this process is to remove any distortion presented in the images due to head pose variation (Jiann-Der et al. 2004). Most 3D methods use this as the starting point for creating a type of 3D model subsequently used for recognition. However many different approaches are used for the recognition phase. These include Support Vector Machine (SVM) (Huang et al. 2003), feature analysis (Jiann-Der et al. 2004), and the use of computer graphics to estimate facial texture from images for comparison (Blanz & Vetter 2003). The research into the use of computer graphics has been limited because, depicting an accurate 3D interpretation from a 2D image is time consuming and requires large amounts of expertise (Blanz & Vetter 1999). Although all of the methods describe above have success in increasing the accuracy of recognition they require large computational resources in order to create the 3D model. A 3D method that may have potential is the latest model proposed by Bronstein, et al., (2005). In this model it is possible to depict the information produced by 3D models without the need to actually reconstruct them.

Although 3D models have been reported to have excellent results, they are not yet practical for a remote verification system. For enrolment, the images need to be

acquired at fairly specific rotations both laterally and vertically and much research has been conducted in trying to determine the optimal view for 3D modelling (Lee et al. 2004). Also the reconstruction of a 3D model from 2D images is computationally exhausting especially when the system may be required to verify potentially hundreds of student simultaneously. If the method proposed by Bronstein, et al., (2005) is used, although it uses less computer resources it requires that very specific images be obtained which require not only rotation but also lighting variations.

5.7 Gabor Wavelet

The Gabor function is named after its creator Denis Gabor who in 1946 conducted experiments that used these functions as a tool for signal detection in noise (Gabor 1946). However it wasn't until the late 1980's when research was being conducted into the human visual system, that Gabor functions found a role in face recognition. At this time studies found that the human visual cortex was compiled of simple cells which could be selectively tuned to orientation as well as to special frequency (Lucey 2003). Understanding the response of these cells in 1988, Daugman suggested that these could be approximated by 2D Gabor Wavelets (1988).

It is a misnomer to call Gabor Wavelets a recognition technique as it must be used in conjunction with other comparative techniques in order to obtain a result. The methods that have been used often with Gabor Wavelets are that of Elastic Bunch graph and direct correlation. The purpose of Gabor Wavelets is to act as a filter on an image, enhancing edge, valley and ridge contours. As such, 2D Gabor Wavelets are able to enhance important fiducial points such as the eyes, nose and mouth. Other prominent aspects on the face used by humans as distinguishing features such as scars, dimples and blemishes are also enhanced. These highlighted areas therefore make faces distinguishable and improve a simple technique such as correlation.

Adding to the work of Gabor and research conducted by Hubel and Wisel (1977), Daugman (1980) was able to show that Gabor wavelets are biologically motivated

convolution kernels in the shape of plane waves restricted by a Gaussian envelope function .

This is denoted by:

$$\Psi(x) = \frac{\|k\|^2}{\sigma^2} e^{\frac{\|k\|^2 \|x\|^2}{2\sigma^2}} \left[e^{jk_i x} - e^{\frac{\sigma^2}{2}} \right] \quad (5.33)$$

where the characteristic wave vector k_i is given by:

$$k_i = \begin{pmatrix} k_{ix} \\ \\ k_{iy} \end{pmatrix} = \begin{pmatrix} k_v \cos\theta_\mu \\ \\ k_v \sin\theta_\mu \end{pmatrix} \quad (5.34)$$

and is restricted by a Gaussian envelope function.

In this function (k_v, θ_μ) represents the centre frequency of the i^{th} filter, noting that each component of the wave is a vector with both magnitude and direction.

The wavelet transform of an image, which essentially forms a low-level feature map of the intensity image, is given by:

$$R_i(x) = \int I(x')\Psi_i(x - x')dx' \quad (5.35)$$

where $I(x)$ is the image intensity value at x

From these relationships it can be noted that Gabor wavelets describe the frequency structure and the spatial relations of an image. In a dissertation compiled by Lucey (2003), he notes that by using five spatial frequencies $(v = 0, 1, \ldots, 4)$ and eight orientations $(\mu = 0,1, \ldots, 7$ the entire frequency spectrum both amplitude and phase can be captured.

By using equation 5.33 and equation 5.34 forty Gabor filters are found, meaning that each pixel is described by a set of forty complex coefficients. As with other algorithms that look to minimise the amount of necessary information to be stored, Gabor wavelets dramatically increase the image size. The benefit of such a

filter is that not all the information in every image needs to be stored. As mentioned earlier the filter enhances the most valuable facial information and as such only these points need to be captured and stored. Figure 5.6 shows some common fiducial points that may be used.

Figure 5.6: Example of Fudicial points on the face

From this understanding of Gabor wavelets it can be determined that pre-processing of the image is necessary in order to locate the desired features. Once the features are found they are sampled in the frequency domain in a log-polar manner (Marcelja 1980), Gabor Transform. The response to the Gabor transform makes up the description of each face.

Once the image is described, verification or recognition can occur using either elastic bunch graph or correlation. If the value returned is above a predetermined threshold then the identity of the person is confirmed.

The Elastic bunch graph technique has not been described for this dissertation. For further information refer to Wiskott, et al., (1997). Correlation can be performed by determining the similarity of each pixel for all features. The average of these is taken as a single value for comparison against a threshold.

5.8 Tensorfaces

Techniques that have been discussed thus far have used linear algebra to describe a 2D image mathematically; in particular PCA, ICA and Fisherfaces are based on this method. The problem associated with using linear algebra is the inability to

describe variations in an image formation. Stated positively linear techniques are only able to model single-factor linear variations of an image or integrate linear combinations from multiple sources (Vasilescu & Terzopoulos 2007). For a robust facial recognition system the desire is for the algorithm to account for as many variations as possible.

Natural images are composed of multiple factors resulting from the interaction of scene structure, lighting, facial geometry, head pose and location and the type of image capturing device used. In 2002 Vasilescu and Terzopoulos published two papers, 'Multilinear Analysis of Image Ensembles: Tensorfaces' (Vasilescu & Terzopoulos 2002a) and 'Multilinear Image Analysis for facial recognition' (Vasilescu & Terzopoulos 2002b) that defined a new technique to solve the problem of multidimensional images used in face recognition. The algorithm was termed TensorFaces, which uses multilinear algebra to define multilinear operators over a set of vector spaces. The name Tensorfaces is derived from the fact that tensors are used to solve the problem, while applying a higher-order generalisation of PCA (eigenfaces).

A tensor is a higher order generalization of a scalar (zeroth order tensor), a vector (first order tensor) and a matrix (second order tensor). While matrices describe linear mappings over a vector space, tensors describe a multilinear mapping over a vector space. Vasilescu and Teropoulos note that there are many ways to orthogonally decompose tensors, however in their study they chose to use an extension of the matrix single value decomposition (SVD) (Vasilescu & Terzopoulos 2002b).

Although Tensorfaces outperform their linear counterparts in facial recognition they require higher processing costs and increased computational resources, exceeding the computer processing capabilities of many computing devices. It has also been noted that because the samples are in a high dimensional space many classifiers perform poorly when given only a small number of training images (Lu et al. 2008). Therefore, for large scale use the method of training images and of comparing the test image needs to be improved. Researchers such as Hosseyninia, et al., (2011), Rana, et al., (2008), and Lu, et al., (2008) suggest a

few methods which have had some experimental results that are still in their infancy but worthwhile mentioning. A multi-linear method that is documented and described well is provided by Vasilescu & Terzopoulos (Vasilescu & Terzopoulos 2007), the main researchers in this area.

More current research has moved away from the name Tensorfaces and prefers to refer to the multilinear techniques based on the processes used. For example, Multilinear Principal Component Analysis (MPCA), Multilinear Independent Component Analysis (MICA) or Multilinear Discriminate Analysis (MDA or MLDA) (Hosseyninia et al. 2011).

5.9 Hidden Markov Model

There are several instances of the Hidden Markov Model (HMM) used for face recognition. These include:

- Luminance-based 1D- Hidden Markov Model (Samaria 1994)
- 2-D pseudo Hidden Markov Model (Samaria 1994)
- DCT-based 1D Hidden Markov Model (Nefian & Hayes 1998) and;
- Low complexity 2D Hidden Markov Model (Othman & Aboulnasr 2000)

HMM was developed because of the inability of PCA and LDA to have high recognition rates when the orientation of the face was altered or the image size changed. Therefore a view based approach was desired to overcome these problems. One such approach is HMM which characterise the statistical properties of a signal.

Nefian & Hayes (1998) describe HMM as consisting of two interrelated processes:

1. An underlying, unobservable Markov chain with a finite number of states, a state transition probability matrix and an initial state probability distribution
2. A set of probability density functions associated with each state

These processes help to understand HMM and therefore the framework documented by Nefian & Hayes (1998) will be used to discuss HMM. It is noted that 2D HMM algorithms are computationally complex and as such are not plausible for a large system. 1D HMM on the other hand performs well with a fraction of the computational requirements.

HMM is mathematically composed of a number of elements. *S* is given as a set of states

$$S = \{S_1, S_2, .., S_N\} \quad (5.36)$$

where N is the number of states.

The length of the observation sequence and therefore the state at time **t** is given by:

$$q_t \ \epsilon \ S, \qquad 1 \leq \ t \ \leq \ T \quad (5.37)$$

The observation set is derived for all possible observations and is given by:

$$V = \{v_1, v_2, \dots, v_M\} \quad (5.38)$$

where M is the number of observations.

A discrete HMM is described by the triplet

$$\lambda = (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{\Pi}) \quad (5.39)$$

where $\boldsymbol{A}$ represents the state transition probability matrix, $\boldsymbol{B}$ is the observation symbol probability matrix and $\boldsymbol{\Pi}$ is the initial state distribution.

In order to create a 1D vector of the face an ordering system is developed for key fiducial points on the face. Under minimal rotation the forehead, eyes, nose and mouth have a natural order from top to bottom. These features are extracted and assigned a state in a 1D continuum from left to right.

In order to extract the features, the image width (W) by height (H) is divided into vertically overlapping blocks such that the width remains as W for each block, the overlap is consistent between blocks and is represented by P. The number of blocks extracted equals the number of observation vectors given by:

$$T = \frac{H - L}{L - P} + 1 \qquad (5.40)$$

where L is the height of the overlapping blocks. A balance must be keep between the amount of overlap and the height of each block. A high amount of overlap has been shown to increase recognition rates. A small block height does not allow enough information to be captured in each block; however, large block heights increase the chance of including multiple features in the same block. The choice is left to the discretion of the programmer.

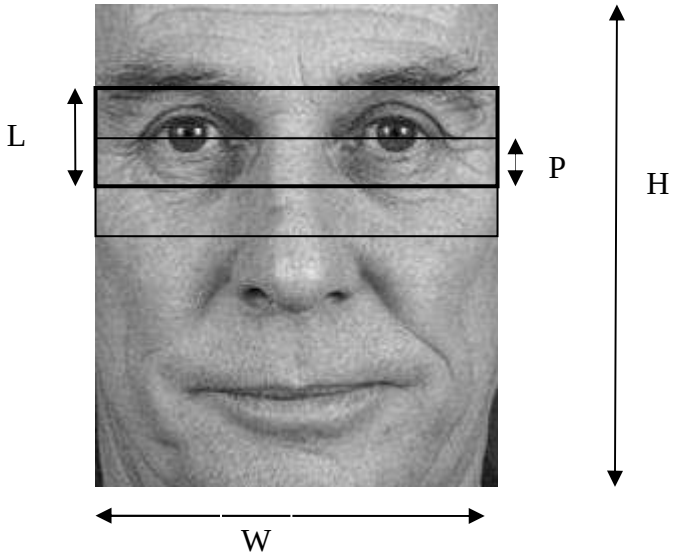

Figure 5.7: Image showing the height (H), width (W), block height (L) and overlap (P) used in HMM

5.10 Chapter Summary

Automated face recognition has been of interest to many researchers over the past 30 years. The techniques employed are essentially pattern recognition and/or pattern matching techniques which have been modified for the express purpose of face recognition and verification. Face recognition is made complicated due to the multi-dimensional aspect of both capturing and viewing the images. Many of the methods described in this chapter reduce the high dimensional space to a low dimensional space by using only the most necessary data required for face recognition. Lower dimensional methods such as 'Eigenfaces' has success in recognising faces in a sterile environment; however, varying environmental conditions may pose a problem. Therefore other methods such as Tensorfaces, Multi-linear Principal Component Analysis or Multi-linear Independent Component Analysis were investigated as they operate in high dimensional space. Although multi-linear algebraic methods may account for greater variation in the image and therefore provide greater accuracy, the mathematical implementation is difficult. Each of the face recognition algorithms suggested have both pros and cons which must be measured when deciding which algorithm to implement in a system. Some techniques are easily implemented, others provide good results under varying light, and some perform well with varying poses. The choice of algorithm is therefore based predominantly on the requirements of the system. The Eigenfaces method proposed by Turk and Pentland (1991) based on principal component analysis was implemented.

Chapter 6

Facial Verification Evaluation Procedure

6.1 Introduction

Facial recognition or verification technology is used in many areas including security and access. For each of these applications it is necessary that the performance statistics found for a particular system or algorithm have not been skewed by the developer or researcher. It is possible for developers to get incredible results in laboratory conditions, however, in real world applications the system may fail catastrophically. Therefore, a standard for testing and evaluating facial recognition software would be ideal so that an alternate system could be compared. A common database of faces is an ideal means of ensuring that algorithms are tested using the same test images, which have been gathered under stringent conditions.

This chapter details the XM2VTS (Extended Multi-Modal Verification for Teleservices and Security Applications) database and evaluation protocol as well as the test database that was developed.

6.2 Evaluation Databases and Protocols

A remote verification system must be able to deal with many environmental variations, and as such the algorithm was tested on a database that included these variations. However, in order to make a comparison between the potential real life applications (environmental variations) and perfect conditions the algorithm was first tested against the XM2VTS database.

As mentioned previously, the direct comparison of results obtained from various authors is difficult due to the inherent nature of testing. The variations in testing, model database size, definition of images, sensors, viewing conditions and background are often significant. Therefore, the results obtained by independent evaluators can be used with greater confidence since there is no bias in testing and the same database is used for all testing. Some of the databases that are often used for testing are the *Yale, Harvard, FERET* and *XM2VTS* databases. One benefit of using the XM2VTS database is that all researchers are given the same data set, unlike the FERET database, where each research group was given a different dataset.

Each database of images has its own protocols of how the images must be trained, evaluated and tested. Training, evaluation and testing are defined as:

- Training – decomposing a set of images into a mathematically meaningful template to which other images can be compared.
- Evaluation – using a set of images, not part of the training set, to determine a suitable threshold for the algorithm.
- Testing – using a set of images, not part of the training or evaluation set, to determine if the algorithm can successfully verify an individual.

The XM2VTS database uses twice as many images for training as it does for both evaluation and testing.

6.2.1 XM2VTS database and protocol

The XM2VTS was developed by the University of Surrey and is an extension to their earlier version M2VTS. The original database contained five images of 37 subjects. The images were captured using a camcorder and subjects were asked to count from '0' to '9' as well as rotating their head from 0^o to -90^o and back and then from 0^o to 90^o. The same technique was used for the XM2VTS database. However, the count from '0' to '9' was replaced by three sentences which were read through twice at the subjects' normal pace. A Sony VX1000E and a DHR1000UX was used for acquiring the images. The VCR has a sampling resolution of 4:2:0 and stored in colour PPM at a resolution of 720 x 576, the audio is captured at 32 kHz at 16 bits per second (Messer et al. 1999). The database contains 8 images of 295 subjects which were captured over a four month period in four sessions. During this period subjects were free to change the appearance of their face as they desired. It is noted that some subjects changed hair colour or hair length during this period.

Figure 6.1: Facial changes during the image capturing period

The 8 images are divided among the three sets; training, evaluation and testing. The protocol requires testing the database with two configurations of the images. Each configuration consists of both clients and imposters. Clients are those which are known to the system while imposters are those that are not known to the system. One subject was set as a client, and a threshold determined; all other subjects were thus considered imposters. These configurations are described in Table 6.1 and 6.2.

Table 6.1: Configuration 1 of the XM2VTS evaluation protocol

Session	Shot	Client	Imposter
1	1	Training	Test
	2	Evaluation	
2	1	Training	
	2	Evaluation	
3	1	Training	
	2	Evaluation	
4	1	Test	
	2		

Table 6.2: Configuration 2 of the XM2VTS evaluation protocol

Session	Shot	Client	Imposter
1	1	Training	Test
	2		
2	1		
	2		
3	1	Evaluation	
	2		
4	1	Test	
	2		

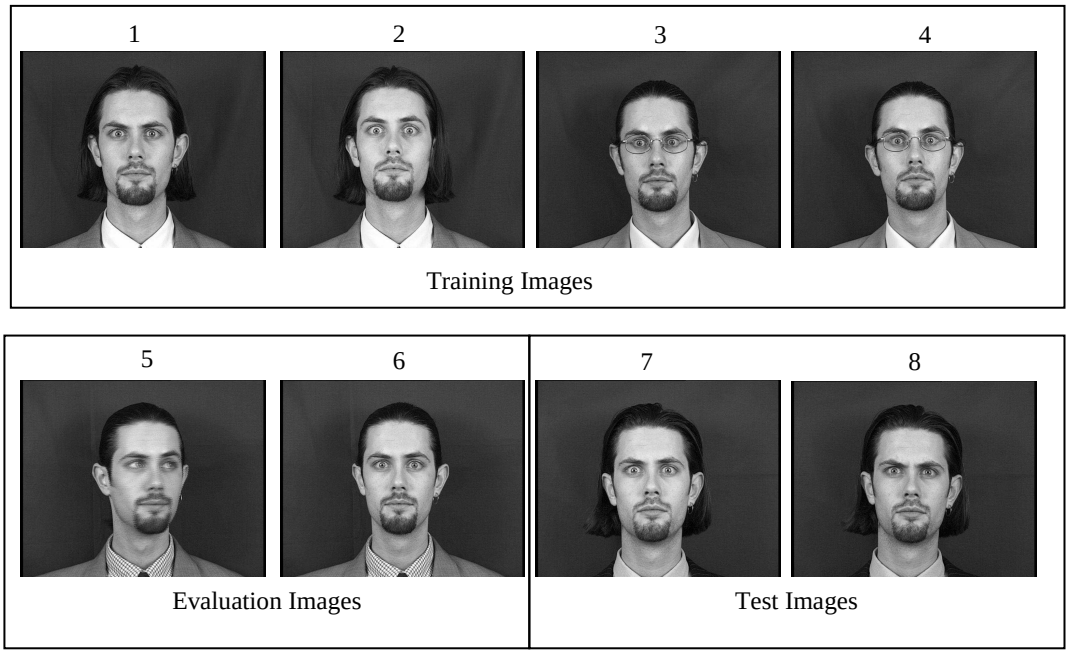

Figure 6.2: Visual display of evaluation protocol 2

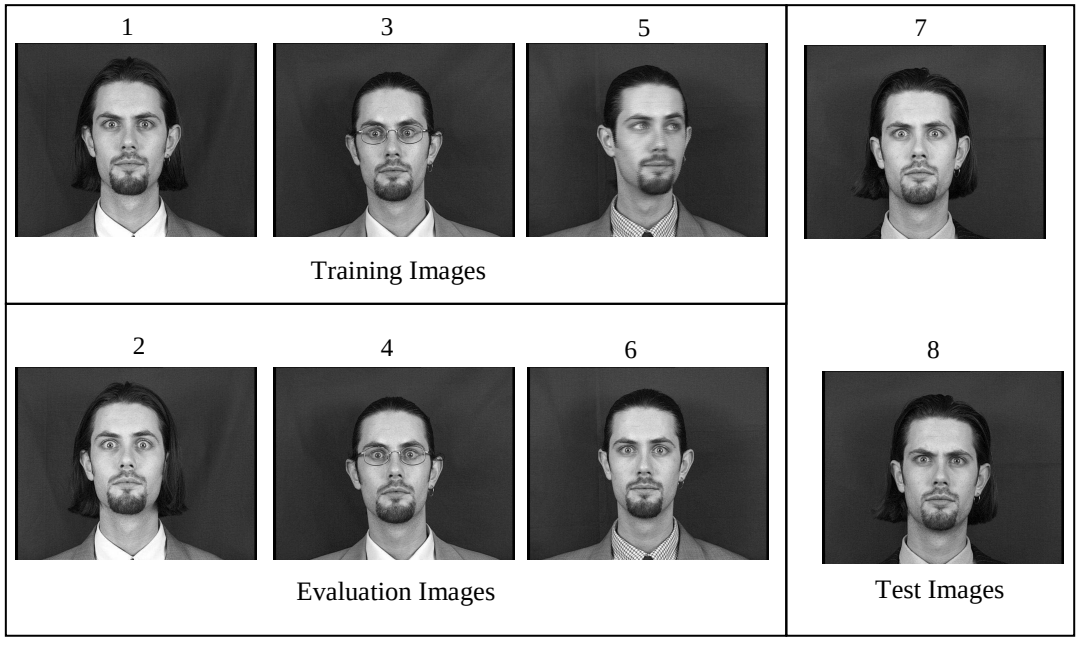

Figure 6.3: Visual display of Evaluation Protocol 1

6.2.2 Test Database

The database included multiple pictures of 10 students currently studying a Bachelor of Engineering at the University of Southern Queensland. Three classes of photos were obtained:

1. A set of photos taken against a plain coloured background, under good illumination and captured with a Kodak EasyShare C1013 10.3 megapixel digital camera. These photos were used for enrolment.
2. Images captured with the same digital camera against a different background, with varying expressions. The lighting conditions were the same as those for class 1.
3. Random images captured with no flash. These images were made to mimic those possibly captured by a webcam during an online examination; they included varying backgrounds, lighting, head position and expression.

Class 1 photos were used as the training set for the facial recognition algorithm, class 2 photos were used for the evaluation phase and class 3 photos were used for testing of the algorithm.

Figure 6.4: Class 1 images for test database

Figure 6.5: Class 2 images for test database

Figure 6.6: Class 3 images for test database

6.3 Remote Verification System

Although the XM2VTS protocol is used for testing it must be noted that the requirements for the remote verification system is different to that required by an access or security system.

When describing the evaluation of an algorithm it is usual to quote figures such as 96% accuracy on a database of 500 people. This percentage is quoted after testing the algorithm against one or two test images.

For a remote verification system to function successfully it may only be necessary to get a match one out of ten times, which would correspond to a success rate of 10%. This is due to the fact that during the duration of a two hour exam it is possible to take multiple snap shots of the student, allowing the system to compare a new photo image at any time throughout the exam. The system may be set up such that if the first image fails, verification of another image can be taken and compared to the template. After ten failures the system is able to flag the activity as suspicious. However, if one of the photos passes verification the

system assumes that no problem exists. Since the student is unaware of when the verification is taking place confidence can be placed in this method.

At the beginning of an exam the student will be asked to verify their identity by posing for the camera. Since it is assumed that most students do not want to fail, cooperation is highly likely. This verification process allows entry into an exam. Likewise during an examination if the captured image fails ten times the system will flag. However, the student will be asked to perform the same steps as in the initial verification. If the system verifies the student from this process the flagged case could either be withdrawn or placed as a low priority case. However if this process fails, the system will treat the case as highly suspicious and manual checking will be required.

6.4 Gaussian Curves

Using the protocols described in section 6.3 the desired result for a facial verification system is to reject imposters 100% of the time and to accept clients 100% of the time. Alternatively the false rejection and false acceptance rate will both be 0%. This can be described visually through the use of Gaussian curves.

The probability of recognising the client as a client can be described as a Gaussian distribution. Likewise the probability that an imposter will be recognised as an imposter can also be described as a Gaussian distribution. A Gaussian curve of a client and imposter showing 0% error rates is given in Figure 6.4. All values to the left of the threshold line are considered to be clients.

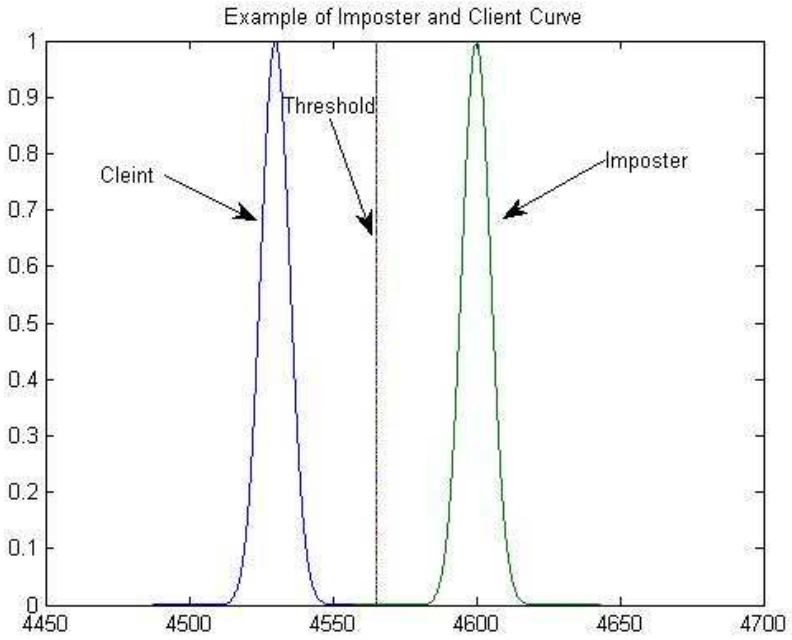

Figure 6.7: Curves demonstrating 0% client and imposter error

For a Gaussian distribution there are two key elements, the mean, μ, and standard deviation σ. The mean determines where the peak of the Gaussian distribution sits, while the standard deviation determines the steepness of the distribution. The smaller the standard deviation the steeper the curve, since 99.7% of data will lie within three standard deviations. Figure 6.5 and 6.6 show differences in mean and standard deviation.

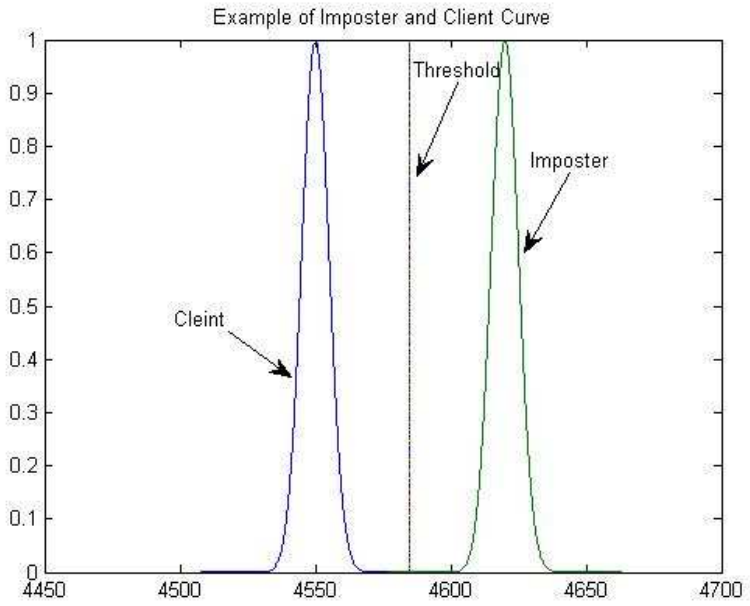

Figure 6.8: Gaussian curves demonstrating a shift in the mean in comparison to Figure 6.4

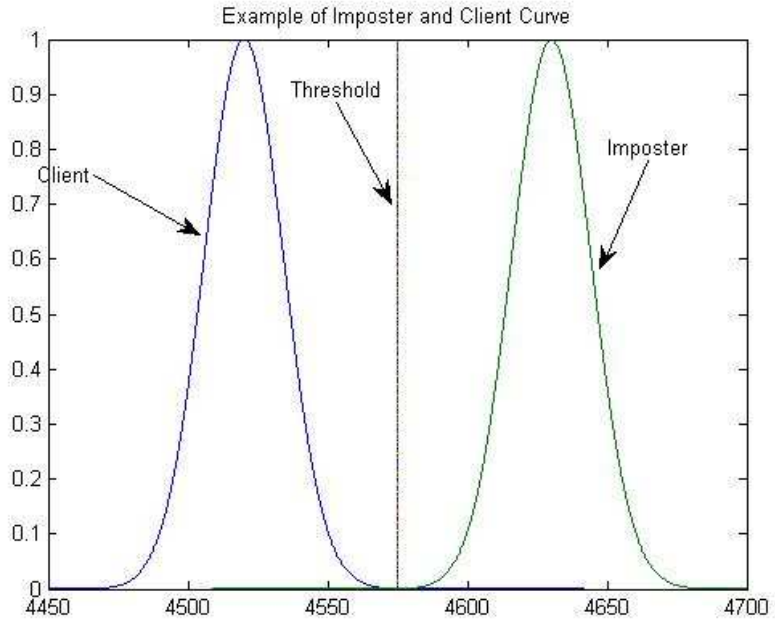

Figure 6.9: Gaussian Curves showing the effect of changing the standard deviation in comparison to Figure 6.4

With regards to facial recognition the standard deviation and mean of the Gaussian distribution can be understood as follows.

The standard deviation is a measure of how good the facial recognition algorithm is at finding differences within an image. The higher the discrimination of an

algorithm the lower the standard deviation will be. As the standard deviation decreases the width or spread of the Gaussian distribution also decreases. This allows curves that have similar means to be distinguishable due to the steepness of the Gaussian curves. The difference in the crossover of curves with varying standard deviations is shown in figure 6.7.

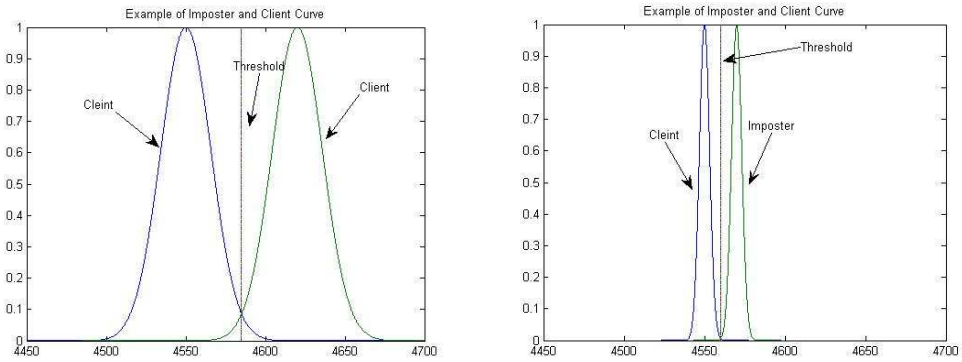

Figure 6.10: Graphs showing the difference in the cross over of curves based on the discrimination of the algorithm.

The mean of a facial image can be any real positive number and will vary for each facial image; however, the mean will remain within a tolerance. This is due to the fact that all face images look like faces and therefore their means will be similar. This is in contrast to an image of a building or vehicle in which case the mean will be significantly different to that of a facial image. Therefore an algorithm can still have significant results, even if the standard deviation is high, as long as the images being compared have no resemblance. This concept is can be seen in figure 6.4.

The analysis of the Gaussian distribution curve shows that an algorithm which provides better discrimination will have less overlap and ambiguity between the client and imposter curves, therefore minimising the errors.

6.5 Chapter Summary

Evaluation of a face recognition algorithm is difficult due to the nature of the images involved and the number of possible variables to account for. For this reason many face databases have been specifically designed to be used for evaluating algorithms. These databases not only provide test images but also the protocols required for testing. The XM2VTS database developed by the University of Surrey provides eight images of 295 subjects over a four month period. The database provides two protocols for evaluation where the training and evaluation images are combinations of the first six images and the test images are images seven and eight in both cases. One of the downfalls to the XM2VTS database is the lack of variations in the environmental conditions. Since the algorithm will be implemented in a remote examination system where environmental conditions will vary a test database to test these conditions was desired. A test database was generated of ten subjects containing four training images, two evaluation images, and two test images for each of the cases where the subject is, against random background, against a plain coloured background and against a high illumination source.

The ideal outcome of testing the algorithm against the database is to have 0% client error and 0% imposter error. The results obtained from testing will be considered by comparing the results to a set of Gaussian distributions with a given threshold.

Chapter 7

Algorithm Implementation

7.1 Introduction

The eigenfaces facial recognition algorithm was implemented in Matlab and tested using the XM2VTS and test databases as defined in Chapter 6. The eigenfaces algorithm was chosen as it has good documentation and has been implemented successfully in Matlab with positive results. It is noted, however, that the images used for testing were gathered under strict circumstances and therefore it is uncertain how the algorithm will act under varying environmental conditions and with non-cooperative subjects.

This section outlines the way the algorithm was implemented in Matlab, the pre-processing techniques used and the testing methodology.

7.2 Eigenface Implementation in Matlab

In Chapter 5 many algorithms were discussed and compared. The eigenfaces algorithm was chosen for implementation as it has been extensively researched, developed and documented. This allows for the results obtained during testing to be effectively compared to previous research. This approach uses principal component analysis to decompose an image into eigenvectors which can then be compared and analysed. This is discussed in depth in Chapter 5. The technique uses information from the entire image and is therefore termed *holistic*, as compared to other techniques which only use fudicial points.

There are three sets of Matlab scripts used throughout the testing process. The first is comprised of the eigenfaces algorithm, the second includes the pre-processing techniques and the third is a script which calculates the results into meaningful data. These have been provided in Appendix B, Appendix C and Appendix D.

7.2.1 Eigenface Matlab Script

The first Matlab script is composed of three main sections, decomposition of the training images into their eigenvectors and eigenvalues, decomposition of the evaluation images to subsequently determine a realistic threshold and decomposition and testing of the test images.

All images were numbered in order from one through to 1000, corresponding to 125 subjects. The script was set to cycle through each subject andto determine if the test image was an imposter or a client. Due to the nature of the test sets, only two images were tested as known clients. This is because four images were used for training and two images for evaluation. 250 images were tested as known imposters.

The test images were then given a value, 1 or -1, corresponding to whether they were recognised as clients or imposters respectively. This information was recorded in a matrix and saved as a MATLAB variable to be used for further analysis in the results script. An example of the output is shown in Table 7.1.

Table 7.1: Example of the raw results from the Eigenfaces Algorithm

	Sub 1	Sub 2	Sub 3	Sub 4	Sub 5	Sub 6	Sub 7	Sub 8	Sub 9
Sub 1	1	-1	-1	-1	-1	-1	-1	-1	-1
Sub 2	-1	1	-1	-1	-1	-1	-1	-1	-1
Sub 3	-1	-1	1	-1	-1	-1	-1	-1	-1
Sub 4	-1	-1	-1	1	-1	-1	-1	-1	-1
Sub 5	-1	-1	-1	-1	1	-1	-1	-1	-1
Sub 6	-1	-1	-1	-1	-1	1	-1	-1	-1
Sub 7	-1	-1	-1	-1	-1	-1	1	-1	-1
Sub 8	-1	-1	-1	-1	-1	-1	-1	1	-1
Sub 9	-1	-1	-1	-1	-1	-1	-1	-1	1

It can be noted that in this example the diagonal is filled with the value 1. In an ideal case this would be the outcome, as the template when compared with an image of the same subject, is recognised as a client. All other images are recognised as imposters. Detailed analysis of the results is provided in Chapter 8.

7.2.2 Pre-processing MATLAB Script

The pre-processing script takes a ‘raw’ image file and alters the information available such that the new information will be more meaningful to the eigenfaces MATLAB script. The images are imported into MATLAB, altered and saved to another folder. This save time for future testing as the pre-processing script, was ran only once in comparison to running it every time the eigenfaces program was run.

The pre-processing scripts are actually a combination of four pre-processing techniques that were run individually in order to determine their individual

successfulness at increasing the accuracy of the algorithm. These techniques are explained in depth in section 7.3.

7.2.3 MATLAB Results Script

The results script takes the raw data, shown in Table 7.1, and converts it to a percentage. It looks at each row and column and determines if the result is correct or not (1 or -1 respectively). If the result is correct (i.e. the value 1) the client tally is incremented, if the result is incorrect (i.e. the value -1) the imposter tally is incremented. The number of clients and imposters is known and therefore the percentage is as follows::

$$Client\ \% = \frac{Client\_count}{Client\_total} \times 100$$

and

$$Imposter\ \% = \frac{Imposter\_count}{Imposter\_total} \times 100$$

The client percentage shows how often the algorithm determines the client as a client and how often it determines the imposter as an imposter. However, in the case of facial recognition it is common practice to quote the error rates. Hence, the error rates can be given as:

$$Client\ error\% = 100 - \frac{Client\_count}{Client\_total} \times 100$$

and

$$Imposter\ error\ \% = 100 - \frac{Imposter\_count}{Imposter\_total} \times 100$$

The final output of the results script is the false acceptance rates, given as imposter error, and the false rejection rates given as client error.

7.3 Pre-Processing techniques

Although the algorithm implemented can be used as a standalone program, it is known that details presented in a raw image can have adverse effects on the ability for the algorithm to distinguish between clients and imposters. Without modifying the algorithm itself, it is possible to enhance its ability by altering the image information available in the image by the means of pre-processing. In this instance there were four pre-processing techniques used to enhance the quality or make the image palatable for the algorithms. These techniques include: converting images to grey scale, face detection and cropping, light normalisation and resizing images.

7.3.1 Converting Images to Grey scale

The eigenface algorithm does not make use of information provided by colour image since it reduces the higher dimensional information to a low dimensional space. The colour image which is expressed as a 3 dimensional matrix of colours Red, Green and Blue, can be expressed as a 256 bit greyscale 2D matrix. This process substantially reduces the amount of information stored and allows for faster processing of the images without losing significant information. This step is essential as the algorithm is unable to decompose the information in a 3-D matrix.

7.3.2 Light Normalisation

From a human perspective it is difficult to determine a person’s identity from an image if the face is only a silhouette. This is due to shadowing or poor lighting conditions. The process is substantially more difficult for computer algorithms as the pixel intensities required to decompose and store as useful information will all be similar. Therefore the image information must be altered to gain a better representation of the original image. To try to account for variations in lighting histogram equalisation was used.

7.3.3 Face Detection

Most captured images include information other than the subjects face. For facial recognition all of the information contained in the background does not provide useful information for the recognition process. In the case of the XM2VTS database, all of the subjects' images were taken against blue backgrounds; therefore the background information increased the similarity of each image to all others. It is possible this causes significant reduction in the ability of the algorithm to distinguish between clients and imposters. Therefore the goal was to crop the image so that only the face of image subject was used during the verification process in a hope that the results would be improved.

The XM2VTS database provides coordinates of the subjects eyes, nose and mouth, which could then be used to crop the subjects face. Although this would allow testing to occur, it does not align with the requirements of a remote verification system since such coordinates could not be obtained during an exam. For this reason the concept of face detection was trialled as a way to gather the facial information only.

The mathematical analysis behind face detection is not covered in this dissertation. What is covered is simply a means of implementing it in conjunction with a face recognition system. For this reason a freely available library, fdlib.dll, for MATLAB was used. The library was treated as a 'blackbox' and only the outputs were adjusted as to mesh with the face recognition algorithm.

The output is an N by 4 matrix where the first column specifies a x-coordinate, the second column specifies a y-coordinate, the third specifies the width of the face and the fourth is a dummy output usually set to 0. It is possible that the algorithm returned multiple rows, which represents multiple faces within each image.

It may be useful for future work to ensure that multiple users are not present during the examination. However, during testing it was known that only one face would appear in each image. Hence, the output needed to be adjusted to ensure that the face of the subject, and not another area, was being cropped.

The algorithm appears to locate points within the image that are distinguishable i.e. points of sharp transition such as an apex. (These tests were performed on a personal database and for ethical reasons have not been added as figures). However on areas such as the door, or corners of the eye, the width of the box that is determined is significantly smaller than that produced when a face is found. Hence, the output was altered to only take the largest value in column 3 and use the corresponding row as the best estimate for the middle of the face. The face was subsequently cropped and saved to be used in the eigenfaces algorithm.

The face detection program works consistently for images where the subjects face has 0^o rotation and the background does not have any sharp objects. This is the case for the XM2VTS database and therefore the face detection worked well successfully cropping 97% of images. However, in images where the subject had their face slightly rotated or the background contained irregularities the program was less reliable. It is therefore noted that this particular algorithm may not be viable for an uncontrolled environment. Although an examination is essentially an uncontrolled environment, it is possible to force the student to look directly at the camera by stopping their exam, so that accurate images can be captured. This need only occur if they have failed the verification process several times.

7.3.4 Resizing Images

The images provided in the XM2VTS database are 720×576. This takes a large amount of room to store, especially considering the number of students participating in examinations each semester. If an image size smaller than 720 x 576 has comparable results, then it is possible to reduce the overall computational requirements of the system as well as the storage space. In order to resize the images you must first determine the effect that reducing the size of the image has on the accuracy of the algorithm.

The image sizes that were tested were:

- 114 x 91
- 60 x 48
- 30 x 24

The result for each of these is discussed in Chapter 8.

7.4 Testing Methodology

As mentioned in section 6.2, there are two databases against which the eigenface algorithm was tested. The XM2VTS database was used as a reference point to ensure that the algorithm functioned correctly. As the database was gathered under strict conditions, the light, background, expression and head position were accounted for. In contrast, the test database was produced with limited guidelines and as such, subjects were free to have varying head positions and rotations, varying light and backgrounds. The test database only consisted of ten subjects which was sufficient to get an understanding of how the algorithm would perform under varying conditions.

The testing procedure for both databases was as follows:

1. Use the outlines provided in Table 6.1 and 6.2 for the training, evaluation and testing phase
2. Use histogram equalisation for pre-processing before training, evaluation and testing
3. Use face detection for pre-processing before training, evaluation and testing
4. Resize images for pre-processing before training, evaluation and testing
5. Incorporate all pre-processing techniques before training, evaluation and testing.

The same sets of images were used in all cases so that a fair comparison could be made.

7.5 Chapter Summary

MATLAB was used as the programming language to implement the algorithm due to its innate ability to handle images in matrix form. The scripts were divided into two (2) areas: algorithm and pre-processing. The algorithm scripts include the eigenface script and the results scripts. Although the eigenface script is able to be run standalone, variations or common areas of each image can hinder the ability of the algorithm to accurately verify subjects. Therefore four (4) pre-processing techniques were used to increase distinctive characteristics in images and to increase processing speed. These techniques included converting grey scale, rescaling images, cropping faces and light normalisation. The algorithm was tested using no pre-processing, only light normalization, only resizing, only face cropping and all pre-processing techniques combined.

Chapter 8

Facial Verification Results

8.1 Introduction

Results were obtained for both the XM2VTS database and the test database according to the evaluation protocols described in chapter 6. The verification rates of the raw images were used as a basis to compare and analyse the effect pre-processing techniques have on the effectiveness of the algorithms ability to verify subjects.

The pre-processing techniques for testing consisted of light normalisation, reduction of image size, cropping of faces and various combinations of each. Although all of the images were initially converted to grey scale images, this process is not considered a pre-processing technique as it is necessary for all testing and as such had no further effect on verification rates.

As mentioned in chapter 5 the Eigenface algorithm calculates a maximum and minimum Euclidean distance. In order for a test image to be verified the maximum and minimum Euclidean distance must be within a predetermined threshold. Therefore the threshold was varied for each test to determine the effect it had on verification rates.

8.2 Verification Rates on XM2VTS database

The XM2VTS database is a professionally developed database which provides facial images of subjects over a four month period. The algorithm developed was tested using 125 subjects comprising of male and female as well as a variation in age and ethnicity. Figure 8.1 shows a sample of images provided in the database.

Figure 8.1: Example of images provided in the XM2VTS database

8.2.1 Verification Rates without Pre-processing

The results obtained for evaluation protocol 1 and evaluation protocol 2 are provided in Table 8.1 and 8.2 respectively, displaying the results for different thresholds. Table 8.1 shows that as the threshold decreases the client error percentage increases; however the imposter error percentage decreases. This is shown graphically in Figure 8.2 and shows that as the threshold drops below 8% the imposter error decreases sharply while the client error increases sharply. It can also be noted the functions intersect at 3%, which corresponds to the threshold that optimises both errors. This is the relationship that would be expected and can be explained by referring to the Gaussian curves described in section 6.4. As the

threshold value is increased, a greater percentage of the client curve is found to be a client; however greater portion of the imposter curve is recognised as a client. Once again, note that all values to the left of the threshold will be regarded as client, while all values to the right are regarded as an imposter.

Table 8.1: Evaluation Protocol 1 Verification rates without Pre-processing

Test	Threshold	Client Error %	Imposter Error %
Evaluation Protocol 1	0.2	15.625	87.8276
Evaluation Protocol 1	0.08	16.4	61.335
Evaluation Protocol 1	0.03	34.8	36.8129
Evaluation Protocol 1	0.01	42.4	26.31

Table 8.2: Evaluation Protocol 2 Verification rates without pre-processing

Test	Threshold	Client Error %	Imposter Error %
Evaluation Protocol 2	0.08	0.8	96.9032
Evaluation Protocol 2	0.03	4.4	93.5226
Evaluation Protocol 2	0.01	5.6	91.667
Evaluation Protocol 2	0.005	6	91.1548
Evaluation Protocol 2	0.0005	6	90.5129

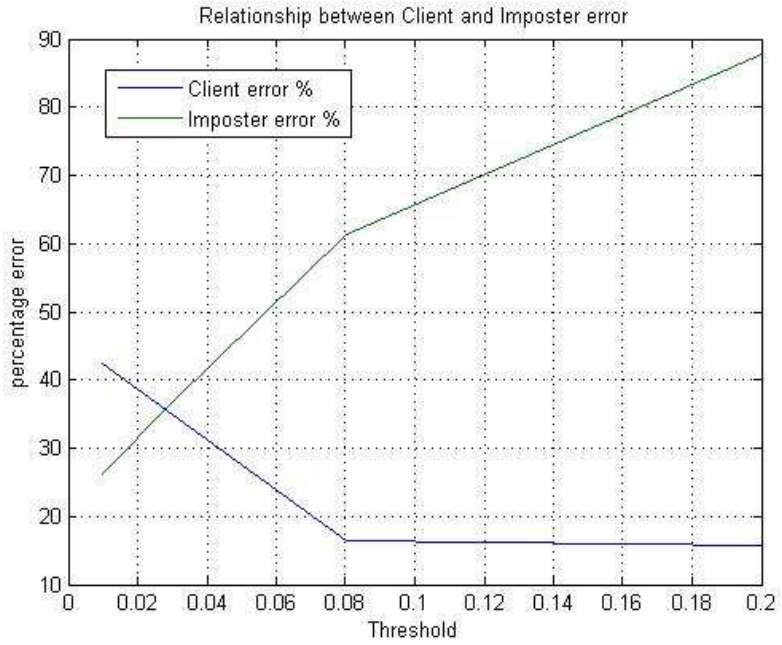

Figure 8.2: Effect of decreasing the threshold on images with no pre-processing, using Evaluation protocol 1

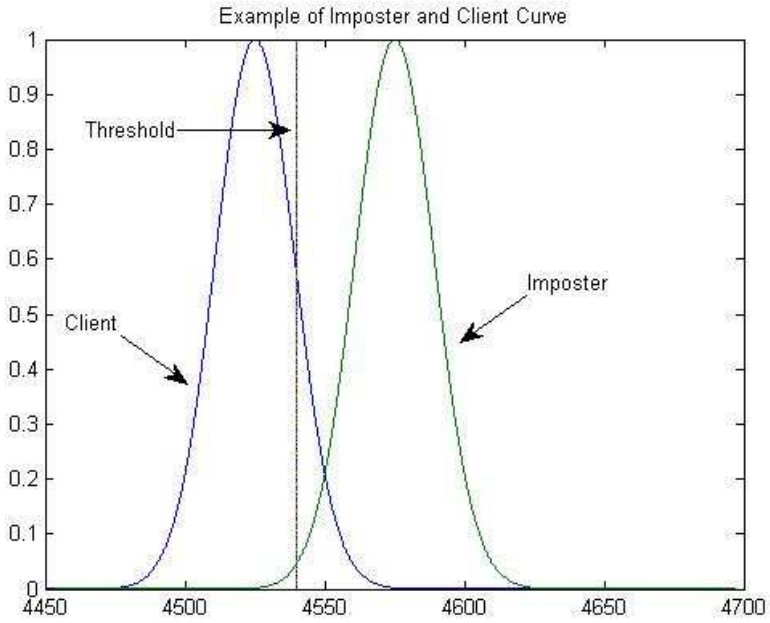

Figure 8.3: Example Gaussian curves showing a small threshold value

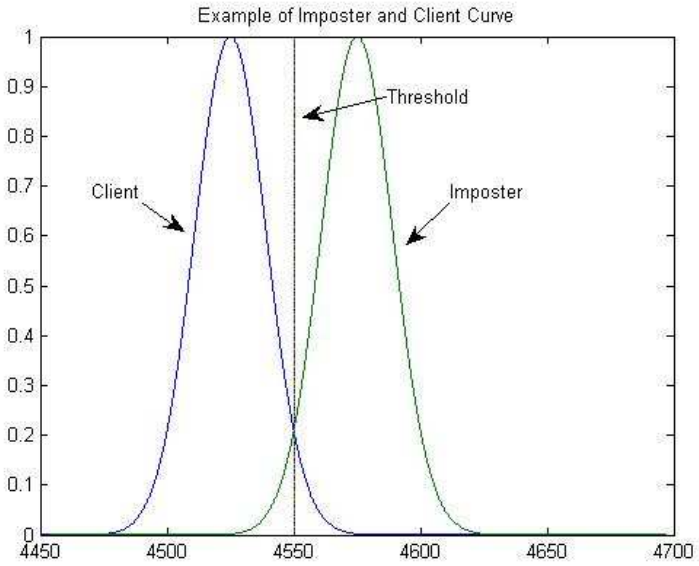

Figure 8.4: Example Gaussian curves showing a mid- range threshold value

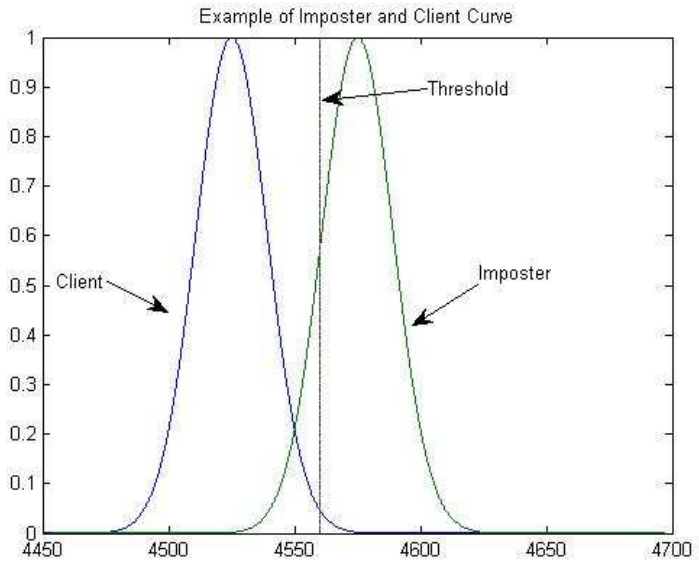

Figure 8.5: Example Gaussian curves showing a large threshold value

Similar results were also calculated for the algorithm using evaluation protocol 2. These results are displayed in Table 8.2. Although the results follow the same pattern as that discussed previously, the imposter error for all cases were not within a suitable range. The threshold was set to 0.0005 (0.05%) to minimise the imposter error; however the error remained significant.

It appears that the Gaussian curves for the client and imposter in this case are almost identical and as such renders distinguishing between client and imposter impossible. This is displayed graphically in Figure 8.6 and 8.7. It is noted that as the threshold is made infinitely smaller the imposter error would decrease; however the client error would increase to an unsuitable level.

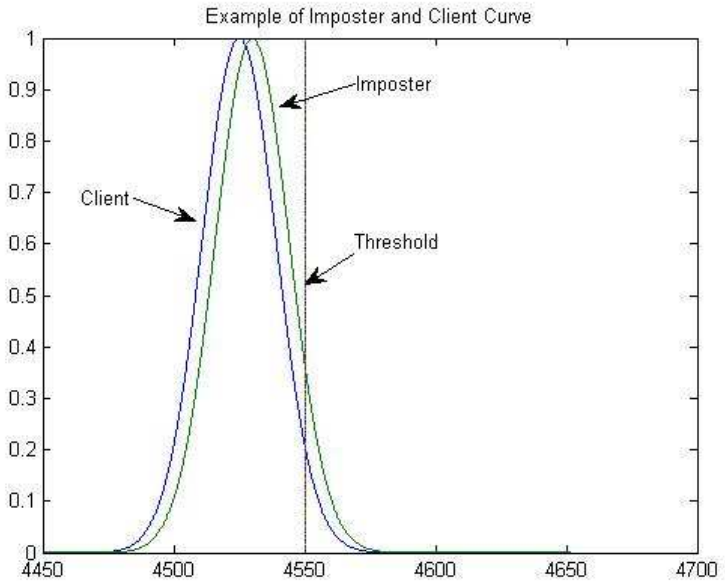

Figure 8.6: Example Gaussian curves with large threshold for evaluation protocol 2

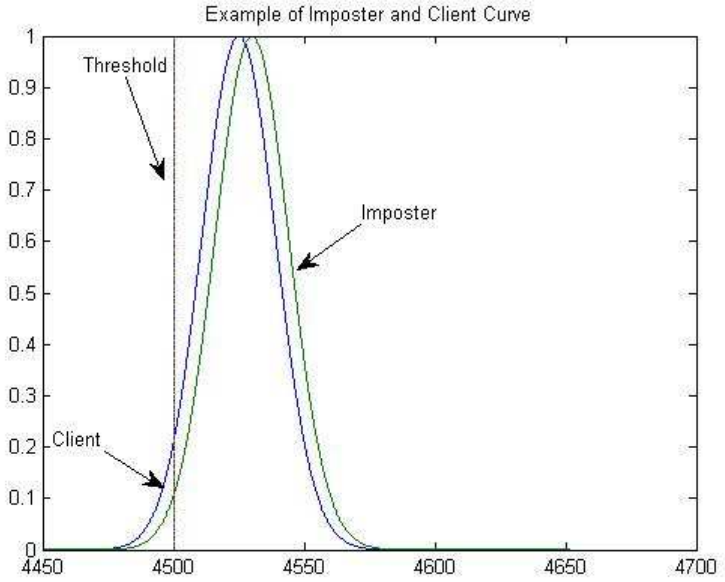

Figure 8.7: Example Gaussian curves with infinitely small threshold for evaluation protocol 2

The error that occurred for evaluation protocol 2 was unable to be identified and therefore further tests on this protocol have been excluded. Therefore the remainder of the tests referred to in this section will be for evaluation protocol 1 only.

The threshold that was found to optimise both the imposter error and client error was 0.03 (3%) and as such, threshold values in close proximity to this value were used for comparison.

8.2.2 Effect of Normalisation

Histogram equalisation was used as a method to normalise the light in each image. The technique effectively changes the intensity of pixels that appear to be outliers so as to fit a normal distribution. A comparison between the original grey scale image and an image that has undergone histogram equalisation is shown in Figure 8.8; comparison of results is shown in Table 8.3.

Figure 8.8: Histogram equalisation (top) in comparison to the original image (bottom)

Table 8.3: Comparison between no processing and histogram pre-processing

Test	Threshold	Client Error %		Imposter Error %	
		Histogram	None	Histogram	None
Evaluation Protocol 1	0.03	15.6	34.8	63.6742	36.8129
Evaluation Protocol 1	0.01	45.6	42.4	35.2	26.31

From the results it can be concluded that histogram equalisation in this instance has increased the errors for both client and imposter. From the images shown in Figure 8.8, histogram equalisation causes the faces to be 'washed out' and therefore making them appear similar and harder to distinguish. It can be concluded that when images are taken under good lighting conditions histogram equalisation may have a detrimental effect on verification rates.

8.2.3 Effect of Image Size

The original images were 720 x 576 which requires a large amount of memory to store and large CPU requirements to analyse. In comparison, smaller images required less storage space and less processing requirements.. The difference in storage requirements is shown in Table 8.4.

Table 8.4: Comparison of memory requirements for different size images

Image Size	Memory Requirement (kB)
720 x 576	39.50
114 x 91	1.70
60 x 48	0.843
30 x 24	0.489

Decreasing the image size from 720 × 576 to 114 × 91 makes is possible to have a 20 fold memory saving. This significantly saves storage space which is worth considering since the current enrolment for distance education students is 18,000

and that they will each be required to submit six images. The total amount of storage space required for a 720 x 576 image would be:

$$40(kB) \times 6 \times 18000 = 4320000$$

Hence, the total storage requirement is a minimum of 4.3GB. While this is not significant with todays storage capabilities, it is still a factor to consider.

In comparison, a 114 × 91 image would require only 183MB, which is a significant advantage, as long as the results are not diminished. The comparison between results gathered for differing image sizes is provided in Table 8.5. A comparison of image sizes is provided in Figure 8.9

Figure 8.9: Comparison of image sizes. The original image (left) has been reduced to a quarter of its original size. The 114 × 91 image (right) has not been resized

Table 8.5: Comparison between results with no pre-processing and various image sizes

Test	Threshold	Client Error %		Imposter Error %	
Evaluation Protocol 1	0.03	None	34.8	None	36.8129
Evaluation Protocol 1	0.03	114 x 91	28	114 x 91	36.9613
Evaluation Protocol 1	0.03	60 x 48	26	60 x 48	37.2226
Evaluation Protocol 1	0.03	30 x 24	24	30 x 24	37.3581

When using an image size of 114 × 91 both the client error is reduced by 6.8% and the imposter error is increased by 0.15%. As the client error is reduced substantially, compared with the increase in imposter error, it is not only more efficient to use a size of 114 × 91 but has been shown to improve results.

It is also noted that there is no significant difference between an image of 114 × 91 and an image size of 30 × 24. While the memory saving is not significant between these two, there is a difference in processing speed.

8.2.4 Effect of Face Detection

All of the images provided in the XM2VTS database were taken against a blue background. As such, each of these images has a large percentage which looks very similar. Although the human brain can distinguish between the background and facial outline easily and hence only analyse the face, a computer does not have such a luxury. By using only the face in the verification process, it is hoped that the verification rates will increase. By using a threshold of 0.03, which was the optimal solution when no pre-processing techniques were used, the results could be compared. These results are given in Table 8.6.

Table 8.6: Comparison of results between face detection and no pre-processing using a threshold of 0.03

Test	Threshold	Client Error %		Imposter Error %	
		Face Detection	None	Face Detection	None
Evaluation Protocol 1	0.03	6	34.8	80.3839	36.8129

From the results, it can be seen that for a threshold of 0.03 the client error is less; however the imposter error has been significantly increased. The Gaussian distribution curves can be used to understand why this has taken place. A sample Gaussian curve is provided in Figure 8.10 which shows the reduction in the standard deviation for the client and an increase in the imposter, when compared with Figure 8.3. This is to be expected as the client faces will look more similar, therefore reducing the standard deviation; however every imposter will look different and simultaneously, the standard deviation will increase. Since the standard deviation of the client curve is low, thus making the curve steep, reducing the threshold should not affect the client error significantly. The

threshold was tested for both 0.005 (0.5%) and 0.001 (0.1%) and these results are given in Table 8.7.

Table 8.7: Face detection results using a threshold of 0.005 & 0.001

Test	Threshold	Client Error %	Imposter Error %
Evaluation Protocol 1	0.005	30.8	34.8129
Evaluation Protocol 1	0.001	40.4	24.8839

At a threshold of 0.005, the client error is 30.8% which is 4% less than the optimal result when no pre-processing is used. The imposter error is 34.8% which is 2% less than the optimal result for no pre-processing. The imposter error can be reduced further by setting the threshold to 0.001; however this is at the detriment of the client error.

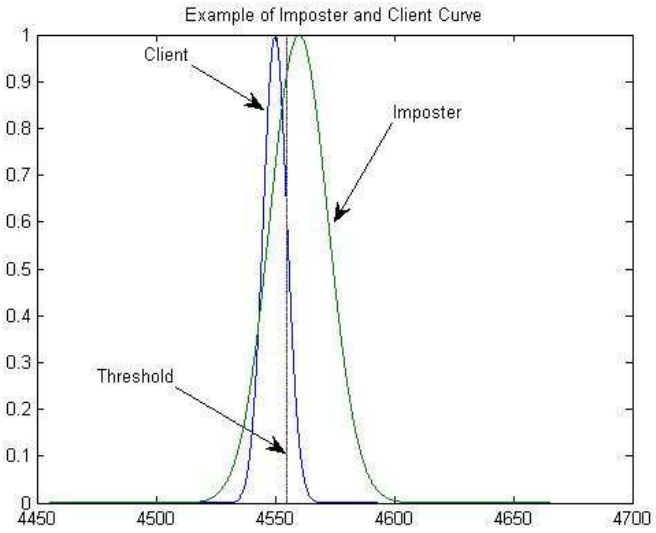

Figure 8.10: Sample Gaussian curve for Face Detection results

In this instance face detection was successfully used to decrease the errors in comparison to no pre-processing being used.

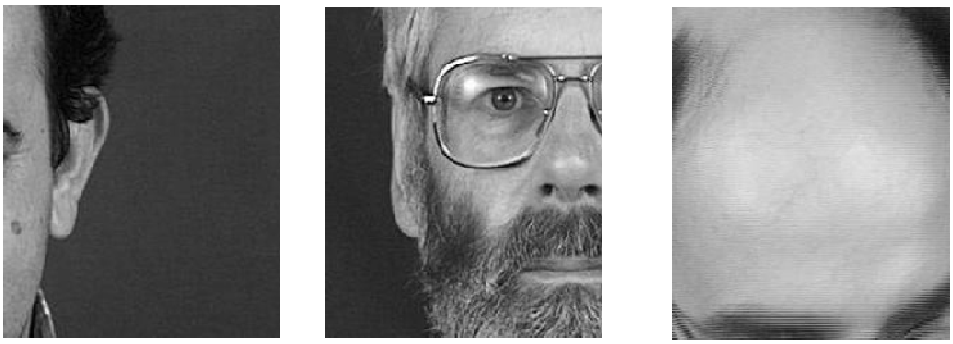

Figure 8.11: Examples of Face Detection not correctly identifying the face

One of the problems with using face detection is its ability to accurately and consistently crop the face. Instances occurred within the cropping process where parts of face (Figure8.11), or no face at all (Figure8.12) were cropped. These images remained in the test database and the results included the effect of having fully occluded or partially occluded faces.

Figure 8.12: Example of Face Detection completely occluding a Face

8.2.5 Effect of all Pre-processing techniques combined

Combining all of the pre-processing techniques should produce a result that is superior to verification rates when no processing is used or only one technique is used. As shown in section 8.2.4, face detection allows the threshold value to decrease. Therefore the values shown in Table 8.8 use a threshold of 0.005 so that the results can be compared to that of only using the face detection pre-processing.

Table 8.8: Results when all pre-processing techniques are used for each size

Test	Threshold	Client Error %		Imposter Error %	
Evaluation Protocol 1	0.005	Face Detection	30.8	Face Detection	34.8129
Evaluation Protocol 1	0.005	All, Size 1	45.6	All, Size 1	19.8774
Evaluation Protocol 1	0.005	All, Size 2	44	All, Size 2	19.8871
Evaluation Protocol 1	0.005	All, Size 3	44	All, Size 3	19.36355

The results show that there is no difference in using histogram equalisation in conjunction with face detection for various size images. However when compared to the results obtained from using face detection pre-processing alone, it can be seen that the client error increases by 15% while the imposter error decreases by 15%. Depending on what is considered more important, this may or may not be a benefit.

Section 8.2.2 shows that histogram equalisation had a negative impact on the verification results. In order to see if this had an impact on the results obtained in Table 8.8, another set of results were obtained where only face detection and resizing techniques were used.

8.2.6 Effects of Face Detection and Resizing images

Two pre-processing techniques proved to be useful in increasing the verification rates, namely, face detection and resizing the image. The results obtained when using these techniques together are shown in Table 8.9. It can be seen that it is possible to decrease the client error by almost 10%, while the imposter error is only increased by 1.6% as the image size of the face decreases.

Table 8.9: Results when using Face Detection and Resizing pre-processing techniques

Test	Threshold	Client Error %		Imposter Error %	
Evaluation Protocol 1	0.005	Face Detection (FD)	30.8	Face Detection (FD)	34.8129
Evaluation Protocol 1	0.005	FD, Size 1	27.2	FD, Size 1	35.3
Evaluation Protocol 1	0.005	FD, Size 2	23.6	FD, Size 2	35.4
Evaluation Protocol 1	0.005	FD, Size 3	21.2	FD, Size 3	36.4903

From Table 8.9 it could be deduced that it is best to use face detection with an image size of 30 x 24 for verification.

8.3 Verification Rates on Test Database

The test database developed was used to determine the effects that light, background, head pose and emotion had on the verification accuracy. From the database, which consisted of photos taken against a white background, coloured background, random background and a high illumination background, three test sets were created. All test sets used the images with the subject against a white background for the training and evaluation phases. The only difference between the sets was the test images provided. This procedure was used to mimic the way a remote verification system would operate. The three test images in each set were:

1. Subject against a plain coloured background
2. Subject against a random background
3. Subject against a highly illuminated background (window)

The images were tested on the algorithm using no pre-processing, histogram equalisation, face detection, resizing images or a combination of all pre-processing techniques.

The same thresholds were used for respective tests so that a comparison could be made between the results obtained from the XM2VTS database and the test database. Table 8.10 to 8.13 shows the results of testing.

Table 8.10: Verification rates on test database without pre-processing

Test	Threshold	Background	Client %	Imposter %
Evaluation Protocol 1	0.03	Random	5	65
Evaluation Protocol 1	0.03	Plain Colour	5	70
Evaluation Protocol 1	0.03	Window	5	55

The client error in each case was 5%, except for the 30 × 24 images where the error was 0%. There were no significant differences between using no pre-processing and using a combination of all pre-processing techniques. The only difference that occured was between the changes in the background. Subjects placed against plain colours performed the worst, followed by a random background, with the best performance being when the subject was standing in front of a window. This was unexpected as the images with subjects against a window are the most difficult to verify, while the subjects against a plain coloured background were the easiest, from a human perspective.

Table 8.11: Verification rates on test database using light normalisation

Test	Threshold	Background	Client %	Imposter %
Evaluation Protocol 1	0.03	Random	5	75
Evaluation Protocol 1	0.03	Plain Colour	5	75
Evaluation Protocol 1	0.03	Window	5	55

The results provided in Table 8.10 to 8.13 are not accurate depictions of what would be expected when evaluating the algorithm under varying circumstances. Since the database only contained ten subjects, the percentages quoted do not have significant meaning. This is due to the fact that the difference of one person being recognised as an imposter could increase or decrease the percentage by

10%. The client error on the other hand is the same in all cases as one image of one person is not recognised as a client. In order to obtain results that will be useful, the database size needs to be increased to match that of the XM2VTS database.

Table 8.12: Verification rates on test database with varying image size

Test	Threshold	Size	Background	Client %	Imposter %
Evaluation Protocol 1	0.03	114 x 91	Random	5	70
Evaluation Protocol 1	0.03		Plain Colour	5	70
Evaluation Protocol 1	0.03		Window	5	55
Evaluation Protocol 1	0.03	60 x 48	Random	5	70
Evaluation Protocol 1	0.03		Plain Colour	5	70
Evaluation Protocol 1	0.03		Window	5	55
Evaluation Protocol 1	0.03	30 x 24	Random	0	70
Evaluation Protocol 1	0.03		Plain Colour	0	70
Evaluation Protocol 1	0.03		Window	0	55

During the testing phase the face detection algorithm was unable to provide sufficient results useful for testing. The results show that 6 out of 10 subjects had four or more photos that were cropped such that useful facial information did not appear in the cropped image. For this reason the face detection was not used on the test database and hence results are not available.

Table 8.13: Verification rates on test database using light normalisation and varying image sizes

Test	Threshold	Size	Background	Client %	Imposter %
Evaluation Protocol 1	0.03	114 x 91	Random	5	75
Evaluation Protocol 1	0.03		Plain Colour	5	75
Evaluation Protocol 1	0.03		Window	5	55
Evaluation Protocol 1	0.03	60 x 48	Random	5	70
Evaluation Protocol 1	0.03		Plain Colour	5	75
Evaluation Protocol 1	0.03		Window	5	55
Evaluation Protocol 1	0.03	30 x 24	Random	5	75
Evaluation Protocol 1	0.03		Plain Colour	5	75
Evaluation Protocol 1	0.03		Window	5	55

8.4 Chapter Summary

Investigations into the accuracy of the eigenface algorithm on both the XM2VTS and test database were discussed. However, it was discovered that the results obtained for the test database were unreliable due to the small sample size used. Also it was noted that evaluation protocol 2 did not produce results consistent with those obtained for evaluation protocol 1 and therefore the results obtained were discarded.

The algorithm was able to accurately verify the client 65% of the time with an imposter error of 36% without the use of any pre-processing, at a threshold of 0.03. When histogram equalisation was used, the results for the algorithm were comparably worse than when no pre-processing was used. Face cropping on the other hand, provided significant improvements to the verification rates, due to only relevant data being used in the verification process. There were no significant changes in the verification rates when the images were at their original size compared to when they were resized to 30 x 24. The processing speed of the algorithm is significantly improved by reducing the size of the image and should therefore be included as a vital pre-processing technique.

In order to produce more accurate results, improvements need to be made to the pre-processing techniques and their implementation. Face cropping in particular is an area that showed promise; however greater accuracy needs to be achieved. Although the algorithm is far from perfect, the results show that it would be possible to use them in a remote verification system for exams.

Chapter 9

Face Verification challenges based on analysis of results

9.1 Introduction

There are many challenges that surround the use of facial recognition for a remote verification system. These include but are not limited to: computational needs, varying backgrounds, illumination, head positioning and fake detection.

9.2 Backgrounds

It can be safely assumed that most students will perform their examination at home in an office of sorts, rather than outside in a park; however even in a relatively sterile environment such as an office background, variation can vary dramatically. Colour variation in the walls, pictures or photos on the wall, windows or highly emitting light sources and constantly changing or moving

background can all cause significant problems to facial recognition software captured through a low resolution webcam.

There are several solutions to these problems, the simplest of which is student cooperation.

Since students do not desire to complicate the examination process, it is highly likely that they will be willing to cooperate with any guidelines required for successful system processing. These rules should include:

- Ensure the camera is facing a plain coloured wall
- Ensure that there are no windows directly behind the position you will be sitting in
- Ensure that the background will not have reoccurring movement i.e. people walking past, curtain moving in the breeze etc.

These are simple solutions that do not require an automatic and self-sufficient system but rather user cooperation. Regardless of how cooperative the majority of students may be, there will always be those who refuse to obey or are ignorant of the requirements of such a system. These students will be refused access to their examination.

Similarly, it can be noted that abstract backgrounds caused significant problems for the face detection algorithm. Hence, the background has been flagged as a challenge for the facial verification process.

9.3 Illumination

Illumination variance can have a dramatic impact on the effectiveness and accuracy of facial recognition algorithms. Although the system is used for the purpose of verification during examinations, it cannot be assumed that students will have good, sufficient or optimal lighting to perform facial recognition. Some students may prefer to work in dark environments while others may prefer natural or artificial lighting, white or yellow light. Under such varying conditions the facial recognition algorithms need to operate effectively. The variation in lighting

can cause partial or complete shadowing of the face causing significant problems in the ability of the facial recognition algorithms to gather meaningful information. Ultimately, the results conclude that if the image is captured under quality lighting conditions, then techniques such as histogram equalization may reduce the quality of the image, rather than increase it. The large variations in lighting during a remote examination need to be dealt with more effectively.

9.4 Pose

All of the images dealt with in this dissertation require the subject to have their head at 0^o for their face not to be occluded. However, during an examination it is possible students may place their hands on their head, cover their face with their hands, stick pencils or pens in their mouth, tilt their head sideways as well as many other variations. This could cause significant problems due to occlusion and head alignment. Occlusion was not specifically tested; however it was noted that images with shadowing of the face provided less accurate results. For this reason the complications relating to pose will need to be dealt with and tested.

9.5 Face location and alignment

It was shown in Section 8.2.4 that cropping the face improved the performance of the verification algorithm. However finding the location of the face is a problem which must be overcome as it is possible for the student's face to be anywhere in the frame. While the face detection program used in this dissertation worked well, there were limitations to its success. The face detection algorithm identified 6 out of 1000 images as having no face. It also cropped another 30 images where a face image was not present or was only partially captured. The success rate of this algorithm was 97%. While this may seem acceptable, it must be remembered that the images were all frontal face images. The algorithm was often unable to identify the face when testing images were not frontal. In an exam situation it is unlikely that the student will be in a full frontal position constantly and as such the face detection algorithm will need to be improved.

In addition to face detection, it is also necessary for faces to be aligned. In computer vision when comparing an image of a face that has a vertical orientation with that of a face image which has a horizontal orientation, it is expected that the results would not be accurate. This is due to the nature of obtaining the vectors used for comparison. Therefore to help improve the algorithm and to ensure that accuracy is maintained it is necessary to align faces. This process involves finding fiducial points on the face, such as the eyes, and ensuring that training, evaluation and test images are appropriately aligned.

9.6 Enrolment

All biometric methods regardless of type require some form of enrolment. While the enrolment of facial recognition is easier them some, it requires a training set of multiple photos. The eigenface algorithm that has been implemented effectively measures variation in facial features in different photos to provide an average facial image. At the beginning of the course it will be necessary for students to send in or upload photos that can be used for training. It must be ensured that the photos used for the training set are indeed a true representation of the claimed student. Currently, distance students are required to send in a photograph that has been signed by a Justice of the Peace before they can receive their student identification card. The images uploaded for biometric verification will need to be compared against this image manually. The set of student photos will then be trained, evaluated and thresholds set accordingly. This process is very time consuming and requires diligence and patience for the algorithm to process thousands of training images.

9.7 Chapter Summary

Many challenges for a remote verification system were identified throughout the testing phase. These included background, illumination, pose, face location, face alignment and enrolment. The background poses a problem primarily to the face cropping pre-processing as it interferes with the algorithms ability to correctly identify the face. This has an overflow effect to the eigenface algorithm as the images being compared are of half faces or not the subjects face at all. Similarly, the ability to locate the face in an image when subjects are in various poses reduces the accuracy of the eigenface algorithm. Further complications include cropping the face and rotating the face so that it aligns with the training images. Comparing images that are not aligned increases the chances for error. Enrolment and training of images must be achieved prior to running the face verification algorithm. If subjects fail to enrol, there is no threshold against which to compare the input image and verification will fail. Each of these challenges needs to be addressed before a working solution can be implemented.

Chapter 10

Conclusion

10.1 Achievement of Project Objectives

An **Analysis of current USQ examination procedures** was performed to determine the various types of security methods used for the end of semester exams provided for external students. USQ provides four (4) types of examinations. They are online, formal, practical and clinical in three (3) different modes closed, restricted and open. Each of these modes has specific requirements that must be followed in order for exam integrity to be maintained. All of the requirements for a remote examination system have been considered and documented for further analysis in the future.

In order for an automated remote examination system to be operational all of the requirements must be fulfilled. In particular, it was discovered that identity verification is the foundation requirement and is of greatest importance. It was discovered that both knowledge and possession verification techniques do not provide the necessary security. Therefore biometric verification was considered as

the most logical means for identity verification due to its greater level of security resulting from the inherent nature of the biological ‘key’.

Research into **suitable biometric verification options** was conducted to determine if a suitable method was available that would meet the requirements of a remote examination system. Passive and active methods were considered in the analysis documenting both pros and cons for every method. Although each requirement for the remote examination system was not considered equally, each was considered vital for correct operation and therefore only biometric techniques which fulfilled all criteria were considered further. From the techniques discussed, only facial biometrics fulfilled each criterion and it was selected for further analysis.

Research into **current algorithms** for facial verification was performed to gain an understanding of what methods have been implemented and if they were plausible for a remote verification system. Most of the current algorithms used in automated systems use a form of pattern recognition based on linear or multi-linear algebra. Each technique described was not unique but had built on the foundation of its predecessors, correcting its flaws. Each iteration became increasingly difficult to understand in its mathematical interpretation and computational complexity. Although multi-linear algebraic techniques were considered to be of greatest use in a remote verification system, the algorithm implemented was a linear algebraic technique known as Principal Component Analysis.

The Eigenface algorithm was successfully **implemented in MATLAB** and **tested on both the XM2VTS and test database**. This algorithm was implemented and tested according to the protocols provided by the University of Surrey for the XM2VTS database. The implemented algorithm was successful at both verifying a client and verifying an imposter the majority of the time. The test database did not prove to be useful in terms of the results returned from the algorithm, however a valuable lesson was learnt, that being, the images need to be captured under almost ideal conditions for the Eigenfaces algorithm to work. To verify these results, further tests on a larger database should be conducted.

The **implementation of pre-processing techniques** was used to determine if the Eigenface algorithm could perform with less error without modifying the image matching procedure but only altering the captured image. While some methods hindered the verification process, such as histogram equalisation, other processes, such as face cropping, decreased the verification errors. It was also discovered that reducing the size of image did not significantly affect the verification rates. However, processing time was significantly reduced.

Each of the achievements set out in the Project Specifications (refer to Appendix A) were achieved throughout the course of preparing this dissertation. The learning acquired in conducting research and implementing a design was invaluable. This included overcoming the limitations in initial design and assumptions, overcoming incompetency in understanding and grasping the complexities both from an engineering and ethical perspective for a project such as this..

10.2 Project Limitations

The major physical limitation to the project was the lack of subjects available for the test database and the ability to capture the images using a webcam. Ideally a sample of at least one hundred students would be needed for half an hour each in order to gather the test images and evaluation images under strict conditions as well as numerous test images under the same environmental conditions.

The time restrictions limited the project from evaluating algorithms further. In particular, the project was limited to evaluating one face verification technique due to the complexity of programming such algorithms in the short time frame available. Also the face detection program was treated as a black box and as such debugging was difficult, causing problems particularly in the test database.

10.3 Future Work

There are three areas of future work which would be beneficial for the verification process: creating a large test database, improving the face detection algorithm and implementing other face verification techniques using the required equipment.

In order to improve the testing for this project, a well-defined student test database must be established. This database should be sufficiently large enough to capture variations in skin colour, age, gender and apparel. It should include four images used for training, two images used for evaluation, and multiple images taken under varying circumstances for the test images. A new set of test images needs to be gathered every six months in order to determine the effects of time on accuracy of the algorithm. This will mimic the remote verification system, since the training and evaluation images will remain the same throughout a student's degree with only the test images changing.

The face detection algorithm could be taken as a final year dissertation and include head tracking through the use of a webcam. Face detection was shown to increase the verification rate of the facial verification algorithm and increasing its reliability would prove beneficial. The detection could also include the capability to locate fiducial points such as the eyes, nose and mouth, therefore allowing alignment of the images.

There are other facial verification techniques that have been discussed which may be superior to the eigenfaces algorithm. These techniques should be considered and tested before the eigenfaces algorithm is implemented in a remote verification system. In particular, the multi-linear algebraic techniques should be given high priority as they take more variations into account rather than simplifying the image.

Due to the large amounts of data that need to be processed, it would be prudent to program the algorithm using a fast programming language, such as C. This would decrease the processing time, thus allowing more testing to take place.

The remote examination system requires more elements than simple verification as discussed in Chapter 2. Each of these elements will need to be analysed and a solution found before a remote verification system can be operational.

10.4 Final Remarks

Although a fully functioning remote verification system was not achieved, this project has shown that it is possible to successfully implement biometrics as a secure way of ensuring the integrity of exams in a remote system.. Verification of student identity is only the first step in a long list of items to be satisfied before it is possible to allow all students in all courses to complete their exams at a remote location.. It is, however, feasible that in the near future facial verification could be used in courses where online assignment and exams already exist as an added security means.

References

Abdel-Ghaffar, EA, Allam, ME, Mansour, HAK & Abo-Alsoud, MA 2008, 'A secure face recognition system', paper presented to Computer Engineering & Systems, 2008. ICCES 2008. International Conference on, 25-27 Nov. 2008.

Amayeh, G, Bebis, G, Erol, A & Nicolescu, M 2007, 'A Component-Based Approach to Hand Verification', paper presented to Computer Vision and Pattern Recognition, 2007. CVPR '07. IEEE Conference on, 17-22 June 2007.

Anil K, J, Rudd, B & Pankanti, S 1999, 'Biometrics: Personal Identificaiton in Networked Society', *The Springer International Series in Engineering and Computer Science*, p. 411,

Arivazhagan, S, Flora, TGA & Ganesan, L 2007, 'Fingerprint Verification Using Gabor Co-occurrence Features', paper presented to Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on, 13-15 Dec. 2007.

Bartlett, MS, Lades, HM & Sejnowski, TJ 1998, 'Independent component representations for face recognition'.

Bartlett, MS, Movellan, JR & Sejnowski, TJ 2002, 'Face recognition by independent component analysis', *Neural Networks, IEEE Transactions on*, vol. 13, no. 6, pp. 1450-64,

Bazin, AI & Nixon, MS 2005, 'Gait Verificaiton using Probabilistic Methods',

Belhumeur, PN, Hespanha, JP & Kriegman, DJ 1997, 'Eigenfaces vs. fisherfaces: Recognition using class specific linear projection', *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 19, no. 7, pp. 711-20,

Bell, AJ & Sejnowski, TJ 1995, 'An information-maximization approach to blind separation and blind deconvolution', *Neural computation*, vol. 7, no. 6, pp. 1129-59,

Blanz, V & Vetter, T 1999, 'A morphable model for the synthesis of 3D faces'.

Blanz, V & Vetter, T 2003, 'Face recognition based on fitting a 3D morphable model', *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 25, no. 9, pp. 1063-74,

Bronstein, A, Bronstein, M & Kimmel, R 2003, 'Expression-invariant 3D face recognition'.

Bronstein, AM, Bronstein, MM & Kimmel, R 2005, 'Three-dimensional face recognition', *International Journal of Computer Vision*, vol. 64, no. 1, pp. 5-30,

Bronstein, AM, Bronstein, MM, Gordon, E & Kimmel, R 2004, 'Fusion of 2d and 3d data in three-dimensional face recognition'.

Burge, M & Burger, W 2000, 'Ear biometrics in computer vision', paper presented to Pattern Recognition, 2000. Proceedings. 15th International Conference on, 2000.

Cavalcanti, GDC & Filho, ECBC 2003, 'Eigenbands fusion for frontal face recognition', paper presented to Image Processing, 2003. ICIP 2003. Proceedings. 2003 International Conference on, 14-17 Sept. 2003.

Changbo, H, Harguess, J & Aggarwal, JK 2009, 'Patch-based face recognition from video', paper presented to Image Processing (ICIP), 2009 16th IEEE International Conference on, 7-10 Nov. 2009.

Cichocki, A, Unbehauen, R & Rummert, E 1994, 'Robust learning algorithm for blind separation of signals', *Electronics Letters*, vol. 30, no. 17, pp. 1386-7,

Comon, P 1994, 'Independent component analysis, a new concept?', *Signal processing*, vol. 36, no. 3, pp. 287-314,

Daugman, JG 1980, 'Two-dimensional spectral analysis of cortical receptive field profiles', *Vision research*, vol. 20, no. 10, pp. 847-56,

Daugman, JG 1988, 'Complete discrete 2-D Gabor transforms by neural networks for image analysis and compression', *Acoustics, Speech and Signal Processing, IEEE Transactions on*, vol. 36, no. 7, pp. 1169-79,

Fisher, RA 1936, 'The use of multiple measurements in taxonomic problems', *Annals of Human Genetics*, vol. 7, no. 2, pp. 179-88,

Gabor, D 1946, 'Theory of communication. Part 1: The analysis of information', *Electrical Engineers - Part III: Radio and Communication Engineering, Journal of the Institution of*, vol. 93, no. 26, pp. 429-41,

Giroux, S, Wachowiak-Smolikova, R & Wachowiak, MP 2009, 'Keypress interval timing ratios as behavioral biometrics for authentication in computer security', paper presented to Networked Digital Technologies, 2009. NDT '09. First International Conference on, 28-31 July 2009.

Goffredo, M, Bouchrika, I, Carter, JN & Nixon, MS 2010, 'Self-Calibrating View-Invariant Gait Biometrics', *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 40, no. 4, pp. 997-1008,

Gordon, GG 1995, 'Face recognition from frontal and profile views'.

Guodong, G, Guowang, M & Ricanek, K 2010, 'Cross-Age Face Recognition on a Very Large Database: The Performance versus Age Intervals and Improvement Using Soft Biometric Traits', paper presented to Pattern Recognition (ICPR), 2010 20th International Conference on, 23-26 Aug. 2010.

Harguess, J & Aggarwal, JK 2009, 'A case for the average-half-face in 2D and 3D for face recognition', paper presented to Computer Vision and Pattern Recognition Workshops, 2009. CVPR Workshops 2009. IEEE Computer Society Conference on, 20-25 June 2009.

Harguess, J, Changbo, H & Aggarwal, JK 2009, 'Fusing face recognition from multiple cameras', paper presented to Applications of Computer Vision (WACV), 2009 Workshop on, 7-8 Dec. 2009.

Hosseyninia, SM, Roosta, F, Baboli, AAS & Rad, GR 2011, 'Improving the performance of MPCA+MDA for face recognition', paper presented to Electrical Engineering (ICEE), 2011 19th Iranian Conference on, 17-19 May 2011.

Huang, J, Heisele, B & Blanz, V 2003, 'Component-based face recognition with 3D morphable models'.

Hubel, DH & Wiesel, TN 1977, 'Ferrier lecture: Functional architecture of macaque monkey visual cortex', *Proceedings of the Royal Society of London. Series B, Biological Sciences*, vol. 198, no. 1130, pp. 1-59,

Jain, A & Lin, H 1996, 'On-line fingerprint verification', paper presented to Pattern Recognition, 1996., Proceedings of the 13th International Conference on, 25-29 Aug 1996.

Jiann-Der, L, Chen-Hui, K & Chen-Min, H 2004, '3D face recognition system based on feature analysis and support vector machine', paper presented to TENCON 2004. 2004 IEEE Region 10 Conference, 21-24 Nov. 2004.

Jutten, C & Herault, J 1991, 'Blind separation of sources, part I: An adaptive algorithm based on neuromimetic architecture', *Signal processing*, vol. 24, no. 1, pp. 1-10,

Juwei, L, Plataniotis, KN & Venetsanopoulos, AN 2003, 'Face recognition using LDA-based algorithms', *Neural Networks, IEEE Transactions on*, vol. 14, no. 1, pp. 195-200,

Klevans, RL 1997, *Voice recognition*, Artech House, Boston.

Lee, J, Moghaddam, B, Pfister, H & Machiraju, R 2004, 'Finding optimal views for 3D face shape modeling',

Leggett, J, Williams, G, Usnick, M & Longnecker, M 1991, 'Dynamic identity verification via keystroke characteristics', *International Journal of Man-Machine Studies*, vol. 35, no. 6, pp. 859-70,

Lin, Z & Lu, B 2010, 'Iris Recognition Method Based on the Coefficients of Morlet Wavelet Transform', paper presented to Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on, 11-12 May 2010.

Liu, C & Wechsler, H 1999, 'Comparative assessment of independent component analysis (ICA) for face recognition'.

Lu, H, Plataniotis, KN & Venetsanopoulos, AN 2008, 'MPCA: Multilinear principal component analysis of tensor objects', *Neural Networks, IEEE Transactions on*, vol. 19, no. 1, pp. 18-39,

Lucey, P 2003, 'Algorithms for Face Recognition',

Marcelja, S 1980, 'Mathematical description of the responses of simple cortical cells*', *JOSA*, vol. 70, no. 11, pp. 1297-300,

Messer, K, Matas, J, Kittler, J, Luettin, J & Maitre, G 1999, 'XM2VTSDB: The extended M2VTS database'.

Moon, H & Phillips, PJ 2001, 'Computational and performance aspects of PCA-based face-recognition algorithms', *PERCEPTION-LONDON-*, vol. 30, no. 3, pp. 303-22,

Moses, Y, Adini, Y & Ullman, S 1994, 'Face recognition: The problem of compensating for changes in illumination direction', *Computer Vision—ECCV'94*, pp. 286-96,

Nefian, AV & Hayes, MH, III 1998, 'Hidden Markov models for face recognition', paper presented to Acoustics, Speech and Signal Processing, 1998. Proceedings of the 1998 IEEE International Conference on, 12-15 May 1998.

Othman, H & Aboulnasr, T 2000, 'Low complexity 2-D Hidden Markov Model for face recognition', paper presented to Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on, 2000.

Parashar, S, Vardhan, A, Patvardhan, C & Kalra, PK 2008, 'Design and Implementation of a Robust Palm Biometrics Recognition and Verification System', paper presented to Computer Vision, Graphics & Image Processing, 2008. ICVGIP '08. Sixth Indian Conference on, 16-19 Dec. 2008.

Peacock, A, Xian, K & Wilkerson, M 2004, 'Typing patterns: a key to user identification', *Security & Privacy, IEEE*, vol. 2, no. 5, pp. 40-7,

Qian, C, Haiyuan, W & Yachida, M 1995, 'Face detection by fuzzy pattern matching', paper presented to Computer Vision, 1995. Proceedings., Fifth International Conference on, 20-23 Jun 1995.

Ramesha, K, Srikanth, N, Raja, KB, Venugopal, KR & Patnaik, LM 2009, 'Advanced Biometric Identification on Face, Gender and Age Recognition', paper presented to Advances in Recent Technologies in

Communication and Computing, 2009. ARTCom '09. International Conference on, 27-28 Oct. 2009.

Ramli, DA, Samad, SA & Hussain, A 2007, 'Preprocessing Techniques for Voice-Print Analysis for Speaker Recognition', paper presented to Research and Development, 2007. SCOReD 2007. 5th Student Conference on, 12-11 Dec. 2007.

Rana, S, Wanquan, L, Lazarescu, M & Venkatesh, S 2008, 'Recognising faces in unseen modes: A tensor based approach', paper presented to Computer Vision and Pattern Recognition, 2008. CVPR 2008. IEEE Conference on, 23-28 June 2008.

Rejman-Greene, M 2002, 'Secure authentication using biometric methods', *Information Security Technical Report*, vol. 7, no. 3, pp. 30-40,

Said, HES, Baker, KD & Tan, TN 1998, 'Personal identification based on handwriting', paper presented to Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on, 16-20 Aug 1998.

Samaria, F 1994, 'Face recognition using hidden Markov models', PhD thesis, University of Cambridge.

Sanjekar, PS & Dhabe, PS 2010, 'Fingerprint verification using haar wavelet', paper presented to Computer Engineering and Technology (ICCET), 2010 2nd International Conference on, 16-18 April 2010.

Singh, AK, Agrawal, AK & Pal, CB 2009, 'Hand geometry verification system: A review', paper presented to Ultra Modern Telecommunications & Workshops, 2009. ICUMT '09. International Conference on, 12-14 Oct. 2009.

Turk, MA & Pentland, AP 1991, 'Face recognition using eigenfaces', paper presented to Computer Vision and Pattern Recognition, 1991. Proceedings CVPR '91., IEEE Computer Society Conference on, 3-6 Jun 1991.

The University Of Southern Queensland 2011, Distance online studies, viewed 15 April 2011, <http://www.usq.edu.au/future-students/why-usq/distance-online-study>

The University Of Southern Queensland 2011, Residential School, viewed 15 April 2011, <http://www.usq.edu.au/currentstudents/reschool/>

The University Of Southern Queensland 2011, Exams, viewed 15 April 2011, <http://www.usq.edu.au/currentstudents/exams>

The University of Southern Queensland 2011, USQ Strategy, viewed 15 April 2011, <http://www.usq.edu.au/aboutusq/strategy>

The University of Southern Queensland 2011, Assessments, viewed 15 April 2011, < http://policy.usq.edu.au/portal/custom/detail/assessment>

The University of Southern Queensland 2011, Examination Procesdures, viewed 15 April 2011, < http://policy.usq.edu.au/portal/custom/detail/examination-procedures>

Vasilescu, M & Terzopoulos, D 2002a, 'Multilinear analysis of image ensembles: Tensorfaces', *Computer Vision—ECCV 2002*, pp. 447-60,

Vasilescu, MAO & Terzopoulos, D 2002b, 'Multilinear image analysis for facial recognition', paper presented to Pattern Recognition, 2002. Proceedings. 16th International Conference on, 2002.

Vasilescu, MAO & Terzopoulos, D 2007, 'A Tensor Algebraic Approach to Image Synthesis, Analysis and Recognition', paper presented to 3-D Digital Imaging and Modeling, 2007. 3DIM '07. Sixth International Conference on, 21-23 Aug. 2007.

Vielhauer, C 2006, *Biometric user authentication for IT security : from fundamentals to handwriting*, Springer, New York.

Weaver, AC 2006, 'Biometric Authentication', *How Things Work*,

Wiskott, L, Fellous, JM, Kuiger, N & von der Malsburg, C 1997, 'Face recognition by elastic bunch graph matching', *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 19, no. 7, pp. 775-9,

Wooju, R & Daijin, K 2007, 'Real-time 3D Head Tracking and Head Gesture Recognition', paper presented to Robot and Human interactive Communication, 2007. RO-MAN 2007. The 16th IEEE International Symposium on, 26-29 Aug. 2007.

Yan, P & Bowyer, KW n.d, 'Ear biometrics using 2D and 3D images'.

Yong, Z, Tieniu, T & Yunhong, W 2000, 'Biometric personal identification based on handwriting', paper presented to Pattern Recognition, 2000. Proceedings. 15th International Conference on, 2000.

Yu, C, Jin, W, Changan, H, Lu, W & Adjouadi, M 2008, 'A robust segmentation approach to iris recognition based on video', paper presented to Applied Imagery Pattern Recognition Workshop, 2008. AIPR '08. 37th IEEE, 15-17 Oct. 2008.

Yuan, L & Mu, Z 2007, 'Ear recognition based on 2D images'.

Zhao, W, Chellappa, R, Phillips, PJ & Rosenfeld, A 2003, 'Face recognition: A literature survey', *Acm Computing Surveys (CSUR)*, vol. 35, no. 4, pp. 399-458,

Appendix A

Project Specification

ENG 4111/2 Research Project

Project Specifications

FOR :	Joshua Hockey
TOPIC:	Biometric Analysis for Remote Examination Purposes.
SUPERVISOR:	John Leis
SPONSORSHIP:	Faculty of Engineering & Surveying
ISSUE:	*Issue B – 30 July 2011*
PROJECT AIM:	This project seeks to investigate an appropriate means of remotely and non-invasively identifying students undertaking external studies to confirm correct user status for on-line examination assessment.

SPECIFICATION:

1. Research background information on biometric analysis options.
2. Analyse current USQ examination requirements and provide system specifications that would need to be implemented for a remote examination system.
3. Research current algorithms for a chosen biometric system and determine their suitability within the context of a remote identification system.
4. Implement a biometric analysis algorithms using MATLAB
5. Evaluate the raw algorithm on both the XM2VTS database and a test database including biometric information of a subject gathered under various conditions, similar to those expected during a remote examination.
6. Determine to what extent the use of appropriate pre-processing techniques can improve the effectiveness of the algorithm evaluated in 5.

As time and resources permits:

7. Design a user-interface for the biometric system that can be run in the background
8. Design and Implement the proximity monitoring system

Agreed:

_____(Student) _____(Supervisor)

___/____/_____ _____/____/_____

Appendix B

Eigenface MATLAB Script

B.1 E_test_eval_1.m

```
%
% This program performs PCA as a method for face recognition.
% The code presented here is a modified version of that provided
% by Santiago Serrano

% This program uses images 1, 3 & 5 as training images and 2, 4 &
% 6 as evaluation images. Images 7 & 8 are used as test images.
% The program will automatically process the entire set and save
% the results to a result file. The only imformation that needs
% to be changed is the
%  total number of images (num_images) and the threshold
(threshold).
%
%
```

```
clear all
close all
clc

%% global variables
dist_vect = zeros(2,2); %This matrix stores the Euclidean
distances at the end of program. it will always be 2 x 2 due the
amount of images

result = zeros(1,2);

next_subject = 0; %initiates a variable that increases the start
num to get number of next subject
PHOTOS_PER_SET = 8; %number of photos for each person

num_images = 1000;

num_subjects = num_images/PHOTOS_PER_SET; %Enter the number of
subjects that you wish to test

thresh_hold = 0.01;
% Set the number of images that will be used in the training set.
%This value is used to loop through the images


%% Start looping

for image_counter = 1:num_subjects %change the second number to
the amount of subjects in test

Start_num = 1+next_subject; %this number is changed to the
starting number
N_image = Start_num+3;   %Add three to start number
```

```
%Set the standard deviation and the mean for use in the
algorithm.
%These values are not critical as long as they are close to that
of the
%images.

init_std = 80;  % Initial standard deviation
init_m = 100; %initial means


%Set a matrix that will be used to store the images, in order to
process
%them.

Gamma = []; %Image matrix

%figure(1);

for i =Start_num:N_image

    im_name = i;  %input('Please enter the name of the image and
its extension \n','s');
    im_name = strcat(int2str(im_name),'.jpg');
    img = imread(strcat('J:\USQ\University 2011 Sem1\ENG4111 -
Project\MATLAB CODE\my_face rec codes\Test Files
1\HIST\',im_name));




    %if the figures need to be shown this line can be added to
show them on
    % a subplot.
    %%
%     figure(1)
%         subplot(2,2,i-Start_num+1)
%         colormap(gray(256));
%         image(img);
%         set (gca,'DataAspectratio', [1 1 1]);
%         box('on');
%         axis('off');
%           if i==3 %only adds a title once the training set is
equal to three images
%             title('Training set','fontsize',18);
%           end
%             drawnow;


    [irow icol]=size(img);    % get the number of rows (N1) and
columns (N2)
    temp=reshape(img',irow*icol,1);     %creates a (N1*N2)x1
matrix
    Gamma=[Gamma temp];         %X is a N1*N2xM matrix after
finishing rehaping
                                 %this is our Gamma
end
```

```
%Use histogram equilization to normalize for lighting error

%Here we change the mean and std of all images. We normalize all
images.
%This is done to reduce the error due to lighting conditions.

%figure(2)
for i=1:size(Gamma,2)

    %temp=(Gamma(:,i));
    %normalized = histeq(temp); %Preprocessing for light
normalization of each image stored in Gamma
    %Gamma(:,i) = normalized;

    %Plot normalised images
    %%
%     subplot(ceil(sqrt(N_image)),ceil(sqrt(N_image)),i)
%         set (gca,'DataAspectratio', [1 1 1]);
%         box('on');
%         axis('off');
%         colormap(gray(256));
%         img=reshape(Gamma(:,i),icol,irow);
%         img=img';
%         image(img);
%         drawnow;
%          if i==3
%         title('Normalized Training Set','fontsize',18)
%         end
end

%compute the eigenvectiors as proposed by Turk and Pentland 1991
%Calculate the mean image


m=mean(Gamma, 2);   %calculates the mean of each row; note that
the columns can be used also. Use (Gamma,1)

m1=uint8(m); %uint8 will store the information in less memory.
Values still range from 0 to 255

img=reshape(m1,icol,irow);   %creates a matrix that is N2xN1
rather and N1xN2x1
img=img'; %use the transpose of the matrix to show the mean
image.

%print the mean image to screen
%%
% figure(3);
% imshow(img);
% title('Mean Image','fontsize',18)


% The image is changed so that it can be manipulated
new_image=[];   % A matrix
for i=1:(N_image-Start_num)
    temp=double(Gamma(:,i));
    new_image=[new_image temp];
end
```

```
%Covariance matrix C=A'A, L=AA'
A=new_image';
Covariance=A*A';
% vector stores the eigenvectors for the covariance matrix
% value stores the eigenvalue for
Covariance=new_image*new_image';
[vector value]=eig(Covariance);

%Where eigenvalues are equal to zero, they are sorted and
discarded

vec=[];
val=[];
for i=1:size(vector,2)
    if(value(i,i)>1e-4)
        vec=[vec vector(:,i)];
        val=[val value(i,i)];
    end
 end


 %sort the eigenvectors & eigenvalues so that they are in
ascending order

 [B index]=sort(val);
 ind=zeros(size(index));
 val_temp=zeros(size(index)); %Create temporary storage in order
to manipulate the eigenvectors and eigenvalues
 vec_temp=zeros(size(vec));
 len=length(index);

 for i=1:len
    val_temp(i)=B(len+1-i);
    ind(i)=len+1-index(i);
    vec_temp(:,ind(i))=vec(:,i);
 end
 val=val_temp; %replace eigenvector and eigenvale vectors with
temporary ones
 vec=vec_temp;


%Normalise each of the eigenvectors
 for i=1:size(vec,2)       %access each column
   norm_vec=vec(:,i);
   temp=sqrt(sum(norm_vec.^2));
   vec(:,i)=vec(:,i)./temp;
end

%Eigenvectors of the Covariance matrix
eigen_vector=[];
for i=1:size(vec,2)
    temp=sqrt(val(i));
    eigen_vector=[eigen_vector (new_image*vec(:,i))./temp];
end

%Normalization of eigenvectors
for i=1:size(eigen_vector,2)
   norm_vec=eigen_vector(:,i);
   temp=sqrt(sum(norm_vec.^2));
```

```
    eigen_vector(:,i)=eigen_vector(:,i)./temp;
end

% show the eigenfaces;
%figure(4);
for i=1:size(eigen_vector,2)
    %%
%     img=reshape(eigen_vector(:,i),icol,irow);
%     img=img';
%     img=histeq(img,255);
%     subplot(ceil(sqrt(N_image)),ceil(sqrt(N_image)),i)
%     imshow(img)
%     drawnow;
%     if i==3
%         title('Eigenfaces','fontsize',18)
%     end
end

%Since  OMEGA'=[omega_1,omega_2,.  .  .,omega_M' ]  will be the
vector containing the
%the weight of each face in the training set.
%This is found by doing a point by point multiplication

OMEGA = [];
for M=1:size(new_image,2)
    omega=[];
    for i=1:size(eigen_vector,2)
          t=eigen_vector(:,i)';
        Image_weight = dot(t,new_image(:,M)'); %Note: dot
produces the dot product of two vectors
        omega = [omega; Image_weight];
    end
    OMEGA = [OMEGA omega];
end



%%

for loop=0:(N_image-Start_num)


%This program is used in conjunction with the
my_eigenface_revamped.m
%Using the template produced in my_eigenface_revamped.m a image
is
%transformed and compared to verify the identity.

%This image should be preprocessed using the preprocessing script
provided.
%

% Acquire new image

In_name = Start_num+loop+4;  %input('Please enter the name of the
image and its extension \n','s');
In_name = strcat(int2str(In_name),'.jpg');
In_img = imread(strcat('J:\USQ\University 2011 Sem1\ENG4111 -
Project\MATLAB CODE\my_face rec codes\Test Files
```

```
1\HIST\',In_name)); %This line needs to be changed depending on
where the image is stored
%%

if (loop < 2)
% figure (5)
% subplot(2,1,loop+1)
% imshow(In_img);
% title('Eval image','fontsize',18)

end


Image=reshape(double(In_img)',irow*icol,1);
temp=Image;
input_mean=mean(temp);
input_std=std(temp);
temp=(temp-input_mean)*init_std/input_std+init_m;
NormImage = temp;
Difference = temp-m;

p = [];
aa=size(eigen_vector,2);
for i = 1:aa
    pare = dot(NormImage,eigen_vector(:,i));
    p = [p; pare];
end

ReshapedImage = m + eigen_vector(:,1:aa)*p;    %m is the mean
image, eigen_vector is the eigenvector
ReshapedImage = reshape(ReshapedImage,icol,irow);
ReshapedImage = ReshapedImage';

%show the reconstructed image.
%%
% subplot(1,2,2)
% imagesc(ReshapedImage); colormap('gray');
% title('Reconstructed image','fontsize',18)

Weight_in_img = [];
for i=1:size(eigen_vector,2)

    In_img_weight = dot(eigen_vector(:,i)',Difference');
    Weight_in_img = [Weight_in_img; In_img_weight];
end

%%
% ll = 1:(N_image-Start_num);
% figure(68)
% subplot(1,2,1)
% stem(ll,Weight_in_img)
% title('Weight of Input Face','fontsize',14)

% Find Euclidean distance
euclidean=[];
for i=1:size(OMEGA,2)

    Final_Weight = Weight_in_img-OMEGA(:,i); %Is the weight
difference between the input and the eignenfaces
```

```
    magnitude = norm(Final_Weight);         %Finds the largest
singular value of Final_weight
    euclidean = [euclidean magnitude];
end

%%
% check = 1:size(euclidean,2);
% subplot(1,2,2)
% stem(check,euclidean)
% title('Eucledean distance of input image','fontsize',14)

%The classification as a face as being verified depends on both
the max and
%min Euclidean distances.

%fprintf (1, 'The new value for the distances are');


MaximumValue=max(euclidean);
MinimumValue=min(euclidean);

%%
%Store the distances for the evaluation images in a vector. Use
these values to determine the
%threshold for the images.

dist_vect (1,loop+1) = MaximumValue;
dist_vect (2,loop+1) = MinimumValue;

%finds the maximum and minimum values in the evaluation set to
determine
%the thresholds

max_high = max(dist_vect(1,:))+thresh_hold*max(dist_vect(1,:));
%try a threshold of 20%
max_low = min (dist_vect(1,:))- thresh_hold*min (dist_vect(1,:));

min_high = max(dist_vect(2,:))+thresh_hold*max(dist_vect(2,:));
min_low = min (dist_vect(2,:))-thresh_hold*min (dist_vect(2,:));



end

in_count =1;
test = 1;
while(test <=num_images) %the amount of images to be tested.
    % Acquire new image

In_name = test;  %input('Please enter the name of the image and
its extension \n','s');
In_name = strcat(int2str(In_name),'.jpg');
In_img = imread(strcat('J:\USQ\University 2011 Sem1\ENG4111 -
Project\MATLAB CODE\my_face rec codes\Test Files
1\HIST\',In_name)); %This line needs to be changed depending on
where the image is stored
%%
```

```
% Show pictures being compared
% figure (6)
% imshow(In_img);
% title('Test image','fontsize',18)



Image=reshape(double(In_img)',irow*icol,1);
temp=Image;
input_mean=mean(temp);
input_std=std(temp);
temp=(temp-input_mean)*init_std/input_std+init_m;
NormImage = temp;
Difference = temp-m;

p = [];
aa=size(eigen_vector,2);
for i = 1:aa
    pare = dot(NormImage,eigen_vector(:,i));
    p = [p; pare];
end

ReshapedImage = m + eigen_vector(:,1:aa)*p;    %m is the mean
image, eigen_vector is the eigenvector
ReshapedImage = reshape(ReshapedImage,icol,irow);
ReshapedImage = ReshapedImage';

%show the reconstructed image.
%%
% subplot(1,2,2)
% imagesc(ReshapedImage); colormap('gray');
% title('Reconstructed image','fontsize',18)

Weight_in_img = [];
for i=1:size(eigen_vector,2)

    In_img_weight = dot(eigen_vector(:,i)',Difference');
    Weight_in_img = [Weight_in_img; In_img_weight];
end

%%
% ll = 1:(N_image-Start_num);
% figure(68)
% subplot(1,2,1)
% stem(ll,Weight_in_img)
% title('Weight of Input Face','fontsize',14)

% Find Euclidean distance
euclidean=[];
for i=1:size(OMEGA,2)

    Final_Weight = Weight_in_img-OMEGA(:,i); %Is the weight
difference between the input and the eignenfaces
    magnitude = norm(Final_Weight);         %Finds the largest
singular value of Final_weight
    euclidean = [euclidean magnitude];
end

%%
```

```
% check = 1:size(euclidean,2);
% subplot(1,2,2)
% stem(check,euclidean)
% title('Eucledean distance of input image','fontsize',14)

%The classification as a face as being verified depends on both
the max and
%min Euclidean distances.

%fprintf (1, 'The new value for the distances are');


MaximumValue=max(euclidean);
MinimumValue=min(euclidean);

     if (MaximumValue >= max_low && MaximumValue <= max_high &&
MinimumValue >=  min_low && MinimumValue <= min_high)

           result (in_count, image_counter) = 1;

        else
            result (in_count, image_counter) = -1;

     end

     test = test + 4; %the 4 can be change to use more photos of
each set for the test. 4 will test 2 photos of each person.
     in_count = in_count +1;
end
next_subject = next_subject+PHOTOS_PER_SET;

%fprintf (1, 'first interation')
%pause(5);

end

savefile = 'results_eval_1_imposter_HIST_0.01.mat';

save(savefile, 'result')
```

Appendix C

Pre- Processing Scripts

C.1 greyscale.m

```
%
%
% This program loads an image file and converts and images that
% are colour into a greyscale image. It will then save the file
% to a folder named greyscale
% The image processing toolbox is required to run this script
%
%
```

```
clc
clear all
close all

Start_num = 1; % Enter the number of the first image to process
N_image = 246; %Enter the last number of image to process


for i =Start_num:N_image

    im_name = i;  %input('Please enter the name of the image and
its extension \n','s');
    im_name = strcat(int2str(im_name),'.jpg');
    img = imread(strcat('J:\USQ\University 2011 Sem1\ENG4111 -
Project\Test Data\Test Resize1\',im_name));


    imageInfo=imfinfo(im_name); %returns information about the
graphics file


    %if(getfield(imageInfo,'ColorType')=='truecolor')

        img = rgb2gray(img); % Read an image using imread
function, convert from RGB color space to
                             % grayscale using rgb2gray function
and assign it to variable inputImage

   % end

    out_name = strcat(int2str(i),'.jpg');
    imwrite(img,strcat('J:\USQ\University 2011 Sem1\ENG4111 -
Project\Test Data\Test Resize1\Resize1 Grey\',out_name));
end
```

C.2 Face_crop.m

```
%
%
% This program loads an image file and performs face detection to
% crop only
% the portion of the face which has information appropriate for
% face recognition. The program requires that the greyscale.m
% script be run first. It also requires that the fdmex and fdlib
% are in the same folder as the script, as this is required for
% correct opperation.
% Newer versions of MATLAB may not be able to process these
% libraries.
%
%


clc
clear all
close all

Start_num = 49; % Enter the number of the first image to process
N_image = 72; %Enter the last number of image to process


for i =Start_num:N_image

    im_name = i;  %input('Please enter the name of the image and
its extension \n','s');
    im_name = strcat(int2str(im_name),'.jpg');
    img = imread(strcat('J:\USQ\University 2011 Sem1\ENG4111 -
Project\MATLAB CODE\my_face rec codes\Test Files 2\light
hist\',im_name));

blah = size(img);
% decision threshold.
% change this to a smaller value, if too many false detections
occur.
% change it to a larger value, if faces are not recognized.
% a reasonable range is -10 ... 10.
threshold = 5;

%img = rgb2gray(img);

imagesc(img); hold on; colormap gray;
s = fdmex(img', threshold);

column_v = s(:,3);

column_v = column_v';

%finds the maximum value of s
```

```
[maxVal maxInd] = max(column_v);

maxInd = maxInd(1,1);

if (maxInd >=1)

    h = rectangle('Position',[s(maxInd,1)-
s(maxInd,3)/2,s(maxInd,2)-s(maxInd,3)/2,s(maxInd,3),s(maxInd,3)],
...
      'EdgeColor', [1,0,0], 'linewidth', 2);
end



  h = rectangle('Position',[s(maxInd,1),s(maxInd,2),2,2], ...
      'EdgeColor', [0,1,1], 'linewidth', 2);

 % take the centre mark and get a rectangle that is on the right
width & height.

 x_axis = s(maxInd,1);
 y_axis = s(maxInd,2);

 %Set the values for the height and width of the box to be
cropped.
 width = 100;        %s(maxInd,3)/2
 height= 120;        %s(maxInd,3)/2


 face_cr = img(y_axis-height:y_axis+height, x_axis-
width:x_axis+width);



% figure(2)
% imshow(face_cr);
% axis equal;
% axis off

%output the file to the specified directory
    out_name = strcat(int2str(i),'.jpg');
    imwrite(face_cr,strcat('J:\USQ\University 2011 Sem1\ENG4111 -
Project\MATLAB CODE\my_face rec codes\Test Files 2\light hist
face\',out_name));
end
```

C.3 Hist_eq.m

```
%
%
% This program loads an image file and performs histogram
% equalisation using the image processing toolbox and the
% histeq() function. As histogram equalisation normalises the
% intensity of a 256 bit image the greyscale.m pre-processing
% script must be run first.
%
%
```

```
clc
clear all
close all

Start_num = 1; % Enter the number of the first image to process
N_image = 72; %Enter the last number of image to process


for i =Start_num:N_image

im_name = i;  %input('Please enter the name of the image and its
extension \n','s');
    im_name = strcat(int2str(im_name),'.jpg');
    img = imread(strcat('J:\USQ\University 2011 Sem1\ENG4111 -
Project\MATLAB CODE\my_face rec codes\Test Files 2\colour
hist\',im_name));

    normalized = histeq(img);

    out_name = strcat(int2str(i),'.jpg');
    imwrite(normalized,strcat('J:\USQ\University 2011
Sem1\ENG4111 - Project\MATLAB CODE\my_face rec codes\Test Files
2\colour hist face\',out_name));
end
```

C.4 resize.m

```
%
%
% This program loads an image file and rescales the image so that
% it does not require as much memory. The images must be number
% as 1.jpg etc in order to be processed. The number of images can
% be changed by changing
% N_image. The images are saved to a new folder which can be
% changed by
% changing the imwrite line.
%
%
```

```
clc
clear all
close all

Start_num = 1; % Enter the number of the first image to process
N_image = 1000; %Enter the last number of image to process

%Set the scale to any of the predetermined sizes
%scale = [91,114];
%scale = [48,60];
scale = [24,30];


for i =Start_num:N_image

im_name = strcat(int2str(i),'.jpg'); %concatenates two strings to
form the image name such as 1.jpg


    img =imread(im_name);

   img = imresize(img, scale);

    out_name = strcat(int2str(i),'.jpg');
    imwrite(img,strcat('J:\USQ\University 2011 Sem1\ENG4111 -
Project\MATLAB CODE\my_face rec codes\Test Files
1\ALL\SIZE3\',out_name));
end
```

Appendix D

Results Script

D.1 result.m

```
%
%
% This program takes the raw results gathered from the
% E_test_eval_1.m program, for imposter and client and
% converts it to a meaningful percentage.
%
%

clc
clear all
close all

load results_eval_1_imposter_0.01.mat


im_total = 0; %imposter total
cl_total = 0; %client total
im_counter = 0; %impopster counter
cl_counter = 0; %client counter

r = length(result); %number of images in test

k = size(result);
k = k(1,2); %number of subjects in test

for j = 1:k

    for i = 1:r

        if (i== j*2 || i==j*2-1)
            if (result(i,j) == 1)
               cl_total = cl_total +1;
               cl_counter = cl_counter +1;
            else
                 cl_counter = cl_counter+1;
            end
        else
            if (result(i,j) == -1)

                im_total = im_total +1;
                im_counter = im_counter +1;
            else
                im_counter = im_counter +1;
            end
        end
    end
end


im_error = 100-(im_total/im_counter*100);
```

```
cl_error = 100-(cl_total/cl_counter*100);


vector =  [im_error cl_error];
%savefile = 'percentage_eval_2_client_0.0005.mat';
%save(savefile, 'vector')
```

Appendix E

CD Attachment

E.1 Contents of CD

The contents of the CD contain the MATLAB scripts that were used for verification as well as the pre-processing techniques incorporated. The samples taken from the XM2VTS have been included in the same format that they were in for testing. The results obtained from the evaluation script have also been added so that the results can be checked without the need to re-evaluate all images, as this is time consuming. Due to ethical reasons only a sample of the test database has been provided. All tests should be able to be reproduced using the scripts and images provided on the attached CD.