



UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

PROJECT REPORT

BIOMETRIC MODEL FOR ONLINE VERIFICATION OF A LARGE CLIENT BASE

BY

MBUGUA, PHILIP MWENJA

P 58 / 70650 / 2008

Submitted for the partial fulfillment of the requirements of the Master of Science in Computer Science


University of NAIROBI Library



0478764 4

DECLARATION

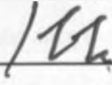
This project, as presented in this report, is my original work and has not been presented for any other University award.

Sign:  Date: 6/7/11

Philip Mbugua

P58/70650/2008

This project has been submitted as partial fulfillment of the requirements for the Master of Science degree in Computer Science of the University of Nairobi with my approval as the University supervisor.

Sign:  Date: 22/8/2011

Prof. W. Okello-Odongo

Project supervisor

School of Computing and Informatics

University of Nairobi

ABSTRACT

Authentication is determining an individual's identity correctly from among many, mostly through observing unique physiological features like face or presentation of a token that is unique for every individual. While these techniques work well for small populations, a challenge arises when the size of the population is large, as is the case with institutions of higher learning, during examinations.

In Kenyan institutions of higher learning, examinations are conducted in lecture halls and student populations may go up to 500 students per sitting. In such cases large auditoriums are used and several invigilators are positioned at the entrance before students enter the hall.

Students are authenticated by providing their student ID card and an examination card. The student ID contains the student's photograph, student's admission number, his/her names, the degree program undertaken and course duration.

The examination card contains the student's admission number, the student names the degree program and examination series. An examination card is not authentic if the exam series is invalid. Authentication ensures that only bona fide students are allowed into the examination facility.

The process begins shortly before the scheduled time for the examination and it involves checking to confirm that the photograph on student ID matches the bearer's facial features and that the examination card is valid before the student is allowed into the examination facility.

The problem with this mode of authentication is the time it takes to take such a population through this process and its effectiveness in terms of ensuring that no impostor ends up doing an examination. In trying to beat the time constraint so that the examination starts on time, the invigilators may quickly rush through the authentication and fail to scrutinize the documents for authentication. Furthermore for such large populations as is the nature of humans fatigue is bound to kick in thus worsening the situation.

This project seeks to address this problem by using fingerprint biometric technology. Biometric technologies are automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic. (Nanavati,2002).

In this project a biometric system is developed to authenticate individuals using their fingerprints which are difficult to forge. It is designed to reduce the time it takes for manual authentication by incorporating biometric readers at the point of entry into an examination facility which capture the sample and quickly compares it with a stored template, if a match is found the student is allowed otherwise he/she is rejected.

The findings of this project show that the time taken to perform manual authentication is twice the time taken using the system.

ACKNOWLEDGEMENTS

I take this opportunity to extend my heartfelt gratitude to all who participated in one way or another in making this work a success. The list is long but I would like to single out the following who played a major role in aiding this work : my supervisor and advisor, Prof. W. Okello-Odongo for his guidance and constructive criticism in all stages of this project, my wife Irene for her care and support, my colleagues in the class of 2008 and my friends in the development community.

To you all I say thank you and may God bless you.

TABLE OF CONTENTS

DECLARATION	1
ABSTRACT	2
ACKNOWLEDGEMENTS	3
LIST OF TABLES	5
LIST OF FIGURES	6
LIST OF ABBREVIATIONS	7
CHAPTER 1: INTRODUCTION	8
1.0 INTRODUCTION.....	8
1.1 AUTHENTICATION TECHNIQUES.....	8
1.2 PROBLEM STATEMENT.....	13
1.3 RESEARCH QUESTION.....	13
1.4 RESEARCH OBJECTIVES.....	14
1.5 JUSTIFICATION.....	14
1.6 CONSTRAINTS.....	ERROR! BOOKMARK NOT DEFINED.
1.7 ASSUMPTIONS.....	14
CHAPTER 2 : LITERATURE REVIEW	15
2.0 INTRODUCTION.....	15
2.1 PROBLEMS WITH BIOMETRICS.....	17
2.2 PERFORMANCE EVALUATION.....	18
2.3 CASE STUDIES.....	19
CHAPTER 3: RESEARCH METHODOLOGY	21
3.0 INTRODUCTION.....	21
3.1.1 SOFTWARE DEVELOPEMENT.....	21
3.1.2 EXPERIMENTATION FRAMEWORK.....	25
CHAPTER 4 : ANALYSIS AND DESIGN	27
4.0 INTRODUCTION.....	27
4.1 OVERVIEW OF CURRENT SYSTEM.....	27
4.2 DESIGN.....	28
CHAPTER 5 : IMPLEMENTATION	32
5.0 INTRODUCTION.....	32
CHAPTER 6: EXPERIMENTATION	34
6.0 INTRODUCTION.....	34
6.1 OBJECTIVES.....	34
6.2 EXPERIMENTAL SETUP.....	35
CHAPTER 7: DISCUSSION OF RESULTS	38
7.1 PERFORMANCE.....	38
7.2 USER ACCEPTANCE.....	38
7.3 IMPLEMENTATION ISSUES.....	39
7.3 RECOMMENDATIONS AND FUTURE WORK.....	40
7.4 CONCLUSION	40
REFERENCES	41
APPENDIX A: SAMPLE CODE	42
APPENDIX B :SAMPLE FORMS	48

LIST OF TABLES

Table 4.1: Database Design	28
Table 6.1: User Acceptance Response 1	35
Table 6.2: User Acceptance Response 2	36
Table 6.3: User Acceptance Response 3	36
Table 6.4: User Acceptance Response 4	37
Table 6.5: User Acceptance Response 5	38

LIST OF FIGURES

Figure 1.1: Fingerprint Image	11
Figure 1.2: Image with Minutiae	11
Figure 1.3: Identification and Verification	12
Figure 1.4: Authentication Process	13
Figure 3.1: Enrollment	24
Figure 3.2: Identification	24
Figure 3.3: Cancelable Biometrics	25
Figure 3.4: Conceptual Model	27
Figure 4.1: Use Case	28
Figure 4.2: Authentication over HTTP	29
Figure 4.3: Enrollment Form	30
Figure 4.4: Verification	30
Figure 6.1: User Acceptance Results	38

LIST OF ABBREVIATIONS

PIN – Personal Identification Number

FRR – False Rejection Rate

FAR- False Acceptance Rate

SDK – Software Development Kit

JDK – Java Development Kit

API – Application Programming Interface

GPL – General Public Licence

CHAPTER 1: INTRODUCTION

1.0 INTRODUCTION

Examinations in Kenyan Universities are an important activity in the university calendar without which no graduation will be held. It is in examinations that a University/College can boast of producing qualified and competent graduates; on the other hand poorly managed examinations can lead to irreparable damage to a university's reputation.

To underscore the importance of examinations, no other learning activities take place during these crucial two weeks of examinations, vigilance is heightened and sitting arrangements rearranged so that cases of cheating and malpractice are minimized.

On the administration side, every student who qualifies to sit for the exam is issued with an examination card to accompany his/her student ID card.

The invigilator's role is to ensure that no student is allowed to sit an examination without a valid student ID and an examination card. The student ID card is used to identify a student to the invigilator as having enrolled to take a certain course, it also contains a student's photograph. An examination card is used to identify those students that have been cleared to sit examinations in that series.

The invigilator authenticates by checking that the photograph appearing on the student ID card matches the student's facial features and that the examination card is valid before a student is allowed in.

This mode of authentication works well where there are few students since the invigilator has time to verify these two documents, however there is increased possibility of error when the number of students is large say five hundred or more and time is limited. In such cases it is easier for impostors to present wrong or forged documents and fail to be detected; under such circumstances the impostors hide behind the large numbers knowing fully well that there is no time for the invigilator(s) to scrutinize the documents fully.

The other challenge is the amount of time it takes to carry out this exercise considering the student numbers vis-à-vis the number of invigilators.

Even though no study has been done to show the extent of this practice and its impact on the credibility of university examinations, a few cases have been cited where a student is caught sitting exams on behalf of another or illegally sitting an examination. In order to minimize these cases of human error, biometric technologies can be of help and this is what this project is about.

1.1 AUTHENTICATION TECHNIQUES

Authentication is the process of ascertaining one's identity. A number of techniques can be used for demonstrating identity; the more traditional ones include username and passwords, Student ID cards, smart cards, credit cards etc.

Generally there are three methods by which users can authenticate themselves:

- Something the user is, that can be recognized as unique – biometrics.
- Something the user has or possesses which is unique – a card or device.
- Something the user knows - a password or PIN.

Passwords

Passwords are by far the most widely used form of authentication based on something the user knows. Users provide an identifier, a typed in word or phrase or perhaps a token card, along with a password which is then matched with a stored copy. Authentication is based on whether or not a match is found.

Password authentication does not normally require complicated or robust hardware since authentication of this type is in general simple and does not require much processing power.

However password authentication has several vulnerabilities, some of the more obvious are:

- Password may be easy to guess.
- Discovering passwords by eavesdropping or even social engineering is always a possibility.
- The system remains vulnerable to active attacks such as the-man-in-the middle attack.
- Session hijacking where an attacker hijacks the connection after a user logs in.
- Users risk losing their passwords.

Identification Cards and Smart cards

Authentication based on "something you have" has for a long time been used to authenticate students entering an examination facility. The "something you have" approach equates identity with possession of a physical device that a person carries such as a physical card, credit card, smart card or cryptographic calculator and uses for authentication. Such devices are subject to theft, so they should only be used together with some other authentication mechanism (e.g. a PIN).

In the case of universities, the student's identification card, which has the student's photograph is used. Authentication involves comparing the photograph on the student ID card and the bearer to see if they match or do not match.

Another example of "something you have" is the smart card. There are several types of smart cards in use today:

- PIN-protected memory cards. Information stored in the memory of such a card can be read only after a PIN has been typed into the card.

- **Cryptographic challenge/response cards.** These cards have on-board memory and processors. Thus, they can store keys as well as performing encryption and decryption.

One of the biggest disadvantages of these methods is that such devices can be lost or and in some cases misused.

Biometric Authentication

The word 'biometrics' is taken to mean the identification of individuals based on a physical characteristic using information technology. This can be done with the contour of a hand or a finger, a fingerprint, the pattern of an iris, face geometry etc.

Biometric identification involves comparing a previously captured physical characteristic e.g. fingerprint image with the result of a new measurement at the time and place of the check in order to establish whether someone is the right person. The result of the previous measurement can be registered in the verifying authority's database and retrieved during authentication. The actual computerized comparison of stored and the newly measured biometric feature can be carried out at the location itself or remotely.

A case for using biometrics

- Biometric templates/images are unique to an individual.
- Unlike password, pin number, or smart card, they cannot be forgotten, misplaced, lost or stolen.
- The person trying to access is identified by his real identity (represented by his unique biometric signature).
- A biometric characteristic cannot be transferred to someone else unobtrusively.
- Biometric techniques are non invasive in nature.
- Biometric techniques are not subject to recognition errors due to faulty observation resulting from preconceptions, distraction or tiredness, for instance.

Among all the biometric techniques, fingerprint-based identification is the oldest method, and has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints - a property that can be used for identification.

A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points, Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

The process of fingerprint identification includes the following stages:

- Scanning (capture, acquisition, enrollment)

- Extraction (image processing)
- Comparison
- Match/Non-match decision.

Fingerprint Scanning

Fingerprint scanning is the acquisition of a person's fingerprint characteristics for identification purposes. This allows the recognition of a person through quantifiable physiological characteristics that verify the identity of an individual.



Figure 1.1: Fingerprint Image.

Source: Chama(1999)

Extraction

For extracting information from our image we require specific algorithms developed for the recognition of certain patterns, however, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images.



Figure 1.2 : Fingerprints image with minutia identified.

Source: Chama(1999)

Comparison and matching

Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows.

Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach, but, it has its own shortcomings as well.

Fingerprint Identification vs. Verification

Identification/recognition is where a sample is presented to the biometric system during an access trail. The system then attempts to find out who is the sample owner (who someone is), by comparing the sample with a database of samples in the hope of finding a match (this is known as a one-to-many comparison).

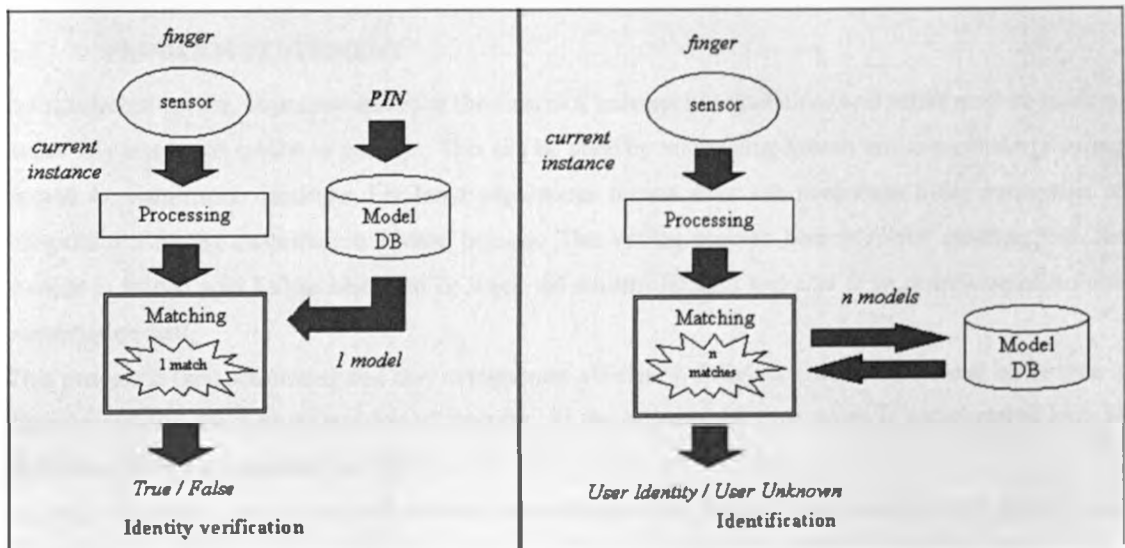


Figure 1.3 Identification and verification

Verification is a one-to-one comparison in which the biometric system attempts to verify an individual's identity. In this case, a new biometric sample is captured and compared with the previously stored template. If the two samples match, the biometric system confirms that the applicant is who he/she claims to be.

So identification/recognition involves matching a sample against a database of many, whereas verification involves matching a sample against a database of one.

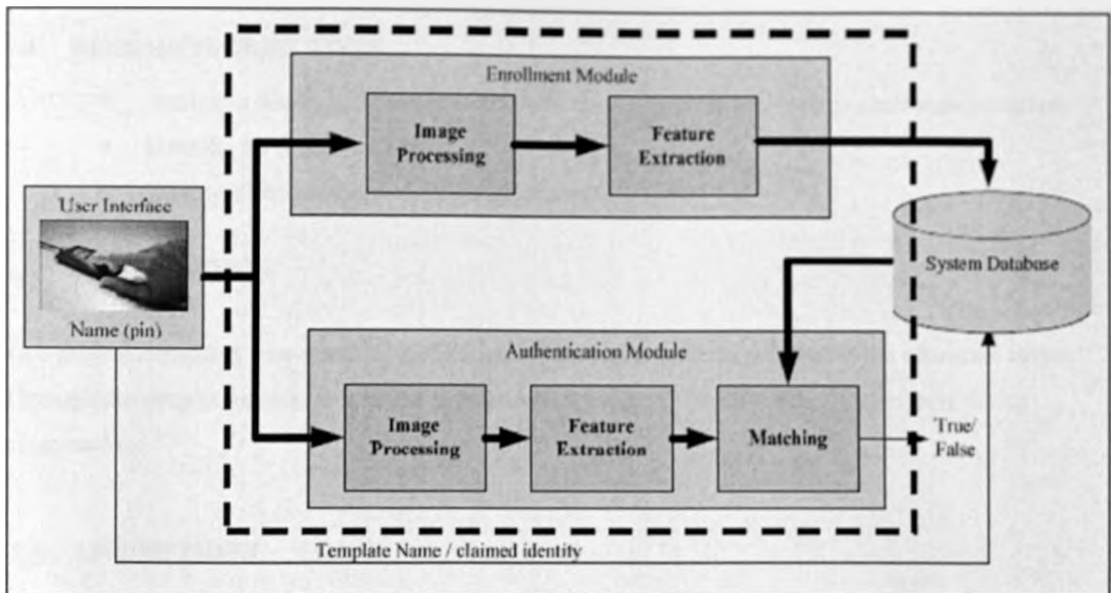


Figure 1.4 : Summary of biometric authentication process

1.2 PROBLEM STATEMENT

As mentioned earlier, examinations are at the centre of universities' operations and effort must be made to make this process as secure as possible. This can be done by minimizing human errors particularly during access to examination facilities. For large populations human error can contribute a big percentage of irregularities during examination vetting process. The vetting process here involves ensuring that the student is indeed who he/she claims to be using the student ID card and also is in possession of a valid examination card.

This process is time consuming and may compromise efficiency. Efficiency here is measured in the time it takes to authenticate a given number of students. At the moment the time taken is unacceptably high in scenarios where the population is high.

Secondly reliability goes down with increase in population size, human beings are known to get fatigued when doing a repetitive task without taking a break. As a result the possibility of not detecting a fraud increases due to this inherent human weakness.

This project seeks to develop a biometric solution that will assist in authenticating large student populations in universities during examinations.

1.3 RESEARCH QUESTION

The project seeks to answer the following questions:

- Is it feasible to offer a fingerprint biometric authentication to control access to examination facilities for large (500 and above) student populations in real time?
- How efficient will such a system be in comparison with current practice?
- How will this system be received by university students?

1.4 RESEARCH OBJECTIVES

- Analyze a distributed biometric authentication model for real-time student authentication.
- Develop the prototype model.
- Testing of the prototype through experiments.

1.5 JUSTIFICATION

This project introduces a new area of application of biometrics hitherto not used in the education sector. Through this project we seek to improve authentication processes in universities particularly during examinations.

1.6 ASSUMPTIONS

It is assumed that the fingerprint scanning device is available and that the students will be willing to have their fingerprints taken for the purpose of this research.

CHAPTER 2 : LITERATURE REVIEW

2.0 INTRODUCTION

In today's world a variety of applications require reliable and secure authentication methods to confirm the identity of an individual requesting a service. Examples of such applications include secure access to buildings, computer systems, high security installations and many more.

At present most authentication models are using what the user has or knows technique to determine authenticity. Whereas these traditional methods are fast and easy to implement, they are highly prone to abuse since these documents can get lost or be forged.

Biometric systems offer one of the most secure authentication systems ever developed.

Biometric technology may be defined as the automated use of physiological or behavioral characteristics to determine or verify an individual's identity. The word *biometric* also refers to any human physiological or behavioral characteristic which possesses the requisite biometric properties (Bolle et al ,2004), which are:

- *Universal* (every person should have that characteristic),
- *Unique* (no two people should be exactly the same in terms of that characteristic),
- *Permanent* (invariant with time),
- *Collectable* (can be measured quantitatively),
- *Reliable* (must be safe and operate at a satisfactory performance level),
- *Acceptable* (non-invasive and socially tolerable), and
- *Non-circumventable* (how easily the system is fooled into granting access to impostors).

Biometric technologies generate computer models of the physical and behavioral characteristics of human beings with a view to reliable personal identification. The first thing the system has to do is to develop a representation describing the discriminating features extracted from the biometric sample.

These discriminating features could, for instance, be the relative locations of minutiae points extracted from a fingerprint or code from an iris. Each sample's representation is referred to as a template.

The development and application of biometric technologies largely rely on pattern matching, which require learning (analysis) and recognition (synthesis). Significant progress have been achieved in this area since developing the computer-aided tools for signal (images, audio signal and other) processing, analysis and pattern recognition systems (Chen and Wang, 2005). Several biometric features which satisfy the above properties can be used among them:

Fingerprints

Fingerprint is, perhaps, the oldest type of biometrics, started in the ancient world. The most popular utilization example of fingerprints is forensic investigations. Today's fingerprint readers are the most developed type of biometric sensors.

One main shortcoming for fingerprint identification systems is that small injuries and burns highly affect the fingerprint. In fact, injury, whether temporary or permanent, can interfere with the scanning process. For example, bandaging a finger for a short period of time can impact the fingerprint scanning process. Something as simple as a burn to the identifying finger could make the fingerprint identification process fail (Jamieson et al , 2005).

Signatures

Current interest in signature analysis is motivated by the development of improved devices for human-computer interaction which enable input of handwriting and signatures(Zhao, 2006). Its main advantage is that it is none intrusive.

Faces

Face recognition systems detect patterns, shapes, and special features in the face, perform feature extraction and recognition of facial identity. In a nutshell, it includes all types of facial processing such as tracking, detection, analysis and synthesis.

Biometric systems can be confused when identifying the same person smiling, aged, or with various accessories (moustache, glasses), and/or in badly lit conditions.

Such facial recognition tools can be improved by training on a set of synthetic facial expressions and appearance/environment variations generated from real facial images (Ekman & Rosenberg, 1997).

The most advance on-going research in this area is devoted to understanding of how humans can routinely perform robust face recognition, in order to improve machine recognition of human faces. This research is relevant to computer vision paradigm. A comprehensive references to the current state-of-the-art approaches to face processing can be found in (Zhao, 2006).

Facial recognition compared to fingerprint recognition performs very poorly when deployed in the real world, especially for recognition at a distance. A facial recognition system deployed in Logan International Airport to detect terrorists failed in 38 percent of the cases to match the identities of a test group of employees, according to a study by the American Civil Liberties Union (Murphy & Bray,). A face-recognition system deployed on the streets of Tampa, Florida to identify criminals was scrapped two years later having not identified, alerted of, or caught any criminals, according to a spokesman for the Tampa Police Department (Bowman, 2003).

Iris and retina

Iris recognition identifies a person by analyzing the "unique" patterns that are visible in the iris of an eye to form an iris code that can be compared to iris templates in an existing database. Retina recognition systems scan the surface of the retina and compare nerve patterns, blood vessels and such features to an existing

code template. Although exhibiting a number of strong points, discussed above, iris recognition suffers from a few problems.

First, it performs well at close proximity and so requires the person's cooperation. Secondly Iris recognition is susceptible to poor image quality, with associated failure to enroll rates

Up until recently, the biggest concern has been reliability of the various biometric techniques – since not all biometric features have the same reliability. However there has been tremendous improvements in this area recently. For example, there are character recognition methods that can reach as high as almost 99.99% accuracy rate. To increase overall reliability, the contemporary biometric systems measure multiple physiological or behavioral traits. This approach is called *multimodal biometrics* (Ross, 2006).

Multimodal Biometric Systems

A biometric system that is based on one single biometric identifier (unimodal) does not always meet the desired performance requirements.

If for example a user cannot provide good fingerprint image due to a cut in the finger, then face and voice or other biometric identifiers can be used instead (or in conjunction).

Secondly , spoofing of biometric data also becomes harder since it is far easier to spoof only one biometric trait whereas with multi biometric systems it would be necessary to spoof several traits simultaneously.

The use of multiple biometric traits therefore improves reliability of these systems , but it comes at a cost to the user. One needs to therefore ask whether it is necessary to go multimodal or there could be other ways of improving unimodal biometric systems. As shall be seen later in this reserach unimodal biometric systems have shown remarkable improvement in reliability when combined with passwords or PINS.

2.1 PROBLEMS WITH BIOMETRICS

Noise

Noisy biometric data like a person having a cold(voice recognition), a cut on ones finger(fingerprint scan) or different lighting conditions(face detection) are some examples of noisy inputs. Other examples are misconfigured or improperly maintained sensors or inconvenient ambient conditions like dirt on a sensor for fingerprints or voice recognition with loud background noise. The problem with noisy biometric data is that authorised personnel may get incorrectly rejected(False Rejection), if the noisy data affects the extracted features so much, that no match can be found in the biometric database.

The other extreme situation would occur if noise would change the extracted features in such a way, that the result feature set would match to another person (False Acceptance).

Distinctiveness

While a biometric trait is expected to vary significantly across individuals, there may be large similarities in the feature sets used to represent these traits. Thus, every biometric trait has a theoretical upper bound in terms of discrimination capability.

Non-universality

The problem of non-universality arises when it is not possible to acquire certain biometric traits from all users. That means that even though a person has a fingerprint, it still may be impossible to acquire that trait because of the poor quality of the ridges which make up the fingerprint.

The other problem is that biometric traits extracted from persons tend to vary with time for one and the same person and to make it even worse, this variation is itself very variable from one person to another.

Privacy of Biometric Data

The nature of biometric data is such that it cannot be altered or changed and so when accessed illegally unlike other forms of authentication it becomes impossible to secure thus biggest strength of biometrics is also its biggest liability (Ratha, 2001). The issue of protecting privacy of biometric systems has inspired the area of research called cancelable biometrics. It was first initiated by the Exploratory Computer Vision Group at IBM T.J. Watson Research Center and published in [<http://www.research.ibm.com/ecvg/biometrics.html> (2002)].

Cancelable biometrics aims to enhance the security and privacy of biometric authentication through generation of "deformed" biometric data, i.e. synthetic biometrics. Instead of using a true object (finger, face), the fingerprint or face image is intentionally encrypted in a repeatable manner, and this new template is used. If, for some reason, the old print or image is "stolen", an essentially "new" print can be issued by simply changing the parameters and or algorithm of the distortion process. This also results in enhanced privacy for the user since his true print is never used anywhere (Cavoukian, 1999).

2.2 PERFORMANCE EVALUATION

In biometrics, performance is ultimately based on the probability of accepting impostors, referred to as False Acceptance Rate (FAR); and the probability of rejecting genuine users, referred to as False Rejection Rate (FRR). Plotting the value of FRR against FAR produces what is known as the Receiver Operating Curve, which could be used for a graphical comparison of performance between different systems. For a simple empirical measure, the Equal Error Rate (EER) is usually used in biometrics, which refers to the point at which FRR and FAR are equal. The lower the ERR the more accurate the system.

Accepting or rejecting a user is a binary decision which is an outcome of decision-making module This module can make two types of errors, i.e.

False Rejection (FR): when an actual client gets identified as an impostor.
False Acceptance (FA): when an actual impostor gets identified as a client.

These two parameters can be measured using the following equations:

$$FRR = \frac{\text{number of false rejections}}{\text{number of client accesses}} \dots \dots \dots (1)$$

$$FAR = \frac{\text{number of false acceptances}}{\text{number of client accesses}} \dots \dots \dots (2)$$

A perfect biometric authentication system would have a FRR = 0 and a FAR = 0 is unrealistic.

Another measure is the Total Error Rate(TER) given by the equation :

$$TER = \frac{\text{number of FA} + \text{number of FR}}{\text{total number of accesses}} \dots \dots \dots (3)$$

At this point it is important to emphasize the fact that these measures could be heavily biased by one or either type of errors (FAR or FRR) depending only on the number of accesses.

2.3 CASE STUDIES

Automated Fingerprint Identification Systems(AFIS)

Many law enforcement agencies often use fast fingerprint identification systems based on a huge amount of fingerprints stored in a database. These systems are called AFIS (Automated Fingerprint Identification Systems).

The FBI's Integrated AFIS maintains the largest biometric database in the world, containing the fingerprints and corresponding history information for more than 95 million subjects, both criminal and civil.[Department of Justice, USA]

Biometric Embedded Passports

The Republic of the Maldives, with the support of BioLink, introduced passports that come with microchips storing fingerprint and face templates. This technology allows for quick and reliable identification of citizens (Biolink 2007).

Mexico City International Airport installed Bioscrypt's V-Smart authentication system to provide access control to high-security areas of its terminals. The system requires use of a smart card that stores one's fingerprint template according to CBC News, [<http://www.cbc.ca/technology/story/2006/11/10/airports-card.html>] (2006)].

Biometrics in Education

Until recently biometric systems have been used in security related applications and rarely in civil applications. This is probably because the use of biometrics is associated with criminal activities and a person may feel stigmatized if their fingerprints are taken.

But this is changing with increased adoption, according to (Cavoukian, 1999), the more the organizations which require the provision of fingerprints as part of their operations the more the adoption of this technology.

Another concern stems from the fact that biometric data is considered private information and sensitive to the extent that if misused can result in irreparable damage. This can be addressed by use of encryption such that the encrypted form of a biometric sample is stored instead of the actual biometric. (Cavoukian, 1999).

In spite of these challenges, schools and colleges have in the last few years began to use automated fingerprint identification systems (AFIS) for registration, library book borrowing and cashless catering. From my literature review I have not come across a biometric system used in monitoring entry into examination facilities for large student populations and this research explores how this technology can be deployed for such services.

CHAPTER 3: RESEARCH METHODOLOGY

3.0 INTRODUCTION

This section outlines how the project is to be undertaken. This methodology for this research will involve three things, Software development , Software Testing and User acceptance survey.

3.1.1 SOFTWARE DEVELOPEMENT

The object-oriented model will be used to develop the new system and will follow the following steps:

1. **Requirements Analysis** : This is where classes of objects and the interaction between them are defined.
2. **Object-Oriented Analysis**: Understanding and modeling a particular problem within a problem domain.
3. **Object-Oriented Design** : Objects are identified and classes of those objects designed..
4. **Object-Oriented Programming (OOP)** : Implementation of the classes using an object oriented language.

Requirement Analysis

The new system will not alter the manual authentication process it only enhances the process to make it more secure, as such no new requirements are being added other than what is already in place i.e.

- ❖ Capture/Enroll students details.
- ❖ Allow a student to access an examination facility based on positive identification outcome.
- ❖ Prevent a student from an examination facility based on negative identification outcome.
- ❖ Report on allowed students.

Object-Oriented Analysis

Unified Modeling Language(UML) will be used to analyze the existing system and represent it in a use case diagram.

Object-Oriented Design

The major classes required to implement the system will be designed using class diagrams. The data modeling component will used the relational model.

Implementation

Fingerprint database

There are two methods of storing biometric information; the first method involves storing the actual biometric image of the sample collected. The second method involves storing a distorted or encrypted form of the biometric sample collected.

The second method is far more secure since it is impossible to reverse engineer the new template generated to produce the original biometric image captured – the two widely used and closely related techniques are Biometric Encryption and Cancellable Biometrics.

Biometric Encryption

Biometric Encryption (BE) is a technique for binding a digital key to a biometric image sample, to produce a Biometric Encrypted (BE) template, without having to store the biometric image itself. (Cavoukian, 2007). What is stored is the BE template. The digital key is randomly generated during enrolment and can be regenerated several times on presentation of a live sample during verification. The live sample therefore serves as the decryption key, if the sample is correct a key is generated otherwise no key is generated. The key is completely independent from the biometric image and can be changed.

The encryption/decryption process is fuzzy, in that the biometric sample is different each time, unlike an encryption key in conventional cryptography.

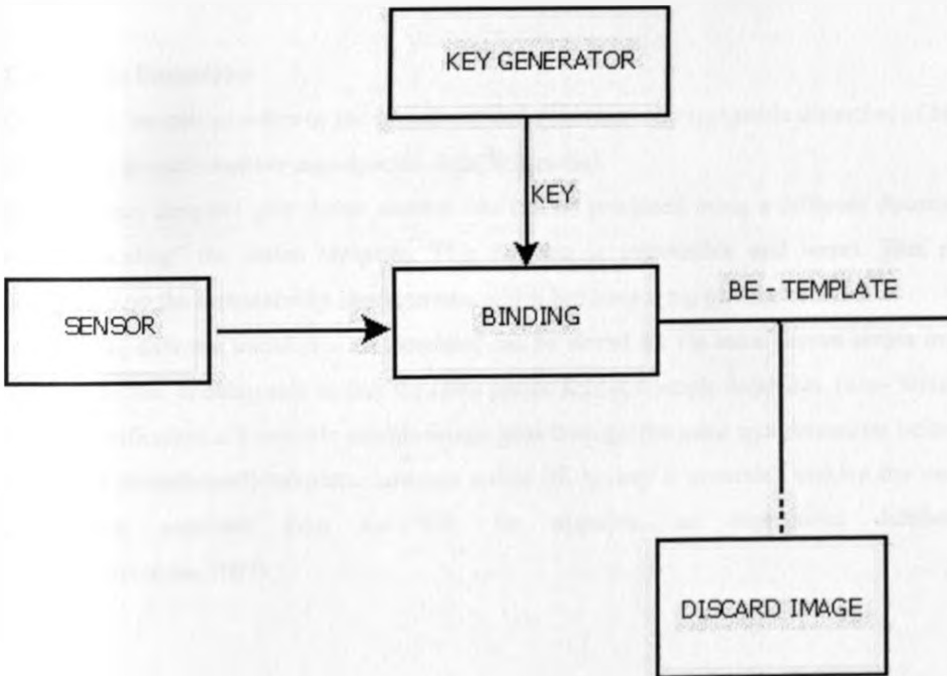


Figure 3.1 : ENROLLMENT

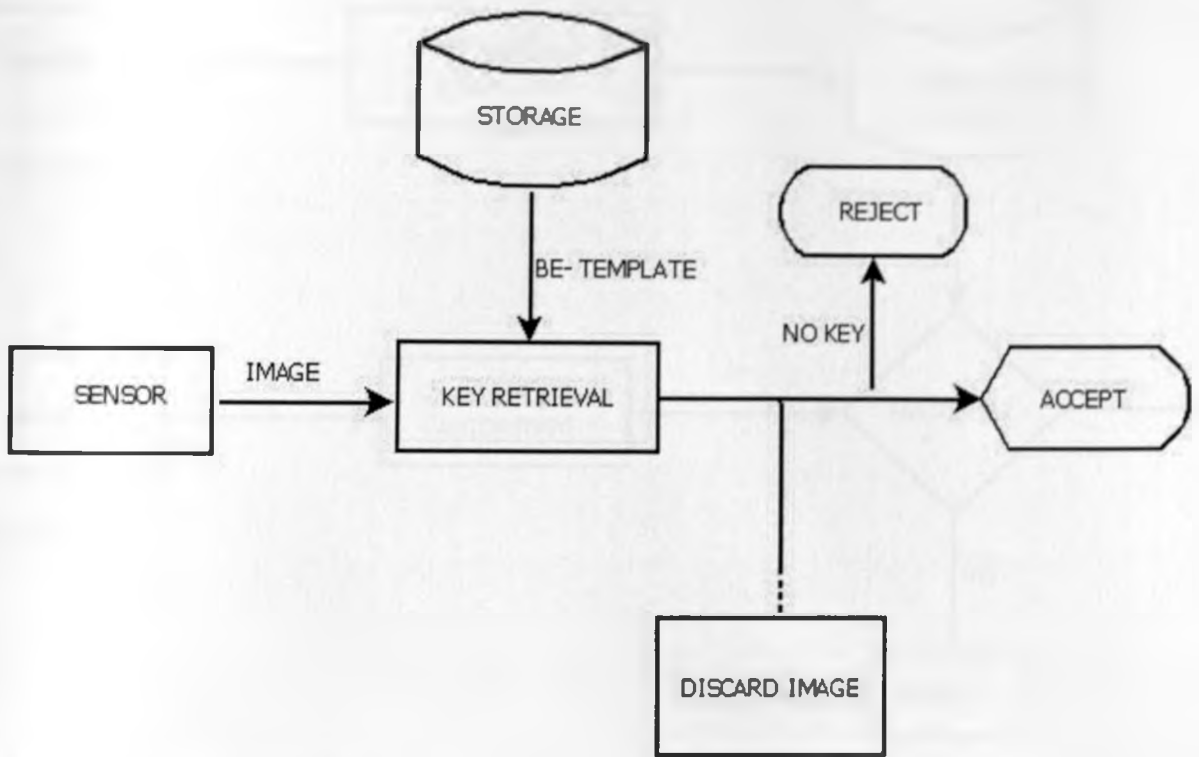


Figure 3.2 : IDENTIFICATION

Cancelable Biometrics

Cancelable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data(Wikipedia).

If the feature template gets stolen another one can be produced using a different distortion function and then “canceling” the stolen template. This function is irreversible and secret. This makes biometric databases lose the immutability characteristic which has been a big privacy concern.

In addition, different transforms of templates can be stored for the same person across multiple databases without the fear of being able to link the same person across multiple databases. (non- linkability).

During verification, a biometric sample image goes through the same transformation before matching with the stored (transformed) template, however unlike BE no key is generated making the variety of potential applications narrower than for BE; for example, an anonymous database cannot be created(Cavoukian,2007).

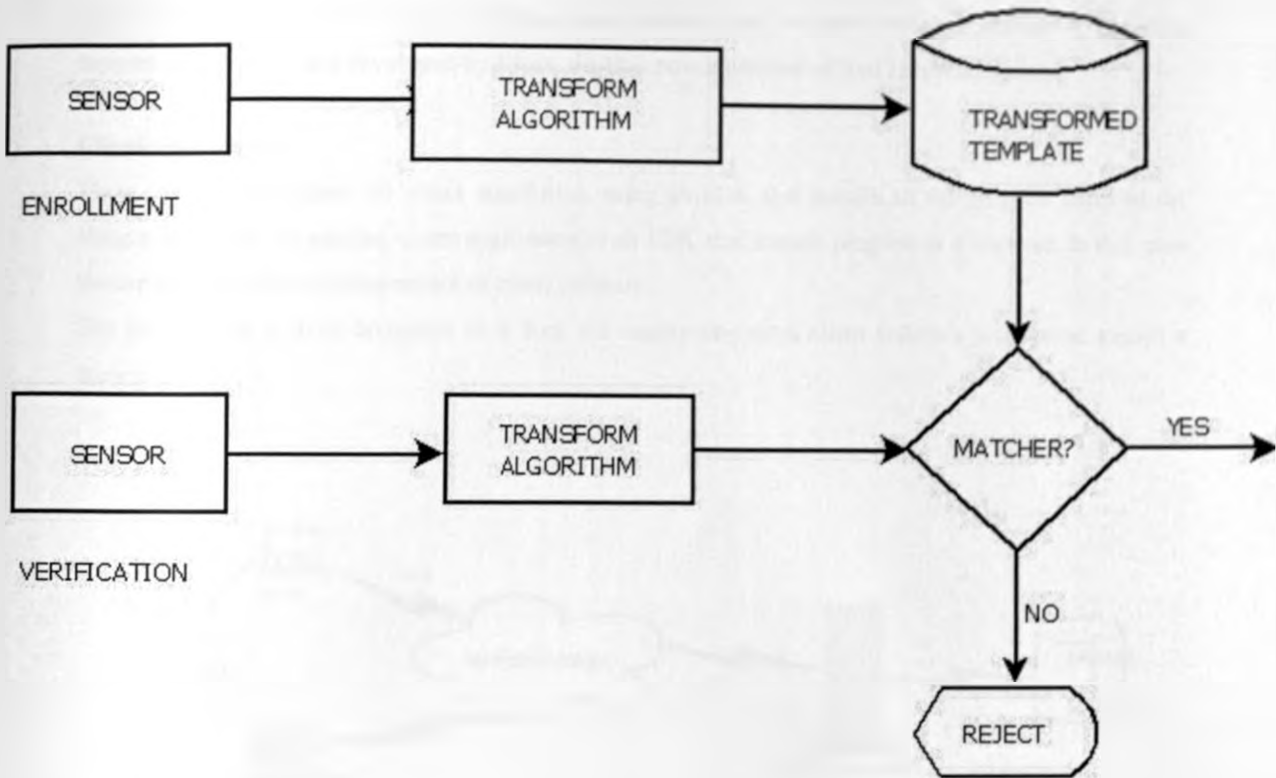


Figure 3.3 : Cancelable Biometrics

Application Sever

An application server is a service layer designed to support development of applications through provision of required API's for application development. An application server abstracts the underlying Hardware and Software platform thus allowing for deployment of various otherwise incompatible applications on one platform.

Types of Application Servers

Java EE

The most popular application server platforms is the Java Enterprise Edition(Java EE) . Sun Microsystems came up with GlassFish (formerly Sun Java System Application Server 9.1) an open source application server project for the Java EE platform which is what will be used for this project. GlassFish is free software distributed under both the Common Development and Distribution License (CDDL) and the GNU General Public License(GPL). This is the main reason why this server was chosen to implement the project.

JBoss

JBoss Application Server (or JBoss AS) is an open-source software based on Java EE. It not only implements a server that runs on Java JDK, also implements the Java EE part of Java. Because it is Java-

based, the JBoss application server operates cross-platform and is usable on any operating system that supports Java. JBoss was developed by JBoss, which is now a division of Red Hat(Wikipedia).

Client Application

There are various options for client installation, using an SDK that installs all the plug-ins required for integration within an existing client application or an SDK that installs plug-ins in a browser, in this case the server application is independent of client software.

The later option is more favorable as it does not require any extra client software installation except a browser.

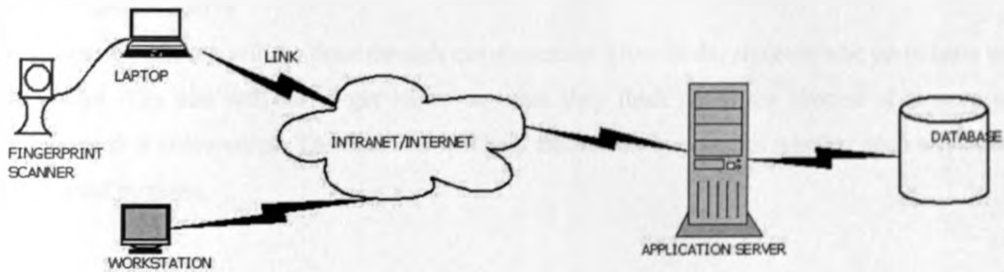


Fig. 3.4 Conceptual model

3.1.2 EXPERIMENTATION FRAMEWORK

Experimentation will begin with building a database of approximately thirty(30) fingerprints collected from a class. This will simulate an exam registration process in a university, where the thirty will be the bona-fide students allowed into an examination facility.

Each student will also have the normal required Student ID and an examination card for purposes of comparison of the traditional system with the new system. In addition another ten(10) students will be included in this experiment who are not registered with the system(impostors).

The experiment will be conducted in a university where the same venue used for examinations will be used and an invigilator/biometric reader will be positioned at the entrance.

Experiments

The following performance measures are going to be tested:

- **Authentication time** – whether the system is able to identify samples presented, within a reasonable time frame.

This will be done by recording the total time taken for all samples to be authenticated and then deducing the time it takes for authenticate one student.

Another experiment will be conducted where the traditional invigilator method is used on the forty students and again the time recorded in a similar manner as above.

The two outcomes will then be compared to assess which performs faster.

- **Enrollment time** : A measure of the time it takes to enroll one student, similar setup as above will be used.
- **Error Rate** – this test will be conducted to ascertain the effectiveness of the biometric system in terms of False Acceptance(FAR) and False Rejection Rates(FRR) using the 30 bona-fide and 10 who are not registered. The results will not be compared with the traditional method for lack of data on the magnitude of human error in manual authentication processes, however there are standard industry benchmarks for fingerprint biometrics which allow for FRR of between 0.3 – 0.7% and FAR of between 0.001 – 0.01%
- **Acceptance** – this test will be done through questionnaires given to the students who participate in this experiment. The aim will be to get views on what they think about the process if it were to be implemented in universities. The outcome will help answer the question of whether such a system can be accepted by users.

CHAPTER 4 : ANALYSIS AND DESIGN

4.0 INTRODUCTION

This chapter analyses the existing system of examination access security and points out areas which need to be addressed by the new system.

The chapter also presents the design of key components of the new system.

4.1 OVERVIEW OF CURRENT SYSTEM

The examination process actually begins when a student registers for the courses to undertake in a given semester. His/Her details will be captured and the student allowed to attend lectures in preparation for examinations. Just before the examination season begins all students who qualify to sit examinations are issued with an examination card which shows proof that student has met all requirements stipulated in the regulations.

The student ID and the examination card must be produced at all times before and during an examination for invigilators to authenticate the students.

Normally for large student populations, there will be two or more invigilators positioned at strategic entry points to the examination venue who check and validate these documents physically and if satisfied they would allow the student in. This is done minutes before time, and therefore time is usually a constraint.

In such circumstances there is no way the invigilator can make reference to the database if in doubt, worse still the invigilator may not distinguish between real and fake documents. This is a vulnerability which can be exploited by unscrupulous students and get away with it.

The proposed system seeks to seal this loophole by the use of biometric features which cannot be forged and making direct reference to the database for authentication.

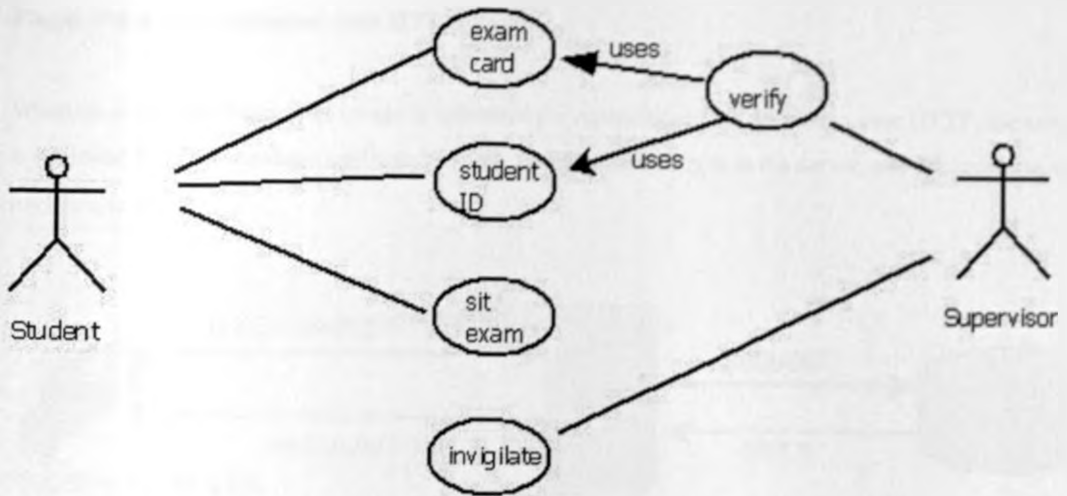


Figure 4.1 : Examination Authentication- Use Case Diagram

4.2 DESIGN

The core components of the system are; the Database, Application Server and Client application.

Database Design

The fingerprint database schema will consist of one relation(table), consisting of five fields as shown below:

Field	Data type	Description
Student_ID	Text	A unique number for every studnets
First_Name	Text	First Name
Last_Name	Text	Last Name
Year_of_Study	Numeric	Year of study
Exam_Series	Text	Examination period
FingerprintID	Text	Biometric template

Table 4.1: Users Table

Finger Print Authentication over HTTP

When an encrypted fingerprint image is submitted for Authentication/Verification over HTTP, the sample is retrieved from the database and matched with the submitted sample in the server, and the response sent back to the client.

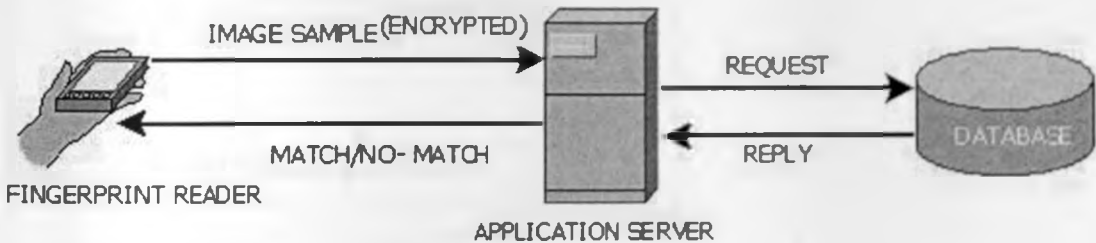


Figure 4.2 : Authentication over HTTP

Authentication Modules Design

The application server will contain the authentication logic which is captured in three modules:

- Register device : Registers and detects a fingerprint scanning device.

```
function register()
{
// detect USB fingerprint scanning device.
//Error if Device not ready
//success if device ready
}
```

- Enrollment : Captures and transforms the image captured into a encrypted form for transmission to the database.

```
function enroll()
{
// open device for capture
//capture image
//enroll to database
}
```

- Verify : matches an enrolled image with a previously captured image and returns a match/no-match result.

```
function verify(image sample)
{
//capture sample
//search database for match
//return match/no-match result
}
```

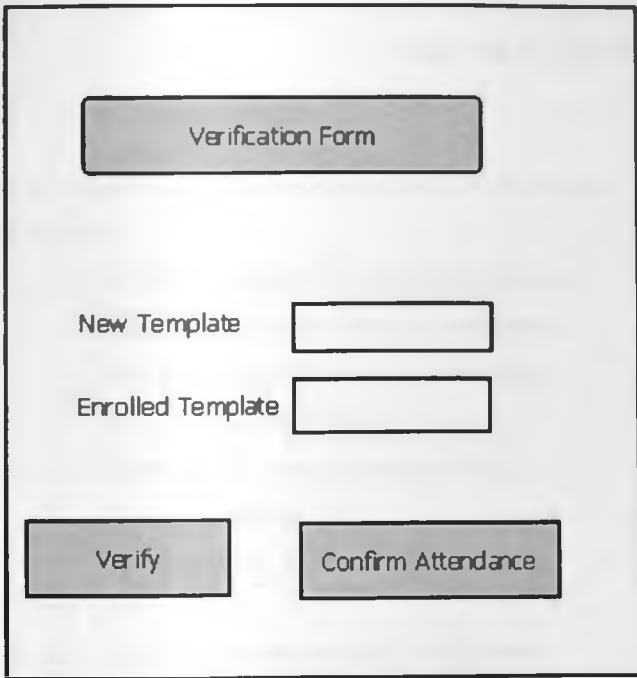
Interface Design

Being a web-based system the interface will consist of a web page incorporating a form with the following input fields:

The diagram shows a rectangular frame containing the following elements from top to bottom:

- A grey rectangular box with the text "Enrollment Form" centered inside.
- A label "Studnet ID" followed by a white rectangular input field.
- A label "First Name" followed by a white rectangular input field.
- A label "Last Name" followed by a white rectangular input field.
- A label "Year Of Study" followed by a white rectangular input field.
- A label "Fingerprint ID" followed by a white rectangular input field.
- A grey rectangular button with the text "Enroll" centered inside.

Figure 4.3 : Enrollment Form



The image shows a rectangular window titled "Verification Form". At the top center is a button labeled "Verification Form". Below this, there are two input fields. The first is labeled "New Template" and the second is labeled "Enrolled Template". At the bottom of the window, there are two buttons: "Verify" on the left and "Confirm Attendance" on the right.

Figure 4.4 : Verification Form

CHAPTER 5 : IMPLEMENTATION

5.0 INTRODUCTION

This chapter describes how the system will be implemented. The following tools will be used to implement the system:

- MySQL Database for the fingerprint database
- Glassfish Application Server for middleware.
- Java Server Pages(JSP) to run on the client.
- Secugen Hamster SDK
- NetBeans IDE a development platform.
- Fingerprint Reader.
- Linux Operating System

MySQL Database Installation and Configuration

MySQL can be installed by downloading directly from the Internet using the following command issued from the command line:

```
# apt-get install mysql-server
```

MySQLadmin

The *mysqladmin* GUI program is used to administrate various aspects of the MySQL database server. Using it, the administrator can perform tasks such as: create and delete databases, shutdown the database server, update the privilege tables, and view running MySQL processes. The program was installed using the following command:

```
# apt-get install mysql-admin
```

To ease query management, a query browser was also installed:

```
# apt-get install mysql-query-browser
```

Netbeans IDE Installation

Netbeans is an opensource platform and framework for developing desktop applications that supports various programming languages including Java, C/C++, Ruby, Python ,PHP etc.

Several versions have been released since its inception.

The NetBeans IDE 6.8 is the first IDE to provide complete support of Java EE 6 and the GlassFish Enterprise Server v3

It offers various services and components necessary for application development including menus and toolbars, window management, visual library etc.

Netbeans installation is preceded by Java Development Kit(JDK) installation using the command

```
# apt-get install sun-java6-jdk sun-java6-plugin
```

Installing Netbeans is fairly straight forward using the following steps:

- Download Netbeans from Netbeans download page into some directory.
- Go to download directory and change permissions to add execute permission.
- Install the package by following instructions.

CHAPTER 6: EXPERIMENTATION

6.0 INTRODUCTION

Testing is the process of verifying that the system meets the set objectives. The performance of a biometric system can be evaluated in one of the following two ways:

i Scenario evaluation

The main objective of scenario testing is to determine the overall system performance in a prototype.

Testing is carried out in an environment that models a real-world target application of interest. Care must be taken to ensure data capture is in the same environment and with the same population as the real system.

ii Operational Evaluation

The aim of operational testing is to determine the performance of a complete biometric system in a specific application environment with a specific target population.

In general, operational test results will not be repeatable because of unknown and undocumented differences between operational environments and offline testing is not possible.

Several types of tests can be conducted under these two categories:

- Decision error rates
 - False accept rate(FAR)
 - False reject rate(FRR)
- Image acquisition errors
 - Failure to enrol rate
 - Failure to acquire rate
- Transaction duration
 - Average time it takes to perform one transaction

Other than performance measures another important measure is user acceptance. This measure assesses the suitability of the system to the intended users.

6.1 OBJECTIVES

The objectives of the experiments are:

- To establish if a biometric examination authentication system is more time efficient compared to manual examination authentication.
- To measure the performance of the biometric system in terms of:
 - **False acceptance rates**
The false acceptance rate is the probability that an unauthorized individual is authenticated.
 - **False rejection rates**
The false rejection rate is the probability that an authorized individual is inappropriately rejected.
 - **Enrollment Time**
The time it takes to enroll a student
 - **Verification time**
The time taken to authenticate a student.
- To ascertain whether the system will be accepted by users

6.2 EXPERIMENTAL SETUP

Enrollment

This process will take place over a period of two days, a total of sixty (60) subjects will be enrolled, divided in two groups, and second year class consisting of thirty(30) subjects and a third year class constituting the other thirty(30).

A group of ten(10) students will be left out in each class.

Verification

Random samples(S) of ten(10) from each class both enrolled and not enrolled will be selected on a day different from enrollment day and their biometric details taken again and verified against those earlier collected. The findings will be tabulated in a table. This will be repeated three times.

Time Measurement

The time taken to verify these subjects using will be captured and a repeat of the same experiments will be done using manual authentication and time recorded.

Manual authentication involves, checking a subject's student ID and matching the photograph with his/her facial features and against a list of bona fide candidates generated from a system. Assuming there is no delay from one student to another, the average time to authenticate one student is the total time divided by the number of students.

For biometric authentication, time is recorded from when a subject submits his/her student ID for verification using the system to the time a match/no match decision is made. The average time is computed as indicated above.

Similar tests will be conducted to measure enrollment time.

The table below shows the items to be captured for each experiment

Sample characteristics

Sample Name	Class	Enrolled	Impostors	Size
S1	2 ND YEAR	7	3	10
S2	2 ND YEAR	8	2	10
S3	2 ND YEAR	6	4	10
S4	3 RD YEAR	10	3	13
S5	3 RD YEAR	6	7	13
S6	3 RD YEAR	10	3	13
TOTAL		47	22	69

Table 6.1 ; Sample Characteristics

PERFORMANCE RESULTS

Sample	Biometric verification time	Time per student(B)	Manual verification time	Time per student(M)	No. of False Rejection	No. of False Acceptance
S1	3.19 mins	0.32 mins	5.06 mins	0.51	0	1
S2	2.72 mins	0.27 mins	3.11 mins	0.31	0	1
S3	2.85 mins	0.28 mins	3.0 mins	0.30	0	1
S4	3.78 mins	0.29 mins	8.25 mins	0.63	1	0
S5	3.95 mins	0.30 mins	5.79 mins	0.45	1	0
S6	3.18 mins	0.24 mins	6.12 mins	0.47	2	0
Average		0.28 mins		0.44 mins	0.08	0.13

Table 6.2 : Results

Sample	False Rejection(%)	False Acceptance(%)
S1	0	0.33
S2	0	0.5
S3	0	0.25
S4	0.1	0
S5	0.17	0
S6	0.2	0

Table 6.3 : False Acceptance/Rejection Rate

Sample	Total time	Average
S1	10.18 mins	1.18
S2	9.74 mins	0.97
S3	9.82 mins	0.98
S4	12.52 mins	0.96
S5	11.03 mins	0.84
S6	10.02 mins	0.77
Average time to enroll one student		0.95 mins

Table 6.4 : Average enrolment time for one student.

USER ACCEPTANCE RESULTS

I. Do you think biometric technologies can be used in authentication in universities?

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	24	96.0	96.0	96.0
No	1	4.0	4.0	100.0
Total	25	100.0	100.0	

Table 6.5

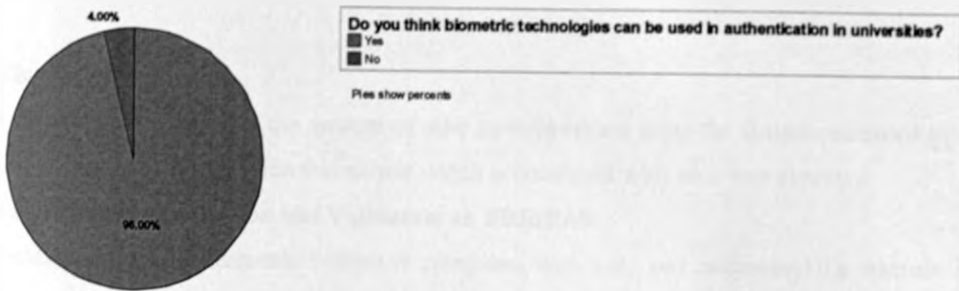


Figure 6.4

CHAPTER 7: DISCUSSION OF RESULTS

The results from the forgoing experiments lead to the following findings and observations:

7.1 PERFORMANCE

i False Acceptance(FAR) and false rejection rates(FRR)

The results from the experiments are consistent with the expected results for both FRR and FAR performance measures.

From literature review, in fingerprint based biometric systems the FRR and FAR ranges from 0.03% – 0.07% and from 0.001% to 0.01% respectively [Langenderfer, 2005].

The intersection of the two graphs gives an Equal Error Rate(EER) of 0.8 which is consistent with literature values.

ii Time efficiency

From the results, it takes half the amount of time to authenticate using the system compared to using the manual method, an indication that slower which is consistent with what was expected.

Comparison between Verification and Validation on FRR/FAR

In a verification system, a biometric feature is compared with only one reference(1:1), whereas in an identification system, it is compared with many(1:N) . The transition from Verification to Identification resulted in a higher FAR.

7.2 USER ACCEPTANCE

The choice of respondents for this survey was done within an institution which heavily relies on technology, in addition all the respondents were Computer Science students mostly second and third years. This has greatly influenced the results of the user acceptance test.

From the results, it is evident that most of the students have an idea of biometric technologies derived mostly from companies (a good proportion are working) and the electoral process. This is an indication that the level of awareness is high for this particular group of respondents.

Another key outcome is that over 40% of respondents do not have faith in the manual authentication process an indication that it doesn't serve the population it is intended for effectively.

There is overwhelming support for the use of biometrics in examination authentication, over 95%. This figure is rather exaggerated probably due to the level of awareness the respondents had with regards to biometrics.

It is anticipated that this rate will reduce significantly in non- ICT populations since the level of awareness is lower.

It is also an indication that if people are well informed and made aware any technology that improves processes can be adopted.

7.3 IMPLEMENTATION ISSUES

i Usability

For this system to be successfully implemented the following issues need to be addressed:

- Positioning of the fingerprint reader – the reader needs to be strategically mounted at the entrance with the USB cord well secured.
- The challenge is where to position the laptop during authentication.
- Training to both staff and students – In order to be successfully implemented extensive training is required. This would preferably be done when students register for courses such that they can be taken through the process.
- Population size – The tests conducted could not give the impact of such a system on large population. It is envisaged that the biggest challenge will be speed, especially when many requests are submitted simultaneously.

ii Cost

- The biggest cost element would be the finger print readers, most of the other infrastructure already exists in most universities. The system runs on a client/server platform.
- Maintenance of the devices.
- Maintenance costs will be minimal since the devices are durable and require replacement every five years. See appendix for estimates

iii Integration

- The current SMIS runs on PHP/Oracle, these two platforms are very friendly to the platform used to develop this system. The Oracle database will be modified to include a biometric template field.
- The Oracle database has API's that can integrate it with Java such that the same Java enrolment and authentication module can be used to read and write to the database.

7.4 OPERATIONAL CHALLENGES

A number of operational challenges are envisaged:

- The server is bound to slow down if the number of request are many and given that exams are done around the same time in the university calendar, it is not known how the server will perform when subjected with many requests.
- Some false rejection, where bona fide students are rejected, according to this research approx. 0.08 % will be rejected falsely. An alternative mechanism needs to be devised to address this shortcoming.
- Legal issues to do with collection of biometric information.

Testing

In order to get the real picture of other operational challenges, an operational evaluation needs to be conducted.

7.3 RECOMMENDATIONS AND FUTURE WORK

This research sought to answer four questions as stipulated in section 2.2, however much attention was given to prototype development than the research component due to time constraints.

It is recommended that more research be conducted in the area of user acceptance and performance testing models which are necessary to validate this system.

Improvements can also be made in the design of the system to incorporate barcode readers to aid in the capture of student details both during enrollment and verification. This will reduce the time it takes to perform these two exercises.

A modification of this system can also take care of class registers and remove the need to manually maintain a class register, which sometimes is not a true reflection of who was/was not in class.

The testing conducted considered a very small population, it is yet to be seen how such a system will perform with large populations in respect to time. Historically client/server systems have performed fairly well when subjected to large populations. Virtualization has also proved to improve the performance of heavy duty client server system and is also recommended for this system.

7.4 CONCLUSION

In conclusion, this research has shown that using the client/server model it is possible to introduce a biometric system to aid in examination authentication. In addition it has shown that the perception that biometrics is only for use by law enforcement agencies is fast fading away and more and university students with the right information are willing to take up the technology.

The study has also shown that with slight improvement such a system can be deployed on the campus wide network and be used to administer examinations from a central point.

The study has however failed to show the behavior of this system under heavy load characteristics as would be the case in the real environment.

REFERENCES

- BioLink, *BioLink fingerprint biometrics in Maldivian passports*, visited on 12th May 2010
<http://www.biolinksolutions.com/print.asp?nItemID=162>.
- Bolle, R.M.; Connel, J.H. and Ratha, N.K. , 2002. *Biometrics Perils and Patches*. Elsevier - Pattern Recognition 35: 2727-2738.
- Bolle R , Connell J , Pankanti S, Ratha N, and Senior A 2004 ,*Guide to Biometrics*, Springer
- Bowman LM, *Tampa drops face-recognition system*, Available: http://www.news.com/Tampa-drops-face-recognition-system/2100-1029_3-5066795.html. [23rd June 2010]
- Cavoukian, Ann. 1999 , *Biometrics and Policing. Comments from a Privacy Perspective*. Information and Privacy Commissioner, Ontario.
- Cavoukian, Ann. 2007, *Biometric Encryption Chapter from the Encyclopedia of Biometrics*, Office of the Information and Privacy Commissioner, Toronto, Ontario, Canada.
- CBC News, Biometric ID cards coming for airport worker[online] Available : <http://www.cbc.ca/technology/story/2006/11/10/airports-card.html>, [12th May 2010]
- Chen, C and Wang, P 2005 Eds. *Handbook of Pattern Recognition and Computer Vision*, World Scientific Publishers,
- Chama, Nimitha, 1999, *Fingerprint Image Enhancement and Minutiae Extraction*, Clemson University.
- Department of Justice- USA , *FBI- AIAFIS [Online]* Available: http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis [13th November 2010]
- Ekman, P and Rosenberg, EL 1997 Eds. *What the Face Reveals: Basic and Applied Studies of Spontaneous Expression Using the Facial Action Coding System (FACS)*, Oxford University Press.
- Jamieson R, Stephen G and Kuma S 2005, *Fingerprint identification: an aid to the authentication process*, Information Systems Audit and Control Association
- Langenderfer, J and Linnhoff, S 2005, *The Emergence of Biometrics and Its Effect on Consumers*, The Journal of Consumer Affairs, Vol. 39, No. 2.
- Murphy, S and Bray F, *Face recognition devices failed in test at Logan*, Available: http://www.boston.com/news/local/articles/2003/09/03/face_recognition_devices_failed_in_test_at_logan/[23rd June 2010]
- Nanavati, S., Thieme, M., Nanavati, N.2002: *Biometrics: Identity Verification in a Networked World*, John Wiley & Sons, New York .
- Ratha, N J. H. Connell and R.M. Bolle,2001: *Enhancing security and privacy in biometrics-based authentication systems*, IBM Systems Journal 40(3), 614–634
- Ross, A , Nandakumar, K and Jain A 2006 *Handbook of Multibiometrics*, International Series on Biometrics Springer.
- Zhao W, Chelappa R 2006 , Eds., *Face Processing: Advanced Modeling and Methods*, Elsevier.

APPENDIX A: SAMPLE CODE

BioBean Class Module

```
package bio;

import javax.annotation.Resource;
import javax.faces.application.FacesMessage;
import javax.faces.context.FacesContext;
import javax.persistence.EntityManager;
import javax.persistence.PersistenceContext;
import javax.transaction.UserTransaction;

/**
 *
 * @author philip
 */
public class BioBean {

    @PersistenceContext(name = "autotrackPU")
    private EntityManager em;
    @Resource
    UserTransaction utx;
    private Users buser = new Users();
    private Attendance attendance = new Attendance();

    private String vstudentno = new String();
    private String fp1 = new String();
    private String fp2 = new String();
    private String sessionID = new String();

    /** Creates a new instance of BioBean */
    public BioBean() {
    }

    public void saveExamAttendance() {
        try {
            utx.begin();
            attendance.setStudentId(vstudentno);
            attendance.setExamDate(new java.util.Date());
            em.persist(attendance);
            utx.commit();
            attendance = new Attendance();
            fp1="";
            fp2="";
            vstudentno = "";
            sessionID="";
            FacesContext.getCurrentInstance().addMessage("message", new FacesMessage("Student enrolled
successssfully"));
            //return "success";

        } catch (Exception expp) {
            expp.printStackTrace();
            FacesContext.getCurrentInstance().addMessage("message", new FacesMessage("Enrollment of the
student failed"));
        }
    }
}
```

```

    //return "fail";
}

public void saveBio() {
    try {
        utx.begin();
        em.persist(buser);
        utx.commit();
        buser = new Users();
        FacesContext.getCurrentInstance().addMessage("bio_form", new FacesMessage("Student enrolled
successfully"));
        //return "success";

    } catch (Exception exp) {
        exp.printStackTrace();
        FacesContext.getCurrentInstance().addMessage("bio_form", new FacesMessage("Enrollment of the
student failed"));
    }

    //return "fail";
}

public String loadFP()
{
    try{
        Users u = new Users();
        u = (Users)em.createQuery("select u from Users u where u.studentNo = " + vstudentno +
""").getSingleResult();
        fp1 = u.getBiodata();
        return "enroll.jsp";
    } catch (Exception e){
        e.printStackTrace();
        FacesContext.getCurrentInstance().addMessage("bio_verify", new FacesMessage("Student not
enrolled"));
    }
    return "enroll.jsp";
}
/**
 * @return the buser
 */
public Users getBuser() {
    return buser;
}

/**
 * @param buser the buser to set
 */
public void setBuser(Users buser) {
    this.buser = buser;
}

/**
 * @return the vstudentno
 */
public String getVstudentno() {
    return vstudentno;
}

```

```

/**
 * @param vstudentno the vstudentno to set
 */
public void setVstudentno(String vstudentno) {
    this.vstudentno = vstudentno;
}

/**
 * @return the fp1
 */
public String getFp1() {
    return fp1;
}

/**
 * @param fp1 the fp1 to set
 */
public void setFp1(String fp1) {
    this.fp1 = fp1;
}

/**
 * @return the fp2
 */
public String getFp2() {
    return fp2;
}

/**
 * @param fp2 the fp2 to set
 */
public void setFp2(String fp2) {
    this.fp2 = fp2;
}

public String getSessionID(){
    return sessionID;
}

public void setSessionID(String sessionID) {
    this.sessionID= sessionID ;
}

/**
 * @return the attendance
 */
public Attendance getAttendance() {
    return attendance;
}

/**
 * @param attendance the attendance to set
 */
public void setAttendance(Attendance attendance) {
    this.attendance = attendance;
}
}

```

Verify Function

```
function fnVerify()
{
    var err
    var str1 = document.getElementById('bio_verify:fp1').value;
    var str2 = document.getElementById('bio_verify:fp2').value;

    try // Exception handling
    {
        // Verify fingerprint.
        document.objSecuBSP.VerifyMatch(str1, str2);
        err = document.objSecuBSP.ErrorCode;

        if ( err != 0 )
        {
            alert('Verification error ! Error Number : [' + err + ']');
        }
        else
        {
            if ( document.objSecuBSP.IsMatched == 0 )
            {
                alert('Verification failed !');
                return;
            }

            else
            {
                alert('Verification success !');
            }
        }
    }
    catch(e)
    {
        alert(e.message);
    }

    return;
}
```

Enroll Fingerprint

```
function fnRegister()
{
    var err, payload
    var tt = document.getElementById('bio_form:enrolltxt');
    try // Exception handling
    {
        // Open device. [AUTO_DETECT]
        // You must open device before enrollment.
        DEVICE_FDP02          = 1;
        DEVICE_FDU02          = 2;
        DEVICE_FDU03          = 3;
        DEVICE_FDU04          = 4;
        DEVICE_AUTO_DETECT    = 255;
    }
```

```

document.objSecuBSP.OpenDevice(DEVICE_AUTO_DETECT);
err = document.objSecuBSP.ErrorCode; // Get error code

if ( err != 0 ) // Device open failed
{
    alert('Device open failed !');
    return;
}

// Enroll user's fingerprint.
document.objSecuBSP.Enroll(payload);
err = document.objSecuBSP.ErrorCode; // Get error code

if ( err != 0 ) // Enroll failed
{
    alert('Registration failed ! Error Number : [' + err + ']');
    return;
}
else // Enroll success
{
    // Get text encoded FIR data from SecuBSP module.
    tt.value = document.objSecuBSP.FIRTextData;
    //document.bsppmain.template1.value = document.objSecuBSP.FIRTextData;
    alert('Registration success !');
}

// Close device. [AUTO_DETECT]
document.objSecuBSP.CloseDevice(DEVICE_AUTO_DETECT);

}
catch(e)
{
    alert(e.message);
}

return;
}

```

Capture Fingerprint

```

function fnCapture()
{
    var err
    var cfp = document.getElementById('bio_verify:fp2');
    try // Exception handling
    {
        // Open device. [AUTO_DETECT]
        // You must open device before capture.
        DEVICE_FDP02 = 1;
        DEVICE_FDU02 = 2;
        DEVICE_FDU03 = 3;
        DEVICE_FDU04 = 4;

        DEVICE_AUTO_DETECT = 255;

        document.objSecuBSP.OpenDevice(DEVICE_AUTO_DETECT);
        err = document.objSecuBSP.ErrorCode; // Get error code
    }
}

```

```

if ( err != 0 )           // Device open failed
{
    alert('Device open failed !');
    return;
}

// Enroll user's fingerprint.
document.objSecuBSP.Capture();
err = document.objSecuBSP.ErrorCode; // Get error code

if ( err != 0 )           // Enroll failed
{
    alert('Capture failed ! Error Number : [' + err + ']');
    return;
}
else // Capture success
{
    // Get text encoded FIR data from SecuBSP module.
    //document.bspmain.template2.value = document.objSecuBSP.FIRTextData;
    cfp.value = document.objSecuBSP.FIRTextData;
    alert('Capture success !');
}

// Close device. [AUTO_DETECT]
document.objSecuBSP.CloseDevice(DEVICE_AUTO_DETECT);

}
catch(e)
{
    alert(e.message);
}

return;
}

```


APPENDIX B :SAMPLE FORMS

Online Fingerprint Enrollment and Verifica

[HOME](#)
[VERIFY](#)

Enrollment Details

Student number:

First Name:

Last Name:

Year of Study:

Exam Series:

finger print

Enrollment Form

Online Fingerprint Enrollment and Verifica

[HOME](#)
[VERIFY](#)

Verification Details

Captured fingerprint

Exam code:

Enrolled fingerprint

Attendance Details

Enter Session ID:

APPENDIX C

APPROXIMATE COST OF IMPLEMENTATION UON (APROX. 10,000 STUDENTS)

ITEM	QUANTITY	COST	TOTAL
M2-S FINGERPRINT SCANNER	100	Ksh. 16,875	1,687,500
CLIENT COMPUTERS	100	Ksh. 80,000	8,000,000