



**Farzad Parvinzmir**

**Fingerprint-based Student Attendance Register**

MSc. Applied Computing and Information Technology  
Masters Thesis Report  
Department of Computer Science & Technology

Dr. Aruna Shenoy

2011/12

Thesis author consent form

AUTHOR'S NAME: FARZAD PARVINZAMIR

TITLE OF THESIS: FINGERPRINT-BASED STUDENT ATTENDANCE REGISTER

DEGREE: MASTER DEGREE

*Please read carefully and sign the following as appropriate.*

I have read and understood the University's regulations and procedures concerning the submission of my thesis.

I understand that I have already signed a declaration agreeing to my dissertations being kept in the Learning Resources Centre (LRC) when I enrolled.

We would like now, to extend this agreement by making the thesis available online. Further to this,

I AGREE AS FOLLOWS:

- That I am the author of the work.
- That I have exercised reasonable care to ensure that the Work is original, and does not to the best of my knowledge break any UK law or infringe any third party's copyright or other Intellectual Property Right.
- The LRC and BREO administrators do not hold any obligation to take legal action on behalf of the Depositor (you), or other rights holders, in the event of breach of intellectual property rights, or any other right, in the material deposited.

**DELETE ONE OF THE FOLLOWING OPTIONS AS APPROPRIATE:**

1. I hereby extend my consent to this thesis being included in the LRC as well as on BREO via online access.

AUTHOR'S PERSONAL SIGNATURE: Farzad Parvinzmir

AUTHOR'S STUDENT NUMBER: 1118797

DATE: 19 September 2012

# Acknowledgments

I would like to show my gratitude to my supervisor “Dr. Auran Shenoy” for her support and supervision.

I would like to thank Gordon Brady for his support and encouragement in this project.

Finally I would like to thank my family for their valuable support.

## Abstract:

Monitoring student attendance in the UK has become a prime concern for Universities in recent months, due to a perceived lack of accuracy in reports submitted to the UK Borders Agency and political pressure about wider immigration issues. This project proposes a biometrics-based solution to that concern which also conforms to legislative pressures on data governance and information security, but which can provide accurate, reliable data for the institution to use in future reports to UKBA. All biometric techniques obviate the need to carry a token or card, or to remember several passwords, and reduce the risk of lost, forgotten or copied passwords, stolen tokens or over the shoulder attacks. This project shall focus on using fingerprint recognition, mainly due to the low-cost of devices for deployment and high user acceptance. Fingerprint recognition has traditionally been used for data access amongst a mobile population with increasingly portable devices, but it can also be employed for monitoring purposes, and this project defines how it could be used in this context to provide a fingerprint-based student attendance register.

This project set out to overcome the drawbacks of the current attendance system, which can be fooled by “buddy swiping” of absent students’ RFID card or signing the register sheet on behalf of absentee students within a university. An application was designed within MATLAB to identify pattern in data, extract vectors from a fingerprint image and map values to the new area, then to verify a student who swipes his fingerprint against those values. The requirement was to make this system work asynchronously so that constant internet and database connections are not required, to deliver outstanding rates of accuracy, and to ensure this could work on machines with very low computing power so that it can be utilized in mobile devices in future.

The delivered application uses the Principal Component Analysis method to compare fingerprints with the new form of harmonized data defined by eigenvectors and eigenvalues in  $n$  dimensions. This high-speed method uses the

lowest computational power to deliver accurate results through making a closest match against stored values. This application has potential to be employed as a modular add-on by a University student monitoring system or connect to its database and transfer data.

## Keywords:

Fingerprint Identification, Principal Component Analysis, MATLAB, eigenvector, and Euclidean distance

# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>10</b>
1.1	Aims and Objectives .....	11
1.2	Problem Statement.....	12
1.3	Project Significance.....	13
1.4	Project Barriers.....	13
1.4.1	Fingerprint Perception.....	13
1.4.2	Ethical issues:.....	13
1.5	Project Risk .....	14
1.6	Layout of this report .....	14
1.7	Summary.....	14
<b>2</b>	<b>Literature Review .....</b>	<b>16</b>
2.1	Introduction .....	16
2.2	What factors should a University FR system consider? .....	16
2.3	Critical comparison.....	17
2.4	Is one type of hardware better than another? .....	18
2.5	Which role should be used?.....	18
2.5.1	Verification (one-to-one) .....	18
2.5.2	Identification (one to many).....	19
2.6	What approach should be taken? .....	19
2.7	Benefits .....	20
2.8	Concerns .....	20
2.9	Other factors.....	21
2.10	Summary .....	22
<b>3</b>	<b>Requirements.....</b>	<b>23</b>
3.1	System Approach .....	23
3.2	Hardware .....	26
3.3	Software .....	26
3.4	Deliverables.....	26
3.5	Summary.....	27
<b>4</b>	<b>Market Survey and Analysis .....</b>	<b>28</b>
4.1	Survey Analysis .....	28
4.1.1	Quantifying the problem .....	28
4.1.2	Assessing the proposed solution.....	31
4.1.3	Time impact.....	34
4.2	Summary.....	36
<b>5</b>	<b>Design .....</b>	<b>37</b>
5.1	Deliverable 1 – Create Dataset using suitable fingerprint SDK .....	39
5.2	Refine dataset to desired parameters .....	40
5.3	Apply PCA process to dataset to get eigenvector map .....	42
5.3.1	Methodology .....	42
5.3.2	Apply a translation vector .....	43
5.3.3	Determine the mean of the data .....	43
5.3.4	Calculating the covariance matrix.....	44
5.3.5	Extracting the eigenvalue and eigenvector .....	45
5.3.6	Develop comparison algorithm-Euclidean Distance.....	46
5.4	Develop user interface .....	46
5.5	Summary.....	49
<b>6</b>	<b>Implementation .....</b>	<b>50</b>
6.1	Development .....	51

6.1.1	Intro .....	51
6.1.2	Main Menu .....	51
6.1.2.1	Creating Database .....	52
6.1.2.2	Identification .....	56
<b>6.2</b>	<b>Summary .....</b>	<b>57</b>
<b>7</b>	<b>Testing .....</b>	<b>58</b>
7.1	Performance .....	60
7.2	Improvement .....	61
7.3	Summary .....	62
<b>8</b>	<b>Conclusion.....</b>	<b>63</b>
<b>9</b>	<b>Reference.....</b>	<b>65</b>
<b>10</b>	<b>Appendices .....</b>	<b>67</b>
<b>10.1</b>	<b>Appendix A.....</b>	<b>67</b>
10.1.1	Market survey – Lecturer .....	67
10.1.2	Market survey questionnaires – Student .....	71
<b>10.2</b>	<b>Appendix B – Gantt chart.....</b>	<b>75</b>
<b>10.3</b>	<b>Appendix C – Matlab Coddng.....</b>	<b>76</b>
<b>10.4</b>	<b>Appendix D - Interim Report .....</b>	<b>82</b>
<b>10.5</b>	<b>Appendix E – Project Proposal .....</b>	<b>89</b>
<b>10.6</b>	<b>Appendix F – User Guide.....</b>	<b>90</b>
<b>10.7</b>	<b>Appendix G – Project Poster .....</b>	<b>92</b>

## List of the Figures

Figure 2.1: Maltoni’s process of verification .....	18
Figure 2.2: Maltoni’s process of identification .....	19
Figure 4.1: Rate of buddy swiping or signing register sheets on behalf of absent student .....	29
Figure 4.2: Lecturers’ opinion of “buddy swiping” and “buddy signing” .....	30
Figure 4.3: Do you utilise the University wall-mounted swipe system?.....	30
Figure 4.4: Percentage of lecturers answering .....	31
Figure 4.5: Fingerprint awareness rate between students.....	32
Figure 4.6: The rate of acceptance of students to give their Fingerprint.....	32
Figure 4.7: Rating student agreement with statements about fingerprint identification .....	33
Figure 4.8: the rate of students’ concerns.....	34
Figure 4.9: Average of teaching hours .....	34
Figure 4.10: Average of student in each lecture.....	35
Figure 4.11: Lecturer opinion about existing attendance system in UoB .....	35
Figure 5.1: Fingerprint application process.....	38
Figure 5.2: The overview of system.....	38
Figure 5.3: Identification progression .....	39
Figure 5.4: A sample fingerprint captured by Microsoft FP scanner .....	41
Figure 5.5: Original captured images before cropping (355×390 pixels) .....	41
Figure 5.6: Cropped fingerprint images (64×64 Pixels) .....	42
Figure 5.7: GrFinger application interface for capturing fingerprints.....	42
Figure 5.8: the vectored image compare with the original one .....	43
Figure 5.9: The new map of data.....	45
Figure 5.10: Example of measuring minimum distance amongst stored data.....	46
Figure 5.11 – Log on page.....	47
Figure 5.12 – Main Menu of System.....	47
Figure 5.13 – Choosing the appropriate database and recent captured fingerprint.....	48
Figure 5.14 – the identification page displays student ID, name, and course .....	48
Figure 6.1 – intro of the system.....	51
Figure 6.2 – system will show the wrong password.....	51
Figure 6.3 – Main menu of the system will show three items.....	52
Figure 6.4 – System asks for choosing datasets directory to create a built-in database.....	53
Figure 6.5 – A sample datasets with 100 fingerprint images .....	53
Figure 6.6: A plot of vectored matrix of 100 fingerprint images .....	54
Figure 6.7: A plot of mean of Vectored matrix with 100 images.....	54
Figure 6.8: An eigenvalue plot of 100 fingerprint vectored matrix .....	54
Figure 6.9: A scatter plot of eigenvector for 100 fingerprints.....	55
Figure 6.10: An screenshot of database creation and its elapsed time .....	55
Figure 6.11: Prompt window.....	56
Figure 6.12 – a schematic of calculating Euclidean distance .....	56
Figure 6.13: Result of identification process.....	57
Figure 6.14: Exit command screenshot .....	57
Figure 7.1 – elapsed time to create a new database from different size of datasets .....	60
Figure 7.2 – elapsed time for identification fingerprint .....	61
Figure F.1: Matlab screenshot.....	90
Figure F.2: Intro screenshot.....	90
Figure F.3: Main menu of system with 3 options.....	90
Figure F.4: Select a datasets directory.....	91
Figure F.5: Identification result screenshot.....	91



# Chapter 1

---

## 1 Introduction

Innovative technologies together with mobility have increased the requirement to have more protected and reliable access through predefined gateways. Many organizations are trying to identify accurate, safe, and reliable techniques to protect access rights to their existing services or operation. Biometrics is one answer to these concerns.

Biometrics, especially in information technology, encompasses methods to analyse physical and behavioural identities to extract unique features for identification or monitoring purposes. Various physical features including faces, eyes, fingers, hands, veins, ears and teeth can be used by this technology, and characteristics such as gaits or voice patterns are also being investigated and analysed as part of the wider biometrics field. Biometrics offers a secure method of access to sensitive services and obviates the need to carry a token, card or to remember several passwords. Biometric techniques also reduce the risk of lost, forgotten or copied passwords, stolen tokens or over the shoulder attacks, yet despite these obvious benefits, most biometric techniques are not pervasive in everyday life.

There are some significant reasons for this. The cost of deployment of many techniques is very high; potentially requiring specialist analytical software and machines with the computing power to run it on. There is a lack of standardisation of many methods, and the wide variance of algorithms results in different performance levels from comparable equipment. Additionally, end users may refuse to use some types of biometric identification due to possible hygiene misunderstandings, cultural differences or ethical issues.

The exception to this antipathy towards biometrics is fingerprint recognition (hereafter referred to as FR); a well-known technique to identify individuals by comparing fingerprint features with a pre-defined template which most people are familiar with nowadays. FR is widely used today in

places such as airports and the legal system, and it is built in to devices such as laptops. More work has been found within the literature, which aims to quantify the best methods and algorithms of FR than any other biometric system; however there is still not a categorical standard algorithm for FR systems. Despite this, identification or authentication through FR still has three main advantages(Maltoni, Maio et al. 2009, Newman 2010):

- Low cost of deployment (cost effective)
- Simple to implement and use
- User must be physically available at the point of identification or verification

This technique can be used for employee monitoring or in the legal system for criminal identification and most significantly, for time and attendance schemes. Monitoring student attendance has become a prime concern for UK universities in recent months because political pressure on the UKBA has focused attention on absentee students, leading to increased auditing of the University of Bedfordshire's Tier 4 status (UKBA July 2012). Many universities use paper-based or smart card systems to check the students' attendance. Other projects have been trying to design an attendance system for universities without taking into account recent issues; however this project, unlike the existing schemes, is trying to improve data accuracy by adding a fingerprint-based register and using a series of techniques to provide a reliable, optimal, and accurate identification procedure. The strength of this project is in taking a different approach for image processing by reducing the size of the template, making very quick comparisons for identification, and making identification work asynchronously.

## **1.1 AIMS AND OBJECTIVES**

The aim of this project is to define a new approach to, and provide an application for, monitoring student attendance by using fingerprint comparison with an unusual PCA technique to improve response time and accuracy in finding the closest match in a massive fingerprint database. The main objectives are:

- To make a dataset
- To investigate and understand current fingerprint identification methods
- To implement a method of identification using Principal Component Analysis
- To determine the accuracy rate
- To identify and improve the appropriate algorithm for data mining
- To investigate data-mining techniques and attempt to strengthen the system
- To design an appropriate interface to integrate with an existing application
- To utilise Prince2 project management techniques as part of the project development

## 1.2 PROBLEM STATEMENT

Survey and analysis of the current monitoring methods has shown that the majority of lecturers use a paper-based attendance method to keep attendance records whilst only 12% use the wall mounted RFID swipe card system available in University of Bedfordshire.

Problems that have been discovered in using the wall mounted swipe card are:

- The swipe card system is not available in all rooms
- Lecturer cannot access collected data
- The system can be fooled by students (“buddy swiping” an absent student or skipping the session after swiping).

Problems that have been discovered in using paper based registers are:

- Paper based registers are not uploaded to a centralised system, so the data is lost for analysis.
- Time taken for data collection impacts on lecturing time.
- The system can be fooled by students “buddy-signing” on behalf of absent students.

Consequently, this project proposes FR as a method to overcome these problems.

### **1.3 PROJECT SIGNIFICANCE**

The benefit of the proposed system is that it requires students to be physically present for identification. Moreover, the new system uses an innovative method to improve the accuracy and reliability of identification the identification process. Additionally, it can connect to any proprietary database and transfer data asynchronously. The provided application as an artefact will demonstrate a comparative evaluation using principal component analysis and data mining technology to deliver accurate results through making a closest match within the built-in database.

### **1.4 PROJECT BARRIERS**

This project has identified a number of barriers and constraints to deploying FR.

#### **1.4.1 Fingerprint Perception**

- Fingerprints introduce security as well as trust for organizations, governments and, individuals. However, individuals from many cultures are suspicious of being monitored by “official organisations”.
- Using fingerprint monitoring could be considered as an invasion of privacy.
- Some misconceptions exist in the general populate concerning hygiene or transfer of disease through using fingerprint devices (Newman 2010, Maltoni, Maio et al. 2009).

#### **1.4.2 Ethical issues:**

- Protection of student responses to questions where the student admits to illegal or improper behaviour.
- Social concerns such as informational privacy, physical privacy, and religious reasons
- Possible misuse of fingerprint information

## **1.5 PROJECT RISK**

The following risks to the project have been defined.

- Risk of equipment failure during project execution e.g. hardware or software failure
- Possible risk of using just one set of fingerprint scanner and related computer
- Risk of using trial application to complete design or implementation system
- Risk of data loss or theft
- Time constraint with deadline for project submission
- Risk of application compatibility
- Risk of unsuccessful project application
- Risk of missing project requirement

## **1.6 LAYOUT OF THIS REPORT**

This document has seven chapters. The first chapter comprises of the introduction, the aim and objectives, and problem statement, which must be solved in the subsequent project. Following a critical review of relevant literature in the second chapter, chapter 3 defines a set of requirements for the system. A related survey along with analysis has been shown in chapter 4, and then system design including making datasets, acquiring algorithms and prototyping will be fully described in chapter 5. Processes of implementation and testing will be placed in chapter 6. A testing of system will be prorated in Chapter 7. Chapter 8 includes conclusion, and challenges. All additional information such as questionnaires, timing plan and coding are available in Appendices.

## **1.7 SUMMARY**

This project will incorporate a fingerprint based student identification system that will complement a student attendance register system within the University of Bedfordshire. The proposed method could be executed in any of the university's lectures and practical sessions using external or portable devices without changing the existing infrastructure. Moreover, this scheme has the

potential capability to connect to any existing database and make use of related data in order to work asynchronously within the system. The collected data will be more accurate, satisfies the need of an audit trail, and can help protect the Tier 4 status of the University.

# Chapter 2

---

## 2 Literature Review

### 2.1 INTRODUCTION

Research was carried out to identify the requirements of any biometric system, and specifically of an FR system for use within the University environment, before comparing FR suitability with that of other biometric techniques. A choice of FR device had to be considered, and consideration given to the role of identification or verification, so that the best method of operation could be applied. Approaches to analysing the captured image were also researched and an approach was chosen which could be tested in the context of this project with currently available equipment. A measure of performance had to be discovered and decided upon, before benefits and concerns of FR systems could be considered.

### 2.2 WHAT FACTORS SHOULD A UNIVERSITY FR SYSTEM CONSIDER?

In designing an FR application, Newman et al (Newman 2010, Maltoni, Maio et al. 2009) have identified seven characteristics for consideration in any system, which uses biometrics for authentication of individuals. Table 2.1 shows Newman's characteristics and how they have been considered.

Table 2.1 Considered characteristics of a biometric system.

Feature	Comments
Universality: every individual should have specific the biometric feature.	A NIST report shows that there are only 98% of the population who can provide a good quality fingerprint; the other 2% would be excluded from this application.
Distinctiveness: the biometric traits should be unique and different among individuals.	It is widely accepted that although unique, fingerprints offer no greater uniqueness than most other biometric elements with the exception of voice.
Permanence: biometric features should be unalterable in different conditions and over time.	It is unlikely that a student's fingerprint will change during the life of their course.

Collectability: biometrics features can be determined quantitatively.	Whereas facial recognition needs a highly professional system, accurate lighting, subject positioning and long scan times, scanning a fingerprint is simple and can be done by small, cheap scanners without changing any of the existing infrastructure in the University.
Performance: speed of obtaining biometrics features and processing, which may define the accuracy of the recognition.	This project will negate this concern by taking off-line scans for identification away from lectures, and then making the identification time per ID in the order of a few milliseconds.
Acceptability: User acceptance of the methods employed by biometrics techniques in their daily lives.	FR, in comparison with other techniques such as iris scanning, has a relatively high user acceptance rate. To confirm this within the University environment, a question on acceptability was included in the student survey shown in Chapter 4.
Circumvention: whether biometric methods can be fooled or hacked by fraudulent methods.	Fooling fingerprint scanners is extremely difficult (O’Gorman 2002, Newman 2010). Different card readers respond to different tricks so no universal “fooling” method can be made, and there are several algorithms, which have been recommended to detect non-natural fingers. In the University, the likelihood of students circumventing the fingerprint scanner is lower than the chance of them fooling the RFID scanners or paper signatory registers.

### 2.3 CRITICAL COMPARISON

A comparison of fingerprint techniques with the other biometrics methods is given here. This comparison is completely based on the scientific literature but examples are given in an attempt to elucidate the findings (Newman 2010, Kothavale, Markworth et al. 2004). Table 1 shows a comparison of each technique’s suitability (low, medium or high) against Newman’s seven concerns.

Table 2.2: Comparison of Biometric Techniques

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Hand/finger vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H



## 2.4 IS ONE TYPE OF HARDWARE BETTER THAN ANOTHER?

The main five mechanical techniques for scanning fingerprints are capacitance, thermal, ultrasound, tactile, and optical. Optical scanners can be fooled by presentation of an image, rather than the actual finger (Maltoni, Maio et al. 2009) and they may not image a real finger properly if the finger is dirty or marked (Maltoni, Maio et al. 2009, Newman 2010). However, they are mechanically robust, less susceptible to electrostatic damage and also one of the cheapest forms to purchase. It is unlikely that a student would have an image of an absent student's fingerprint to scan, or would attempt to do so, therefore optical scanners were used throughout this project.

## 2.5 WHICH ROLE SHOULD BE USED?

To understand the role of the FR system it is vitally important to understand the difference between verification and identification.

### 2.5.1 Verification (one-to-one)

An identity is authenticated by matching the stored biometric features of a specific individual with those of the point-of-checking biometric characteristics. This process performs a one-to-one comparison in order to authorise the individual's identity. A working verification scheme only has two results, accept or reject the provided identity (Maltoni, Maio et al. 2009).

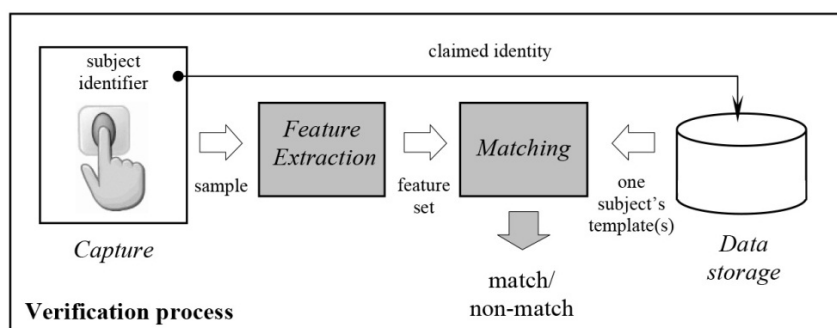


Figure 2.1: Maltoni's process of verification

### 2.5.2 Identification (one to many)

An identification scheme authenticates a person by examining all the templates in a dataset in order to find a match. It performs one-to-many evaluation in order to determine if the captured biometric features are available in the enrolled biometrics database or not. The result should return the enrolment reference, which is match to the captured biometric or indicate that individual is not enrolled in the database (Maltoni, Maio et al. 2009). Errors in this type of system are more serious, as they could potentially apply the wrong ID to the person trying to gain access. The failure modes of a functional scheme are False Acceptance Rate (FAR) where an unregistered user is given access and False Rejection Rate (FRR) where a registered user is not given access.

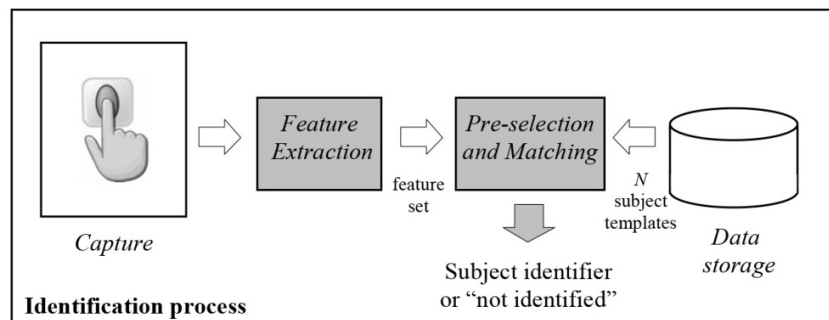


Figure 2.2: Maltoni's process of identification

In the University context, it is not suitable to require a lecturer to attend each class with a portable dataset of user IDs and matching templates. The system is not providing access control; it is simply being used to verify a student presence. Therefore the best process to use is identification, where the data capture and feature extraction (steps 1 and 2 in Maltoni's process) can take place in the lecture, but the matching process can take place later on, using the templates on the server rather than downloading them to the client.

## 2.6 WHAT APPROACH SHOULD BE TAKEN?

Yongxu et al describe a statistical approach to fingerprint image recognition using Principal Component Analysis (PCA) to extract vectors to describe the fingerprint (Wang Yongxu, Ao Xinyu et al. 2006). They tested this approach with images from the FVC database, with an effective image size of 300×200

pixels. This project follows the same approach, but tests response accuracy and time where the fingerprint image has been reduced to 64×64 pixels. This would allow a smaller database size, easier computational load, but may provide less accurate results. The process requires some manual intervention to achieve this. An image such as a tiff or jpeg file of an individual's fingerprint is captured by the provided scanner. The image is then manually resized to 64×64. A number of features are extracted from the captured fingerprint by using specific extraction algorithms and converting the features into a vector form. The newly extracted template will be saved into the database and will be used for identification or verification purposes.

## **2.7 BENEFITS**

FR is trying to increase the metrics of the security mechanisms whilst reducing the complexity of the data capture. It eliminates many, if not all, of the risks and issues associated with token-based access protocols. The major benefits of FR systems are (Cavoukian 2008, Boatwright, Luo 2007, Newman 2010):

- Fingerprint features cannot be forgotten, stolen, or lost
- It is hard to forge or share a fingerprint
- Fingerprints can be combined with token use or other ID structures, meaning they could be added to a current security scheme without changing existing infrastructure

## **2.8 CONCERNS**

Fingerprint systems need to scan “living individual” fingers for authentication process. Spoofing techniques such as latex fingerprint masks might be used for identification or verification in place of the real live finger. Although these are highly unlikely to happen in the University, the system should be designed to provide an integrated algorithm or mechanism to combat this issue. Furthermore, there are other issues, which are listed in the following (Newman 2010, Cavoukian 2008, Boatwright, Luo 2007, Mordini, Petrini 2007, R. Heckle, S. Patrick et al. 2007):

- Storing and transmitting biometric data using encryption – standards have been defined for encrypting biometric data (Tilton 2009) ISO/IEC19785-1, many software packages do not support these standards. This was a concern, which may have had significant impact on the progress of this project, therefore it was decided that all the data would remain unencrypted.
- Biometrics impacts on multifactor authentication strategies – the balance between “what I am” and “what I have” can change if the biometric template is stored on the token. This could impact the University if they decided to store the student fingerprint template as part of the information held on the Student’s ID card, and is not recommended as it would degrade the integrity of the captured registers.

## **2.9 OTHER FACTORS**

The system will be evaluated on a very small scale initially, but it is important to know whether it can be used across the whole institution in future. (Wang Yongxu, Ao Xinyu et al. 2006) tells us that FR systems are scalable for adoption by different sizes of organisation from small companies to national governments, so this should not be a problem. As the identification software is designed to run on a central server will make future project deployment more straightforward. The server would need to provide a client interface for use over the web, which has not been developed within this project.

Every biometric system is subject to a rate of FAR and FFR. The UK Biometrics Working Group has suggested that relative biometric accuracy rates can be classified as shown in Table 1. This project has no external guidelines on the required accuracy of captured data, and it was decided that the system should at least perform to the Medium standard in testing, given that the database size is very small.

Table 2.3: A Scheme for Understanding Relative Biometric Strengths

<b>FAR</b>	<b>Far %</b>	<b>Strength</b>
1 in 100	1.0%	Basic
1 in 10,000	0.01%	Medium
1 in 1,000,000	0.0001%	High

## 2.10 SUMMARY

Biometric technology has evolved in recent years, and FR is one of the most popular techniques because of its cost effectiveness, compact equipment and easy implementation. Compared to other methods, FR does not need large amounts of memory to store the extracted template and is not computationally expensive, which is a big advantage in data mining. Moreover, identity theft is close to impossible for FR and there is no chance of re-construction of the original sample from the extracted template.

FR methods with all its benefits would be ideally suited for adoption by Universities to employ identification amongst large number of students. (Bhargav-Spantzel, Squicciarini et al. 2010, IBG 2002, Klokova 2010, Kothavale, Markworth et al. 2004, Saraswat, Kumar 2010, Zhang, Li et al. 2010).

# Chapter 3

---

## 3 Requirements

Developing any software system requires a framework or process to follow. This project followed the Prince2 methodology, which does not specify exact methods of requirements capture, therefore a combination of survey, interview, observation, research and best practice has been used. Stakeholders were identified as Lecturers, Students, University Administration, and Gordon Brady as developer of a complementary MSc project and the UKBA. The actual requirements list captured from these stakeholders has been divided into three sub sections; System approach, Hardware and Software to produce a list of deliverables.

### 3.1 SYSTEM APPROACH

#### Captured from Interview

- The fingerprint student attendance application needs to provide a simple interface to choose whether to use an existing database or to create a new database on the system.
- Lecturers should be allowed to provide students' fingerprints for authentication process and likewise should be able to change the selected fingerprints templates folder for each lecture/practical session if required.
- An accredited lecturer should be allowed to configure student identification as required.
- The authorised user (lecturer) should be able to access all identification options
- The authorised user (lecturer) should be able to update the database
- The authorised user (lecturer) should be able to see the matched student fingerprint within the database

- The lecturer should be able to see the name and ID of the student who has been identified by the application
- All captured students fingerprints should be destroyed after leaving or graduation

#### **Captured from Survey**

- The fingerprint application must have the quickest response time in order to process students' fingerprints rapidly.
- Three user levels will be required; Lecturer, Faculty Admin, DBA Admin.
- There should be different functionalities for different user levels.
- The system should be able to deal with multiple concurrent users.
- It is possible for a student to “swipe” himself or herself as present twice in one lecture. The Student Attendance database system will filter double entry student IDs from each register.
- The system is to plug in as an additional module to the Student Attendance System, not to replace other data captures methods.
- Fingerprint scanners are not allowed in biology labs, so the system will not work for those lectures.
- Very clear user instructions; education and University policy guidelines will have to be deployed before first use of the system.
- Fingerprint scans must be secure.
- All captured students fingerprints should be destroyed after leaving or graduation

#### **Captured from Observation**

- The scanning device should be unobtrusive.
- The scanning device can ideally be portable and passed around the class.
- Data size for captured images should be <200kb so a whole dataset for a semester can be carried on a 1Gb flash memory stick.

### **Captured from Research**

- It is necessary to check the quality of captured students' fingerprints during each lecture because poor quality of the template may cause high level of FRR. To aid this, the system should display a visual representation of the captured fingerprint and provide an image quality measurement to ensure the captured fingerprint meets the required conditions.

### **Captured from Best Practice**

- The proposed application should offer functions in order to carry out identification such as access to the system, load default database, and make or choose appropriate database.
- An administrator must be able to access all system data for maintenance.
- The fingerprint student attendance application should be matched with the University of Bedfordshire network settings (clients and server). This scheme should follow maintenance policy and offer the applicable mechanisms for managing the potential errors that could occur during system operation. The application must come up with standard performance in terms of accuracy and reliability. This information was not available for this project, but it must be stated in the requirements so that it is not overlooked if real world deployment takes place.
- The authorised user (lecturer) should be able to enter any fingerprint number into the prompt message return box to perform random identification
- The system should deliver an application, user guide, fingerprint scanner, and related drivers.
- The scheme must provide data maintenance
- The scheme must supply the proper scanning module
- The scanning component must be come with BioAPI standard API



- The matcher should return the appropriate matched message for an accepted entry.
- The lecturer should be able to quit the fingerprint application

### **3.2 HARDWARE**

Sets of hardware, which will be using in this project, are:

- Microsoft fingerprint scanner
- Digital Persona fingerprint scanner for comparison
- Pentium 4 PC (University of Bedfordshire security laboratory) and AMD 64x PC (University of Bedfordshire Computer laboratory)+LAN connection
- Toshiba laptop Intel core i3+LAN connection
- MacBook Intel core i5

### **3.3 SOFTWARE**

The list of software, which will be used in this project, is as follows:

- Mathwork® Matlab R2012
- Microsoft Visual Studio ® 2008 – 2010
- Microsoft Access 2010
- Digital Persona SDK
- GrFinger 4.2 / VeriFinger / BioEnable SDK
- Java Development Kit
- Oracle 11g

### **3.4 DELIVERABLES**

1. Create Dataset using suitable fingerprint SDK.
2. Refine dataset to desired parameters.
3. Apply PCA process to dataset to get eigenvector map.
4. Develop comparison algorithm
5. Develop user interface

6. Perform tests and produce results.
7. User guide
8. Final Report
9. Poster

### **3.5 SUMMARY**

Prince 2 was a suitable method for capturing requirements, but much thought had to be given to the non-functional requirements, which were not captured from stakeholder surveys. These had to be created from experience and from known best practice.

# Chapter 4

---

## 4 Market Survey and Analysis

There are a two main ways to record students' attendance at the University of Bedfordshire (UoB); Paper-based attendance registers and wall mounted swipe cards. Monitoring student attendance has become a priority for the institution in recent months because the UKBA has focused attention on absentee students, leading to increased auditing of the University's Tier 4 status(UKBA July 2012). Other projects are addressing the design of an attendance system; this project is trying to refine these solutions with the addition of a fingerprint-based register system.

Two distinct surveys have been carried out; one polled the student body and the other polled the lecturers' opinions, to determine how effective the existing methods are in monitoring students' attendance, why they are still used if they are known to be ineffective, and to understand the likely obstacles to adopting a biometric based approach. The surveys have been distributed electronically via the SurveyMonkey website. The original questions and respondent data of these surveys can be found in Appendix A.

### 4.1 SURVEY ANALYSIS

#### 4.1.1 Quantifying the problem

This student survey was filled out by 25 UoB students from different national backgrounds. The survey shows that 52% of students have tried to swipe an absent student's card or sign a paper-based register sheet on behalf of others at some point. The responses to the question "Have you ever tried to swipe an absent student's ID (buddy swiping) or sign the register sheet on behalf of other students?" are shown in Figure 4.1 below.

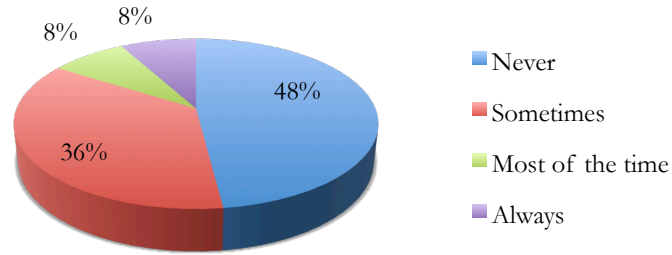


Figure 4.1: Rate of buddy swiping or signing register sheets on behalf of absent student

If we extrapolate this data to a lecture session of 100 students, the number of absent students is approximately 25 for each session- calculated as follows;

100 students supposed to be present.

- 1) Eight students ALWAYS swipe for someone else – meaning at least eight students are absent if a student only swipes/ signs for 1 other student. Follow up interview revealed that one person routinely swipes for three others, but this is discounted here to give an objective minimum.
- 2) Eight students MOSTLY swipe for someone else – It is likely that 75% of the eight are signing for one other person – therefore six absentees are marked as present.
- 3) 36 students SOMETIMES swipe for someone else – It is likely that only 25% of these students are buddy-swiping at a given lecture, which adds a further 9 students to the total.

When lecturers were asked their opinion of how widespread the “buddy signing” problem is, half of the lecturers who have participated in the survey believe that the paper-based signature method is compromised by some students signing the register sheet on behalf of absentees (Figure 4.2).

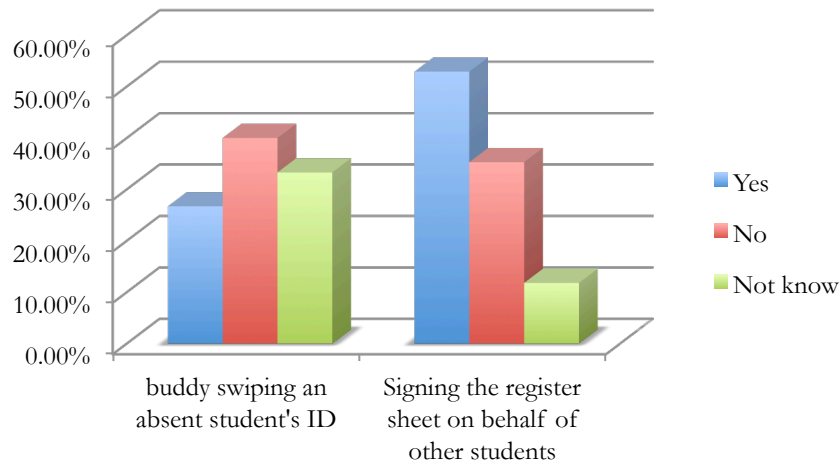


Figure 4.2: Lecturers' opinion of "buddy swiping" and "buddy signing"

Given the volume of responses, which held negative views of the integrity of the manually signed registers, lecturers were asked whether they routinely used the wall-mounted swipe card system instead. Surprisingly, 88% of lecturer respondents never use the wall mounted swipe card system (Figure 4.3). The reasons given for this are as follows -

- Cannot access the data of swipe card system (Integrity - Unable to see resultant data for proofing)
- The swipe card device is not installed in all rooms (Availability)
- Some devices do not work properly (reliability)
- There are no instructions for using swipe card system (usability)
- The system is being fooled by students (integrity)

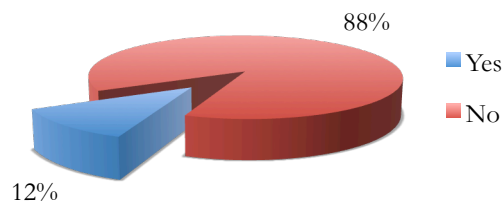


Figure 4.3: Do you utilise the University wall-mounted swipe system?

It can be concluded that many lecturers do not feel that there is any accurate way of using the existing data capture systems for students to self-record their attendance. Therefore the only trusted way to capture the data using existing technology within the university would be for the lecturer to physically call the attendance register. When asked what problems were encountered generally with taking attendance in teaching sessions (Figure 4.4), there were a variety of responses:

- Time taken for registers takes away from time for lectures
- The time taken for re-entering the manual data into a computer system as an administration task (double entry)
- Problem with inserting data manually into computerised systems
- Difficulty finding accurate register sheets with correct student names in correct groups

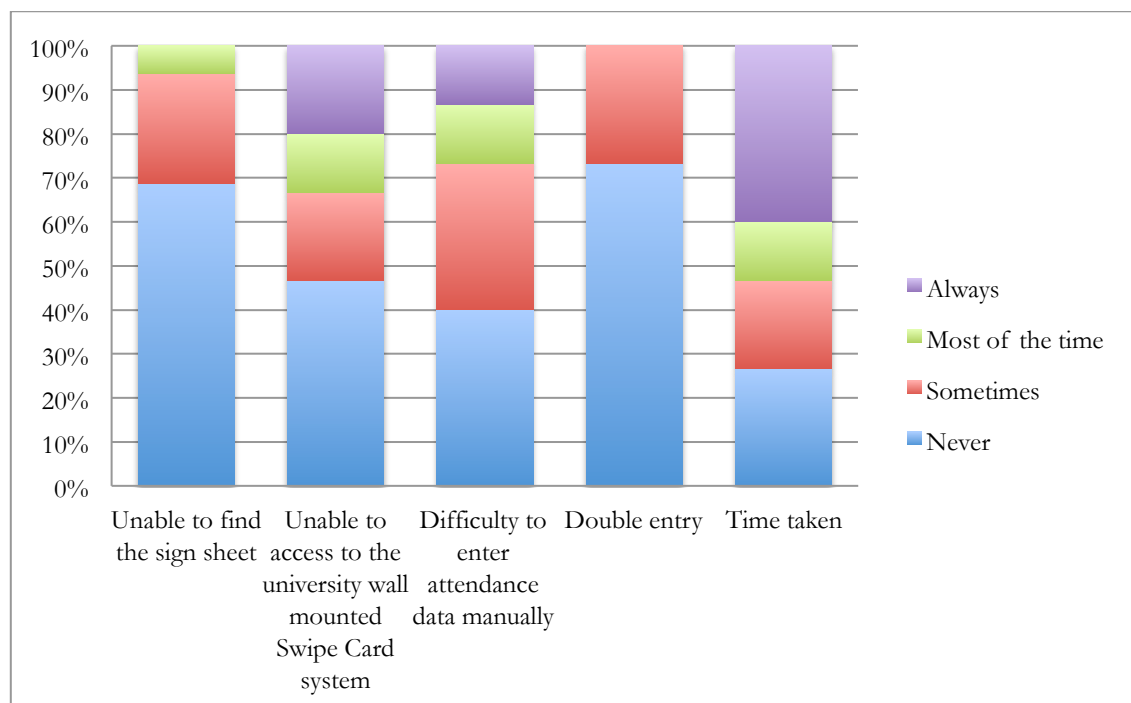


Figure 4.4: Percentage of lecturers answering, “What difficulties do you encounter with recording student attendance?”

#### 4.1.2 Assessing the proposed solution

Student perception of biometrics is a crucial potential limitation in the acceptance of any proposed fingerprint scanning solution. Students, who do not trust the technology, or the way it is used, may take measures to avoid using it or simply ignore it.

It is necessary to make a clear definition and explain the fingerprint advantages for those who are not familiar with fingerprint to reduce avoidance of using it. Regarding fingerprint awareness amongst students, more than 68% of students who responded have some knowledge of fingerprint capture methods (Figure 4.5). It should be noted here that the majority of students who responded might be from the CATS faculty, so this could be an abnormally high result.

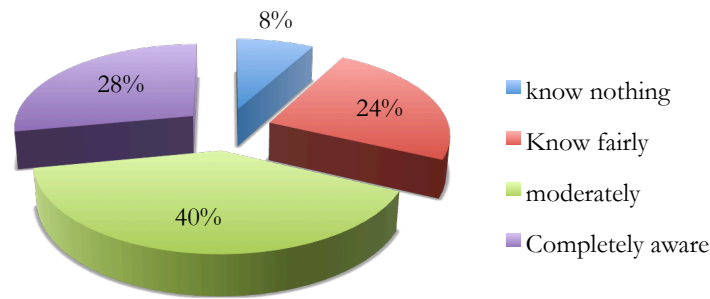


Figure 4.5: Fingerprint awareness rate between students

The majority of respondents stated that they would be happy to give their biometric data to the university to record attendance by means of fingerprint scanning (Figure 4.6) but this was far from a unanimous decision. Almost 1/3 of students stated that they would not be happy for this to happen. Further discussion between the author and the University Registry indicated that the University would be within its legal rights to insist on such data being held and used, but coercing students into using a poorly explained or understood system is likely to lead to rapid failure of the project.

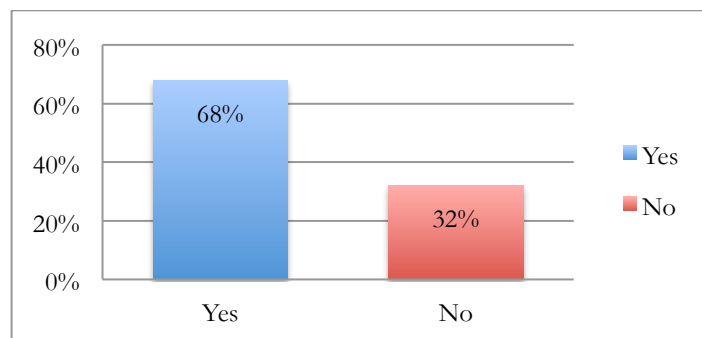


Figure 4.6: The rate of acceptance of students to give their Fingerprint for recording attendance

It was therefore necessary to understand the reasons behind the students' reluctance to the use of fingerprint scanning. Students were asked to respond to various issues around fingerprint usage by rating their agreement or disagreement with each statement. The results can be seen in figure 4.7 and 4.8 below.

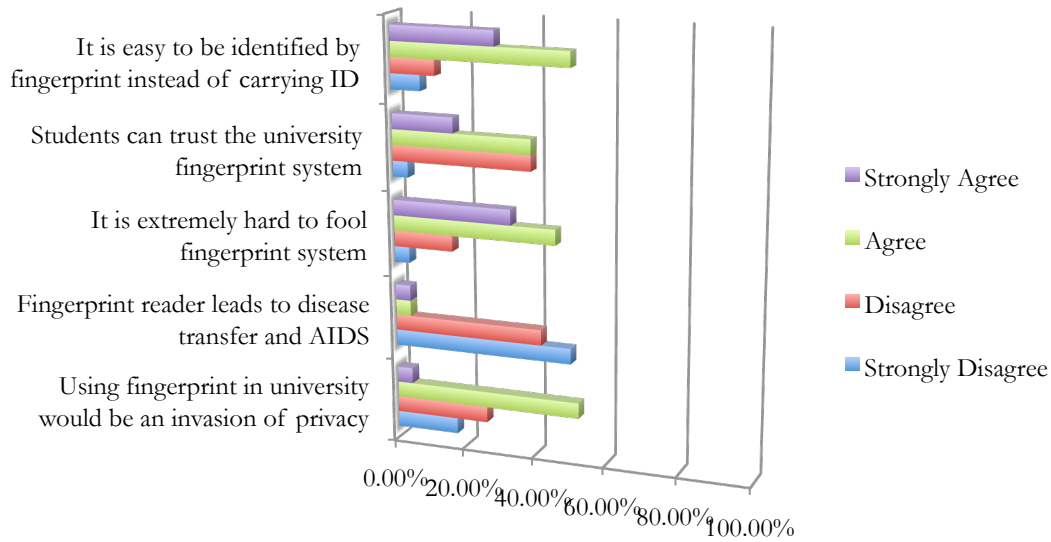


Figure 4.7: Rating student agreement with statements about fingerprint identification

The biggest concern is that two students believe that scanners can spread disease or AIDS. A focused education process may be needed to overcome difficulties such as this at the student enrolment point in order for the student to be reassured. 52% of students were concerned about invasions of privacy through utilization of the fingerprint system. This project requires a good terms and condition for covering the student concern and also describes what will happened for fingerprints template after leaving the university e.g. removing the fingerprint template from database after graduation.



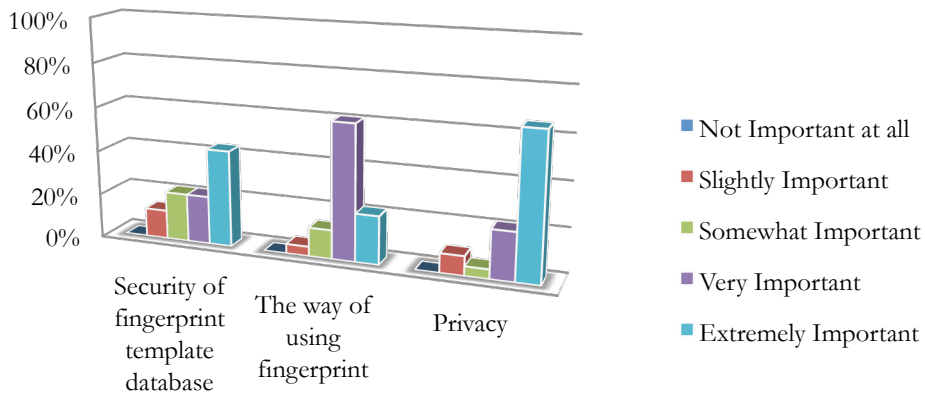


Figure 4.8: the rate of students' concerns

Other issues, which were asked in the survey, concerned the security of the biometric template. To overcome trust issues, this project has to fully explain the privacy policy as well as the way templates will be stored, used, protected and destroyed. For instance, the entire fingerprint template will be using only for recording student attendance.

### 4.1.3 Time impact

17 lecturers of different UoB faculties were surveyed to find their attitudes to time spent recording attendance and the integrity of the systems used. The majority of respondents have taught more than 10 hours a week in the last academic years (Figure 4.9) and more than 47% of lecturers have got over 51 students in their lecture whilst 17.6% of the lecturers have taught to above 100 students (Figure 4.10).

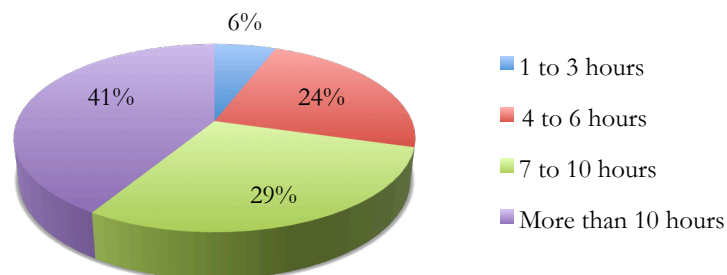


Figure 4.9: Average of teaching hours

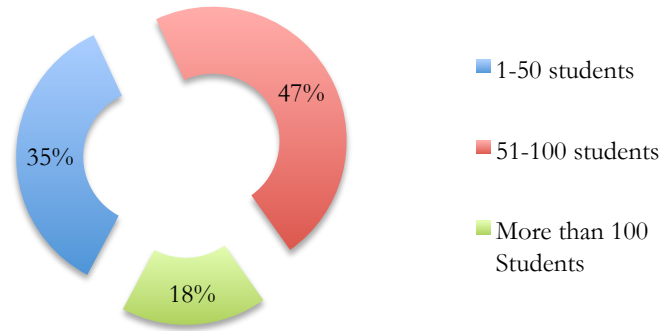


Figure 4.10: Average of student in each lecture

It is therefore vital that any system of recording attendance either has to be so quick that it reduces the current amount of time lost or else it has to not involve the lecturer in general.

This explains the popularity of the current paper-based registers. The lecturer simply hands out the register at the beginning of the class, and collects it at the end, with a total time cost of approximately one minute. The biometric system proposed must therefore match or improve on that performance. It is quick and convenient for the majority of the lecturers to ask students to scan their finger in the fingerprint device in lecture or practical.

Although the majority of lecturers agree with the possibility of fooling the paper-based system or swipe card system (Figure 4.11), this analysis shows that they persist in using it because it has the least impact on teaching time whilst complying with the minimum standards required by the institution.

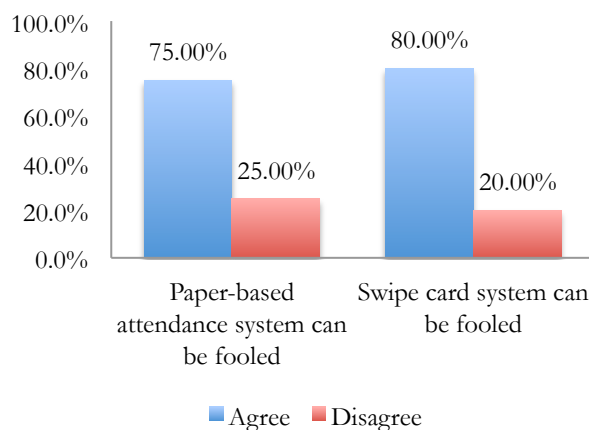


Figure 4.11: Lecturer opinion about existing attendance system in UoB

## 4.2 SUMMARY

Analysing the survey shows that 52% of students have tried to swipe an absent student's card or sign a paper-based register sheet on behalf of others at some point. The student survey displays 32% of students do not prefer to be identified by fingerprint owing to the lack of knowledge of FR. Hence, it needs to set up workshop in order to give useful information to students about fingerprint method. However, a big concern is trust to the university fingerprint system. The survey shows 46% of students do not trust to the proposed method.

The aim of lecturer survey was trying to qualify the responders. The majority of responders were lecturers or senior lecturers with the rate of 94%. There were a set of question about the number of hours and students for each lecture or practical session. These questions have been designed to clarify how hard would it be to monitor students' engagement for each lecturer during the academic year with different number of teaching hours and students. Two methods – wall mounted swipe card and paper register - are available at the University of Bedfordshire for monitoring student engagement. Surprisingly, none of lecturers using the wall-mounted swipe card system, which are provided in lectures rooms owing to its problems. Hence, the only method for monitoring attendance is paper-based register. 75% of responders believe that both methods – RFID card and especially Paper register – can be fooled during their lectures/practical sessions. Nevertheless, lectures have to use the paper register because they are responsible for their lectures. Half of the lecturers deprecate time taken of paper-register as well. Furthermore, 53% of responders said the paper-based method is time-consuming process most of the time and it shows us another pitfall of the current method. We can conclude that the University needs an accurate and reliable monitoring system to cope with the current problems along with deploying very clear user instructions; education and University policy guidelines before first use of the system.

# Chapter 5

---

## 5 Design

In this Chapter, the high level view of the system is given, showing how it must integrate with existing infrastructure, and the process to be followed in using the application. The mechanism of creating datasets and capturing the principal components of a fingerprint are explained, before describing how the principal components are analysed through the use of eigenvectors and Euclidean distance. Finally, a demonstration of the design of the prototype application is presented with accompanying screen shots.

A lecturer should access the fingerprint attendance application by logging into the new web-based student monitoring system, which has been created in parallel with this project by Gordon Brady as a complementary body of work. The Fingerprint Student Register System works as a modular bolt-on application to the web-based monitoring student system.

In a lecture, the lecturer simply plugs in a mobile flash drive and a fingerprint scanner. The fingerprint scanner is used to scan fingerprints of all students who attend, but no verification takes place at this point, so the time impact is very little. The scanned fingerprints are saved to the flash drive by the scanner application, together with a class identifier. When the lecturer returns to an office where the fingerprint software is running, he plugs in the flash drive. The fingerprint application then scans through the saved fingerprints and makes matches with the stored database, which return the student ID. This student ID and the class identity are then sent to the student attendance system as the class register. The entire process works asynchronously, but could be used in synchronous mode if the fingerprint application were installed on the client in the lecture room. (Figure 5.1).

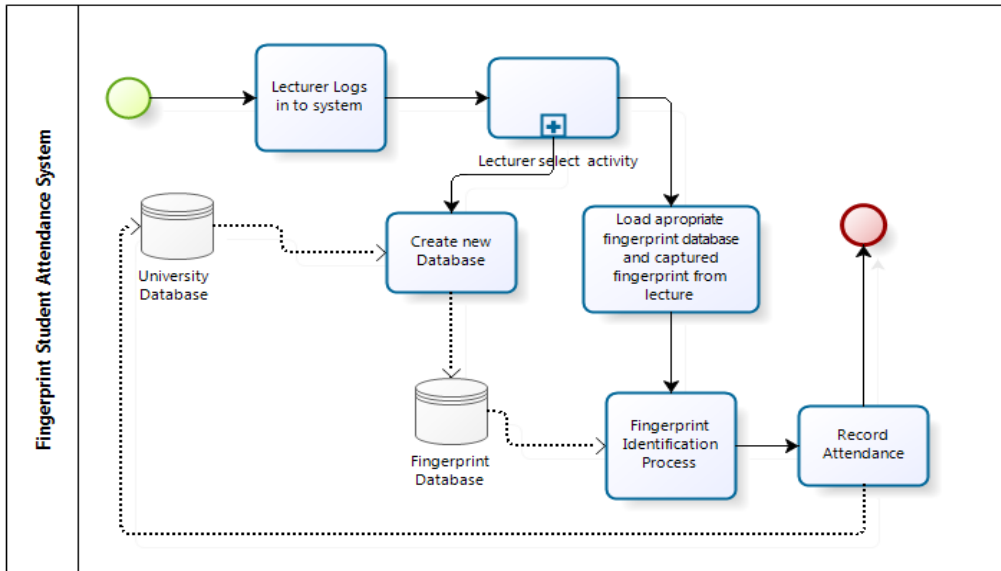


Figure 5.1: Fingerprint application process

System administrators can make a new database for new students' fingerprints, those who are recently enrolled within the university (Figure 5.2). Lecturers would then be able to ask students to swipe their finger through the fingerprint scanner in order to record student attendance.

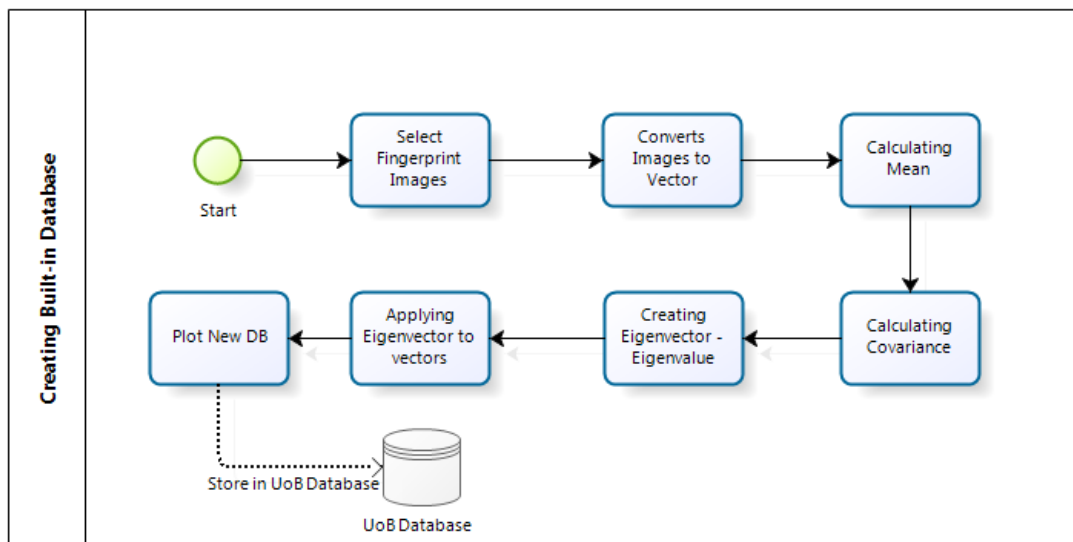


Figure 5.2: The overview of system

The fingerprint student attendance register performs the identification (one-to-many) process by using Principal Component Analysis (PCA). This system needs a build-in database in order to perform the authentication. The process consists of inserting a test fingerprint image, applying PCA, and finding minimum distance amongst the test images and enrolled images in the database (Figure 5.3).

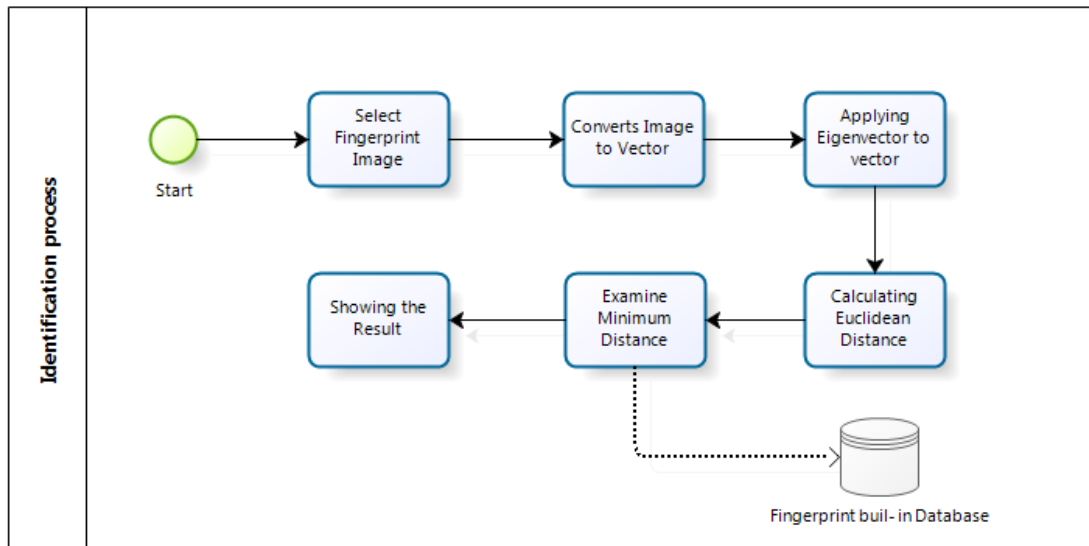


Figure 5.3: Identification progression

This system uses three different algorithms to complete the identification process. The first stage is creating a built-in fingerprint database by employing the following process:

1. Make datasets vector
2. Compute PCA
3. Apply PCA to datasets

The second step is identification. This process involves:

1. Make a test image vector
2. Apply computed PCA to test image
3. Calculate distance of provided test image with all images in database
4. Select the minimum distance

All the mentioned processes need preparation to create datasets, appropriate algorithms, and the knowledge of how to address them.

## 5.1 DELIVERABLE 1 – CREATE DATASET USING SUITABLE FINGERPRINT SDK

The first step to start the project was building a dataset. Investigations in the security lab of UoB showed that a standard database had already been made, and this provided a template so the next step was to populate the database. A set of fingerprints was collected from live subjects, and additionally a further set of 70 fingerprints were downloaded from the FVC 2002 and 2004 datasets

available online to create a suitably “noisy” background population. As explained in Chapter 3, it is a requirement identified from research that fingerprint images are of a certain quality. As the live fingerprints were captured, the GR Fingers software evaluated the quality of images and provided instant feedback on image quality.

All fingerprint images were taken by Microsoft fingerprint devices and stored as a .bmp format in a temporary folder. Each image was named as a left hand /right hand without declaring the name of participants.

All participants who were asked to take part in this project were informed that their fingerprint template will be saved anonymously and destroyed after finishing the project.

The resulting dataset comprised the following:

- Right and left index finger of faculty staff (12 fingerprint images)
- Index finger of each hand from Business student (2 fingerprint images)
- Index, middle, and ring finger of each hand from a Applied Computing and IT student (6 fingerprint images)
- All fingers of the project designer (10 fingerprint images)
- 70 anonymous images from FVC.

## **5.2 REFINE DATASET TO DESIRED PARAMETERS**

The size of each fingerprint image on disk was 140KB - 355×390 pixels. The sample-captured image is shown in figure 5.4, which was provided by the GrFinger X sample application. This software also stored an extracted feature of each scanned finger into a default Microsoft Access database with an auto numbering feature.

All images had been cropped and resized for placing into the new datasets. The best size for processing in Mathwork MATLAB software was between 30×30 pixels to 200×200 pixels, dependent upon the number of dataset files and how much further processing on them would be required. The purpose of this

project was to determine whether a very small image size resulted in too many errors. Therefore, all images were resized to 64×64 pixels.

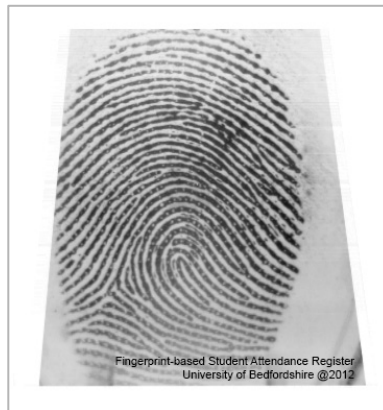


Figure 5.4: A sample fingerprint captured by Microsoft FP scanner

64×64 Pixels images were selected because the effective part of the original pictures varied for different fingers, and this compromise gave the best data quality but the smallest size of database. The application used for capturing the fingerprint, GR Finger, was developed in Java. Some investigation took place into modifying the Java code to create and refine the image in one transaction, but this was abandoned due to time constraints.

All sample fingerprint images were cropped and resized by Adobe Photoshop CS6. The process of cropping and resizing is listed in the following:

- Cropping image from 355×390 pixels to 180×180 pixels in order to have an effective area of each image (Figure 5.5)
- Resizing image to 64×64 pixels (Figure 5.6)
- Saving as a tiff format



Figure 5.5: Original captured images before cropping (355×390 pixels)



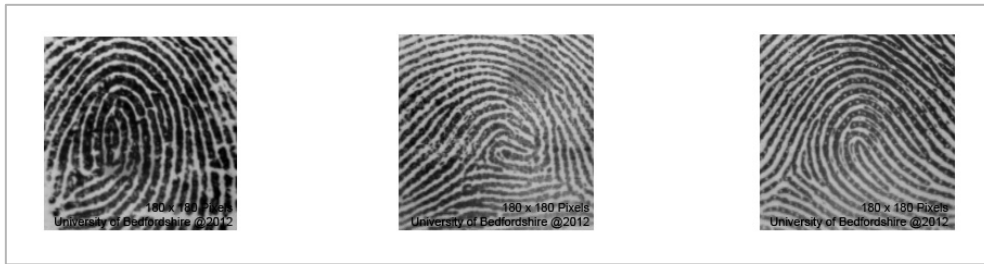


Figure 5.6: Cropped fingerprint images (64×64 Pixels)

The extra fingerprint images from external databases such as FVC2004, FVC2000, etc. were also cropped and resized in the same way to give a standardised dataset with enough images to create data “noise.”

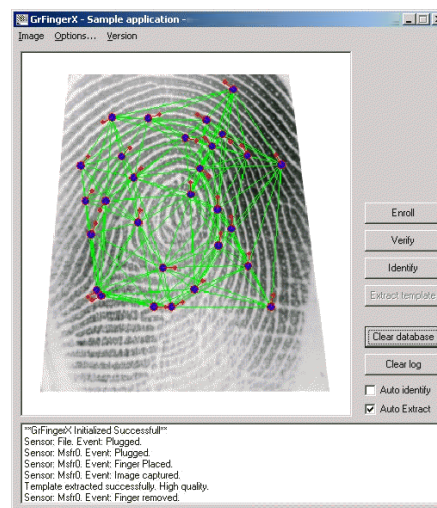


Figure 5.7: GrFinger application interface for capturing fingerprints

## 5.3 APPLY PCA PROCESS TO DATASET TO GET EIGENVECTOR MAP

### 5.3.1 Methodology

PCA is a technique of analysis to reduce the size of stored data without losing the important data itself. It brings compression as well as noise filtering and data can be classified better. This technique was first described in 1901 and many computational processes use PCA in order to achieve an accurate result. The process of Principal Component Analysis is to apply a translation vector to all the images in the dataset, then to determine the mean of the data before calculating the covariance matrix and finally extracting the eigenvalue and eigenvector to map them to a new space (Wang Yongxu, Ao Xinyu et al. 2006, Zhengmao Ye, Yongmao Ye et al. 2007).

### 5.3.2 Apply a translation vector

Each fingerprint image has been standardised at  $64 \times 64$  pixels, which was defined in the datasets section. After inserting the image, the result was a  $64 \times 64$  matrix. Applying a translation vector to this image helps the system to convert images into only one line (in this case  $1 \times 4096$ ) for database storage. The following example will show how it works on images.

Example:

Assuming a  $3 \times 3$  matrix, the created vector would be as follows;

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{bmatrix} \Rightarrow Av = [1 \ 1 \ 1 \ 2 \ 2 \ 2 \ 3 \ 3 \ 3]$$

The fingerprint images were translated and placed into a new matrix by this method. The schematic of vectored image compared with the original one is shown in figure 5.8.

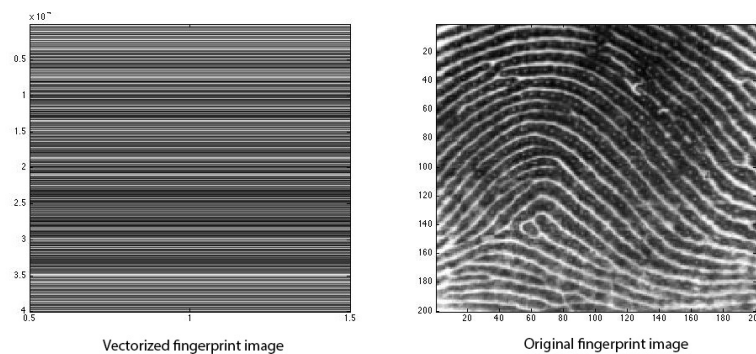


Figure 5.8: the vectored image compare with the original one

### 5.3.3 Determine the mean of the data

The first step in PCA is subtracting the mean of inserted  $m \times n$  matrix in order to adjust data. The average matrix  $\Psi$  will be calculated from original matrix, and then subtracted from the fingerprints ( $\Gamma_i$ ) and stored in  $\Phi_i$  (PISSARENKO 2002, Turk, Pentland 1991, Zhengmao Ye, Turner 2007, Wang Yongxu, Ao Xinyu et al. 2006):

$$\Psi = \frac{1}{M} \sum_{n=1}^M \Gamma_n$$

$$\Phi_i = \Gamma_i - \Psi$$

For example, assuming  $N$  images with  $m$  pixel, which have been converted to vectors; the new  $D$  matrix with  $N \times m$  is:

$$D = \begin{bmatrix} 160 & 142 & \dots & 265 & 233 & \dots & 257 \\ 121 & 153 & \dots & 223 & 212 & \dots & 268 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 132 & 154 & \dots & 121 & 236 & \dots & 234 \end{bmatrix}_{N \times m}$$

The first step in PCA is to transfer the original data of the matrix to the mean of the data. The mean image from each image of the dataset (each row of matrix  $D$ ) can then be subtracted to create the mean centred data vector. Suppose that the mean centred image is:

$$\Psi = [140 \quad 125 \dots 121 \quad 215 \quad \dots \quad 250]$$

The result would be as shown in the formula and graphical preview in figure 5.10:

$$\Phi = \begin{bmatrix} 20 & 17 & \dots & 144 & 18 & \dots & 7 \\ -19 & 28 & \dots & 102 & -3 & \dots & 18 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ -8 & 29 & \dots & 00 & 21 & \dots & -16 \end{bmatrix}_{N \times m}$$

### 5.3.4 Calculating the covariance matrix

Covariance formula relates measurements between two dimensions, seeing how much both dimensions change together. If a dataset comes with more than two dimensions, the result of covariance would be more than one calculated measurement. For instance, a three dimensional dataset ( $x, y, z$ ) we could determine  $cov(x,y)$ ,  $cov(y,x)$  and,  $cov(x,z)$ . In fact, for an  $n$ -dimensional dataset,  $\frac{n!}{(n-2)! \times 2}$  different covariance values can be computed.

For example, making up the covariance matrix for a three dimensional dataset would be the covariance matrix with 3 rows and 3 columns, and the values like this:

$$C = \begin{bmatrix} cov(x, x) & cov(x, y) & cov(x, z) \\ cov(y, x) & cov(y, y) & cov(y, z) \\ cov(z, x) & cov(z, y) & cov(z, z) \end{bmatrix}$$

To calculate the covariance matrix, a subtracted mean is used ( $\Phi$ ) and the following formula (Turk, Pentland 1991, PISSARENKO 2002, Yonghwa Choi,

Tokumoto et al. 2011, Wang Yongxu, Ao Xinyu et al. 2006):

$$C_{ij} = \frac{1}{M} \sum_{n=1}^M \Phi_n \Phi_n^T = AA^T$$

$$L = AA^T \quad L_{n,m} = \Phi_m^T \Phi_n$$

Where  $L$  is a  $m \times m$  matrix. However, the matrix  $C$  covariance has been calculated by  $C = AA^T$  formula in order to have efficient computation. This gives a square matrix.

### 5.3.5 Extracting the eigenvalue and eigenvector

As the covariance matrix is square; it is possible to then calculate the eigenvectors and eigenvalues for this matrix. These provide useful information about the data. It is essential to know that an  $m$  dimensional matrix of data can be used to calculate  $m$  eigenvectors and  $m$  eigenvalues, and then only the first  $l$  eigenvectors are selected, so the final data set has only  $l$  dimensions. The Eigen-fingerprint would be calculated by applying feature vector  $v_{lk}$  to mean data (PISSARENKO 2002, Turk, Pentland 1991, Smith 2002, Wang Yongxu, Ao Xinyu et al. 2006).

$$U_l = \sum_{k=1}^M v_{lk} \Phi_k \quad l = 1, \dots, M$$

Where  $v$  is  $M$  eigenvectors of  $L$  and  $U$  are Eigen-fingerprints. This could be mapping the new  $n$  dimension of data into the new space (Figure5.9).

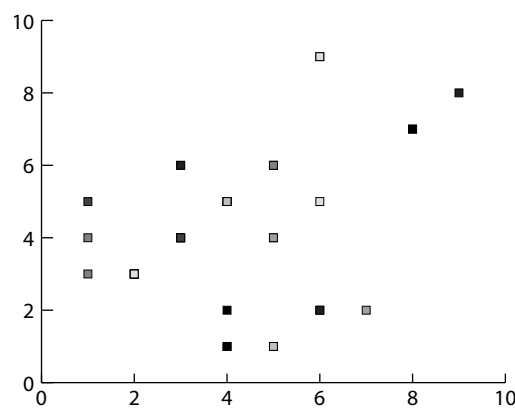


Figure 5.9: The new map of data

### 5.3.6 Develop comparison algorithm-Euclidean Distance

Euclidean distance is an ordinary distance between two or more instances and has been defined as (Turk, Pentland 1991):

$$d(x, y) = \sqrt{\sum_{i=1}^n (x_i - y_i)^2}$$

In this project after applying the PCA, the system must determine the minimum distance between the provided fingerprint and stored template in database. Obviously, the minimum distance would be a fingerprint match. The preview of finding minimum distance has been illustrated in figure 5.10.

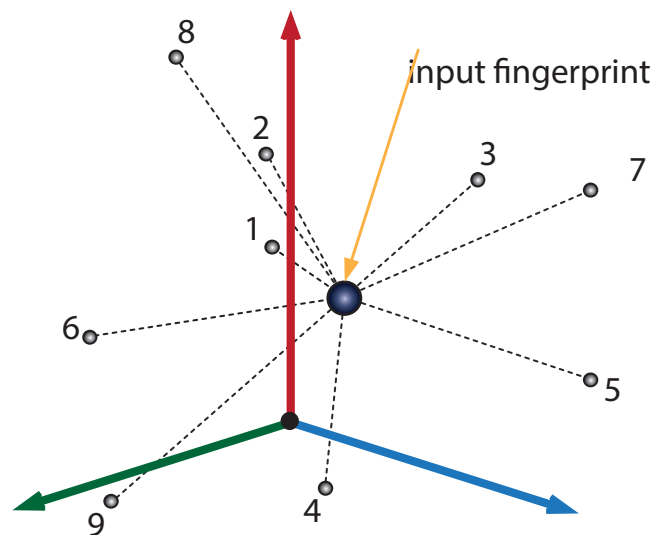


Figure 5.10: Example of measuring minimum distance amongst stored data

## 5.4 DEVELOP USER INTERFACE

In this section, the original model of this system has been illustrated in order to show its features and functionalities.

The first page with the common security gateway will allow a lecturer or administrator to log on to the system (Figure5.11).

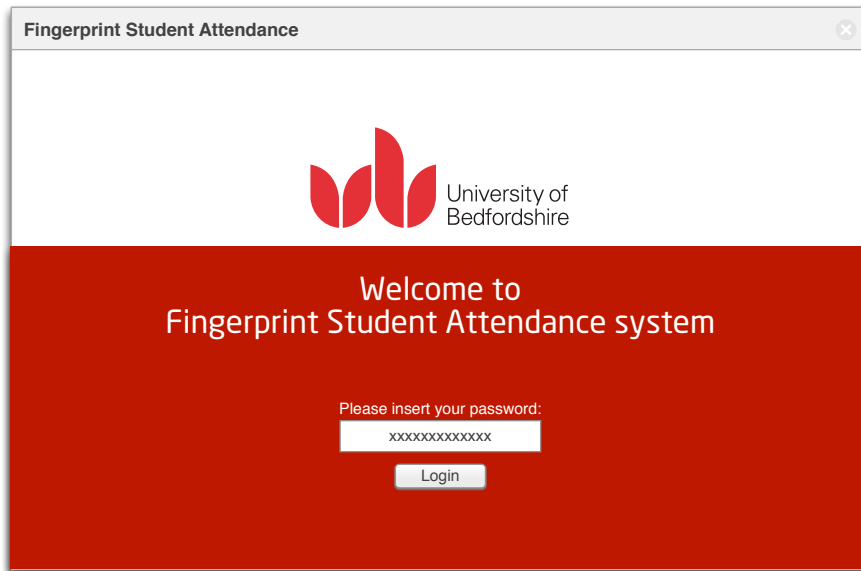


Figure 5.11 – Log on page

After logging on the system, a lecturer can choose the activity required to perform an identification process. To execute creating the new database, the user must have administrator permission (Figure 5.12).

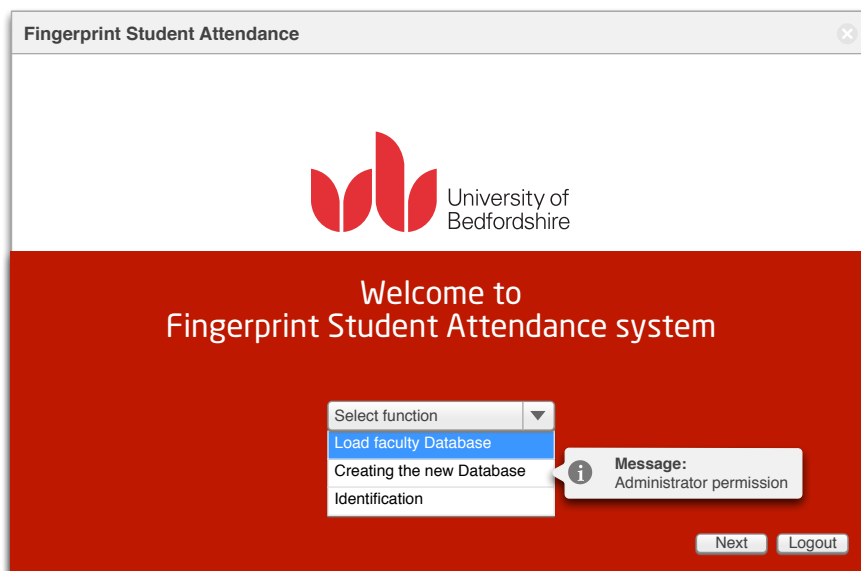


Figure 5.12 – Main Menu of System

To load the faculty database, a lecturer can choose the appropriate faculty to compare fingerprints with (Figure 5.13). Lecturers also should be able to select lecture enrolment within this page.

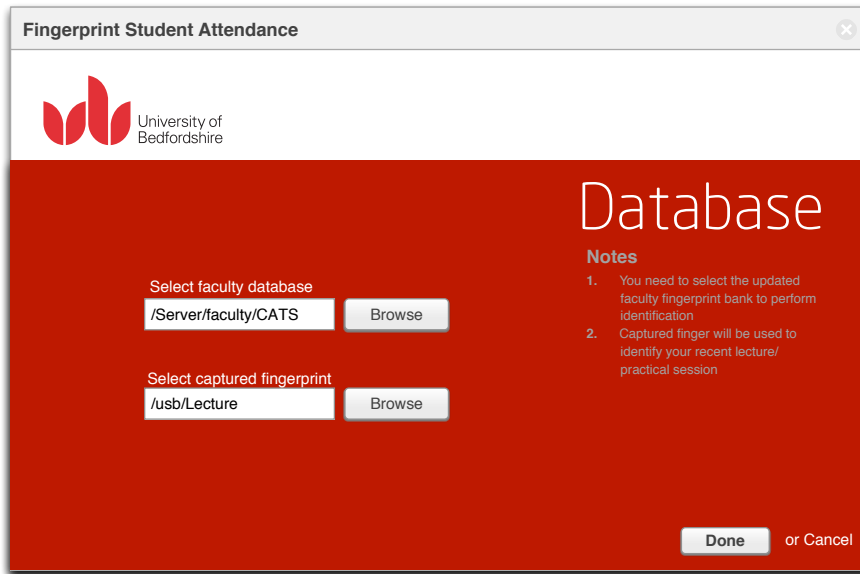


Figure 5.13 – Choosing the appropriate database and recent captured fingerprint image to perform identification within the monitoring system.

The next screen has presents the identification demo of this application (Figure 5.14). The system asks for a number of fingerprints and compares them against the whole database to identify a student. After identification, the system will display the identity of a specific fingerprint on the screen.

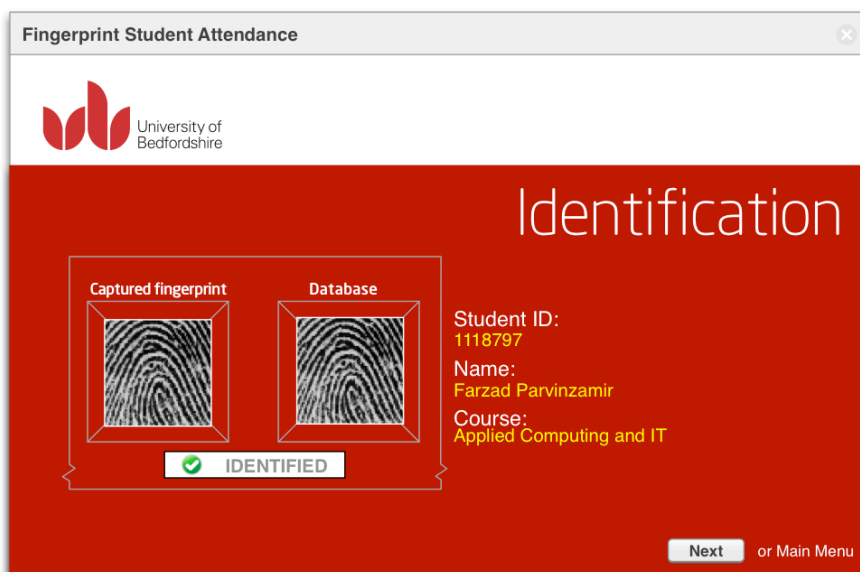


Figure 5.14 – the identification page displays student ID, name, and course of the identified fingerprint owner. It also shows the captured fingerprint images and the stored one in built-in database. Lecturer can retry for another fingerprint or get back to man menu by pressing the next or main menu respectively.

## **5.5 SUMMARY**

In this Chapter, the high level view of the system has been depicted in order to present how it must integrate with current infrastructure. The mechanism of creating datasets and Acquiring the PCA of a fingerprint datasets has been explained. Moreover, the process of comparison via Euclidean distance has been described. Lastly, a demonstration of the prototype application has been presented with accompanying screen shots. In the next chapter, the implementation of system, and how the PCA affects the data will be defined.



# Chapter 6

---

## 6 Implementation

The fingerprint student attendance has been developed in Mathwork MATLAB R2012 running under the Unix platform on a Mac Operating System. This application has been divided into:

1. Login
2. Main Menu
3. Creating database
4. Identification

All mathematical processes and references have been depicted in chapter 5. In this section, a brief demonstration will be provided to show how system works with regard to using vectored image, PCA, and Euclidean distance. This system would be an add-on application for the web-based student monitoring system being developed by Gordon Brady as his final Master's Project.

All the MATLAB coding is available in Appendix C, and a final version of this application can be found on the attached CD. As has been mentioned before, this application was originally compatible with Mac OS, but the author has managed to provide a Windows based application for PC which will also be available on the CD. Additionally, a quick user guide has been provided as a deliverable in Appendix F for users and in particular for administrators for maintenance purposes.

## 6.1 DEVELOPMENT

### 6.1.1 Intro

The source code of the home page has been developed purely to provide access to the application. Note that this page uses a simple form of password-based authentication.

The preview of this step will show in Figure 6.1 and Figure 6.2.

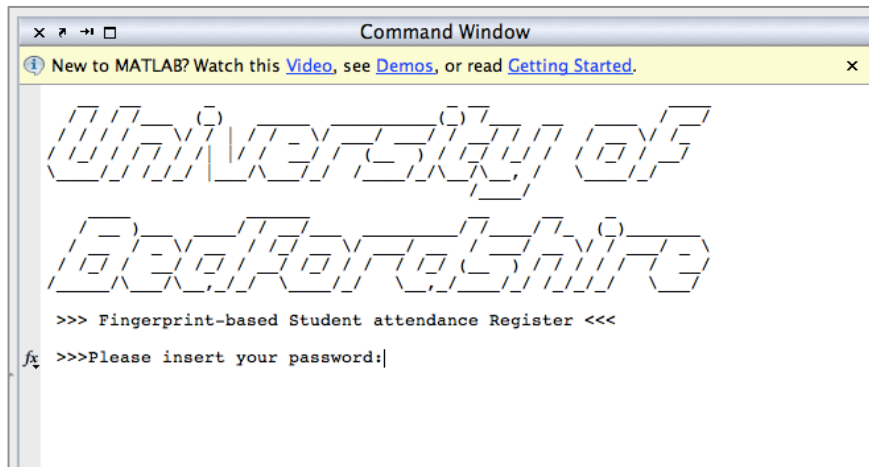


Figure 6.1 – intro of the system



Figure 6.2 – system will show the wrong password if user wants to enter to the fingerprint application without provided password.

### 6.1.2 Main Menu

This page will give users (Lecturers or Administrator) three options, which are “load default database”, “creating database”, and “performing identification process”. The first option, shown in figure 6.3, is loading the default fingerprint

database. Users can load the pre-built database and use it to start the identification process.

The second option needs higher privileges to operate. All users who have been authorized as an administrator can use this option to build a new fingerprint database. This part will be depicted in the section “Create database” later in this chapter. The last option is to run the identification process, which needs selecting captured fingerprint images. The identification will be demonstrated later in this chapter.

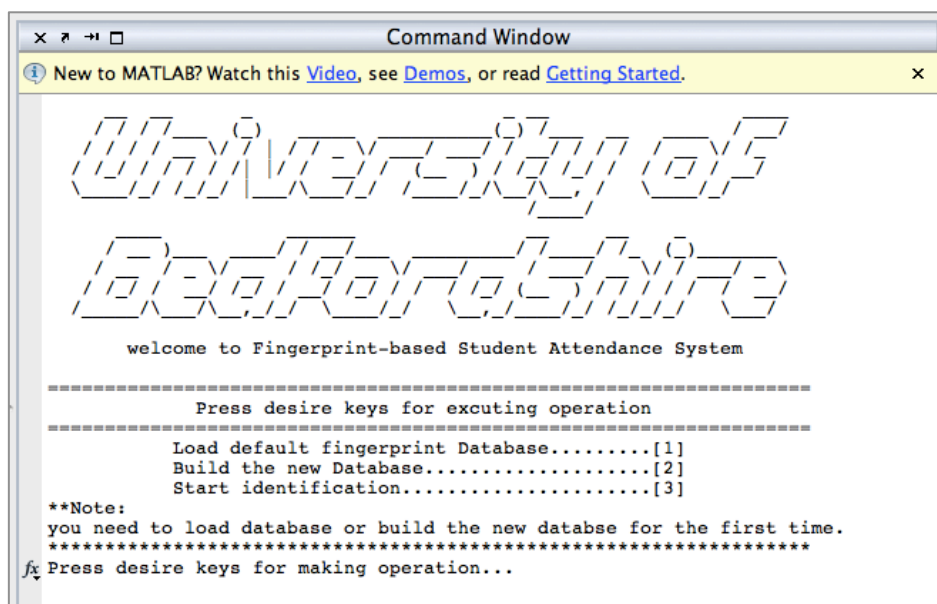


Figure 6.3 – Main menu of the system will show three items, which are completely clear in the screenshot. There is a note in this page, which reminds end-users that without loading default database or creating the new database you cannot use the system.

#### 6.1.2.1 Creating Database

This part of the application will create custom fingerprint recordsets in selectable directories for storing “in-lecture swipes” of students/ end users. The process consists of:

- 1- Select installation directory (by administrator/ lecturer)
- 2- Read all images being enrolled
- 3- Apply Principal Component Analysis to swiped fingerprints (datasets)

First, application will ask the user to select the installation directory for creating a new database, for instance to create a recordset of students who

attend a particular lecture (Figure 6.4). This function was specifically designed for customizing databases for each lecture session/ module during the academic year. An example of a fingerprint database is shown in figure 6.5.

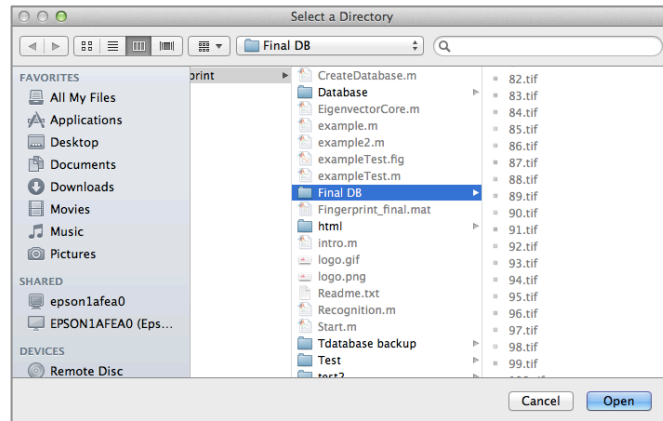


Figure 6.4 – System asks for choosing datasets directory to create a built-in database



Figure 6.5 – A sample datasets with 100 fingerprint images

After choosing a directory, all the fingerprint images will be inserted into the directory and converted to vectors using the process described in chapter five (Figure 6.6).

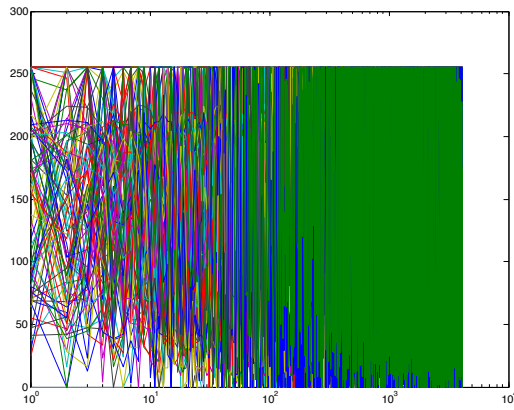


Figure 6.6: A plot of vectorized matrix of 100 fingerprint images

The next step is in automatically extracting the mean, covariance, eigenvalue, and eigenvector of each image (chapter 5 – PCA). The graphical graphs have been provided in figure 6.7, 6.8, and 6.9.

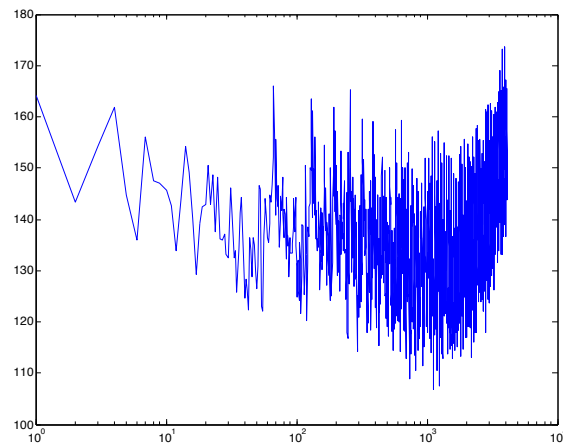


Figure 6.7: A plot of mean of Vectorized matrix with 100 images

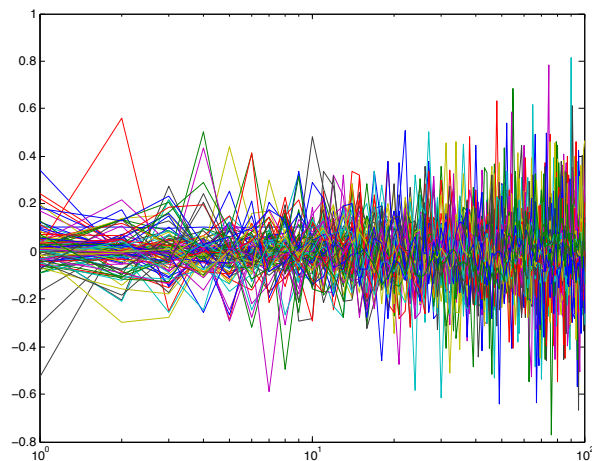


Figure 6.8: An eigenvalue plot of 100 fingerprint vectorized matrix

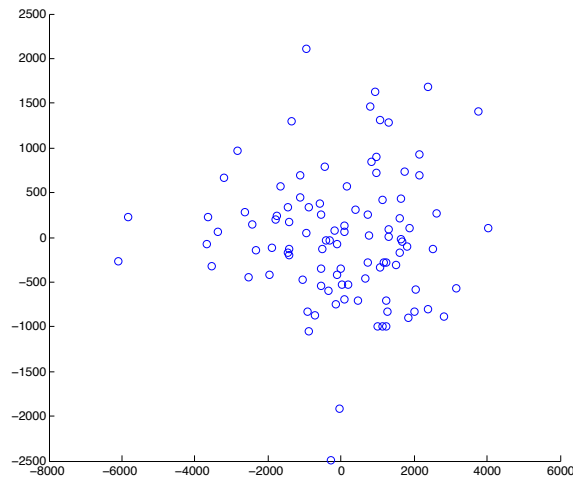


Figure 6.9: A scatter plot of eigenvector for 100 fingerprints

When this has been completed, the system will show a message that the dataset has been created successfully and also show the elapsed time for creating the dataset. At the bottom of page, the system asks for the user if they wish to use this dataset to identify students. Pressing “Y” begins performing the identification process by asking a user to select fingerprints from the database for comparison with the master recordset. Pressing the second option “N” quits the application (figure 6.10). In practical use, a lecturer would opt to create a recordset for a given module, and any student who attends that module would be “swiped” into the recordset, ready for subsequent identification.

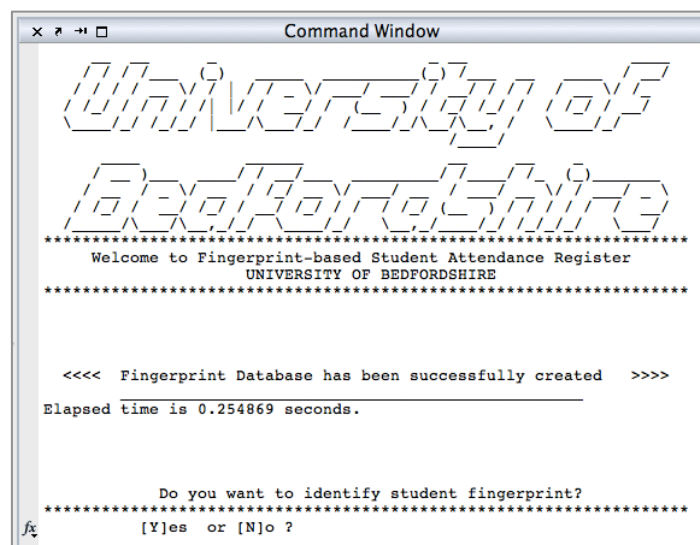


Figure 6.10: An screenshot of database creation and its elapsed time

### 6.1.2.2 Identification

This part of the application is accessed from the main menu by selecting “Start identification” or after creating a new database by pressing “Y”. At first, the system asks the user to select one of the images stored in the new database for identification. Next, the system will show a prompt window and asks user to enter the number of files (e.g. 1,2,3...) to check for identification (Figure 6.11).

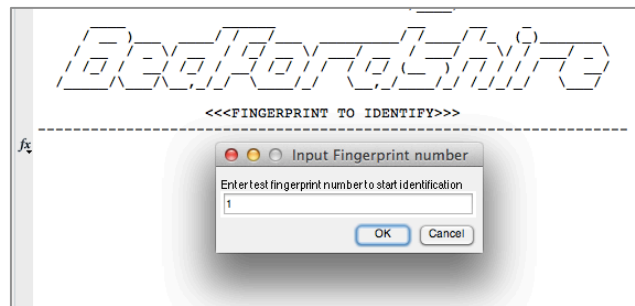


Figure 6.11: Prompt window

After clicking OK, the system will calculate the Euclidean distance of the chosen image against the database and show the result (Figure 6.12)(chapter 5 – Euclidean Distance).

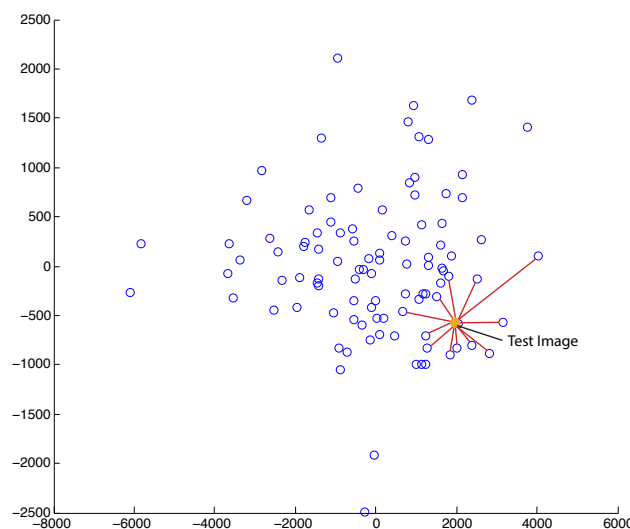


Figure 6.12 – a schematic of calculating Euclidean distance

The return from the comparison process consists of Student information (Student ID) and a picture of his/her stored fingerprint image, so the user can visually check the match (Figure 6.13). The end-user can try identifying more students or quit the application. Figure 6.14 displays an exit screenshot.

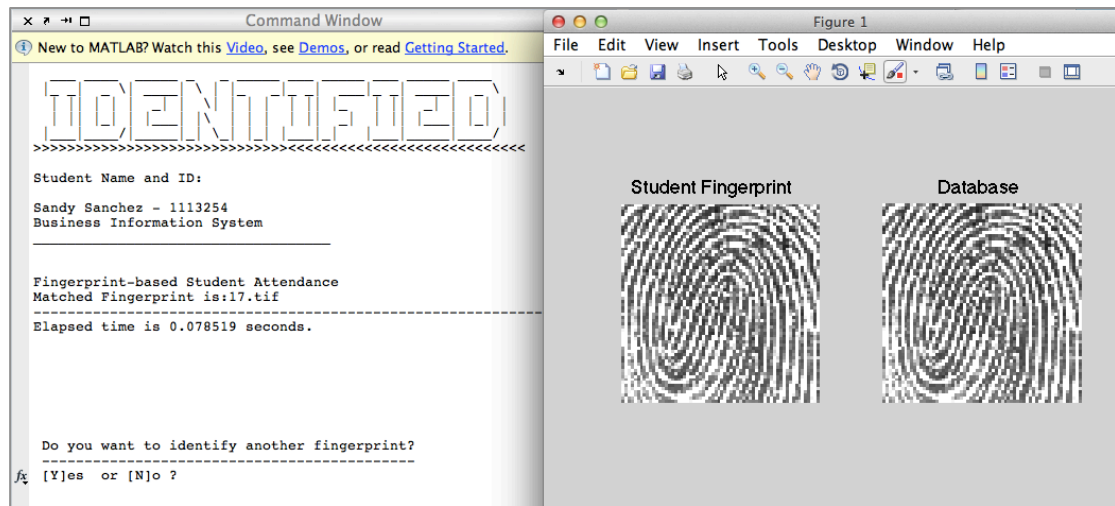


Figure 6.13: Result of identification process. Command window shows the name, ID, and related course of the identified student. Additionally, displays matched fingerprint number in database as well as elapsed time for completing identification. It also shows the comparison of database and the inserted fingerprint.

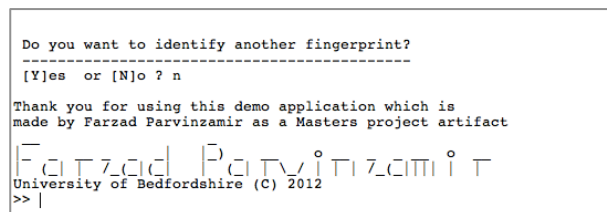


Figure 6.14: Exit command screenshot

## 6.2 SUMMARY

This application has been developed by MATLAB, which is suitable for image processing and high computational purposes. All four parts of the implementation have been described and the graphical figures have been located to show how fingerprint datasets would be affected during implementation. After this part, system needs to be tested and produces a testing result as a deliverable. Hence, The next chapter will set out the output and testing result.



# Chapter 7

---

## 7 Testing

In order to conduct a testing the list of requirements was used to find out which function must be examined. Additionally, it was important to prepare testing for the user interface and other components. This chapter as a testing section can be identified that the application:

- Meets the requirements
- Satisfies the need of the project's stakeholders
- Works as estimated

The achievable testing result of each function has been categorised into 5 score which are depicted in table 7.1:

Table 7.1 –definition of each testing grade

A	B	C	D
Item is available and working perfectly.	Item is available and working, but there are some bugs. Needs improvement	Item does not work and gives error due to problem in coding. Needs debugging	Item is not available. Needs to be developed in future work.

The following list will display the test result on this application:

Table 7.2 – Testing checklist

Testing items	Score
The fingerprint student attendance application needs to provide a simple interface to choose whether to use an existing database or to create a new database on the system.	A
Lecturers should be allowed to provide students' fingerprints for authentication process and likewise should be able to change the selected fingerprints templates folder for each lecture/practical session if required.	A
An accredited lecturer should be allowed to configure student identification as required.	D
The authorised user (lecturer) should be able to access all identification options.	A

The authorised user (lecturer) should be able to update the database	A
The authorised user (lecturer) should be able to see the matched student fingerprint within the database	A
The lecturer should be able to see the name and ID of the student who has been identified by the application	B
The fingerprint application must have the quickest response time in order to process students' fingerprints rapidly	A
Three user levels will be required; Lecturer, Faculty Admin, DBA Admin	D
There should be different functionalities for different user levels	B
The system should be able to deal with multiple concurrent users	D
It is possible for a student to "swipe" himself or herself as present twice in one lecture. The Student Attendance database system will filter double entry student IDs from each register	D
The system is to plug in as an additional module to the Student Attendance System, not to replace other data captures methods	A
Check the quality of captured students' fingerprints during each lecture	A
Application should offer functions in order to carry out identification such as access to the system, load default database, and make or choose appropriate database	A
The fingerprint student attendance application should be matched with the University of Bedfordshire network settings (clients and server). Future work.	B
Provides user guide, fingerprint scanner, and related drivers	A
The identification item should return the appropriate matched message for an accepted entry	A
The lecturer should be able to quit the fingerprint application	A

This application meets most of the requirements. Additionally, it has potential to integrate with the University student monitoring system, proposed and implemented by Gordon Brady, in order to obtain system integration score. A set of codes is available in the application and Appendix C in order to make a connection to any external system as a future work.

## 7.1 PERFORMANCE

This application has been designed to identify fingerprints quickly and show the visualise result. All processes display elapsed time after completing in the command window. The performance of two major parts of this application was tested with different size of database for creating database (Part 1) and identification process (Part 2). The first part consists of conducting vector and PCA computation. Time taken to build a new database with respect to size of datasets fingerprint images, has been illustrated in figure 7.1. Moreover, the size of datasets on disk and its elapsed time is available in table 7.3.

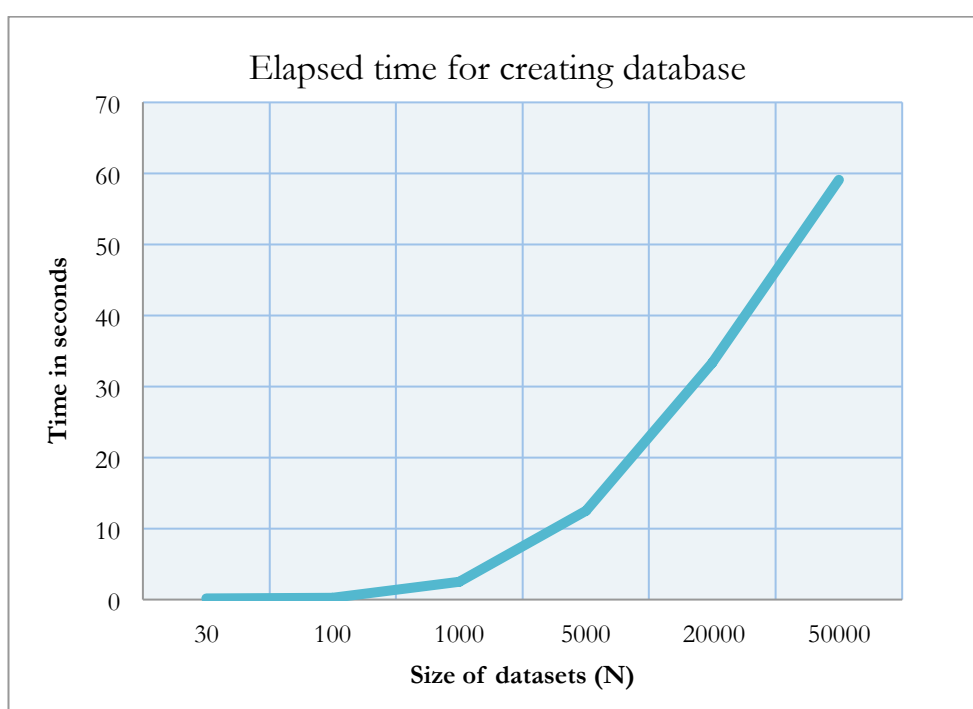


Figure 7.1 – elapsed time to create a new database from different size of datasets

Table 7.3 – Size of the datasets on disk and elapsed time to make a new database

Number of images in Datasets	Size on Disk	Elapsed time (Sec.)
<b>30</b>	1,144,962 bytes	0.1725
<b>100</b>	3,936,105 bytes	0.2503
<b>1000</b>	39,936,105 bytes	2.5008
<b>5000</b>	199,680,538 bytes	12.5049
<b>10000</b>	399,360,176 bytes	25.5501
<b>20000</b>	798,720,352 bytes	33.2906
<b>50000</b>	1,996,800,000 bytes	59.0427

We used different size of database for testing the second part of this application which comprising transform to vector input images, applying PCA and, measuring Euclidean distance. Figure 7.2 shows the time taken to identify each fingerprint by performing mentioned process. The time of comparing fingerprint has been increased with selecting a larger size of the database. This means, the elapsed time for identification has been affected by the different size of database. It is anticipated, by selecting the largest database, the time of identification would be boosted.

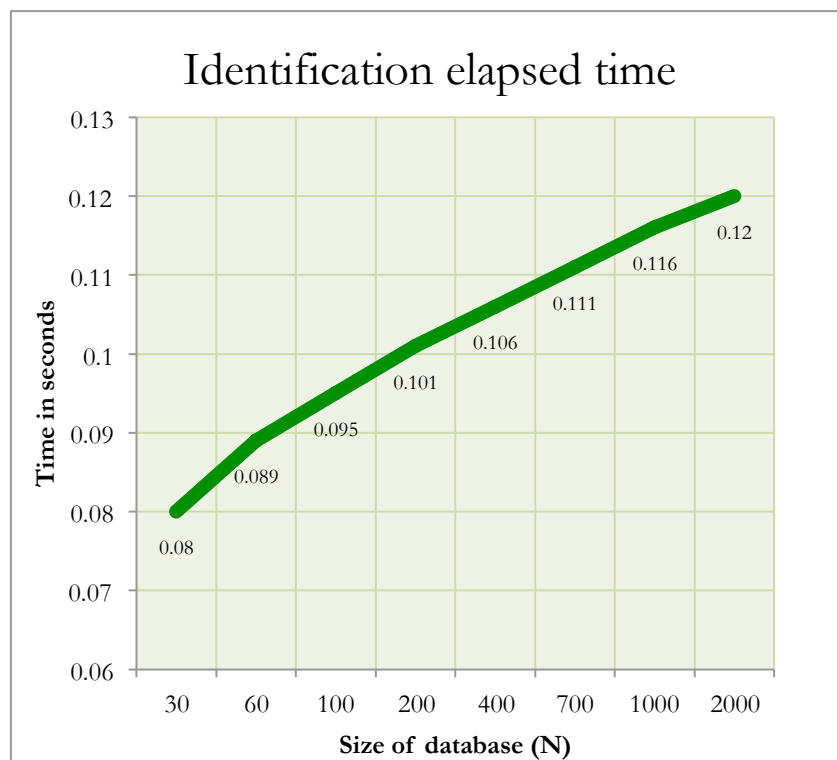


Figure 7.2 – elapsed time for identification fingerprint with respect to different size of database. Identification has taken 0.08 seconds to match provided fingerprint against database with 30 images. This was amplified by increasing the size of the database to 0.12 seconds.

## 7.2 IMPROVEMENT

Creating database with executing PCA was a big challenge in this project. The first test in acquiring PCA and building a new database with 30 images was taken 105.37 seconds. It did not satisfy the requirements because:

- The elapsed time was too long
- System would be crashed during heavy processing
- High computational complexity
- It needed a powerful computer to execute creating database.

Therefore, all algorithms related to PCA have been reconsidered. The problem was that the covariance matrix  $C$  (Chapter 5) was calculated by a  $n^2 \times n^2$  dimension, thus we can have  $n^2$  eigenvector and eigenvalues. For a  $64 \times 64$  image system needs to calculate a  $4096 \times 4096$ , which was an immense computation. So, the method has been replaced by “Turk and Pentland” scheme (Turk, Pentland 1991, Wang Yongxu, Ao Xinyu et al. 2006, PISSARENKO 2002). The new algorithm is trying to compute covariance by using this formula, which has been depicted in chapter 5:

$$C_{ij} = \frac{1}{M} \sum_{n=1}^M \Phi_n \Phi_n^T = AA^T$$

Normally,  $M$  has a few relevant principal components (Eigen-fingerprint). The number of calculations in PCA has been reduced by using the number of datasets images ( $M$ ) (For this project now we calculate 30 for datasets with 30 images or 100 for datasets with 100 images) instead of using the number of pixels ( $n^2 \times n^2$ ).

### 7.3 SUMMARY

This section evaluated the FR application, which has been developed as a artifact under the Unix platform. The predefined test list has been produced for testing application with regard to the project requirements. The result of testing has been portrayed in 5 scores. Additionally, the performance of the system for creating a new database and performing identification process has been tested and analysed. The number of bugs has been detected and improved by replacing the new algorithm. Accuracy of this system after several tests was still high due to the small size of the database (100 images). However, it is anticipated that increasing the number of images in the database would cause to reduce the rate of accuracy.

# Chapter 8

---

## 8 Conclusion

The Fingerprint-based Student Attendance Register set out to overcome the drawbacks of the current attendance system, which can be fooled by “buddy swiping” of absent students’ RFID card or signing the register sheet on behalf of absentee students within a university. A combination of survey, interview, observation, research and best practice has been used to capture the project requirements with regard to Prince2 methodology. This project has been implemented in four phases including create datasets, apply PCA process to datasets, develop comparison process, develop user interface, and finally test and evaluation in order to provide all deliverables.

An application was designed within MATLAB under the Unix platform to create vectors and values from a fingerprint image, applying PCA to map the new data into the new space, and then to verify a student who swipes his fingerprint against those values. The delivered application with a simple interface uses the Principal Component Analysis method and algorithms to compare fingerprints and meets %80 of the project requirements. This high-speed method uses the lowest computational power to deliver accurate results through finding eigenvalues and eigenvectors, deciding on which are significant, forming a new harmonize system which is described by eigenvector, plotting data to the new area, and making a closest match against stored values in order to identify fingerprints. This application works asynchronously so that constant Internet and database connections are not required. Moreover, it has potential to be employed as a modular add-on by a University student monitoring system or connect to its database and transfer data.

The developer has acquired knowledge about the Principal Components Analysis and the different kind of measuring the  $n$  dimension data distance in systems. This project also has increased the developer's familiarity with MATLAB software to develop an operative code in this area. It is essential to be familiar with your chosen language and development tools.

The recommendation from this project is that using PCA for fingerprint identification is definitely valuable and provides high rate of accuracy along with low computational complexity.

## 9 Reference

- BERRY, J., 1994. The history and development of fingerprinting in *Advances in Fingerprint Technology*. In: H.C. LEE and R.E. GAENSSLEN, Florida: CRC Press, pp. 1-38.
- BHARGAV-SPANTZEL, A., SQUICCIARINI, A. and BERTINO, E., 2010. Biometrics-Based Identifiers for Digital Identity Management. , pp. 84-97.
- BOATWRIGHT, M. and LUO, X., 2007. What Do We Know About Biometrics Authentication? *Information Security Curriculum Development Conference*, 28-29 September 2007 2007, ACM.
- CAVOUKIAN, A., 2008. *Fingerprint Biometrics: Address Privacy Before Deployment*. Toronto: Information and Privacy Commissioner of Ontario.
- IBG, 2002. *Comparative Biometric Testing*. New York: International Biometrics Group.
- KLOKOVA, A., 2010. **COMPARISON OF VARIOUS BIOMETRIC METHODS**. Southampton: Interactive Multimedia Systems, Electronics and Computer Science, University of Southampton.
- KOTHAVALA, M., MARKWORTH, R. and SANDHU, P., 2004-last update, Computer Security SS3: Biometric Authentication. Available: <http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS3/handout/>.
- MALTONI, D., MAIO, D., K. JAIN, A. and PRABHAKAR, S., 2009. *Handbook of Fingerprint Recognition*. Second edn. London: Springer.
- MORDINI, E. and PETRINI, C., 2007. Ethical and social implications of biometric identification technolo. **43**(1), pp. 5-11.
- NATIONAL SCIENCE & TECHNOLOGY COUNCIL SUBCOMMITTEE ON BIOMETRICS & IDENTITY MANAGEMENT, 2005-last update, Biometrics info. Available: [www.biometrics.gov](http://www.biometrics.gov).
- NEWMAN, R., 2010. *Security and Access Control using Biometrics Technologies*. 1st edn. Boston: Cengage Learning.
- O'GORMAN, L., 2002-last update, FINGERPRINT VERIFICATION [Homepage of Michigan State University], [Online]. Available: <http://www.cse.msu.edu/~cse891/Sect601/textbook/2.pdf>.
- PISSARENKO, D., 2002-last update, Eigenface-based facial recognition [Homepage of Penn State], [Online]. Available: [citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.13.233.pdf](http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.13.233.pdf).
- R. HECKLE, R., S. PATRICK, A. and OZOK, A., 2007. Perception and Acceptance of Fingerprint Biometric Technology, *Symposium On Usable Privacy and Security*, 18-20 July 2007 2007.
- SARASWAT, C. and KUMAR, A., 2010. An Efficient Automatic Attendance System using Fingerprint Verification Technique. *International Journal on Computer Science and Engineering*, **2**(2), pp. 264-269.
- SMITH, L.I., 2002-last update, A tutorial on principal components analysis [Homepage of Department of Computer Science - University of Otago], [Online]. Available: [http://www.cs.otago.ac.nz/cosc453/student\\_tutorials/principal\\_components.pdf](http://www.cs.otago.ac.nz/cosc453/student_tutorials/principal_components.pdf).
- TILTON, C., 2009-last update, CBEFF (Common Biometric Exchange Formats Framework) [Homepage of W3C], [Online]. Available: <http://www.w3.org/2008/08/siv/Slides/Daon/CBEFF-Tilton-2009-short.pdf>.



TURK, M.A. and PENTLAND, A.P., 1991. Face recognition using eigenfaces, *Computer Vision and Pattern Recognition, 1991. Proceedings CVPR '91., IEEE Computer Society Conference on 1991*, pp. 586-591.

UKBA, July 2012-last update, Tier 4 of the Points Based System - Policy Guidance [Homepage of Home Office], [Online]. Available: <http://www.ukba.homeoffice.gov.uk>.

WANG YONGXU, AO XINYU, DU YUANFENG and LI YONGPING, 2006. A Fingerprint Recognition Algorithm Based on Principal Component Analysis, *TENCON 2006. 2006 IEEE Region 10 Conference 2006*, pp. 1-4.

YONGHWA CHOI, TOKUMOTO, T., MINHO LEE and OZAWA, S., 2011. Incremental two-dimensional two-directional principal component analysis for face recognition, *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on 2011*, pp. 1493-1496.

ZHANG, P., LI, C. and HU, J., 2010. A Pitfall in Fingerprint Features Extraction, *11th Int. Conf. Control, Automation, Robotics and Vision*, 7-10th December 2010, IEEE.

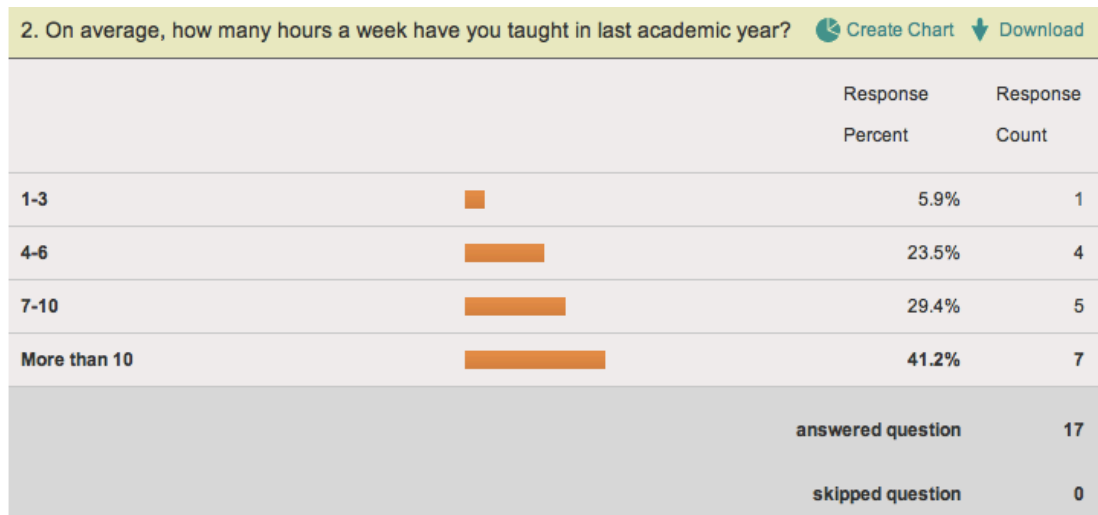
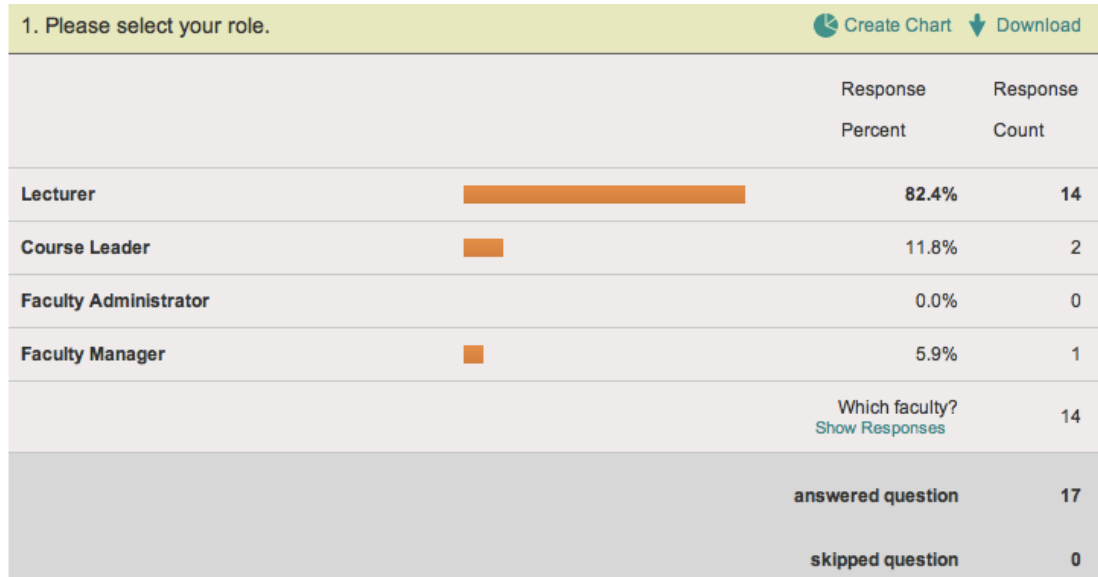
ZHENGMAO YE and TURNER, R., 2007. Intelligent Linear and Nonlinear Analysis for Biometric Fingerprint Recognition, *System Theory, 2007. SSST '07. Thirty-Ninth Southeastern Symposium on 2007*, pp. 315-319.

ZHENGMAO YE, YONGMAO YE and MOHAMADIAN, H., 2007. Biometric Identification via PCA and ICA Based Pattern Recognition, *Control and Automation, 2007. ICCA 2007. IEEE International Conference on 2007*, pp. 1600-1604.

# 10 Appendices

## 10.1 APPENDIX A

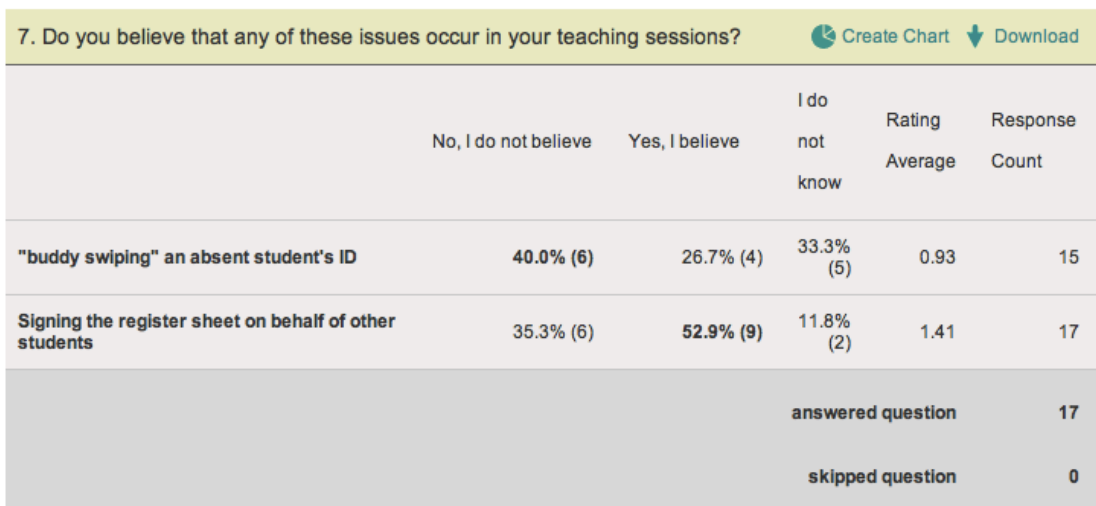
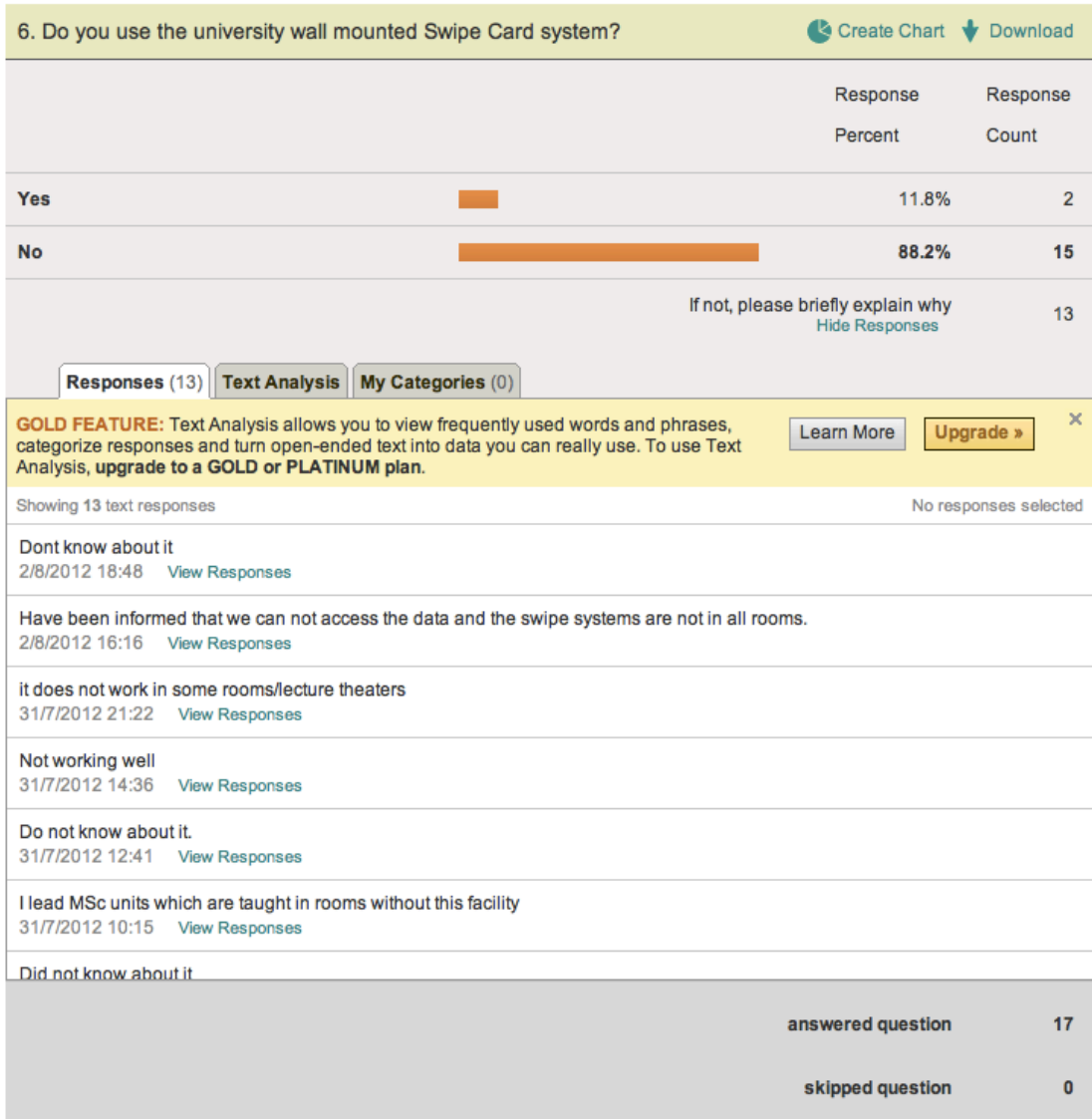
### 10.1.1 Market survey – Lecturer



3. Approximately how many students attend your lectures?		<a href="#">Create Chart</a>	<a href="#">Download</a>
		Response Percent	Response Count
1-50		35.3%	6
51-100		47.1%	8
More than 100		17.6%	3
		<b>answered question</b>	<b>17</b>
		<b>skipped question</b>	<b>0</b>

4. Approximately how many students attend your practical sessions?		<a href="#">Create Chart</a>	<a href="#">Download</a>
		Response Percent	Response Count
1-20		58.8%	10
21-40		35.3%	6
41-60		5.9%	1
More than 60		0.0%	0
		<b>answered question</b>	<b>17</b>
		<b>skipped question</b>	<b>0</b>

5. Which method/s do you normally use to record students' attendance?		<a href="#">Create Chart</a>	<a href="#">Download</a>
		Response Percent	Response Count
Paper based registers for self-signature		58.8%	10
Paper based registers which you fill out (ie as a roll-call)		41.2%	7
Swipe card system mounted on wall		0.0%	0
Swipe card system held by lecturer		0.0%	0
		Other (please specify) <a href="#">Show Responses</a>	1
		<b>answered question</b>	<b>17</b>
		<b>skipped question</b>	<b>0</b>







8. Have you ever faced the following issues in the process of recording student attendance?

[Create Chart](#) [Download](#)

	Never	Sometimes	Most of the time	Always	Rating Average	Response Count
Unable to find the sign sheet	68.8% (11)	25.0% (4)	6.3% (1)	0.0% (0)	1.38	16
Unable to access to the university wall mounted Swipe Card system	46.7% (7)	20.0% (3)	13.3% (2)	20.0% (3)	2.07	15
Difficulty to enter attendance data manually	40.0% (6)	33.3% (5)	13.3% (2)	13.3% (2)	2.00	15
Double entry	73.3% (11)	26.7% (4)	0.0% (0)	0.0% (0)	1.27	15
Time taken	26.7% (4)	20.0% (3)	13.3% (2)	40.0% (6)	2.67	15
<b>answered question</b>						<b>16</b>
<b>skipped question</b>						<b>1</b>



9. Using a scan of the student's fingerprint could provide a highly accurate, quick and reliable method of recording student attendance. How convenient is it for you to ask students to scan their fingerprints into a recording/ comparison device such as a PC with a plug-in fingerprint reader?

[Create Chart](#) [Download](#)

		Response Percent	Response Count
Extremely convenient		29.4%	5
very convenient		17.6%	3
Slightly convenient		29.4%	5
Not at all convenient		23.5%	4
<b>answered question</b>			<b>17</b>
<b>skipped question</b>			<b>0</b>

10. Do you agree with the following items?							<a href="#">Create Chart</a>	<a href="#">Download</a>
	Strongly Disagree	Disagree	Agree	Strongly Agree	Rating Average	Response Count		
Paper-based is not effective	23.5% (4)	29.4% (5)	<b>35.3% (6)</b>	11.8% (2)	2.35	17		
swipe card system is not effective	13.3% (2)	33.3% (5)	<b>40.0% (6)</b>	13.3% (2)	2.53	15		
Paper-based attendance system can be fooled	12.5% (2)	12.5% (2)	<b>62.5% (10)</b>	12.5% (2)	2.75	16		
Swipe card system can be fooled	6.7% (1)	13.3% (2)	<b>73.3% (11)</b>	6.7% (1)	2.80	15		
Fingerprint-based attendance system can eliminate common problems for monitoring students engagement	12.5% (2)	0.0% (0)	<b>62.5% (10)</b>	25.0% (4)	3.00	16		
Fingerprint technique makes possible accurate and rapid authentication	12.5% (2)	0.0% (0)	<b>62.5% (10)</b>	25.0% (4)	3.00	16		
						<b>answered question</b>	<b>17</b>	
						<b>skipped question</b>	<b>0</b>	

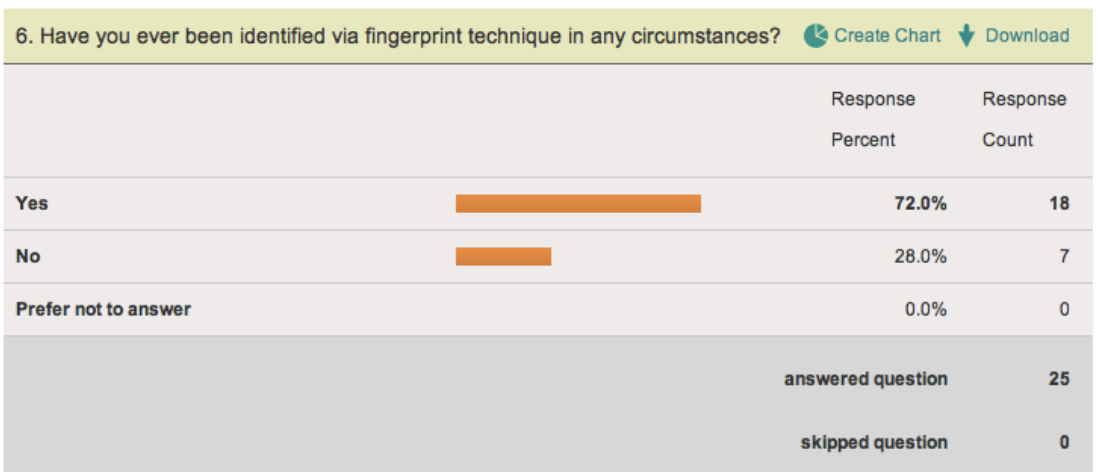
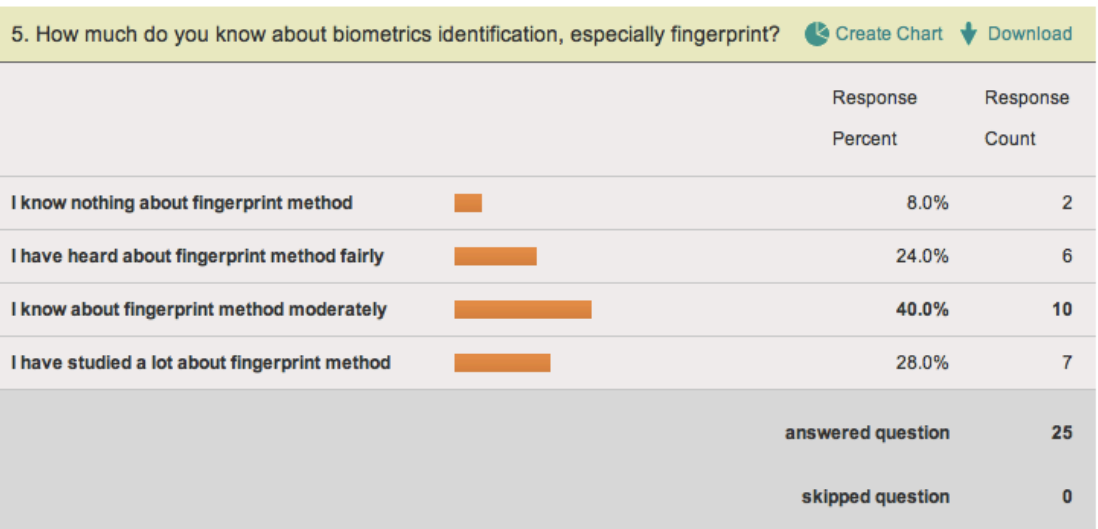
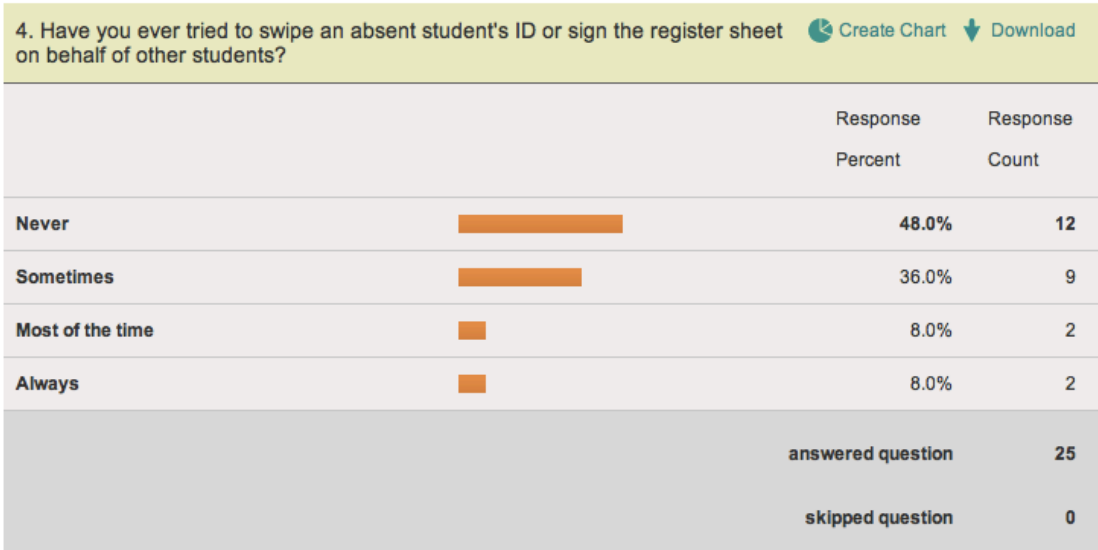
### 10.1.2 Market survey questionnaires – Student

1. What is your gender?				<a href="#">Create Chart</a>	<a href="#">Download</a>
		Response Percent	Response Count		
Female		20.0%	5		
Male		80.0%	20		
			<b>answered question</b>	<b>25</b>	
			<b>skipped question</b>	<b>0</b>	

2. Which category below includes your age?		<a href="#">Create Chart</a>	<a href="#">Download</a>
		Response Percent	Response Count
17 or younger		0.0%	0
18-24		20.8%	5
25-34		62.5%	15
35-44		16.7%	4
45-55		0.0%	0
56 or older		0.0%	0
		<b>answered question</b>	<b>24</b>
		<b>skipped question</b>	<b>1</b>

3. What is your originality?		<a href="#">Download</a>
		Response Count
		<a href="#">Show Responses</a>
		23
		<b>answered question</b>
		<b>23</b>
		<b>skipped question</b>
		<b>2</b>

<b>Belgian</b> 31/7/2012 11:10 <a href="#">View Responses</a>
<b>Asian</b> 31/7/2012 10:08 <a href="#">View Responses</a>
<b>Africa</b> 31/7/2012 10:04 <a href="#">View Responses</a>
<b>Indonesian</b> 31/7/2012 9:02 <a href="#">View Responses</a>
<b>English</b> 30/7/2012 23:04 <a href="#">View Responses</a>





7. Identification based on fingerprint method eliminates the need to carry smart card/ token, remember a password, or sign the register sheet. With regard to this information, do you prefer to be identified by fingerprint-based attendance system in your university? [Create Chart](#) [Download](#)

	Response Percent	Response Count
Yes	68.0%	17
No	32.0%	8
If not, please briefly explain why <a href="#">Show Responses</a>		5
<b>answered question</b>		<b>25</b>
<b>skipped question</b>		<b>0</b>

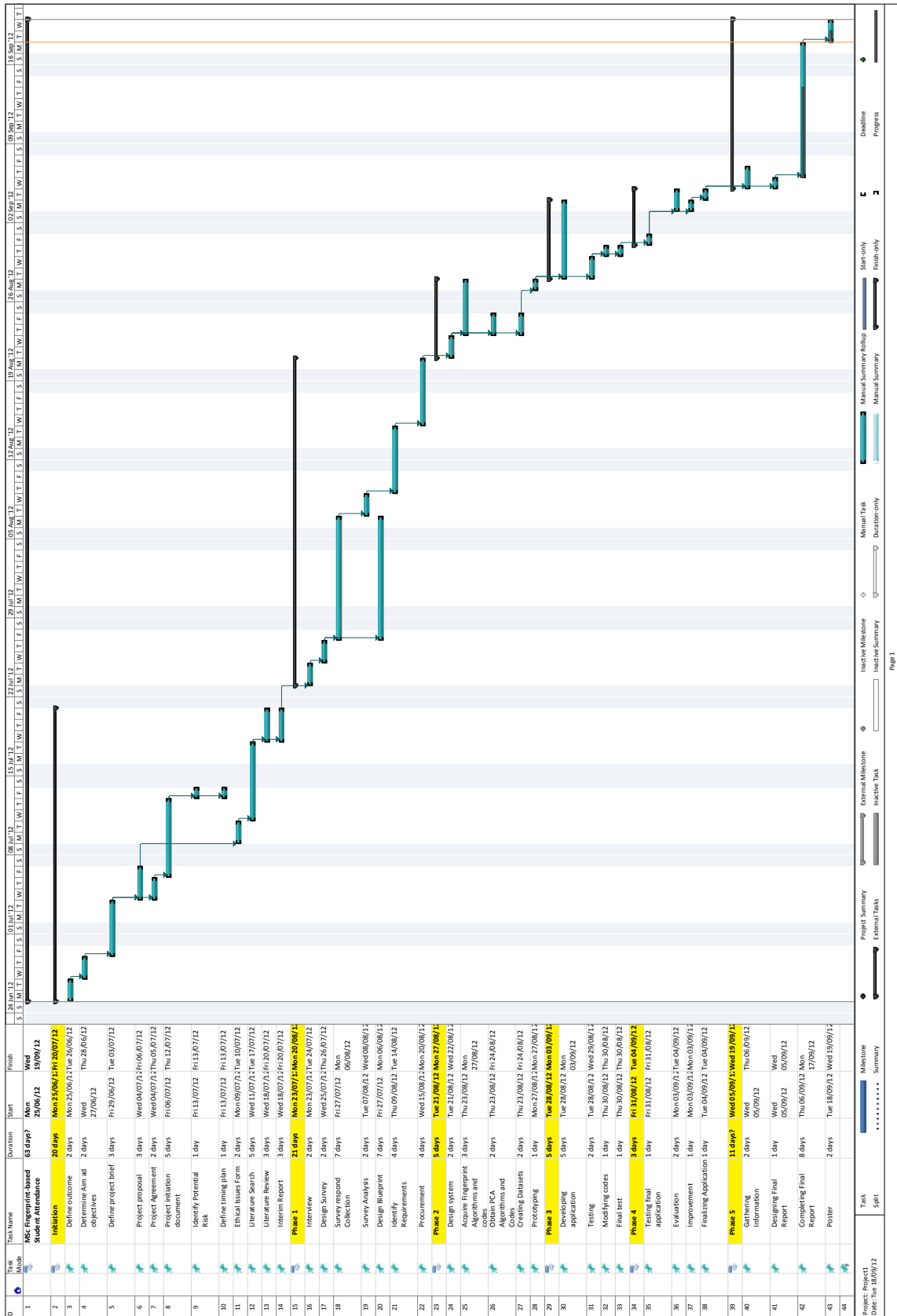
8. Do you agree with the following items? [Create Chart](#) [Download](#)

	Strongly Disagree	Disagree	Agree	Strongly Agree	Rating Average	Response Count
Using fingerprint in university would be an invasion of privacy	17.4% (4)	26.1% (6)	52.2% (12)	4.3% (1)	2.43	23
Fingerprint reader leads to disease transfer and AIDS	50.0% (12)	41.7% (10)	4.2% (1)	4.2% (1)	1.63	24
It is extremely hard to fool fingerprint system	4.2% (1)	16.7% (4)	45.8% (11)	33.3% (8)	3.08	24
Students can trust the university fingerprint system	4.3% (1)	39.1% (9)	39.1% (9)	17.4% (4)	2.70	23
It is easy to be identified by fingerprint instead of carrying ID card, remembering password or signing the register sheet	8.3% (2)	12.5% (3)	50.0% (12)	29.2% (7)	3.00	24
<b>answered question</b>						<b>24</b>
<b>skipped question</b>						<b>1</b>

9. Which one is important to you? [Create Chart](#) [Download](#)

	Not Important at All	Slightly Important	Somewhat Important	Very Important	Extremely Important	Rating Average	Response Count
Security of fingerprint template database	0.0% (0)	13.0% (3)	21.7% (5)	21.7% (5)	43.5% (10)	3.96	23
The way of using fingerprint	0.0% (0)	4.3% (1)	13.0% (3)	60.9% (14)	21.7% (5)	4.00	23
Privacy	0.0% (0)	8.7% (2)	4.3% (1)	21.7% (5)	65.2% (15)	4.43	23
<b>answered question</b>							<b>23</b>
<b>skipped question</b>							<b>2</b>

# 10.2 APPENDIX B – GANTT CHART





```

-----
% Reading images and creating vector matrix
% Reference: Mathwork Central Library/ A.Omidvarnia

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% File management
TrainFiles = dir(TrainDatabasePath);
Train_Number = 0;

for i = 1:size(TrainFiles,1)
    if
not(strcmp(TrainFiles(i).name, '.')|strcmp(TrainFiles(i).name, '..')|strcmp(Tr
ainFiles(i).name, '.DS_Store'))
        Train_Number = Train_Number + 1; % Number of all images in the
training database
%     elseif Train_Number ~= TrainFiles(i)
%         Train_Number;

    end
end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Construction of 2D matrix from 1D image vectors
T = [];
for i = 1 : Train_Number

    % The reason why we are using this code is that the all images are
provided in
% corresponding number.
str = int2str(i);

str = strcat('/',str, '.tif');
str = strcat(TrainDatabasePath, str);

img = imread(str);
%     img = rgb2gray(img);

[irow icol] = size(img);

temp = reshape(img', irow*icol, 1); % Reshaping 2D images into 1D image
vectors
T = [T temp]; % 'T' grows after each turn
end

-----

function [m, A, Eigenvector, V, D] = EigenvectorCore(T)
% Use Principle Component Analysis (PCA)

% Reference: Mathwork Library / A. Omidvarnia
%

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Calculating the mean image
m = mean(T,2); % calculating the average fingerprint image m =
(1/P)*sum(Tj's) (j = 1 : P)
Train_Number = size(T,2);

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Calculating the deviation of each image from mean
image
A = [];
for i = 1 : Train_Number
temp = double(T(:,i)) - m; % Calculating the difference between the mean
images and original images in the training set Ti - m = Ai
A = [A temp]; % Merging all centered images
end

L = A'*A; % L is the surrogate of covariance matrix C=A*A'.
[V D] = eig(L); % Diagonal elements of D are the eigenvalues for both L=A'*A

```







```

disp(' << This database including fingerprint of UoB students >>');
disp(' ');
disp(' ');
disp('Press any key to continue.....');
pause;
disp(' ');
disp(' ');
disp('System is about to come back to the main menu');
disp(' You can choose 3 to start the identification');
disp(' Press any key to continue...');
pause;
Start; %Start again this process to give end-user another chance to
select identification process

    case '2'
        example; %Executing example one to ask for desire fingerprint
datasets directories

    case '3'
        example2; %Executing identification part
end

```

#### DATABASE CONNECTION -----

```

% Fingerprint-based Student Attendance Register
% Farzad Parvinzamid

```

```

% This part has been provided to show a further work on the project
% Fingerprint-based application can connect to Microsoft Access /ORACLE
database with the following command

```

Oracle:

```

conn = database('test_db','scott','tiger','Vendor','Oracle',...
'DriverType','oci','Server','remotehost','PortNumber',1234)

```

MS Access

```

dbpath = '/Users/farzadpz/Documents/MATLAB/DB/Database2.accdb';
conurl = ['jdbc:odbc:Driver={Microsoft Access Driver (*.accdb)}; DBQ='
dbpath];
con = database('','','','sun.jdbc.odbc.JdbcOdbcDriver', conurl)

```

% Example query

```

insertQuery=['insert into Image values(' name ',' imagePath ',' ICC ');' ]
e = exec(con,insertQuery);
colnames={'imgName', 'imagePath', 'iCC'};
values={name, imagePath, ICC};
insert(con, 'Image',colnames, values ) %This statement inserts the values
which are contained by values %array variables
% %e = fetch(e);
% %data = e.Data

```



## 10.4 APPENDIX D - INTERIM REPORT

### 1. INTRODUCTION

The rate of applying for the UK's universities has been increased. Undoubtedly, an accurate and reliable system to monitor student attendance is required. Government Agencies and others may require information on student attendance, which is verifiable for audit purposes. The current issue, which has been faced by a large number of universities, is lack of a reliable student attendance system. Many universities use paper-base or smart card to check the students' engagement. However, the university's attendance system could be fooled by "buddy swapping" the smart cards or signing the register-sheet on behalf of absent students. The best method to cover this issue would be biometric and especially fingerprint. Biometrics provide limited as well as secure and trustworthiness access to sensitive facilities, public and private assets. It is based upon the automatic identification or verification of living persons with regard to their behavioural or physical features (Newman 2010). Biometric system is using numerous approaches, which are related to body parts, imaging, and personal characteristics such as hand, face, veins, signature, and so forth. This technology brings the physical features measurements into play. This project will propose the fingerprint based attendance register for the university of Bedfordshire to monitor student attendance and keeping the system away from the mentioned problem.

### 2. BACKGROUND

The biometrics has a couple of meanings: *bio* means a live human and *metrics* means the capability to determine an object (Newman 2010). The biometric fingerprint method was used first as a form of autograph in earliest societies. In the 18<sup>th</sup> century, scientists had found two fundamental features regarding fingerprints. They were: i) no two fingerprints have the same pattern, and ii) the fingerprints patterns do not permute or reform during the time. These finding were cause of employing fingerprint for criminal identification at first in 1986 in Argentina, and afterward in 1901 at Scotland Yard (O'Gorman 2002, National Science & Technology Council Subcommittee on Biometrics & Identity Management 2005). The first commercial biometric device based on hand-geometry was implemented for physical access control, personal identification, and T & A (Time and attendance) in 1970s. The Japanese NEC Company also had deployed the leading AFIS (Automated Fingerprint Identification System) in 1971 (Berry 1994). This system used to scan a card, which has got ink fingerprint pattern, convert to a template, and store them into a database for matching fingerprint for the next time. This system had been taken up in all over the world by many law enforcement organizations e.g. FBI in 1975. After introducing the two innovative product in the 1980s, optical scanner and personal computer, the fingerprint biometrics method had enabled for non-criminal purposes (O'Gorman 2002).

### 3. WHY USING BIOMETRICS

Biometrics is a general term employed for defining a feature or a process. Concerning process, it is a procedure for recognizing a person with regard to measurable biological or behavioural trait. When the feature is concerned, it is a measureable biological and behavioural characteristic, which is appropriate for automatic recognition. Moreover, there is an application, which utilizes particular individual

characteristics on behalf of access control through examining biometrics-based authentication and biological data. There are a couple of main purposes that shows why the biometric technique is preferred over old-fashioned approaches (Newman 2010):

- The identification process needs an individual to be physically present at the identification's point.
- Carry a smart card or remember a password will be eliminated through the biometric based identification.

Today, the number of IDs, smart cards, tokens, passwords, and PIN numbers are being increased and it makes life much more complicated. People, for example, has to carry a couple of smart cards, IDs, Pin centric devices among remember more than two or three passwords of their work emails, credit cards and the like. There are several risks concerning IDs and passwords which are named in the following (Newman 2010):

- The password or ID cards may be lost or forgotten
- Possible to be copied or stolen
- Needs to be changed on a regular basis
- Occasionally not accurate enough

The top solution to well identify and verify that “you are who you say you are” is to make use of a unique bodily characteristic such as iris or fingerprint. Generally, there are various kinds of biometrics available today e.g. fingerprint, iris scan, facial recognition system and all of these methods have to meet three cornerstone items as a good biometric identifier (National Science & Technology Council Subcommittee on Biometrics & Identity Management 2005):

- Universal: the biometrics elements should be found in all individual
- Unique: biometric should be unique to each person
- Permanent: the biometric characteristic ought remains permanent over the time

### **3.1. ADVANTAGE**

The biometric approaches carry outstanding features by adding complexity to authorization structures and making it hard to reach thru a common tactics. It is also cover the existing risk and problem for authentication by common method e.g. password. The significant advantages of biometric are (Cavoukian 2008, Boatwright, Luo 2007):

- Biometric characteristics cannot be lost, stolen, or forgotten
- It is difficult to forge or share
- It could be used together with smart cards and PIN, hence refining the current security system without changing them

### **3.2. ISSUES**

It is important to define the “living individual” term. Non-natural stuff like latex finger, prosthetic eye, or plaster hand may be used in place of the real live item. In fact, the biometric devices may have an opportunity to integrate exclusive algorithm to deal with this issue and control the living features. Moreover, there are specific issues, which are positioned in the following (Newman 2010, Cavoukian 2008, Boatwright, Luo 2007, Mordini, Petrini 2007, R. Heckle, S. Patrick et al. 2007):

- Acceptance of biometrics from users or customer
- Improve biometrics technology obstacles
- Software and hardware necessities
- Integrated biometrics with infrastructure
- Store and transmit biometrics data thru encryption technique
- Biometrics effect on multifactor authentication strategies

### 3.3. BIOMETRIC APPROACHES

There are more than 14 methods has been presented on behalf of biometric identification such as fingerprint, ultrasound fingerprint, facial feature recognition, retinal and iris scan, hand geometry, ear shape, body odor, signature dynamic, voice verification, foot dynamic, skin pattern, computer keystroke dynamic, and DNA analysis. The brief definition of three prevalent biometrics approaches will be depicted in this section. Likewise, the comparison table with regard to definition of biometric trait will be provided to show the characteristics rate of above-mentioned techniques (National Science & Technology Council Subcommittee on Biometrics & Identity Management 2005, Newman 2010, Klokova 2010, Boatwright, Luo 2007).

#### 3.3.1. Fingerprint

The fingerprint-scanner captures an image of the user’s finger, which is located on a device. The taken image then will be converted into a map of details points in order to extract features and enter into an algorithm for generating the binary template. Afterwards, the recent binary template will be stored and it will be used to compare throughout the identification and verification procedure (Figure 1 and 3). The fingerprint patterns, which have been displayed in figure2, are categorized into three core units comprising whorls, loops, and arches. There are five techniques for scanning fingerprint including thermal, optical, capacitance, tactile, and ultrasound. Fingerprint provides high accuracy, fooling the system is extremely difficult, and users willingly accept to be identified with (O’Gorman 2002, Newman 2010).

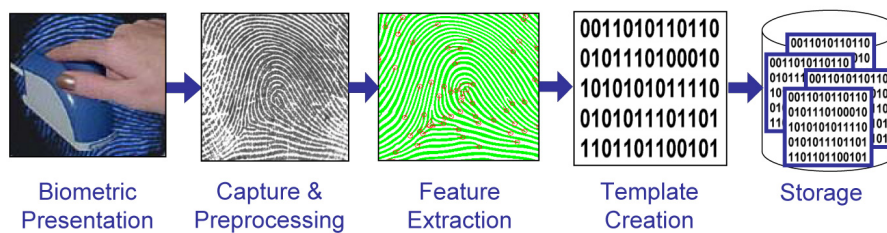


Figure 1: Enrollment process (Source: [www.biometrics.gov](http://www.biometrics.gov))

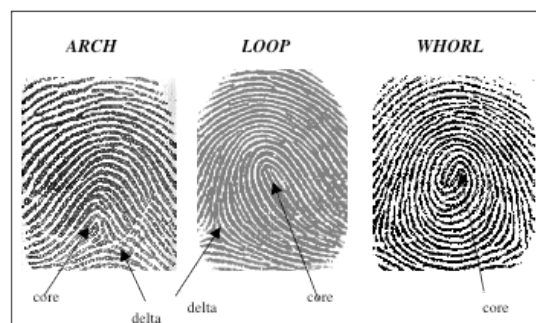


Figure 2: Fingerprint patterns including landmarks (O’Gorman 2002)

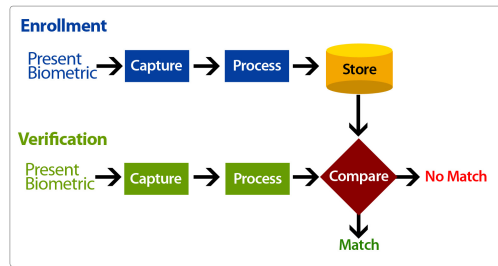


Figure 3: Enrollment and verification process schematic (Newman 2010)

### 3.3.2. Iris imaging

The individual's iris pattern is one of the complex and unique structures, which is fit for identification. Iris patterns consist of specific features for instance corona, crypts, filaments, and so forth. Image of iris can be captured by black and white video camera. Extracted unique features from the image will be converted into an exclusive iris code (Figure 4) and compared to recognize the user later. This approach has provided extraordinary accuracy. This is easy to use although there is refusal to accept from users.

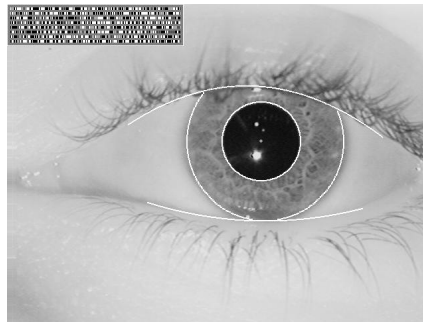


Figure 4: Iris scan and exclusive iris code (Source: [www.biometrics.gov](http://www.biometrics.gov))

### 3.3.3. Face Recognition

A face image will be captured, mapped a set of points on the face, and finally a unique individual's face model will be illustrated (Figure 5). There is no need for direct interaction with this scheme. However the most important weakness of this type of recognition would be changing the facial features during the time. The system has to be combining the recent stored information with the earlier accumulated image to consider this issue. This approach also would be affected by wearing glasses, poor lightning, and aging the individuals.

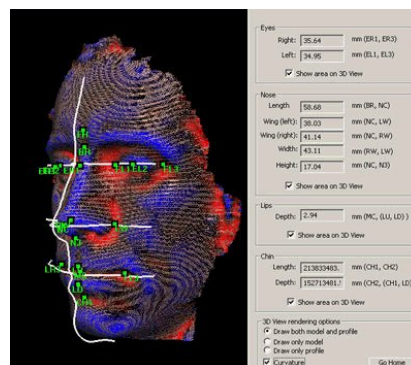


Figure 5: Face recognition process

### 3.4. BIOMETRIC CHARACTERISTICS

In order to choose the best biometrics method with respect to the requirements, the following traits should be evaluated. This section ended up with the comparison chart (Table 1) to show the rate of each biometric method with these factors in brief (Newman 2010, Kothavale, Markworth et al. 2004).

- *Acceptability*: it is related to the general public. Fingerprint, for instance, has high acceptance, Face recognition has faced some users who are reluctant to be recognized whilst DNA has low user acceptance.
- *Circumvention*: the biometric technique must be difficult to fool.
- *Collectability*: easy to attain biometric trait. For instance, fingerprint image would be easily obtained thru a scanner and commonplace process, however face recognition needs well-ordered environment and good equipment to perform. DNA also has a complex process.)
- *Performance*: the technique has to provide precise outcomes in different environmental conditions.
- *Permanence*: the feature should not change during the period. A face of individuals may change with elderliness.
- *Uniqueness*: mostly, there should not the same distinguishable characteristic with individuals. (For example: DNA is unique excluding amongst twins who have the similar DNA.)
- *Universality*: the particular feature should be found in all individuals.

Biometrics	Acceptability	Collectability	Circumvention	Performance	Permanence	Uniqueness	Universality
Fingerprint	H	H	H	H	H	H	M
Hand Geometry	M	H	M	M	M	M	M
Retinal Scanning	L	L	H	H	M	H	H
Iris Scanning	L	M	H	H	H	H	H
Facial Recognition	M	H	H	M	L	H	H
Dynamic Signature	H	H	L	L	L	L	L
Keystroke Dynamics	M	M	M	L	L	L	L
DNA	L	L	L	H	H	H	H
Voice Recognition	H	M	L	L	L	L	M

H= High, M= Medium, L= Low

Table 1: Comparison of Biometric Techniques

### 4. EXAMPLE OF SIMILAR SYSTEM IN USE

There are a large number of universities in the world especially in the united state have employed biometrics (fingerprint and hand geometry) system to identify or verify their staff and students alike. The following list shows the small number of former universities:

- Keene State College
- The University of California at Santa Barbara
- Rutgers University
- The University of New Hampshire
- Johnson & Wales University at Denver
- The Bio design Institute at Arizona State University
- The University of Georgia

## 5. WHY FINGERPRINT

The biometric technology especially fingerprint has been advanced in tininess and dropped in cost. Hence this technology is being readily affordable for a large number of businesses with the different size, and government alike. The most outstanding advantages of fingerprint are (Bhargav-Spantzel, Squicciarini et al. 2010, IBG 2002, Klokova 2010, Kothavale, Markworth et al. 2004, Saraswat, Kumar 2010, Zhang, Li et al. 2010):

- Fingerprint is using simple algorithms and not computationally expensive. (Face recognition algorithm, compare with fingerprint, are somewhat more complex. DNA also needs a lot processing power because of its complexity.)
- Cost: Fingerprint requires low cost hardware and software to implement. (The cost of hardware and software in face recognition are more than fingerprint due to its complexity. Nevertheless, DNA needs professional hardware, which is costly because it is not fully automated and requires knowledge, laboratories, sequencer, and assembler.)
- Memory requirements: Fingerprint no needs much memory, but face recognition requires lots of memory particularly to store 3D models. DNA also needs a large amount of memory depending upon the length of DNA
- It is non-invasive to get hold of a fingerprint thru a scanner.
- It has a largely wide acceptance with law enforcement, general public, and forensic society.
- It is extremely difficult to forge or share
- There is no way to re-construct the unique fingerprint pattern from the template (identify theft)
- FRR is characteristically less than 0.1% whilst FRR are under 0.01%
- Fingerprint is the best mutual biometric method in the market by 48% (Figure 6)

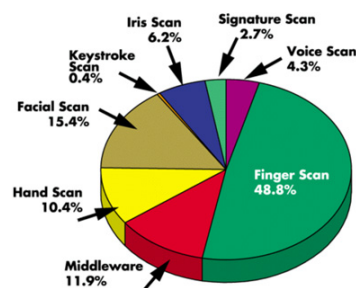


Figure 6: The biometrics methods in market (Source: [www.findbiometric.com](http://www.findbiometric.com))

## 6. PROPOSED PROJECT

This project will incorporate a fingerprint based student identification system that will maintain student attendance register within the University of Bedfordshire for various modules to monitor the physical student's attendance and find a key to eliminate paper-base process together with fooling the system by swapping absent student's smart cards or signing the attendance sheets on behalf of other students.

The proposed identification method could be executed in the university's lectures and practical sessions by external or portable devices without changing or improving university's infrastructure. The benefit of biometric based attendance system is that the attendance system expects students to be physically present for identification process. Using this scheme will overcome the drawbacks of the current system within

this university that can be fooled by “buddy swapping” of an absent classmate by the use of his/her smart card and the like.

The delivered application will provide a comparative analysis and use the data mining technology to provide accurate results with regard to making a closest template match within the database.

## **7. CONCLUSION**

The benefit of fingerprint based student attendance system in this project is that the attendance process expects students to be physically present for identification. Fingerprint technique comes up with high acceptability, collectability, circumvention, performance, permanence, uniqueness, and medium universality. This method is cost effective and dose not need a complex hardware and software. Using this scheme will overcome the drawbacks of the current system within the university that can be fooled by “buddy swapping” of an absent classmate by the use of his/her smart card and the like. The presented application will provide a new comparative analysis and use the data mining technology.

## 10.5 APPENDIX E – PROJECT PROPOSAL

### MSc Project Proposal Form

AY11/12, Semester 3

<b>Student Number</b>	1118797	
<b>Student Name</b>	Farzad Parvinzmir	
<b>Degree Course</b>	Applied computing and information technology	
<b>Supervisor Name</b>	Dr. Aruna Shenoy	
<b>Title of Project</b>	Biometric based student attendance register	
<b>Description of your artefact</b>	<p>This project will incorporate a fingerprint based student identification system that will maintain student presence register within the University of Bedfordshire for various modules to monitor the physical student's attendance, which is the vital issue for a large number of universities.</p> <p>The benefit of biometric based attendance system is that the system expects the student to be physically present for identification. This scheme will overcome the drawbacks of the current attendance system within this university that can be fooled by "buddy swapping" of an absent classmate by the use of his/her smart card. The delivered application as an artefact will provide a comparative analysis with respect to FAR and FRR and use the data mining technology to provide accurate results with regard to making a closest template match within the database. This project will use 50 fingerprints templates, and examine within 10 live individuals.</p>	
<b>What methodology (structured process) will you be following to realise your artefact?</b>	<p>PRINCE2 framework.</p> <ul style="list-style-type: none"> <li>• Create Project brief and Gantt chart</li> <li>• Literature review, executing enrolment process</li> <li>• Produce initiation document</li> <li>• Developing fingerprint attendance system</li> <li>• Evaluate and test</li> <li>• Project report and conclusion</li> </ul>	
<b>How does your project relate to your degree course and build upon the units/knowledge you have studied/acquired</b>	<p>I will perform this project with respect to these unit in which I have studied before: Computer security, Data modelling and management, Applied programing</p>	
<b>Resources</b>	<ul style="list-style-type: none"> <li>• University's security laboratory</li> <li>• Fingerprint scanner and fingerprint SDK (GrFinger)</li> <li>• New Student database</li> <li>• Microsoft Project</li> <li>• CATS computer laboratory</li> <li>• Mathworks Matlab</li> <li>• J2EE (NetBeans, BlueJ) / Visual C# (subject to change)</li> </ul>	
<b>Have you completed &amp; submitted your ethics form?</b>	<b>Yes</b>	No



## 10.6 APPENDIX F – USER GUIDE

To start the application you should open MATLAB software, place the whole directory of this application into your Matlab current folder by drag, and drop. Next, you need to type “intro” into the command window (case sensitive) (Figure F.1).

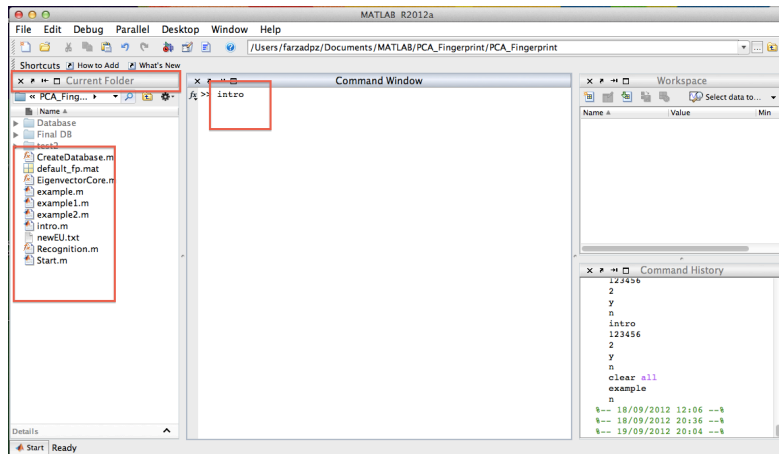


Figure F.1: Matlab screenshot. You should be able to see all the application part in the Current Folder window

After executing intro, you will be asked to enter a password. The default password is “123456” without any space or symbols (Figure F.2).

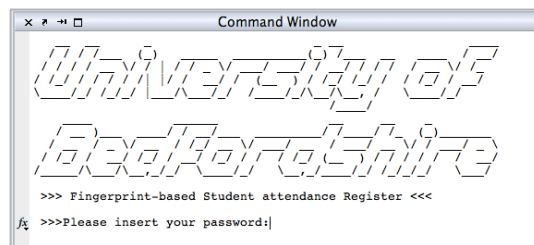


Figure F.2: Intro screenshot

Afterwards, you can see the main menu with 3 options to choose. They are:

- 1- Load default database
- 2- Creating new database
- 3- Identification

All of these options come with a representative number. You can choose the appropriate number to execute one of the provided options (Figure F.3).

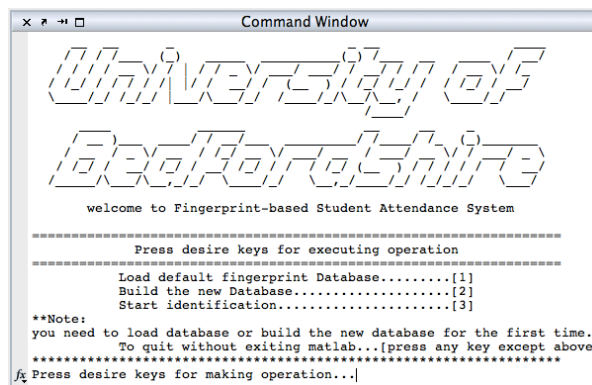


Figure F.3: Main menu of system with 3 options

Application would guide you for choosing each of these items. You need to follow the given instruction to perform each part of this application. For example, if you select “Load default database” it will do this automatically and inform you that database has been loaded successfully, and after that, you can perform identification without building a new database.

Note:

If this is the first time you run this software, you must load default database or create a new database by using your fingerprint datasets.

Creating database is easy. You just need to insert “2” and then system guide you to select directory of your datasets (Figure F.4). All the rest of process will be done automatically and system will show a message which comprising “Database has been created successfully”.

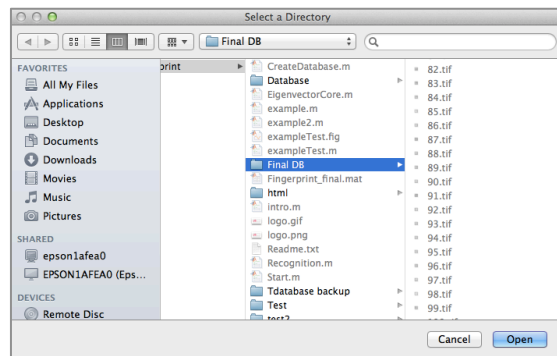


Figure F.4: Select a datasets directory

The last option is identification. By selecting number “3”, you can perform this step. System will ask you to select the captured fingerprints that you want to identify. After that, you need just to select the number of file (e.g. student ID or 1, 2, 3 . . .) to identify the chosen finger against all fingerprints in databases. The result would be the name of student, ID, and his/her course. Moreover, a figure could show the matched fingerprint in database with your selected fingerprint image (figure F.5).

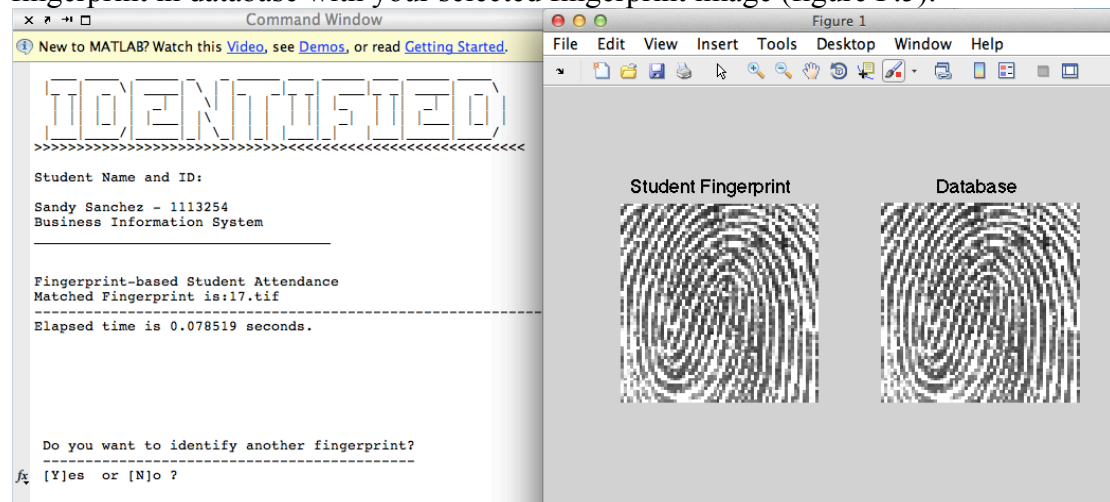


Figure F.5: Identification result screenshot

# 10.7 APPENDIX G – PROJECT POSTER



University of Bedfordshire

## Fingerprint-based Student Attendance Register

Name:  
Farzad Parvinzmir  
Student ID:  
1118797  
Course:  
MSc. Applied Computing  
and Information  
Technology  
Supervisor:  
Dr. Aruna Shenoy

---

### Introduction

#### Biometrics Approaches



1- Low-cost of devices for deployment  
2- High user acceptance  
3- Good accuracy  
4- Fast response

**Fingerprint**

Buddy Swiping or Signing the Paper Register for absentees

88% Paper Register

Home Office UK Border Agency

Paper-based & RFID Card can be fooled (ineffective), time taken, not available

### Achievements

Creating datasets with 100 fingerprint images

Developing application to identify Student fingerprint based on PCA, and capability to connect to university database

Compute:

- the Mean of Data
- Covariance
- Eigenvector and Eigenvalues
- Map data to new space

Recognize input fingerprint as a closest stored data (Euclidean Distance)

Acquiring high accuracy, performance, and reliability

---

### Features & Benefits


#### PCA Based on

Principal Component Analysis


- Identifying patterns in data
- Compressing Data by reducing the number of dimensions
- Forming a new coordinate system
- Mapping data to the new space




**Identification**  
one-to-many




**Developed**  
by MATLAB




**Data-mining**  
PCA & Euclidean Distance



**High Accuracy**  
99% correct result



**Fast Response**  
7ms average per fingerprint



**Connect to**  
any database

### Conclusion

- Performance
- Accuracy
- Small size of DB
- Work with any scanner
- Capability to work offline
- Low computational complexity

REFERENCES:  
MALTONI, D., MAIO, D., K. JAIN, A. and PRABHAKAR, S., 2009. *Handbook of Fingerprint Recognition*. Second edn. London: Springer.  
NEWMAN, R., 2010. *Security and Access Control using Biometrics Technologies*. 1st edn. Boston: Cengage Learning.  
SMITH, L.L., 2002. *A tutorial on principal components analysis*. [http://www.cs.otago.ac.nz/cosc453/student\\_tutorials/principal\\_components.pdf](http://www.cs.otago.ac.nz/cosc453/student_tutorials/principal_components.pdf) edn. Otago: Department of Computer Science - University of Otago.  
TURK, M.A. and PENTLAND, A.P., 1991. Face recognition using eigenfaces. *Computer Vision and Pattern Recognition, 1991. Proceedings CVPR '91, IEEE Computer Society Conference on* 1991, pp. 586-591.