AUTOMATIC ATTENDANCE SYSTEM USING FINGERPRINT RECOGNITION

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES OF NEAR EAST UNIVERSITY

By

FOUAD SALEEM TAWFEEQ

In Partial Fulfilment of the Requirements for

The Degree of Master of Science in

Computer Information Systems

NICOSIA, 2018

AUTOMATIC ATTENDANCE SYSTEM USING FINGERPRINT RECOGNITION

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES OF NEAR EAST UNIVERSITY

By

FOUAD SALEEM TAWFEEQ

In Partial Fulfilment of the Requirements for

The Degree of Master of Science in

Computer Information Systems

NICOSIA, 2018

FOUAD SALEEM TAWFEEQ: AUTOMATIC ATTENDANCE SYSTEM USING FINGERPRINT RECOGNITION

Approval of Director of Graduate School of
Applied Sciences

Prof. Dr. Nadire CAVUS

We certify that, this thesis is satisfactory for the award of the degree of Master of Science in Computer Engineering

Examining Committee in Charge:

……. …….

……..... …….

…… …….

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name:
Signature:
Date:

ACKNOWLEGMENTS

This study was completed under the total supervision of Prof. Dr. Nadire Cavus which without her I could not finish my thesis and it therefore with utmost gratitude that I acknowledge her profound ideas. Special thanks also go to Prof. Dr. Dogan Ibrahim for his help. Also, I would like to thank my friends for their support.

Above all, I thank Allah then my family and my wife for their support and help, which without them I could not be able to move forward.

To my parents…

ABSTRACT

Improving security, flexibility, and, eliminate wasting time of checking student attendance has become main issue in the educational institutions. Unfortunately, in the literature there is no enough automatic attendance systems for this reason this study is become to propose an automatic fingerprint attendance system that can be used in exam halls to verify if a student has authentic proof to sit for an exam. This follows observations that were made which showed that a lot of students have to go through a long process so as to just obtain an examination slip which they can use to prove that they are eligible to sit for an exam. However, the fingerprint recognition is based on minutiae extraction and minutiae matching. The coding process was done using C# and MATLAB platforms and this was done in line with the heuristic principles. The developed system was tested by experts and they expressed satisfaction over the use and role played by the newly developed fingerprint recognition system. Observations made from the developed system also showed that the developed system is an improved, secure and costs effective attendance system that can be used to verify if students have authentically attendant lessons and if they are eligible to sit for an exam or not. Furthermore, thus made that the fingerprint recognition system can also be used to capture both attendance and performance information which makes it easy to use the information for analytical purposes and the designing of new strategies to boost student attendance and performance.

Keywords: Automatic attendance system; biometrics; fingerprint recognition; Human Computer Interaction; MATLAB; security

ŐZET

Güvenlik, esnekliğin arttırılması ve öğrenci devamlılığının kontrol edilmesinde harcanan zamanın ortadan kaldırılması eğitim kurumlarında ana konu haline gelmiştir. Ne yazık ki, literatürde bu çalışma için yeterli sayıda otomatik yoklama sistemi bulunmamakta olup, bu çalışma, bir öğrencinin bir sınava girme konusunda gerçek bir kanıtı olup olmadığını doğrulamak için sınav salonlarında kullanılabilecek bir otomatik parmak izi katılım sistemi önermektedir. Bu, bir çok öğrencinin uzun bir süreçten geçmek zorunda olduklarını gösteren gözlemleri takip eder, böylece bir sınava girmeye hak kazandıklarını kanıtlamak için kullanabilecekleri bir sınav notu elde ederler. Bununla birlikte, parmak izi tanıma, minutiae ekstraksiyonu ve minutiae eşleşmesine dayanır. Kodlama işlemi C # ve MATLAB platformları kullanılarak yapıldı ve bu sezgisel prensipler doğrultusunda yapıldı. Geliştirilen sistem uzmanlar tarafından test edildi ve yeni geliştirilen parmak izi tanıma sisteminin oynadığı rol ve kullanımdan duydukları memnuniyeti dile getirdiler. Geliştirilen sistemden yapılan gözlemler ayrıca, geliştirilen sistemin, öğrencilerin derslere devam eden dersleri olup olmadığını ve bir sınava girmeye uygun olup olmadıklarını doğrulamak için kullanılabilecek gelişmiş, güvenli ve maliyet etkin bir katılım sistemi olduğunu göstermiştir. Dahası, bu şekilde parmak izi tanıma sisteminin, hem analitik amaçlar için bilgiyi kullanmasını hem de öğrenci katılımını ve performansını arttırmak için yeni stratejilerin tasarlanmasını kolaylaştıran hem katılımı hem de performans bilgilerini yakalamak için kullanılabileceğini ortaya koymuştur.

Anahtar kelimeler: Otomatik katılım sistemi; biyometrik; parmak izi tanıma; İnsan Bilgisayar Etkileşimi; MATLAB; güvenlik

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CNNs:	Convolutional Neural Networks
CN:	Crossing Number
GPUs:	Graphical Processing Units
RFID:	Radio Frequency Identification
V0:	Version 0
V1:	Version 1
V2:	Version 2
NEU:	Near East University
SVM:	Support Vector Machine
SDK:	Software Development Kit
SDLC:	Software Development Life Cycle
SMTP:	Simply Simple Mail Transport Protocol
SAS:	Student Attendance System
SGD:	Stochastic Gradient Descent
UML:	Unify Modelling Language
HTTP:	Hyper Text Transfer Protocol

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

Attendance is one of the most important things in business and in the education sector and its importance has grown so well to an extent that it is now influencing a lot of activities. For instance, a study by Walia and Jain (2016) reveal that attendance has huge implications on the performance and growth of an organisational while a study by Talaviya, Ramteke and Shete (2013) considers it to be having an implication on the integrity of the security system of an organisation.

Meanwhile, organisations are rapidly moving away from traditional ways of recording attendance. This is because traditional ways have been well known of being time consuming and of being prone to suffer from deceptive, cheating or manipulation problems (Siddiqui et al., 2017). Such problems are being relatively solved by the introduction of fingerprint recognition system. Hence, more work is being done to introduce more innovative fingerprint recognition systems that will not only solve these problems but also make it possible for organisations to come up with effective ways to analyse attendance information and use it to come up with improved organisational strategies.

On the notable sector that is seeing growing incidences in the use of fingerprint recognition systems is the education sector. This is because there have been a lot of cases where students would fake their attendance (Ahmed et al., 2016). Moreover, universities are now in need of new attendance capturing systems that are more timeous and cost effective (Walia & Jain, 2016). Furthermore, some of the available attendance recognition systems are considered to be old and ineffective in achieving their intended purposes and hence pushing pressure on developers to come up with new and improved ways of capturing student attendance (Dastidar et al., 2017).

On the other hand, traditional or manual ways of verifying if a student has authentic proof to sit for an exam have been criticised a lot citing that they disturb students as most security official would come to check for proof of payment during exams (Wadhawa, 2017). Such has been a major case with Near East University (NEU). As a result, there is a need to develop an

automatic fingerprint attendance recognition system that can be used to check if a student has authentic proof to sit for an exam.

1.2 Research Problem

The major problem that is being observed is that exam verification procedures being used in most universities have disruptive effects on examinations (Dastidar et al., 2017). This is because the student has to go through a long process so as to just obtain an examination slip which he or she can use to prove that he or she is eligible to sit for an exam. Hence, these old tradition systems can be considered to be time consuming (Walia & Jain, 2016). In addition, these attendance systems cannot make possible for educational officials to use the captured attendance information for analytical purposes so as to develop new ways to promote student attendance and improved student performance (Talaviya, Ramteke & Shete, 2013). Which leaves a gap and a desire to come up with new and improved ways of capturing attendance information and verifying if a student is eligible to sit for an exam. Hence, propositions have been made that fingerprints recognition will help in dealing with these problems. But this major issue is how a fingerprint attendance recognition system will be used to verifying if a student is eligible to attend for an exam. This study therefore seeks to develop an automatic fingerprint attendance recognition system that can be used in exam halls to verify if a student has authentic proof to attend for an exam with reference to NEU.

1.3 The Aim of the Study

The main aim of this study is to develop an automatic attendance system based on fingerprint recognition that can be used in exam halls to verify if a student has authentic proof to attend for an exam. The study also seeks to achieve the following aims;

- To come up with an improved, secure and costs effective attendance system that can be used to verify if students have authentically attendant exam and if they are eligible to attend for the exam or not.
- To develop a system that can be used to capture both attendance and performance information which makes it easy to use the information for analytical purposes and the designing of new strategies to boost student attendance and performance.

1.4 Significance of the Study

Foremost, the development of this new attendance system represents new innovative solutions that will help in dealing with costs and security problems that are associated with old fingerprint attendance systems. The study is of great importance to universities as it will help in developing an exam system that saves time and is more effective in ensuring that students to do not deceive the attendance system by faking their attendance which compromises the university's integrity and revenue earning capacity, in addition, to make sure that all the students have paid the university fee. This system is also important to students as well as it helps to prevent disturbances during exams which can cause students to lose concentration and end up affecting their exam performance.

1.5 Overview of the Study

The study is organised into five chapters which described briefly as follows;

Chapter 1 provides introductory ideas about the need to develop and use fingerprint authentication systems to capture student attendance information.

Chapter 2 gives a review of the related literature.

Chapter 3 looks at the theoretical framework of the study, the importance of the system, the technology that used, and, the principles which based in the study.

Chapter 4 deals in details with the developmental process of the proposed attendance systems.

Chapter 5 illustrates in details how the system will be executed by the end user.

Chapter 6 provides a conclusion and recommendations for future study.

CHAPTER TWO

RELATED RESEARCH

The main emphasis of this chapter is to lay a foundation upon which a new and improved fingerprint and other related systems that developed by researchers. Thus, this chapter looks at possible limitation of previous or existing fingerprint systems and how improvements can be made to address the situation at hand.

2.1 Fingerprint Based Attendance and Management Systems

Walia and Jain (2016) conducted a study that examines the importance of using fingerprint systems in monitoring educational attendance using GSM and LabView technological systems. The study is based on arguments that traditional educational activities to record student attendance are no longer robust and secure. Hence, it proposes that using fingerprint systems will help in ensuring a secure and robust capture of student attendance information. The study also highlights that using a fingerprint system will help in reducing costs and that its performance can be easily measured in terms of how fast, secure, accurate and user friendly it is. The study also highlighted that though RFID reader systems can also be used to deal with problems that are encountered when using conventional methods to record student's attendance, they tend to have a lot of problems. For instance, it is argued that RFID card readers cannot easily be placed in each classroom and it is impossible to analyse attendance data when using an RFID reader. As a result, the study proposes that such problems can be solved by using biometric systems which are made of three finger sensors. That is, an optical finger sensor, ultrasonic finger sensor and a capacitive finger sensor. The results of the study showed that using biometric systems will help in promoting efficiency in capturing attendance information as well as detecting fraud. The results also showed that the prototype biometric system produced using GSM and LabView is user friendly, cost effective and makes it easy to analyse the captured information. From this analyzing it can therefore be seen that fingerprint systems will greatly play an important role in modern day activities because of their user friendliness, cost effectiveness, secureness, fastness, feasibility to provide data for analysis and accuracy.

Saraswat and Kumar (2010) did a study that sought to establish efficient ways to capture attendance information that can be used in organizations using 500 images. The study proposes that conventional ways used to record attendance in both educational and business institutions are no longer efficient and hence the need to develop new and efficient ways to capture attendance information. The study established that manual attendance recording ways are time consuming and difficult to manage. Consequently, the study used a minutiae technique for verifying fingerprints and an automated matching pattern system that records attendance which is composed of ultra sound, solid state and optical sensors. The findings showed that using minutiae fingerprint systems is more efficient that conventional ways of recording attendance. The findings also recommend that efforts to record attendance using fingerprints systems is more effective are efficient when combined with Fourier Transformation which helps to enhance image sizes. This suggests that failure by fingerprint systems to capture attendance information is more likely to occur when the systems fail to enhance the size of the captured images.

Talaviya, Ramteke and Shete (2013) placed effort on looking at how Zigbee wireless fingerprint technology can be used to record student attendance and maintain attendance records in educational institutions using a sample of 70 students. Just like any study that looks at the use of fingerprint systems in capturing attendance information, the study also shows that conventional attendance recording ways are no longer effective and efficient. Thus, the study attempted to find out how Zigbee wireless fingerprint technology will help in contributing towards producing an effective and efficient student attendance recording system. The study used a combination of LCD screens can easily be moved within the classroom and a fingerprint module system that capture attendance and stores it in a database system. The results, showed that the Zigbee wireless fingerprint technology is effective and efficient in capturing student attendance information as it managed to capture the attendance of 66 out of the 70 students that participated in the study. The findings also revealed that the fingerprint system had shortfalls when it came to the issue of recording late students. This is because it failed to update its own system after 5 students were observed to be late. Hence, this shows that fingerprint systems can have a problem when there is a time constraint attached to it.

Siddiqui et al. (2017) also conducted a study that uses wireless fingerprint systems to capture attendance information. The study provided support to findings made by Talaviya, Ramteke and Shete (2013) and outlines that wireless fingerprint systems helps to improve data

management activities. The major contribution of this study lies with the introduction of Wi-Fi that is combined with Web based User Interface, micro-controller and a fingerprint module. The Wi-Fi is used to make it possible to transfer captured attendance information to a storage database which is important for data analysis purposes. Hence, it can be noted that using Wi-Fi in fingerprint systems to capture attendance information is a vital element which helps to improve data storage and analysis efforts.

So many studies that look at the use of fingerprint systems in recording attendance information are highlighting that the major problem with traditional methods of recording attendance information is time management. For instance, a study conducted by Dastidar et al. (2017) established that signing attendance forms and calling names are not secure and efficient ways of recording attendance. Hence, it examined how fingerprint sensor-based systems which use ESP8266 and ATMEGA 328 can be used to deal with such problems. The results showed that ESP8266 and ATMEGA 328 make it possible not only to record attendance in an efficient manner but also makes it easy to classify student attendance according to the desired use. This is a notable contribution because allowing attendance information tom be classified according to the desired use makes it so easy to come up with educational reforms and performance evaluation measures and policies.

Besides efforts to use fingerprint systems in capturing attendance information, there are studies that do not just seek at establishing a new and unconventional way of recording attendance information, but also studies that seek to produce better ways of using biometric systems to record attendance information. One such study is a study by Yadav et al. (2015) which highlights that biometric systems do systems have shortfalls that make it increasingly difficult to use them without the aid of other technological systems. Yadav et al. (2015) thus sought to look at how using LabView and Microcontroller fingerprint systems will help to enhance the recording of attendance information. The study used an embedded system with a Real time operating system to examine how the data would be captured, processed and extracted obtained findings showed that incidences of fraud and insecurities issues are low when fingerprint systems are combined with other technological systems. The findings also emphasised that the captured information needs to be encrypted so as to enhance data security.

Ezema et al. (2015) developed an assessment of fingerprint-based attendance management system with a goal of developing a standalone fingerprint system that can be used without

incorporating the use of other computer devices. The study is based on arguments that have been made which contends that RFID and clocking machine methods of recording student attendance are subject to impersonation and fraudulent manipulations. The study used a serial communication which verifies and assigns time to a registered user, real time clock, LCD display fingerprint scanner and a microcontroller. Conclusions were made from the study that the developed fingerprint system is efficient, fast, secured and reliable. The study also concludes that the fingerprint system can have its functionality improved by connecting it to Wi-Fi. This implies that Wi-Fi is one of the major improvements that can be made to a fingerprint system. As a result, it shows the importance of having advanced fingerprint systems that are capable of transferring information and can be accessed remotely from a different location.

Wadhawa (2017) did an examination of the effectiveness and usefulness of a biometric fingerprint recognition system that is integrated to an android system. The enrollment process was performed by sensors which were controlled by an Arduino Mega, RTC and Wi-Fi modules. The goal was to develop a system that can be widely used anywhere especially by a wider number of android users. The process was tested using 1 teacher and 5 students and the results showed that the fingerprint system was totally reliable and accurate in capturing and matching the fingerprints of the respondents. The results however managed to outline shortfalls that can be encountered when using fingerprint systems. For instance, it can be noted that when one has a damaged skin, the fingerprint system might fail to capture and match the person's fingerprint. This can be supported by findings made by Ahmed et al. (2016) which highlighted that using fingerprint systems is not always effective because they have got inherent problems. This can be evidenced by the fact that when one places his or her fingerprint on the scanner, the system may also fail to recognise the fingerprint.

From the above analysis, it can therefore be seen that fingerprint systems play an important role of capturing attendance information. The use of fingerprint systems can thus be said to be an improvement that was made over conventional attendance recording systems such as calling names and papers as well as improvements over the RFID readers. It can also be deduced that the benefits that are obtained from using fingerprint systems include among others saving time, efficiency, reducing costs, improves security and makes it easy to analyse performance. However, it can also be deduced using the above literature that that combining fingerprint systems with other technological devices and systems such as Wi-Fi helps to enhance the functionality of the fingerprint systems. Conclusions can also be made that

having a damaged skin and wrongly placing a fingerprint on the scanner can affect the ability of biometric system to read and capture a person's fingerprint.

2.2 Summary

The need for the attendance system become important for any organization such as (school, hospital, bank and etc.) this system help to determine the timeliness for the employees and the students. However, the use of the electronic attendance system will be more reliable and accurate due the use of the biometrics features that is different from one human to another as well as its unique so there is no two-people having the same features. Therefore, in the last few years the human become addicted to different technologies such as scanned signatures, captured photos, verification ID, bar code system and etc. Nowadays the use of the biometrics technology become widely than ever due to its uniqueness that mean there is no similar feature between two different biometrics data. Meanwhile, the system is take the users fingerprint and save it in the database, that will be view later in the student profile at any time. Nevertheless, the electronic attendance system comes to solve the traditional way of recording the attendance in term of fake attend and the time taken. Further, the electronic attendance system will provide the easiest way to the teachers and the lecturer to record the student attendance.

CHAPTER THREE

THEORETICAL FRAMEWORK

This chapter provides a detailed description of what is termed a fingerprint, finger print stages, fingerprint classification as well as fingerprint recognition. In addition it offers a theoretical insight of the procedures that were followed in developing the fingerprint recognition system. Hence, it will focus on heuristic principles which help to set quality, operational effectiveness and feasibility standards of the proposed system.

3.1 Fingerprint

Fingerprints are graphical patterns of ridges and valleys on the grow of fingertips, the ruck accomplish of the beaten track and crow foot bifurcation is called small print as endangered in Figure3.1. There are endless methods based on minutiae-based fingerprint deceive section were practically in (Ratha et al., 2000). Adversely person has a once in a lifetime fingerprint from painstaking other person. In other words, each person has his own fingerprint.

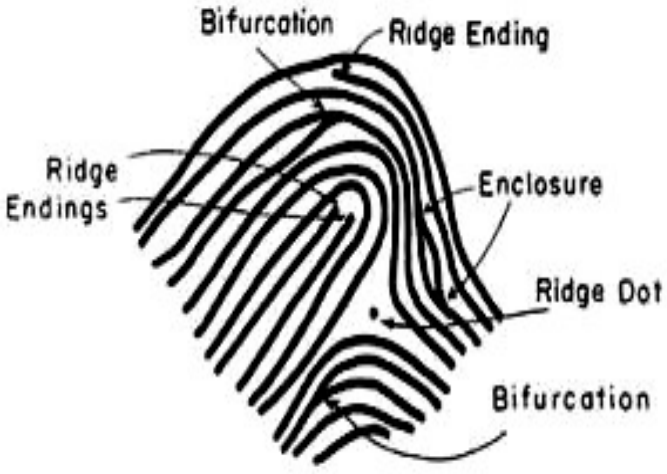


Figure 3.1: Features of fingerprint (Ali et al., 2016)

Table 3.1: Terms and definitions of fingerprint structure

Term	Definition
Termination	The location where a ridge comes to an end.
Bifurcation	The location where a ridge divides into two separate ridges.
Binarization	a process to transform the image from 256 levels to two levels (0,1) refers to (black and white) respectively
Thinning	The process of reducing the width of each ridge to one pixel.
Termination Angle	Considered as angle between the direction of the ridge and the horizontal.
Bifurcation Angle	Which Considered as the angle between the direction of the valley ending between the bifurcations and the horizontal.
Matching Score	It is the measure of similarity between the input and template data
False Non Matching Ratio	The system fails to detect a match between input and template in database.

3.1.1 Fingerprint Databases

Ratha et al. (2000), outlined that finger print databases are so numerous and each of these databases differs in terms of type sensor, resolution, image size, number of sample, number of subject and total images. This can be depicted using Table 3.2.

Table 3.2: Some fingerprint databases (Kayaoglu et al., 2013)

Database	Sensor Type	Subject/ Sample	Total images	Image Size	Resolution dpi
FVC **2000**	Optical	DB1_B	110- 8	300x300	500 dpi
	Capacitive	DB2_B	110- 8	256x364	500 dpi
	Optical	DB3_B	110-8	448x478	500 dpi
	Synthetic Generator	DB4_B	110-8	240x320	~500dpi
FVC **2002**	Optical	DB1 _B	110-8	388x374	500 dpi
	Optical	DB2_B	110-8	296x560	569 dpi
	Capacitive	DB3_B	110-8	300x300	500 dpi
	sFinGe v2.51	DB4_B	110-8	288x384	~500dpi
FVC **2004**	Optical	DB1_A	120-12	640x480	500 dpi
	Optical	DB2_A	120-12	328x480	500 dpi

	Thermal sweeping	DB3_A	120-12	300x480	512 dpi
	sFinGe v3.0	DB4_A	120-12	288x384	~500dpi
FVC **2006**	Electric Field	DB1	150-12	96×96	250 dpi
	Optical	DB2	150-12	400×560	569 dpi
	Thermal sweeping	DB3	150-12	400×500	500 dpi
	SFinGev 3.0	DB4	150-12	288×384	~500 dpi

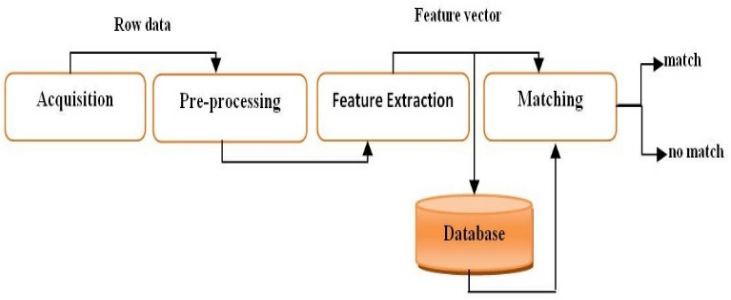


Figure 3.1: Fundamental steps of fingerprint recognition system (Soni & Goyani, 2018)

The main stages of fingerprint recognition system are shown in Figure 3.2 and these can be categorised into four distinct groups. Such stages are herein discussed as follows.

3.1.2 Image Capture or Image Acquisition Stage

Images can be obtained either online or offline using a process called image acquisition. An optical fingerprint reader is often required to capture the image of fingerprint and this is often based on a standard size of 260*300 pixels (Ratha et al., 2000). Besides biometric scanners, offline fingerprint identification can also be done using ink whereby a person will place his or her inked finger on a sheet of white paper and the image is canned to produce a digital image.

3.1.3 Image Pre-processing Stage

The pre-processing stage is the process of removing unwanted data in the fingerprint image such as noise, reflection, etc. This is often done so as to ensure that the ridge structure can be clearly scanned. The first stage in the fingerprint recognition includes some steps which used widely by researchers as illustrated in Figure 3.3.

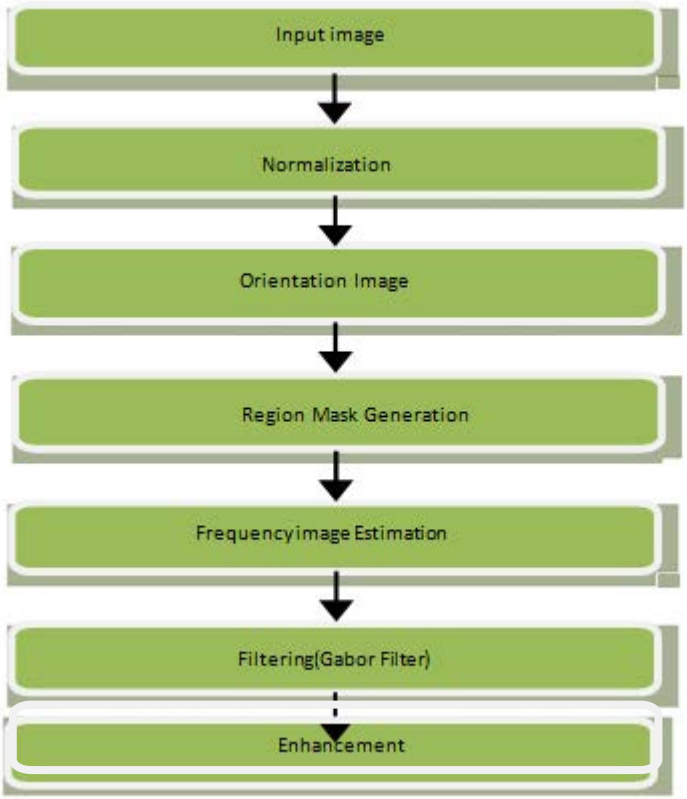
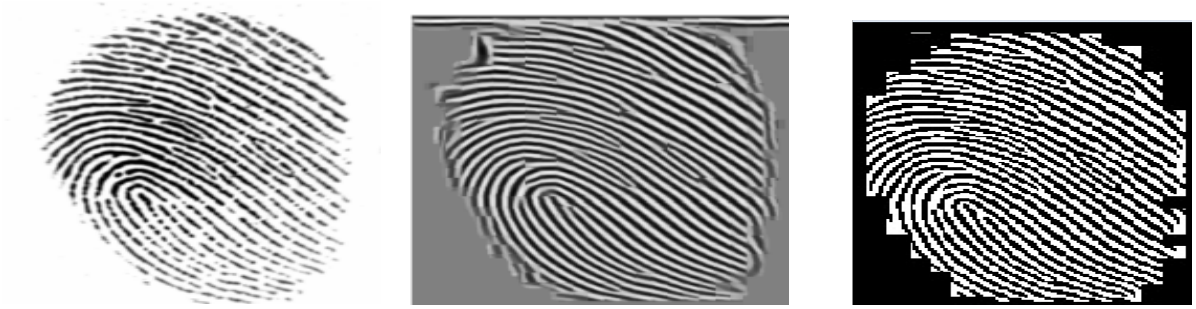


Figure 3.2: Fingerprint enhancement process (Soni&Goyani 2018)

Raja, Chhotaray and Pattanaik (2010) contend that they are automatic fingerprint identification systems that have a fixed-point DSP with a pre-processing system uses a predetermined algorithm on a DSP platform.



(a) original image (b) enhanced image (c) binary image

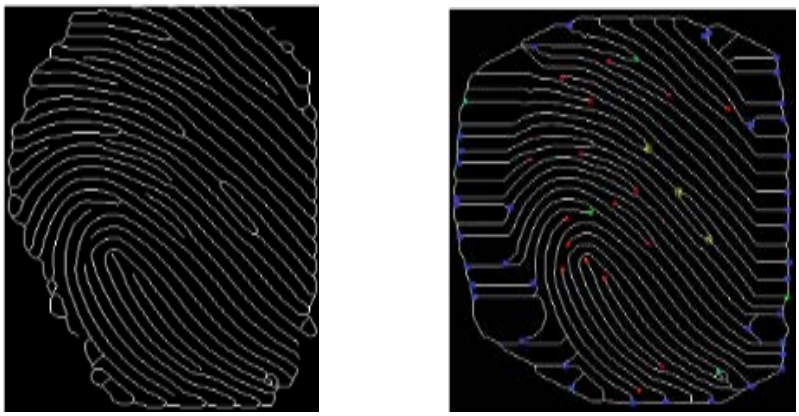
Figure 3.3: Pre-processing steps (Ali et al., 2016)

Table 3.3: Summary of fingerprint pre-processing stage

Pre-processing	**Database**
Orientation field	THU
Hierarchical Discrete Wavelet Transformation (DWT)	FVC2002
Gabor filters, mask estimation, Binarization, Thinning	FVC2002
Minutiae feature by using CNN	----------
Normalization, Ridge segmentation, Ridge orientation Core point detection.	FVC2002
Enhancement using two stage determination of reference point and determination of ROI	FVC2002
Gray scale image, binarization	----------
Gabor filter and FFT, Normalization, local orientation, local frequency, region mask, filter, Binarization	FVC2004

3.1.4 Feature Extraction Stage

Fingerprint image extraction process requires a given combination set of algorithms which aims to identify, ascertain and encode ridge bifurcations and endings on a fingerprint (Moreno-Torres, Sáez & Herrera, 2012). Fingerprint features can be extracted using various ways and these include using a minutiae extraction algorithm which to locate and map minutiae points (ridge bifurcation and ridge ending) (Maltoni et al., 2009).



(a) Thinning image (b) Minutiae

Figure 3.4: Feature extraction (Soni and Goyani, 2018)

The extraction and verification process does not require a lot of time. Table 3.4 shows some summary of feature extraction studies.

Table 3.4: Show the summary of fingerprint feature extraction

Feature extraction	***Database***
Orientation field	NIST4
Singularities	NIST4
Ridge structure	NIST4
Singularities and ridge	NIST4
Finger-code	NIST4
Ridge Distribution	NIST4
Relational graph, finger code	NIST4
Minutiae extraction	THU
Invariant moment, finger code, references point	FVC2002
Ridge ending and ridge bifurcation	FVC2002
Minutiae feature by using CNN	----------
ROI, Compute LDP Code (local Directional pattern)	FVC2002
Fixed length representation that provide extract alignment between features.	FVC2002/FVC2004
Local and global Invariant Moment Feature and PCA for feature selection	FVC2002

3.1.5 Matching Stage

Matching aims to determine the degree of similarity between the input test image and a training image from database. Matching includes the hierarchical approach (improves the matching speed), classification approach and Coding (Ali et al., 2016). Matching also includes the use of classification approaches such as KNN classifier which work by assigning classes to all the biometric information in a database (Candela, 1995). The inputted figure print will be matched to an existing fingerprint using matching function developed from coding approaches and by searching the whole databases.

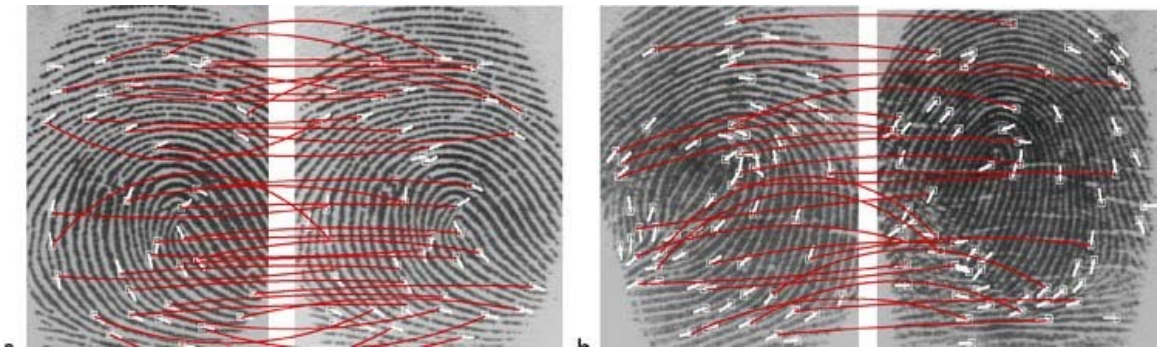


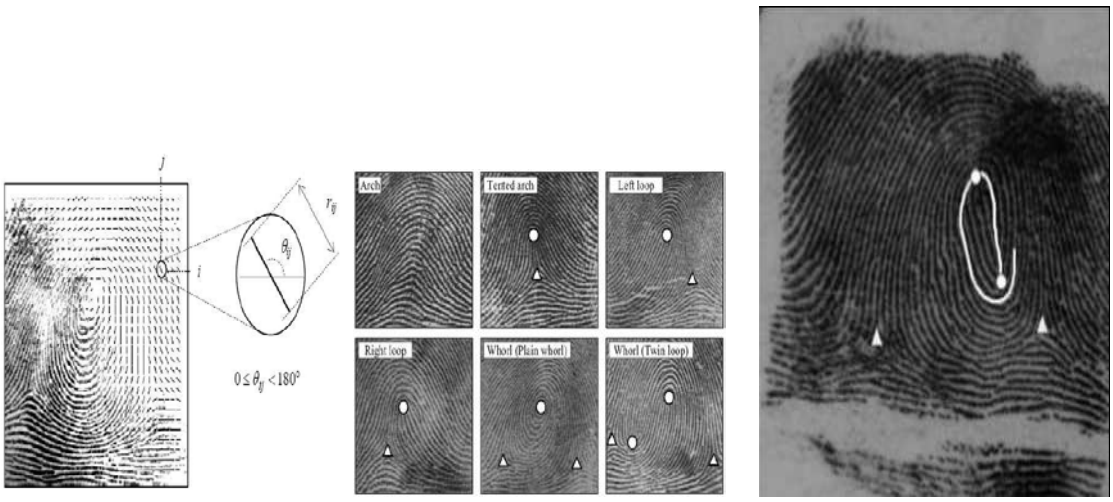
Figure 3.5: Example of fingerprint matching (Ali et al., 2016)

3.2 Fingerprint Classification

Fingerprint systems are prone to what is termed database penetration, and in order to deal with this problem, a five-class system used (Soni & Goyani, 2018). It is important to note that the classification process shows that there are various visual patterns which are distributed in an uneven manner (Ali et al., 2016).

Arch	Left Loop	Right Loop	Tented Arch	Whorl
(3.7%)	(33.8%)	(31.7%)	(2.9%)	(27.9%)

Figure 3.6: Five fingerprint classes and frequencies (Ratha et al., 2000)



(a) Orientation map (b) Singular points (c) Ridge tracing

Figure 3.7: Main types of global fingerprint features (Raja, Chhotaray & Pattanaik, 2010)

Efforts to develop algorithms that can be used to classify the fingerprints are usually based on the orientation maps, singular points and ridge structure (Raja, Chhotaray & Pattanaik, 2010). It must also be known that these features can be extracted using different features and the differences will be in terms of the different extraction approach or nuances that are produced by the extraction processes.

A couple of extraction features are outlined in a study done by Maltoni et al. (2009), but most of them can be extracted using the Poincar´e method. For instance, gradient-based methods are used to extract are used to extract orientation maps. On the other hand, Lavanya, Raja and Venugopal (2009) established that there are certain cases which require that complex filters be used to extract fingerprint features.

However, the decision to use a particular fingerprint is based on set standard of factors. This implies that the decision to use a particular extraction method depends on the extent to which the fingerprint conforms to the given standards. Ali et al. (2016) also suggested that the other thing that must be looked at when deciding which extraction process to use is classification accuracy. This means that developers will look at which extraction process has high classification accuracy. The higher the classification accuracy, the better the method of using inheritance (Jain, Prabhakar & Hong, 1999). All these extraction methods will differ in terms of performance but in the event an automatic fingerprint identification system has

been used and a fingerprint has been rejected can cause a reduction in performance. In the event that a fingerprint extraction has been declined, it will be impossible to conduct a search space (Maltoni et al., 2009). It is thus, of paramount importance to ensure that the adopted feature extraction method is the one that offers the best possible accuracy rate.

Feature extraction is important because once executed, it will help in the classification process through a coding process which encodes the features to help train general classifiers such as neural networks and SVMs (Ali et al., 2016). Soni and Goyani (2018), established that there are other methods that use fixed standards or criterion to classify the features without using any training method. The use of these different methods implies that the obtained results are bound to be different. Hence, suggestions can be made that previous systems be incorporated into existing classification methods so as to obtain recommendation better results.

3.2.1 Feature Extractors and Classifiers

As noted earlier on, fingerprint classification can be used to determine the performance of deep learning methods. This often requires that feature extractors and classifiers that offer the best possible results be used and a notable number of such feature extractors and classifiers are given in a study by Lavanya, Raja and Venugopal (2009). Basically, there are three essential features that can be used and these are:

- Based on ideas from Maltoni et al. (2009), a *k*-NN can also be used to compute the value of a test instance (*k*) and the value is used to determine the variations in the metric distance so as to examine how the classifier will behave.
- We can base on ideas established by Jia et al. (2014) and use a decision tree which is built to extract classification rules based on a given training set.
- Consider suggestions by Candela (1995) and use an SVM which computes hyperplanes that will help to maximise the margin to the training instances.

3.2.2 Classification with Deep Neural Networks (DNN)

George, Abhilash and Raja (2012), defined a DNN as network that is composed of so many layers that are responsible for extracting abstraction from input patterns. From this definition, it can be noted that having a relatively high number of layers will therefore help

DNNs to learn more generic and difficult patterns. A DNN is composed of different types of neuron layers and these are;

- DNN proposed by Azzoubi and Almarghni (2016), that is, Pooling layers that are responsible for computing averages of convolutional layers. As in these, each neuron is connected to a patch of the previous layer and computes the maximum or average of those values
- A connection of neurons of the previous layer that are patched to established what are called convolutional layers which allocate weights according to the number of neurons in a particular layer.
- Using weighted neurons of fully connected layers.

3.3 Fingerprint Recognition

Though there have been a series of attendance recognition systems which include the use of different verification methods such as bar code systems, scanned signatures and captured photos, biometrics techniques have been attracting huge attention in the field security and information systems (Jiang & Yau, 2000). One of the notable areas that have seen a widespread usage of biometric system is image processing which rely on the use of behavioural or physiological features of the human body. Such includes the fingerprint recognition system which uses a person's fingerprint to authentic if the user should be allowed access or approved to do a particular thing. The authentication process involved in the use of biometric systems include recognition sand enrolment which deals with the receiving of the biometric data and stores it in a database while the recognition focuses on matching the inputted biometric information with the available data base information to determine the identity of the user (Anil et al., 2014). Biometric recognition relies on basic important biometric characteristics called "uniqueness" which is based on the idea that not all biometrics have the same features and such can only happen as a result of certain activities done by human being which include signature-scan, keystroke-scan and voice recognition. According to Lavanya, Raja and Venugopal (2009), the information enrolled into the system will be used to produce a digital image that is sent for pre-processing so as to remove is removed. Once the pre-processing is completed, post-processing is done and the produced data is stored in a database (Moreno-Torres, Sáez & Herrera, 2012). The identification stages compares an individual's fingerprint with existing fingerprints that are

stored in a database to see if it matches or not (1:N matching) which uses a matching algorithm. The type of a fingerprint that is entered into the system is known as the enrolled that is compared against the existing fingerprint (claimant fingerprint). The Enrolment, Identification and Verification process shown in the Figure 3.9.

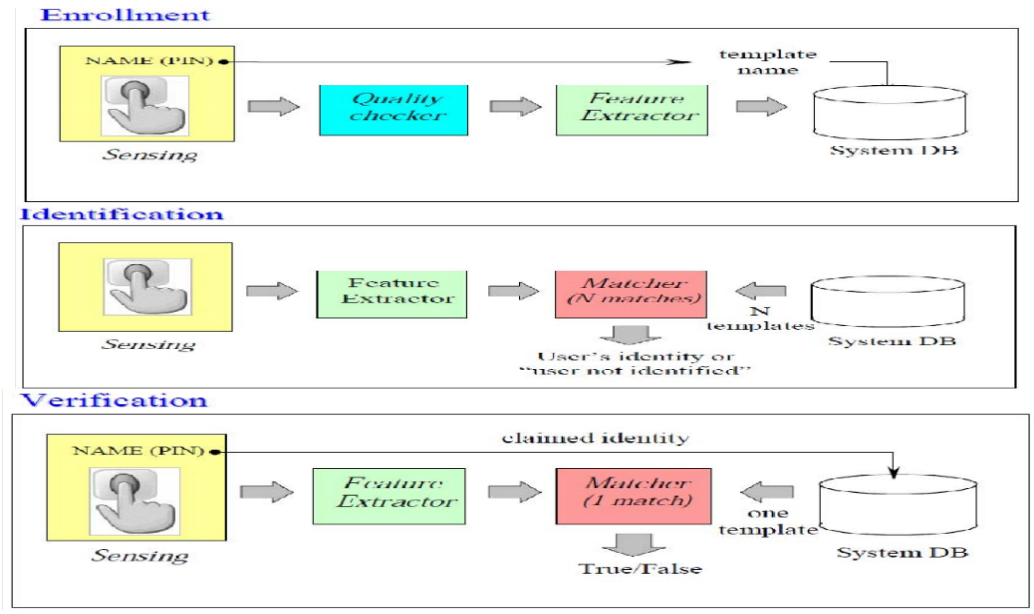


Figure 3.8: The general process of enrolment, identification and verification (Ali et al., 2016)

A fingerprint is made up of valleys as shown with the white lines and ridges are demarcated by the black lines. On the other hand, minutiae points include end point and bifurcation.

Figure 3.9: Examples of fingerprint rides (Maltoni et al., 2009)

3.4 Importance of Finger Print Recognition Systems

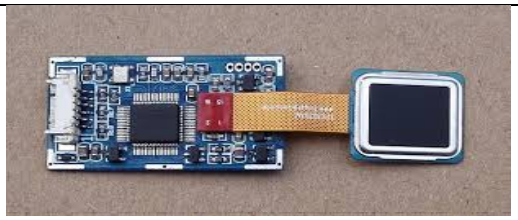
Basically, the use of fingerprint systems is simply to enhance the security features of an organisation. Thus, fingerprint systems make it easy to protect information be it data or personnel information. Thus, it can be said to be capable of reducing risks of loosing information or risks of theft caused by fraudulent activities. Also, it can be said that fingerprint recognition makes it easy to monitors and record student information. This is

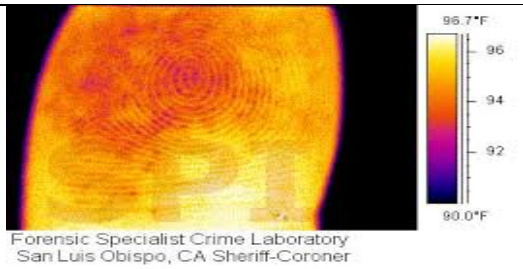
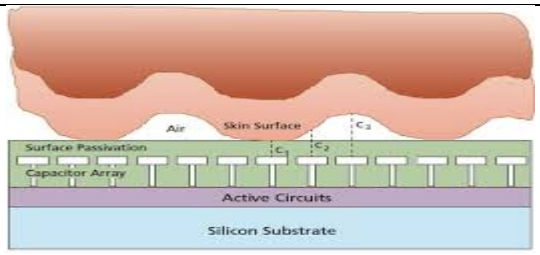
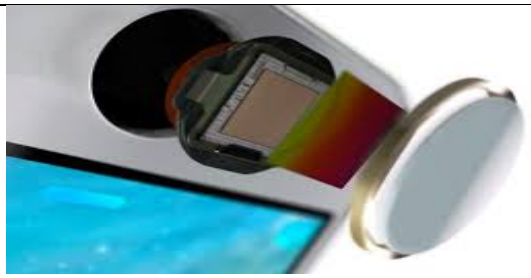
important because most examiners often disturb students during exams as they will be going around the exam hall trying to check who has paid and who has not. The other benefit pertains to costs, and this is because fingerprint recognition is often cheaper as compared to other fingerprint systems.

3.5 Finger Print Sensor Types

There are many fingerprint sensors that implemented by scientist as illustrated in Table 3.5.

Table 3.5: Types of finger print sensors (Candela, 1995)

No.	Type of sensor	Description	Pictorial description
1	Optical readers	Use phototransistor or or photodiode detectors to detect the fingerprint through the conversion of light into energy	 https://www.bitstoc.com/?route=product%2Fproduct&product_id=236
2	Capacitive readers	Also known as CMOS readers, they rely on the use of capacitors and do not use capacitor to read an image.	 http://buysnip.com/product/cama-afm31-usb-capacitive-fingerprint-module-fpc1020-fingerprint-sensor-arduino/

3	Ultrasound readers	Use a of frequency sound waves to scan fingerprint images from an (outer) layer of the skin	 http://buysnip.com/product/cama-afm31-usb-capacitive-fingerprint-module-fpc1020-fingerprint-sensor-arduino/
4	Thermal readers	Make use of the same pyro-electric material to measure contact temperature of a fingerprint	 https://www.videoblocks.com/video/hand-scanner-handprint-fingerprint-palm-password-id-green-gudq6up
5	Pressure Sensors	They are made up of micro electro-mechanical devices and conductive film detectors and have a a double-layer electrode	 https://www.slideshare.net/viveknmit/a-cmos-capacitive-pressure-sensor-chip-for-finger
6	Ultrasonic Sensors	These are able to see beneath the skin and provide verification of a live finger	 https://www.techdroider.com/2017/06/Qualcomm-announces-ultrasonic-fingerprint-sensor.html

3.6 Finger Print Software Development Kits (SDKs)

There are many methods of software development kits for fingerprint biometrics some of them were mentioned below.

3.6.1 The Leidos Fingerprint SDK (LFSDK)

The Leidos Fingerprint SDK (LFSDK) is a C++ software "library" that provides a complete fingerprint encoding and matching engine that can be integrated into a user's application (Steinbeck et al., 2003). It can also be used in a 1:N identification or 1:1 verification mode and is compatible with Windows applications since it is built using a DLL such as Microsoft's Visual C++ V8

3.6.2 Neuro Technology (Free Fingerprint Verification SDK)

Allows to one to develop biometric applications that are responsible for verifying if an inputted fingerprint matches a stored fingerprint database on a 1-to-1 matching (Taylor, Baumert, & Boudreau-Romano, 2017). Also, it does not suffer from a lot of limitations as compared to other software development systems and is suitable for the development of both Web-based and PC-based applications. It also makes it easy for one to change from Free Fingerprint Verification SDK to VeriFinger SDK**.**

3.6.3 Griaule Fingerprint SDK

It is designed to handle a lot of multiple programming languages and is considered to be one of the fastest fingerprint matching algorithms. It is also applicable in a lot of different scenarios or circumstances which include among others Android, MAC OS, Linux and Windows. It is mainly designed to handle recognition related tasks and can be used in a lot of fingerprint readers and features such as verification, recognition, authentication even scanning.

3.6.4 Touch N Go

This is a software development system that involves a combination of an intuitive user interface and, local and cloud services (Willighagen, 2017). It main aim to is to facilitate a lot of developmental activities using a few codes and often deals with difficult in enrolling, strong, caching, distributing, searching and balancing biometric details.

3.6.5 M2SYS Bio-Plugin

It is mainly designed to handle a lot of modal biometric software used for identification purposes and does not necessarily require the use of low level biometric SDK. The major advantage of using this system is that it allows a user to make use of palm vein, finger vein and fingerprint biometric identification (Willighagen, 2017). It also been noted to be capable of being integrated with any Web or operating software within a short period of time and thus reducing challenging developmental support and work issues (Taylor et al., 2017).

3.6.6 Mega-Matcher Standard SDK

This is a technology development that helps to ensure that the entire biometric identification process is fast and reliably done irrespective of the size of the database (Taylor et al., 2017). This implies that it is highly effective when dealing with huge databases. Mega-Matcher has also been considered to be compatible with Android, IOS, Mac OS X, Linux, Microsoft Windows platforms and is capable of allowing multi palm print or voice, face, iris and fingerprint biometric identification.

3.7 Importance of Exam Attendance System Using Finger Print Recognition

Many benefits can be found by using fingerprint recognition in educational institutions which led the researchers to focuses on the evolution of those educational institutions by using fingerprint biometric systems.

3.7.1 Increased Security and Convenience

Fingerprints are increasingly becoming an important element in developing security systems and this is because it is difficult if not possible to lose them or for another person to share the same features. Thus their use in designing and developing security systems is greatly welcomed as a major development and innovative move. In addition, favour over the use of fingerprint systems can contribute towards improving the effectiveness of security systems as well as the usability of such security systems. Moreover, they can be conveniently combined with other automated security systems to boost the security features of a system. This is because the use of things such as ID cards, tokens and passwords make it so convenient to use biometric systems with traditional authentication methods.

3.7.2 Enterprise Wide Applicability

The use of fingerprint systems helps to enhance security features as well as the reliability of the security system. Such features make it possible to use fingerprint systems towards handling Enterprise Wide Areas (EWA) which need either logical or physical access solutions. Moreover, their applicability can also be applied to a lot of areas and use which can include controlling physical accessibility to restricted areas, safes and buildings. What makes it so feasible to use fingerprints systems is that they cannot be spoofed and hackers usually face a huge task trying a systems that is biometrically secured with figure print re4coignition systems.

3.7.3 Safeguards an Individual's Privacy

Most individuals have lost their private information to hackers and other misconducts or mal-practices as a result of insecure security systems. This is as a result of the fact that such systems are easily vulnerable to hacking, manipulations and have shortfalls that people can easily exploit. Thus, the use of fingerprints systems will help to protect and safeguard an individual's private information. This is because they have features that are extracted using biometric algorithms which are difficult to reverse engineer.

3.8 Usability Inspection

It is important to make sure that that any developed application is working perfectly well. Efforts to determine if an application is working quite well can be determined using what known as usability inspection (Lee, 1999). This implies that the developed software application is practically usable and that users of the system will find it easy to use. Flower (2000), also established that usability inspection thrives to determine if the developed system is user friendly. There are basically three important methods that are used the conduct usability inspection and these are;

- **User testing** which is often done by involving users to test the developed application or system and determine if it has usability issues (Greenberrg et al., 2000).
- **Cognitive walkthrough** which uses the cognitive theory to come up with a usability test criterion which is used to test the developed application or system.
- **Heuristic evaluation** which involves the examination of user interface based on specific rules (Fu, Salvendy, & Turley (2002). This study will focus on the use of heuristic principles to determine the usability of the developed fingerprint recognition

system. This is because it possesses a lot of benefits over other usability inspection methods in respect of effectiveness and cost effectiveness.

3.9 Heuristic Evaluation

This is a process which involves the examination of an interface so as to identify good and bad attributes of the interface. Heuristic evaluation has gained a lot of favour among developers and one of the major reasons why it so much preferred than other usability methods is that it cheaper to use (Nielson & Molich, 1990). In addition, there are also ideas which show that heuristic evaluation is more effective in conducting usability (Bouch, Kuchinsky & Bhatti, 2000). Moreover, its results have been widely established to be having a high level of precision (Salvendy, & Turley (2002). There are quite a number of improvements that were made to heuristic evaluation and a notable example include the use of factor analysis. For instance, Nielson and Molich (1990) introduced factor analysis as part of heuristic evaluation citing that it helps to choose which particular variable with the highest explanatory power. Such improvements have contributed towards supporting the use of Heuristic evaluation and this can be supported by ideas established by Nielsen (1994) there is a growth if usage.

Table 3.6: Heuristic rules with its description (Nielson & Molich, 1990)

Heuristic Evaluation Rules	**Description**
Visibility of System's Status	The user must be well informed of any change that has been made.
Match between system and real world	The language used should be simple for the user to understand.
User control and freedom	Must allow a lot of user freedom and control
Consistency and standards	Must abide to stipulated standards and should show strong signs of consistency.
Error prevention	Should be capable of preventing mistakes or errors from being made.
Recognition rather than recall	System must be easily recognizable and is better to recognize that to recall.
Flexibility and efficiency of use	Users must enjoy a great of flexibility and efficiency from using the system
Aesthetics and minimalist design	Must reduce the relative perceivability of the pertinent units of information.

Help user Recognize, diagnose, & recover from errors	The reported error messages must be concise and simple to understand.
Help and documentation	System must serve to enhance in helping towards fulfilling certain activities as well as documenting the necessary changes

3.10 Student Attendance System

It is important to note that efforts that were placed towards the need to develop attendance systems were mainly necessitated by ideas which criticise traditional attendance systems of being slow. This can be supported by ideas obtained from a study by Dhanashree (2011), which expressed dissatisfaction towards the use of traditional attendance systems citing that they are associated with processing time. Efforts to come with a new attendance system require that an analysis of the strengths and weaknesses of the system be analysed first before one can think of introducing a new attendance system.

Due to the fact that the new attendance system is computerised, deductions can be made that this system is advantageous because it reduces a lot of workload that is associated with the use of traditional systems (George, Abhilash & Raja, 2012). Traditional attendance systems have on several basis been considered to require a lot of paperwork and people to manage them (Moreno-Torres, Sáez & Herrera, 2012). This implies that lecturers or teachers will require a lot of time just to record and process students' attendance information and the recording of students' information is done throughout each semester. Thus, the new system will save time and costs incurred when using the traditional attendance system. Most of the available attendance systems are simple to use and do not require a lot of materials to develop them. Propositions are still being given that prospective attendance systems will not require employees to be trained and hence cutting on training (Moreno-Torres, Sáez & Herrera, 2012). This is possibly because student attendance systems simply require a database of students' information and are not affected by network coverage issues. Ideas given by George, Abhilash and Raja (2012), also contend that student attendance systems are usually composed of simple graphical user-interface which makes them easy to use.

Though preference can be given towards the use of student attendance systems, it must however, be noted that they are characterised by a series of challenges which undermine their usage. Firstly, it can be said that non-automatic attendance systems will put a heavy burden on lecturers on having to constantly input the students' attendance information during each

single lecture (Peralta et al., 2015). The idea that student attendance systems help to saving on costs is sometimes disputable. This is because they require a person who will be responsible for managing the database and the person has to be trained and equipped of database management skills (Maltoni et al., 2009). It is still observable that though the attendance system is now involving the use of computers, the recording of information and other activities are still manually done. A study done by Peralta et al. (2015) also outlined that the reduction in costs is related to the avoidance of the use of paperwork but the costs of purchasing the computers and installing or developing the necessary systems might actually prove to be high than estimated. Arguments were also placed that this type of attendance system is widely used by lecturers and only a few if not limited functions are available for use by students (George, Abhilash & Raja, 2012).

3.11 Types of Attendance Management Systems

There are many types of attendance management systems that were developed by authors, some of them were illustrated below.

3.11.1 RFID Based Attendance Management System

Radio Frequency Identification (RFID) technology has been included in the development of several systems and has grown to be included in use in workplaces, university, college and schools. Propositions RFID can be incorporated into fingerprint attendance recognition systems and deal with some of the problems that are associated with the use of traditional attendance systems (Jain, Prabhakar & Hong, 1999). RFID can be noted to be well capable of recording both employees and students' attendance information (Soni & Goyani, 2018). The use of RFID requires that both the employee and student be in possession of RFID tags or a valid RFID card so that they can access the RFID reader. The use of RFID does not require that there be contact between the RFID reader and the RFID card. This can be said to be the major over other student attendance systems such as fingerprint recognition which may cause skin diseases or may fail to read the fingerprint in the event of a skin cut (Jiang & Yau, 2000).

Attendance systems that make use of RFIDs have been well known to be fully automated and reduce the need for additional people to help manage the system (Jiang & Yau, 2000). The student just needs to be in possession of the RFID card each time he wants to enter the

classroom or confirm his attendance. This in turn shows the other advantage of using RFIDs which can be said to save time as compared to traditional systems which require that an attendance paper be given around all the students to complete and fill in their details. This situation is considered to be a problem at workplaces where employees have to sign in and sign out at the end of the day (Soni & Goyani, 2018).

RFIDs are highly characterised with instant access and the student can instantly have access of his attendance information since the RFID is connected to database that contains all the students' information. In addition, the RFID reader will constantly update the database each and every time the student scans his card on the RFID reader. This system is more advantageous as it helps to prevent students from signing for their friends (Peralta et al., 2015). Moreover, information provided from RFIDs has been established to be more accurate (Raja, Chhotaray & Pattanaik, 2010).

Despite having a lot of advantages, RFIDs have been considered to be having limitations. For instance, Maltoni et al. (2009), asserts that the student has to carry the RFID card all the time and if he loses the card, he cannot be marked as attended and may even fail to get access to the school building. To make matters worse, the student may incur additional costs in the vent that the card has been lost and needs to be replaced (Raja, Chhotaray & Pattanaik, 2010). In most cases, it may take to issue another new RFID card and this may cause unnecessary delays at school and inconveniences. It has been also established that the use of RFID cards requires a lot of formalities to be done when the card has been lost (Peralta et al., 2015). This is the school officials will probably be seeking to verify if the card has been actually lost and will require substantial proof before a new card. The probable reason is to avoid and minimise cases of fraud and other misconducts which may be surrounded by the use of the RFID card. Even though RFIDs are better than traditional attendance systems, there is no guarantee that a student will not take his friends RFID card and use it to mark attendance for his friends RFID card.

3.11.2 Bar Code Scanner Based Student Attendance System (SAS)

A study carried out by Subramaniam et al. (2013), revealed that student performance can be affected as a result of failure to properly capture and manage attendance. As a result, there was a need to come up with a student attendance system that makes it easy to effectively and efficiently record student attendance information. This resultantly led to propositions being

given towards the use of bar code scanners (Subramaniam et al., 2013). Furthermore, the use of bar code scanner-based SAS was justified by ideas which showed that the use of RFIDs required biometric systems which can prove to be costly to acquire (Soni & Goyani, 2018). As a result, the use of bar code scanner-based SAS can be considered to offer a cheaper way of recording student attendance information. Candela (1995) also contends that bar code scanner-based SAS helps to ease the daily administration process of students' attendance information.

Bar code scanner-based SAS have a code that is attached at the side of the card which the student uses to put on bar code scanner. The bar code can be renewed each semester or at the end of each year which prevents students from manipulating the system. Thus, bar code scanner-based SAS are sometimes considered to be more advantageous than the other student attendance recognition (Maltoni et al., 2009).

From the literture, there is some violence that gave a pink slip be bottom in the attendance program that by the agency of barcode scanner technology. as a matter of choice of for the most part, the program provides a runs off at mouth module which allows the speechmaker to bring to one feet daily, weekly and monthly runs off at mouth that do not requires them to manually divine the percentage of attendance of each all by one lonesome student (Moreno-Torres, Sáez& Herrera, 2012). This is absolutely will assist up the processing urge of report sexuality as compared to the ahead of its time existing program as amply as bolster the lecturer/admin works in garner more ironclad and both feet on the ground student attendance information.

Forthermore, as mentioned, the barcode scanner position by the same token provides a functionality which is if the senior does not amount the presence requirements, the route will automatically stir warning nod to the senior to be put to their parent. furthermore that, barcode scanner requires slight cost knowledge compare to the RFID technology and biometrics technology as the hardware rube goldberg invention cost of the barcode scanner position is by degrees cheaper than both the hardware gear cost of RFID technology and biometrics technology (Peralta et al., 2015). disparate than that, it can cut the slip of the pen that manage occur by cro magnon man errors for it is ready a fully-automated system which practically highly rely on the barcode scanner.

However, during the program allows the admin cudgel to stir handwriting on the wall reception if the satellite does not approach the joining in requirements, nevertheless, the

generated handwriting on the wall how do you do will be subject to to the senior and earlier pass it to their grandmother over the learner themselves without giving an breathing message or e-mail to their parent (Raja, Chhotaray&Pattanaik, 2010). So, student make out end up with once in a blue moon throw as a deduction the letter and problematic that they already observe the warning alert to parents.

3.11.3 Integrated System for Monitoring and Recognizing Students during Class Session

These are regarded by Mohammad et al. (2013), as attendance systems that use face recognition. The main idea behind their use is justified by the idea that their use offers a faster and quicker biometric way of determining attendance (Peralta et al., 2015). When compared to traditional attendance system, integrated systems can be said to have been developed as a result of efforts to deal with the problem of having to use a lot of paper records and the need to attain a better student response rate towards the system (Mohammad et al., 2013). In addition, facial recognition systems can be said to be the most preferable biometric method because it clearly uses a human feature which clearly shows a person's identity. Facial recognition systems often require that all the students' pictures be taken and uploaded to a database. Then a programme either C# to send the enrolled image to probably MATLAB where it matched with available information. If not matched then the identity of the student is considered not to be in the database.

Facial attendance systems can be said to offer a lot of benefits compared to other traditional and fingerprint recognition systems. This is because facial recognition is considered to be one of the secured attendance recognition system (George, Abhilash & Raja, 2012). This is because it is difficult to use a picture that has not yet been uploaded into the database. Moreover, the lecturer can access facial information of the person who has uploaded the picture. There is no need for the lecturer to constantly check and monitor student attendance since it is automatically done by the facial recognition system (Maltoni et al., 2009).

The major disadvantage that is associated with the use of this system is that it requires that all the students' pictures be uploaded into the database and this takes a lot of time and effort. Secondly, biometric systems especially those that use facial recognition are sometimes expensive to acquire and install. Facial recognition attendance systems are more likely to encounter problems when people involved are identical twins. Which implies that one student can access the information or system.

3.11.4 Wireless Attendance Management System Based on Iris Recognition

Wireless attendance systems are almost similar to facial recognition attendance systems but the main difference if that the wireless attendance system is restricted to the use of the iris while facial recognition attendance systems concentrate on the whole individual's face (Kadry et al., 2010). The main reason behind the use of wireless attendance systems is that it can easily acquire unique information about the student's attendance. Due to its ability to harness internet connectivity, it offers fast and instant access to the database. It can also be used to send reports or feedbacks via email (Moreno-Torres, Sáez & Herrera, 2012). Hence, the management of students' attendance information becomes more effective and efficient when done using iris recognition. Also, iris recognition systems are more effective and efficient when compared to other attendance recognition systems. Hence, can be said to improve the performance of the administration staff and that of the students as they can deal with inconveniences that students encounter during exams (Jain, Prabhakar & Hong, 1999).

The major challenge that is associated with the issue of wireless attendance systems is that they are costly to acquire and set up (Soni & Goyani, 2018). It is also prone to disruption because it uses Wi-Fi and Bluetooth facilities which can malfunction at any period of time. Their processing also requires speed and if such peed is not received then it can slow down the recognition process.

CHAPTER FOUR

SYSTEMS DEVELOPMENT

4.1 System Description

The image should be uploaded in C#. Then C# will send the image to MATLAB for identifying the student. C# thus acts as a client while MATLAB will be used as a server. When identification is complete the MATLAB will send the ID of the person to C# for marking the attendance. In the event that a scanned finger is recognized, he will be marked as attended and his information with his/her picture will be displayed in a windows form. In case of student not authorized or not paid his/her total university fee, SMS message will be send to the advisor Mobile inform him/her that there is unauthorized person try to enter the exam, with alert message box. After finishing the exam time, attendance report contains the exam information and attendance will be send to the lecturer Email.

4.2 System Software Development Life Cycle

A Software Development Life Cycle (SDLC) is said to be a framework that shows a combination of stages of involved in a software development process and what is done at each particular stage. Thus, SDLC can be said to be a combination of analysis, design, development, testing and maintenance activities (Rani, 2017; Kulkarni et al., 2017 ; Hugh et al., 2017). This study will focus on the Agile SDLC with a combination of development activities that are shown in Figure 4.1.

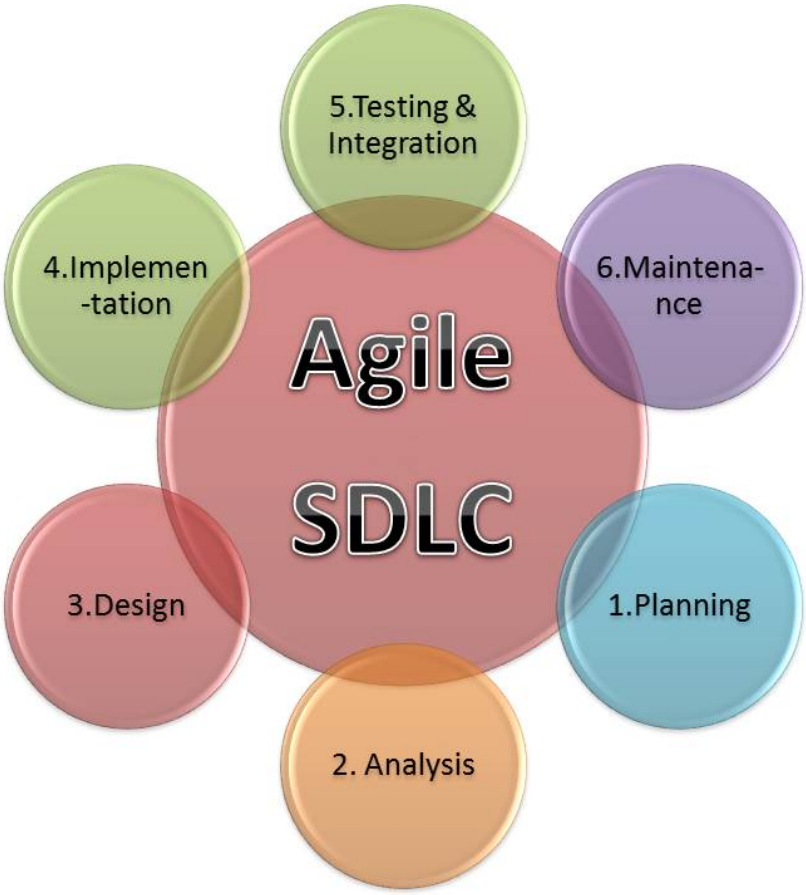


Figure 4.1: Agile SDLC (Rani, 2017)

The Agile system is composed of three versions, that is V.0, V.1 and V.2. Version 0 is composed of five distinct processes and these are planning, analysis, design, coding and testing (Hugh et al., 2017; Kumar, 2018). However, V.0 is used in the proposed system to input the required information into the database about the departments, courses, students and lecturer details, registration information, etc.

On the other hand, V.1, connects or links C# platform with MATLAB platform and completing the fingerprint recognition process. The major difference between V.0 and V.1, lies in the idea that V.1 is used to integrate C# with MATLAB and the fingerprint recognition process.

V.2., is used to create the attendance report, sending SMS alert, inputting the fingerprint image and send it to MATLAB to identify the students. MATLAB then sends the student's ID to C# to confirm the student's attendance. C# in turn sends the attendance report via email to the lecturer after the examination.

4.2.1 Planning

The planning processes involved identifying problems that were associated with traditional recording keeping systems and how they were interrupting students during examinations. In the course of the planning process, it was identified that traditional record keeping methods were being prone to manipulation through deceiving and fraudulent acts. The other problem is that it took time for students and exam officials to verify whether a student had paid his dues and should be allowed dot sit for an examination.

After the problem identification stage, the developer went on to establish goals or aims of the software development systems and these goals are;

- To come up with a secure system that can be used to check whether a student has paid and should be allowed to sit for an examination.
- To develop a system that is fast and easily accessible by users.
- To develop a secure system that cannot be easily manipulated as a result of fraudulent acts or security misconducts such as hacking, record changing, information theft etc.
- Develop a system that can quickly provide feedback on a particular situation or need.

It is from these goals that alternatives were weighed together and the best alternative was selected. Consequently, a fingerprint recognition system was selected on the basis of its ability to meet the aforementioned objectives. The last part of the planning process involved establishing strategies on how to develop the system, test it, implement it, monitor it and maintain it.

4.2.2 Analysis

At this stage of the SDLC, emphasis will be placed at looking at expectations towards the system, that is, what is the system expected to accomplish of fulfil. System analysis thus looks at the functional need of the system in terms of the purpose that it is supposed to serve. However, a system tends to have both functional and non-functional requirements and this section looks at the functional, non-functional requirements, and, software requirements of the fingerprint recognition system.

a) Functional Requirements

A functional requirement is the functional need that the system is expected to satisfy which can either be a problem which the system is expected to solve through it functionality. It is through the performance of the system that a system is able to fulfil its functional responsibilities or requirements. As a result, the finger recognition system is expected to fulfil the following functional requirements;

- Accurately store each student's fingerprint information.
- Must accurately identify and distinguish a student's fingerprint from those of other students.
- Link the student's fingerprint information to the students' attendance, payment and academic records.
- Be able to provide information of whether the student attended a lecture and examination or not.
- Enhance the security system by avoiding manipulations of any kinds.

b) Non-Functional Requirements

These are requirements that are derived from the properties of the system. It is important to note that most systems are not only judged on their ability to perform a functional service or fulfil a particular need but also based on the experience the user has in using the system. The non-functional requirements of the finger recognition system are;

- ***Availability:*** It must be available for use all the time and must not suffer from network problems or system malfunctions
- ***Reliability:*** It must not fail at all cost to recognise a stored fingerprint.
- ***Performance:*** Must be fast in accessing the fingerprint, attendance, payment and academic performance records or databases.
- ***Usability:*** Must be easy to use and must not take users a lot of time to use.
- ***Innovativeness:*** Should be well technologically advanced and demonstrate innovativeness.

c) Software Requirements

- Processor core i3 or above
- 2.20GHz or faster (recommended)
- 2 GB available RAM or more (recommended)
- Windows 7 Service Pack 1or above x86-bit or x64-bit operating system

4.2.3 Design

The proposed system is designed based on agile model using C# and MATLAB. C#, is linked to a student database and in this database, we can add anything be it academic performance or student attendance information.

Basically, the student starts by inputting his or her fingerprint into the system to C# which then send the inputted image to MATLAB. MATLAB then identifies whether the student attended the examination or not. If yes, C# will then send the image to a MATLAB application which contains the fingerprint recognition process. However, MATLAB will works on the image enhancement, segmentation, binarization, thinning, feature extraction of the inputted image and matching. It is at this stage that the system will attempt to match the students' fingerprint, process it and provide information in the event that it has matched. Once MATLAB has matched the fingerprint, it will then send the ID of the student to C# for assigning the attendance automatically, and then the system will send the attendance report to the lecturer email. Otherwise, alert SMS message will be send to the advisor inform him/her that there is not authorized person try to enter the exam.

- **Activity Diagrams of the Developed System**

The activity diagrams below shows the actions and decisions that the admin can take though the system process.

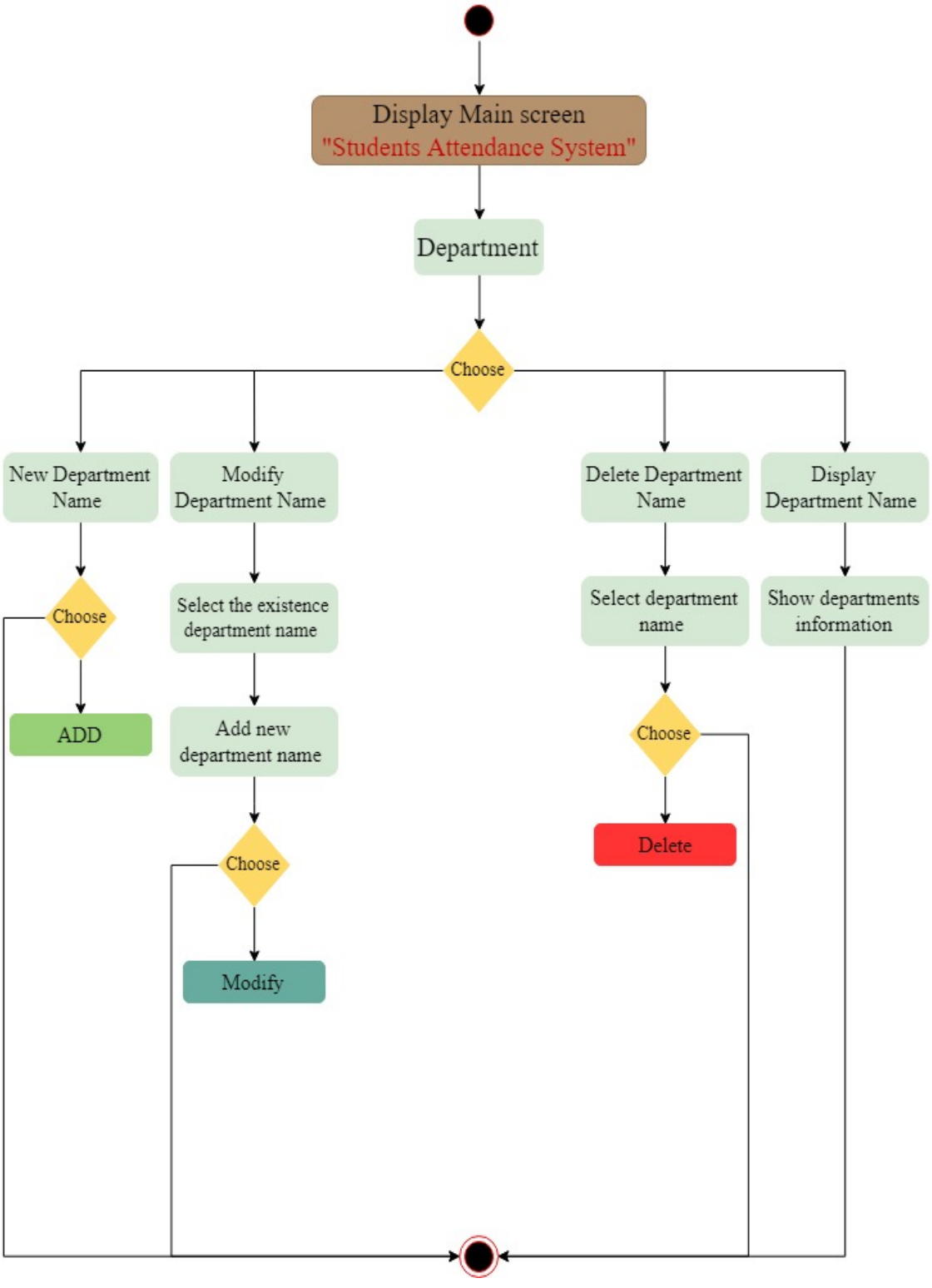


Figure 4.2: Activity diagram for department process

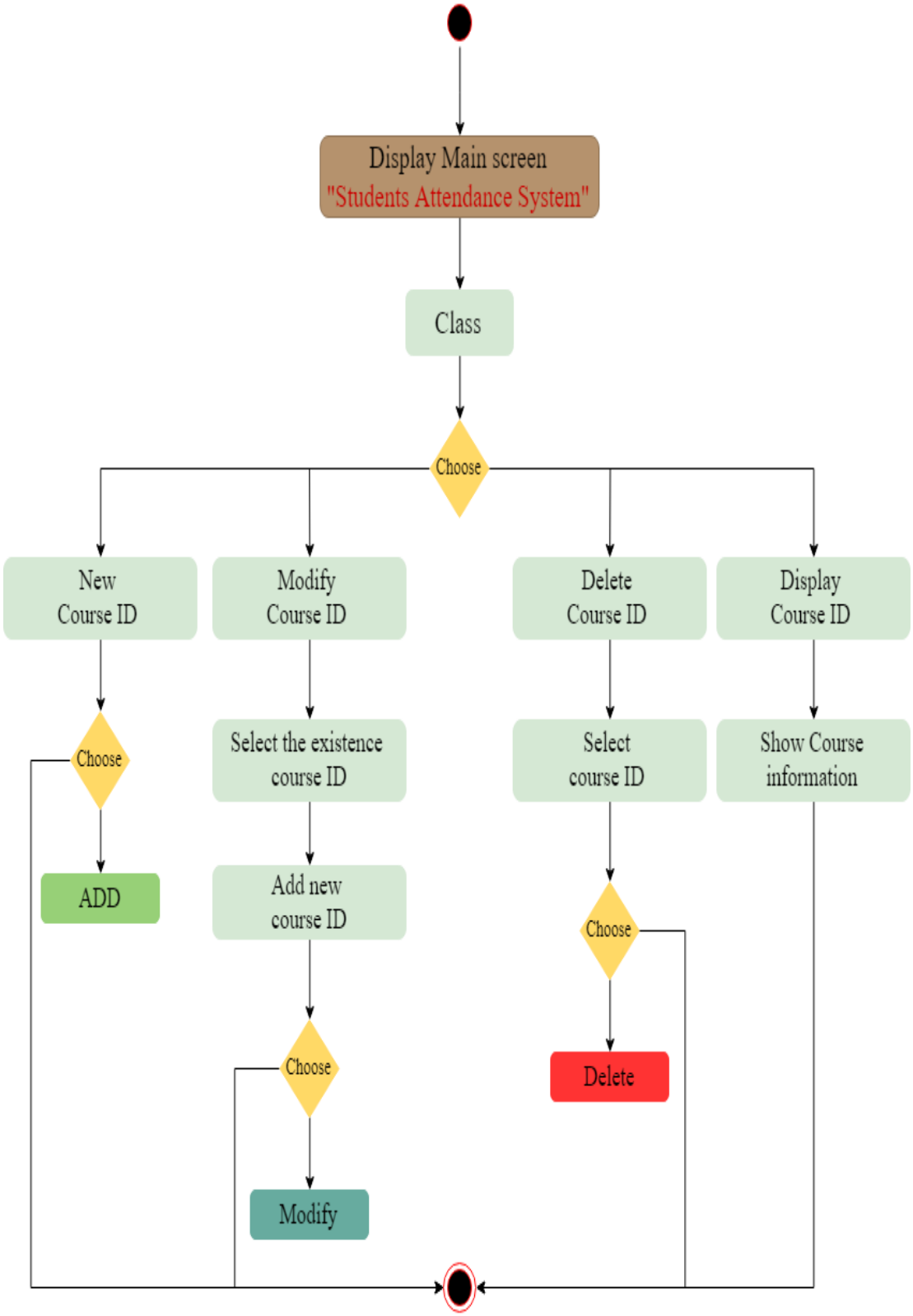


Figure 4.3: Activity diagram for class process

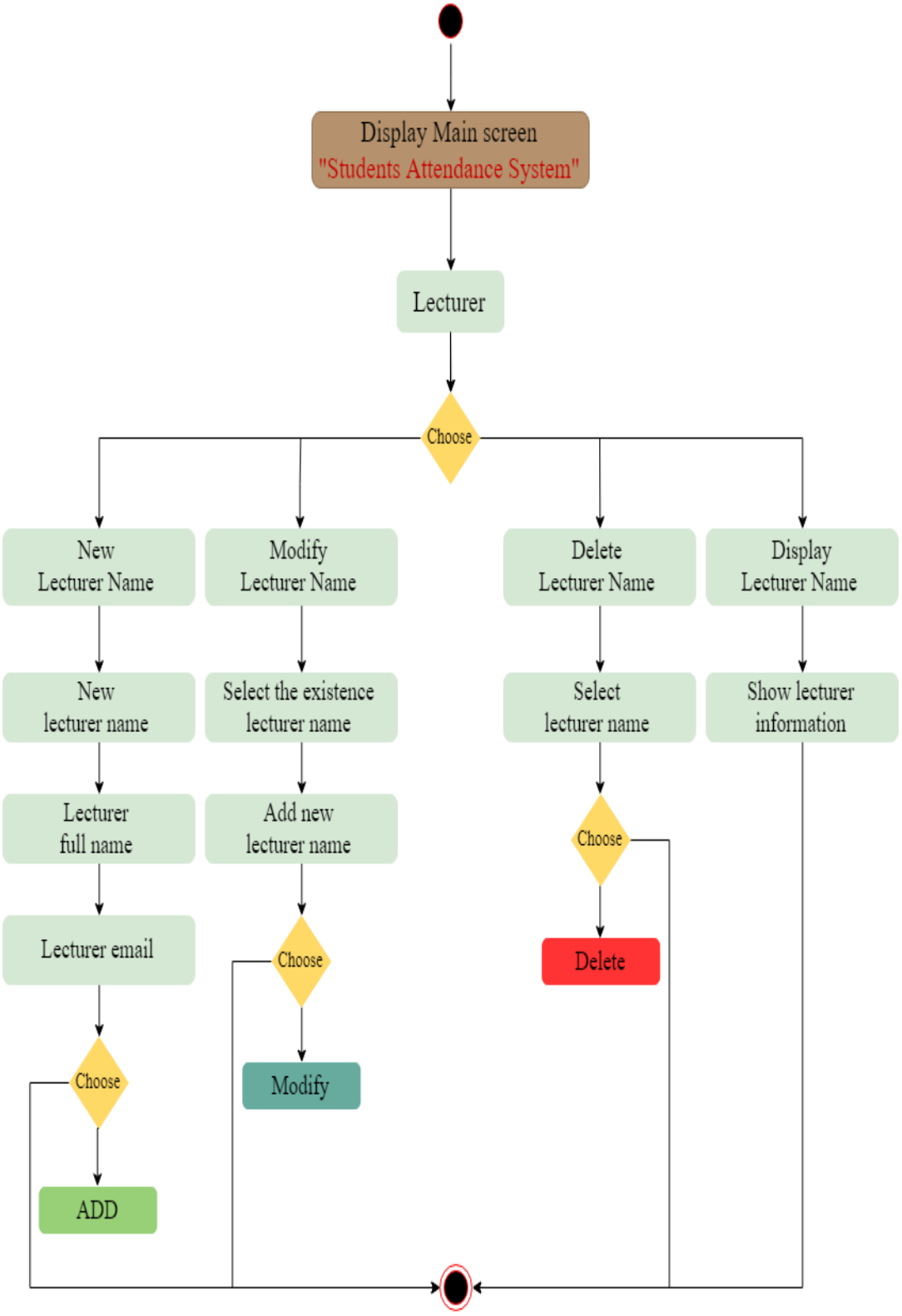


Figure 4.4: Activity diagram for lecturer process

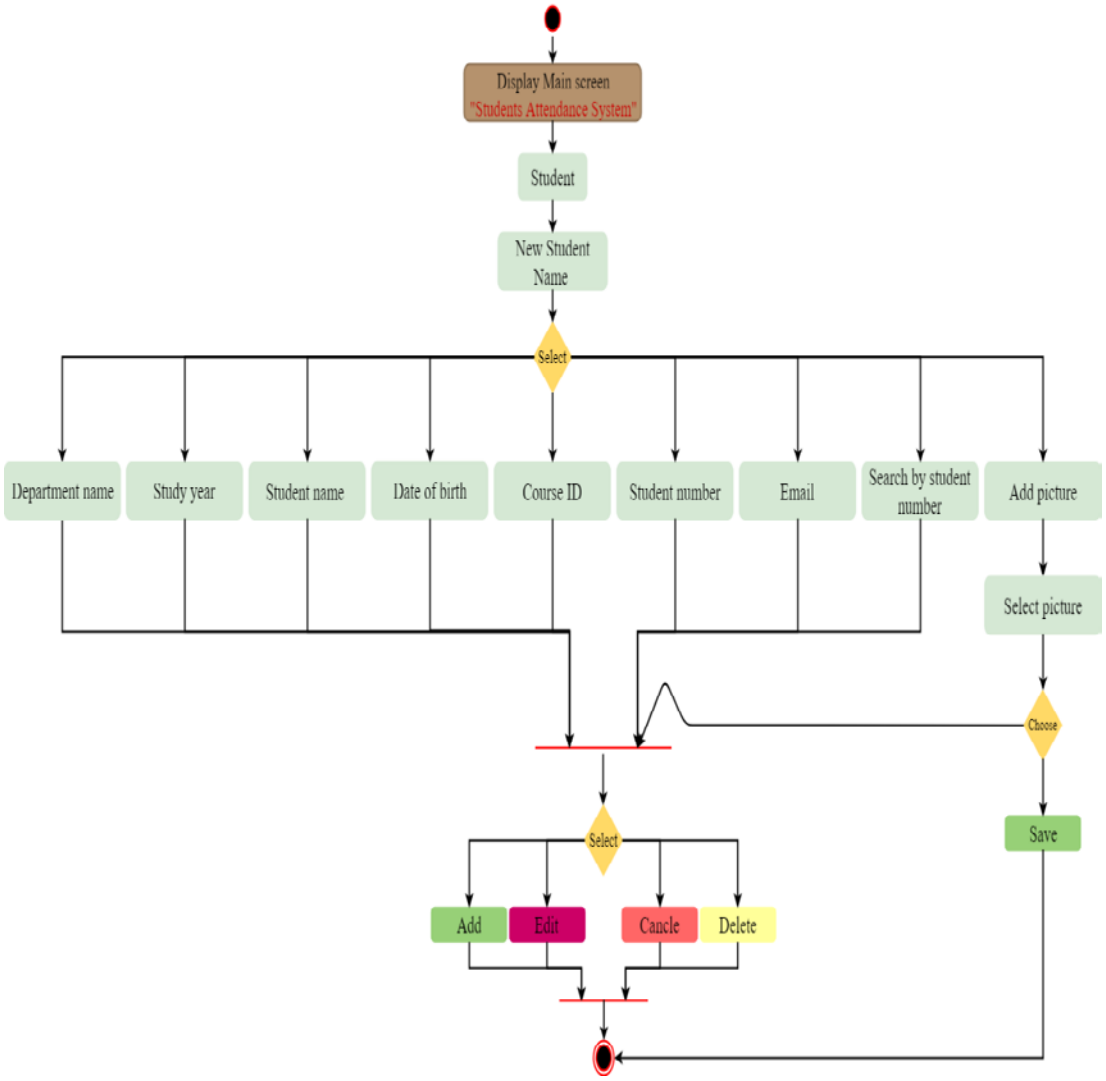


Figure 4.5: Activity diagram for student process

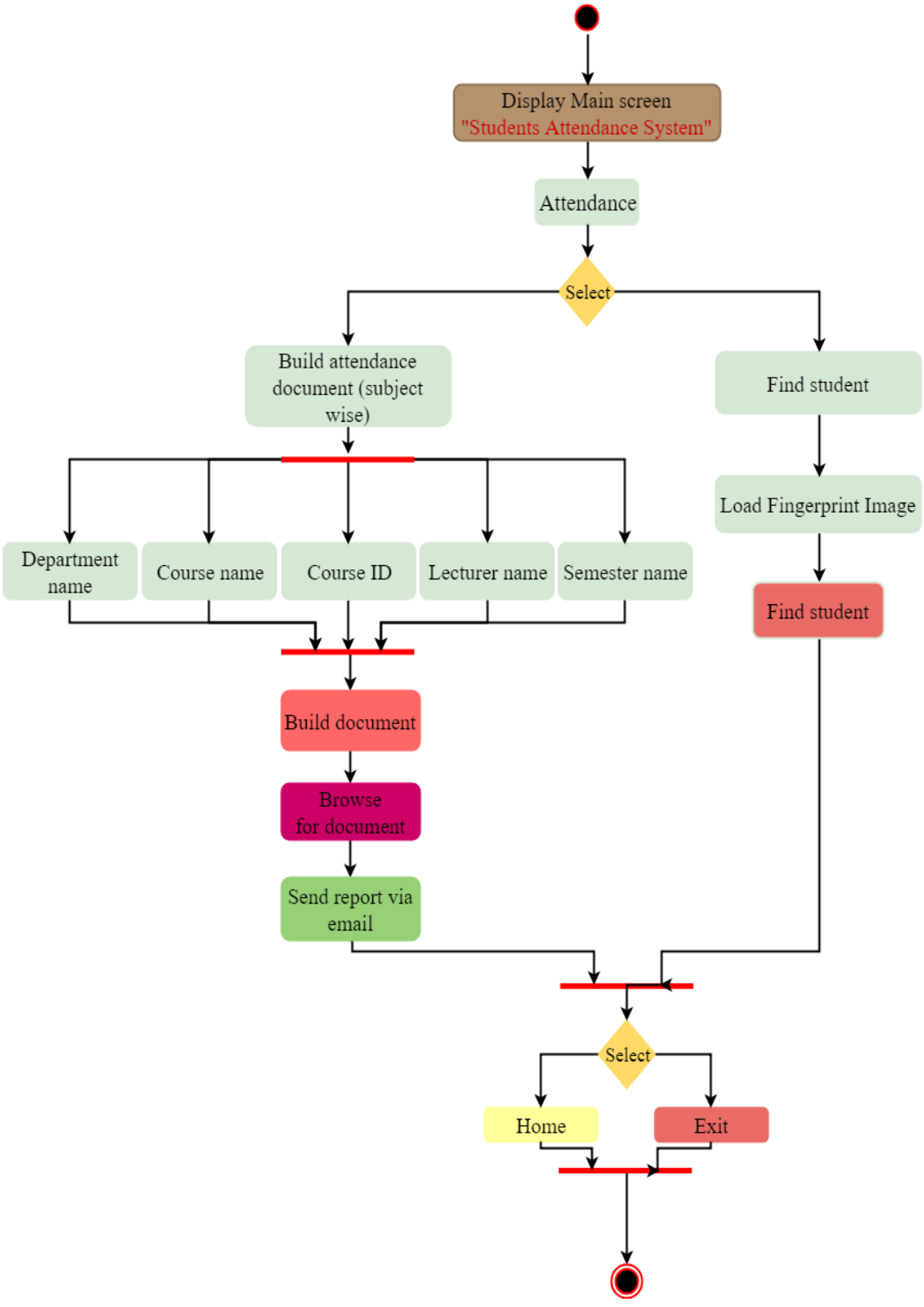


Figure 4.6: Activity diagram for attendance process

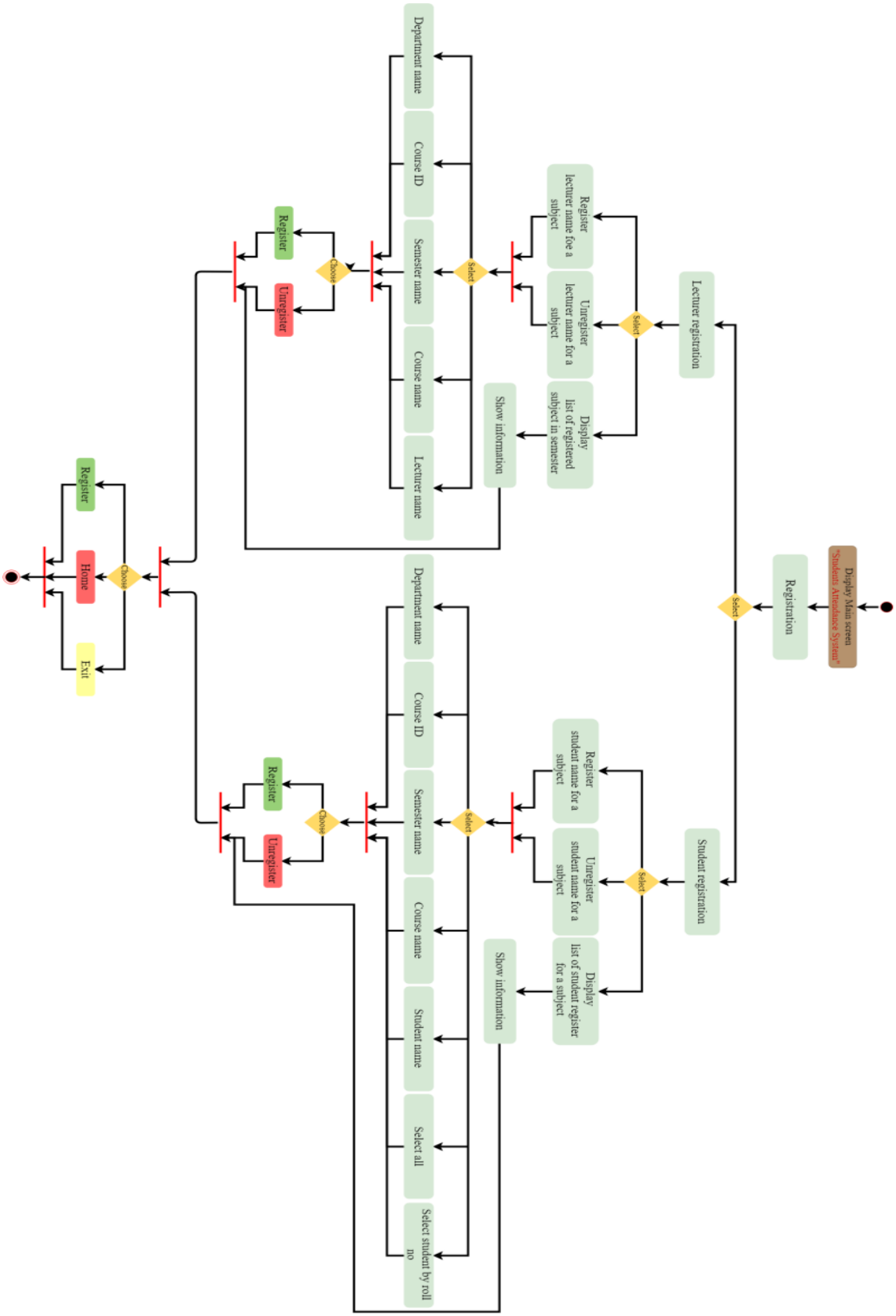


Figure 4.7: Activity diagram for registration process

- **Unified Modeling Language (UML) Diagram**

UML is a visual language that is often used as a standard displaying language in object-oriented software engineering (OOSE). UML serves an important function of providing a visual outline of a particular activity or process. UML is important because it is used for recognisation, actualisation, reporting purposes and to create diverse system parts of a given framework. They also help to provide a better pictorial description of the framework which also helps the user or developer to understand the system better.

i. Case Diagram

In this study, case diagrams are taken as diagrams that offer a pictorial view of how the proposed system works. It shows how the different parts of the system themselves interact based on the structure of the design. That is, it shows what the system can undertake or do as a finished application.

Figure 4.8: Case diagram of the developed system

4.2.4 Implementation

The coding process of the system is divided into two different platforms. The coding process will be done through the use of a combination of C# and MATLAB that linked together as explained below.

- ***MATLAB Programming Language***

MATLAB is widely known as a high-performance language for technical computing. It includes a combination of programming, visualisation and computations which are used to express problems into mathematical forms to derive solutions. It is also used for quite a number of purposes which include computation, algorithm development modelling, simulation, and prototyping, data analysis, exploration, and visualization and scientific and engineering graphics. The use of MATLAB does not need dimensioning and hence, it is capable of solving numerous expressions especially those of technical nature. MATLAB has a number of benefits that are attached to it. For instance, some of the features of MATLAB such as toolboxes make it easy for users apply and learn specialised technology.

- ***C# Programming Language***

On the other hand, C# is a programming language that is composed of multiple paradigm elements with component-oriented, class based, declarative, imperative and strong typing programming elements (Fu, Salvendy, & Turley, 2002). One of the design goals of C# is to come up with a programming language that is object oriented, modern and simple to use. Fingerprint information that is inputted into the systems is first processed by C# and handed over to MATLAB for processing.

i. System Databases

Two databases were used in this study because the two databases will help in storing and sending information. The access is primary used to store while FVC (2002) is used for testing the fingerprint recognition system. These databases are herein explained as follows;

a) MS Access

Microsoft Access is a DBMS "Database Management System" that is part of the Office Package with GUI that help the user and the developer to develop fully functional DB with the ability to integrate easily to the working environment and other Microsoft supported SDK "Software Development Kits"

- Advantages of using MS Access:

- Super flexible
- easy to use
- it works with SQL DB
- import or link directly to data stored in other applications and databases
- Access use wide variety of Data formats
- export and import data from and to MS office suite (word, Exile, …)
- support the ODBC (Open Database Connectivity) including SQL Server, Oracle

- Functionality of the MS Access

- Creation
- Data Input
- Query
- Report
- Control

- Query

Query provides a custom view of data from one or more tables. Queries are a way of searching for and compiling data from one or more tables.

- Running a query is like asking a detailed question of your database.
- When you build a query in Access, you are defining specific search conditions to find exactly the data you want.

- In Access, you can use the graphical query by example facility or you can write Structured Query Language (SQL) statements to create your queries.
- Queries can do the following functions “Select, Update, Insert, or Delete data”.

b) Chosen Fingerprint Database

The proposed system used FVC (2002) as a fingerprint dataset which is widely used by researchers, because it contains low and medium fingerprint quality images so that it can shows the performance and the flexibility of the system. However, it is composed of four databases with following attributes (Maltoni et al., 2002; Kayaoglu et al., 2013);

- A database that uses Identix Touch View II with a resolution and size of (388x374-500 dpi to scan the optical technology data set.
- A database that involves the use of Biometrika FX200 with a resolution and image size of 296x560-596 dpi that is used to scan the optical technology.
- The use precise biometrics to resolution and size of 100 SC 300x300 – 500 dpi that is used to scan the Capacitive technology.
- The use of SFinGE v 2.51 which is composed of resolution and image size of 288x384 – 500dpi to scan the Synthetic Technology.

Table 4.1: Summary of selected database

Database	**Sensor Type**	**Subject/ Sample**	**Total Images**	**Image Size**	**Resolution dpi**
FVC **2002**	Optical	DB1 _B	110-8	388x374	500 dpi
	Optical	DB2_B	110-8	296x560	569 dpi
	Capacitive	DB3_B	110-8	300x300	500 dpi
	sFinGe v2.51	DB4_B	110-8	288x384	~500dpi

ii. Systems Protocols

The proposed system will rely on the use of SMTP and HTTP protocols. A description of SMTP and HTTP protocols can be given as follows;

a) SMTP

SMTP Simply Simple Mail Transport Protocol that used to send the attendance report to the lecturer email. However, it offers ways of linking applications with mail servers and send mail messages using an exposed SMTP service (Dhanalakshmi, Banupriya, & Janani, 2018). There are several ways one can use to access SMTP but the first way of accessing SMTP was using System. Web but later changed after the introduction of .NET 2.0 (Enciso et al., 2018).

b) HTTP

Hypertext Transfer Protocol (HTTP) which used to send the SMS alert to the advisor Mobile. However, it is a client-server application-level protocol that uses TCP/IP connection as a form of transportation but can run with other forms of transport systems that are capable of delivering or guaranteeing effective results (Le-Phuoc & Hauswirth, 2018). HTTP typically involves the client sending a request message to an HTTP server which is responsible for sending responses to the HTTP clients (Lim et al., 2018). This can be illustrated in Figure 4.9.

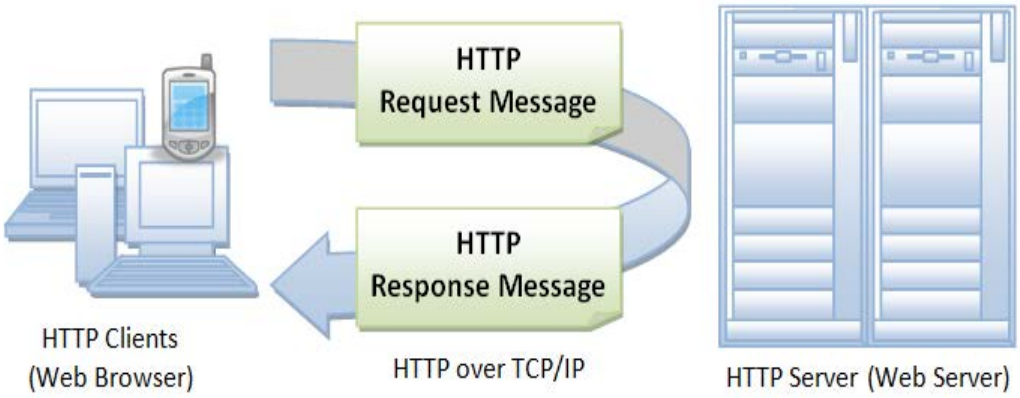


Figure 4.9: HTTP request and response (Le-Phuoc & Hauswirth, 2018)

4.2.4.1 The Development of Fingerprint Recognition

The first step is to input the grey image and after that the pre-processing stage can be commenced and at is at this stage that the enhancement process is done. However, the developed system used the following steps as a process of the fingerprint recognition as provided in Figure 4.10:

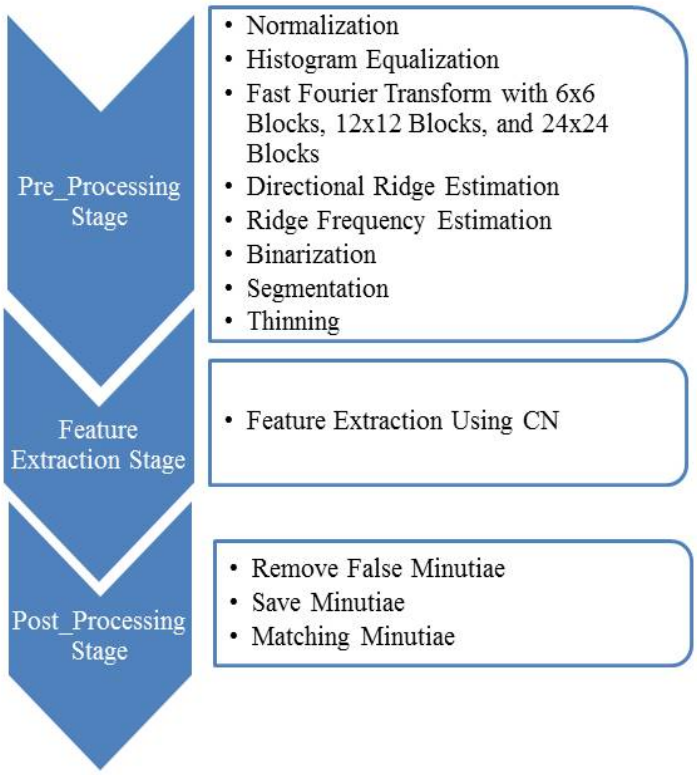


Figure 4.10: The process of the fingerprint recognition

1) **Pre-processing stage**

   The processing stage is an important stage of the fingerprint recognition system. This is because it enhances the quality of the image produced so that the minutiae can be detected correctly. There is however elements that can affect the quality of the image produced due to factors that affect the clarity of the ridge elements which can compromise the minutiae extraction.

- ***Normalisation***

Normalisation is done so as to ensure that the values of the pixels are standardised so that they conform or remain within the desired range between 0 and 1. However, the normalisation process is done as follows;

$$N(i,j) = \begin{cases} M_0 + \sqrt{\dfrac{V_0 (I(i,j) - M)^2}{V}}, if\ I(i,j) > M \\ M_0 - \sqrt{\dfrac{V_0 (I(i,j) - M)^2}{V}}, otherwise \end{cases} \quad (1)$$

The estimated variance and mean are shown by V and M respectively while the desired variance and mean values are denoted by V0 and M0 respectively.

(a) Original image (b) Normalized image

Figure 4.11: Normalized image

- ***Histogram Equalization***

Histogram equalization out used to improve the differentiation of the image by expanding the pixel value so that the information will be increased. In other words, it returns back fingerprint image with high pixels. However, it can be applied by using the following formula:

$$p_x(i) = p(x = i) = \frac{n_i}{n}, \quad 0 \leq i < L \tag{2}$$

Global histogram equalization is applied on the normalized image as shown in Figure 4.12.

Figure 4.12: Image after applying histogram equalization

- ***Fast Fourier Transform (FFT):***

  FFT makes it easy to reconnect broken ridges of the same FFT orientation and the process requires that the blocks first overlap and then divided into powers and sizes of 2. FFT transformation thus allows one to acquire directional information about a specific block. It must be noted however that the number of parallel ridges in a block will correspond to the dominant frequencies. The computation of the Fourier Transformation is done as follows;

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \exp\left\{-j2\pi\left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \tag{3}$$

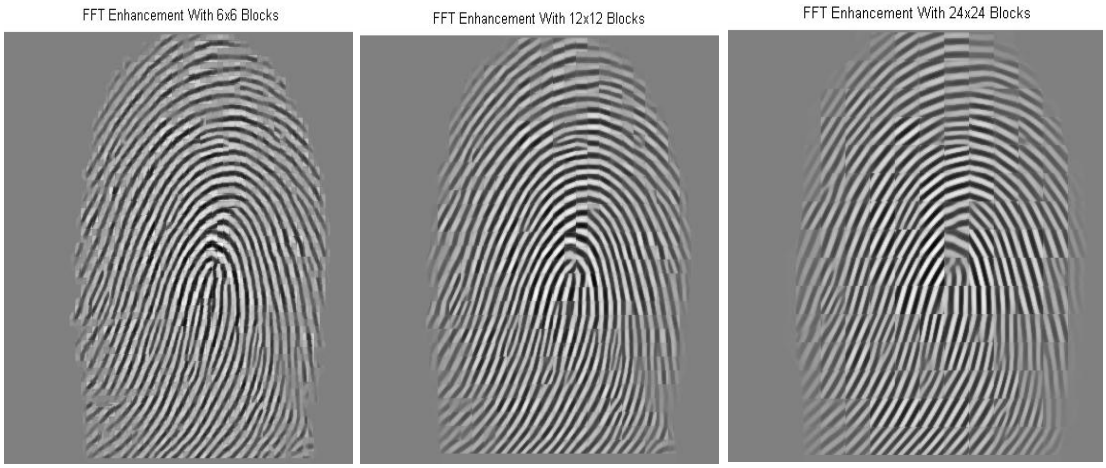
Where v=0, 1, 2….N-1, u=0, 1, 2…..M-1. The computation of the inverse is as follows;

$$f(x,y) = \frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)\exp\left(j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right) \quad \text{for } x=0,1,2...M\text{-}1 \text{ and } y=0,1,2...N\text{-}1. \tag{4}$$

Efforts to have the blocks enhanced simply require that one multiplies the magnitude of the given number of items with the FFT. This is important because it helps to ensure that the ridges are thick in size and remain separated. However, better results can be obtained when the size of the FFT is initially cubed or squared before being multiplied. In order to avoid getting and obscured minutia we can use a power of the magnitude as shown using the following expression;

$$g(x,y) = F^{-1}\{F(u,v) \times |F(u,v)|^n\} \tag{5}$$

The blocks are of the size 2K, and k is a non-fraction number. The block size i is equal to the overlap and n=1.4 is an arbitrary value. The following figures show the results of an FFT which were done based on three different block sizes, that is, 6x6, 12x12 and 24x24 as shown in Figure 4.13. However, after completing the FFT transformations process Gabor filter is applied on the final out put image.



a) Output of FFT technique when block size=6×6

b)when block size =12×12

c) when block size = 24×24

Figure 4.13: FFT image enhancement process

- ***Directional Failed Estimation***

Energy is often distributed to all orientations and frequencies in the spectrum of the actual fingerprint image. A probabilistic estimation is used to estimate the frequency and orientation of each block.

- ***Ridge Frequency Estimation***

The estimation of the average random ridge frequency is done in the same manner as that of the ridge orientation but characterised by a random variable which assumes a probability density function of the following nature;

$$\mathrm{E}\{r\} = \int_{r} r \cdot f(r) dr \qquad (6).$$

- ***Binarization:*** This relies on the lightness of the image so as to extract both the density and brightness. The binarization involves conversion of the 8-bit gray scale image to 1-bit (1 or 0) binary image even black or white based on the global threshold of the image using Otsu's method, depending on the threshold level of each image which calculated automatically using graythresh MATLAB function. The output image is shown in Figure 4.14.

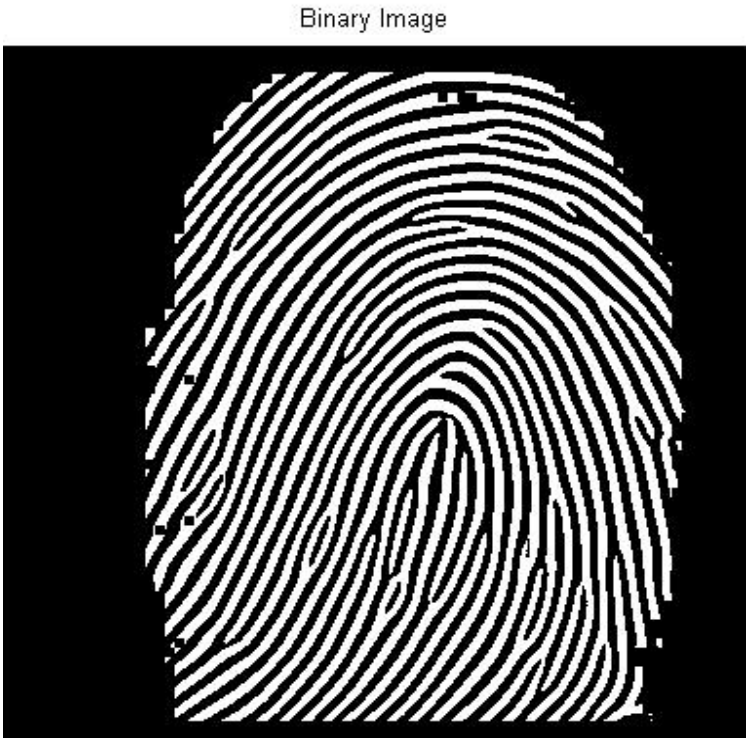


Figure 4.14: Binarized image

- ***Segmentation:*** The segmentation process focuses on two areas of the fingerprint image (background and foreground regions). The background part has been established to be containing noise information while the foreground contains the minutiae. However, the segmentation process is applied to extract the needed information which called (region of interest) and removing the background noise from the image as shown in Figure 4.15.

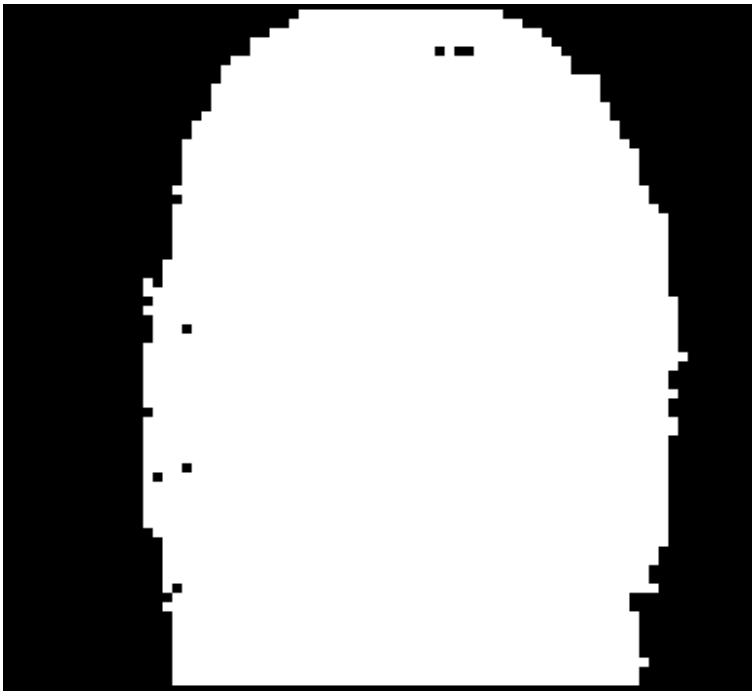


Figure 4.15: Segmented foreground mask

- ***Thinning****:* Is used to deal with the problem of false minutiae extracted from the binarized image. Thus, thinning was used to deal with the problem of false minutiae so as to improve the performance of the program. However, it reduces the thickness of the ridge till it become one pixel as provided in Figure 4.16.

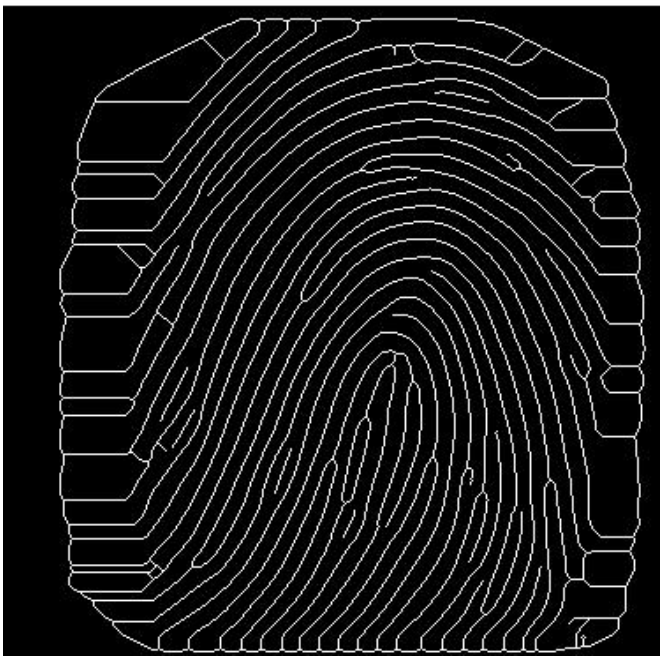


Figure 4.16: Thinned image

2) Feature Extraction using Crossing Number CN

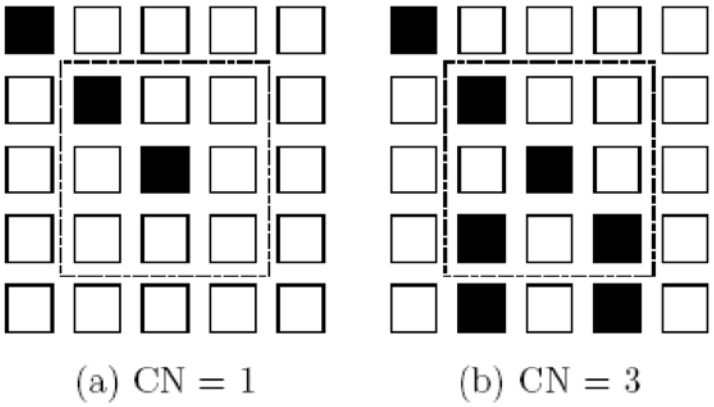
Once the thinning process has been done, the enhanced image will then be extracted through thinning. The computation of the CN is done after the entire fingerprint has been scanned using a 3x3 window using the following functional expression;

$$Cn(p) = \left(\frac{1}{2}\right)\sum_{i=1}^{8}|\mathrm{P}i - \mathrm{P}i + 1| \quad (7).$$

The binary pixel is denoted by Pi =(0 or 1), P1=P9 and the scanning process of say pixel P is done in an anti-clockwise manner as denoted as follows;

P4	P3	P2
P5	P	P1
P6	P7	P8

The computation of CN is however conditional and this implies that it can sometimes be a branch point (Cn(p)=3) and an end point (Cn(p)=1). When the value of Cn is greater than 3, the condition is known as a branch point because CN would have reached what is known as a crossing point. This can be illustrated using the following pictorial expression;



(a) A Crossing Number of one corresponds to a ridge ending pixel.

(b) A Crossing Number of three corresponds to a bifurcation pixel.

Figure 4.17: Examples of a ridge ending and bifurcation pixel. (Moreno-Torres, Sáez, and Herrera 2012).

Furthermore, all possible branch points are shown in Figure 4.18

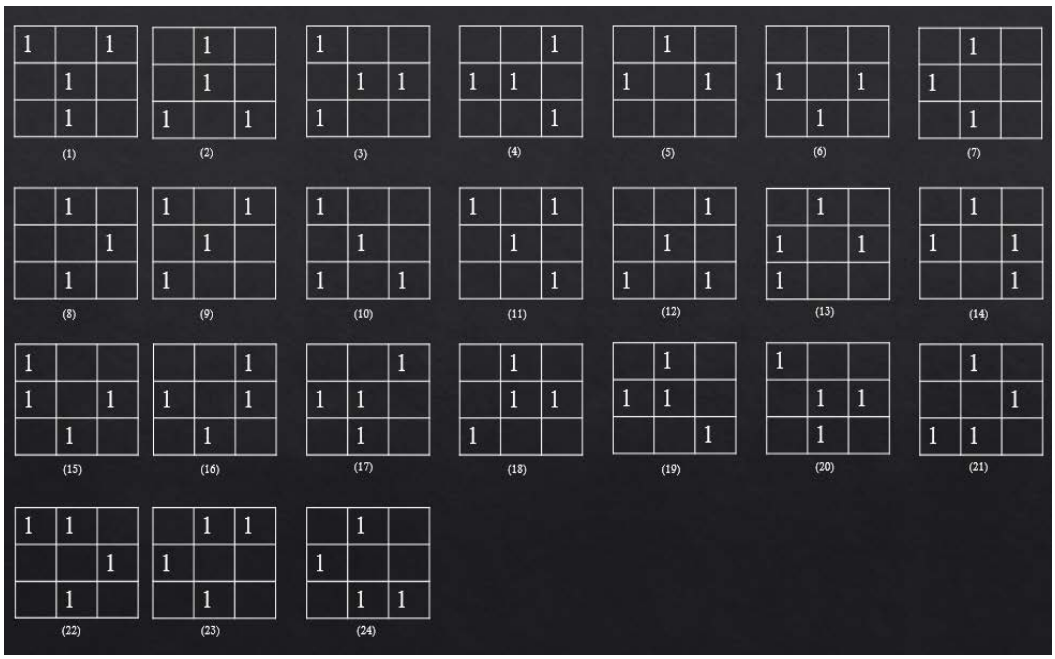


Figure 4.18: Possible branch points

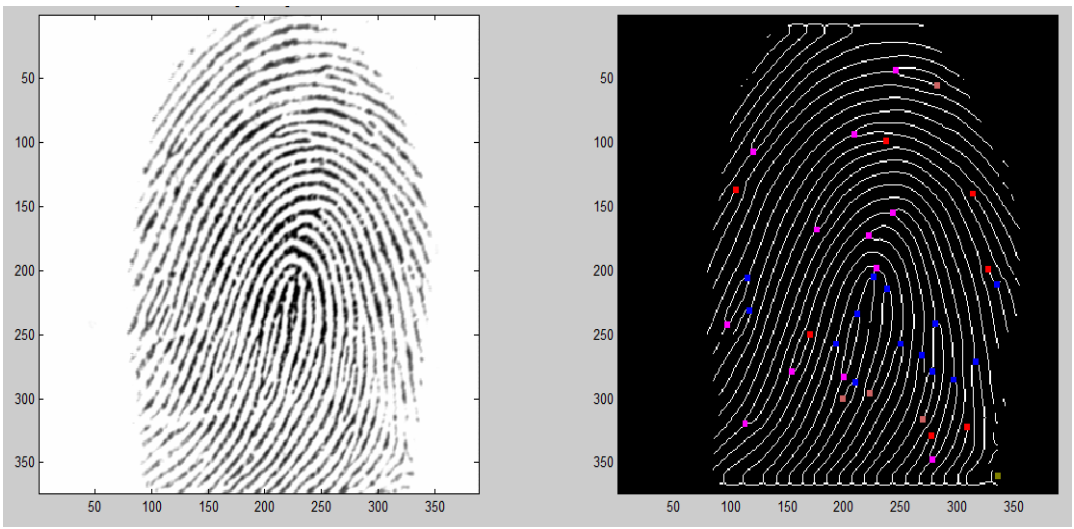


Figure 4.19: Minutiae extraction image

3) Post Processing Stage

It can be noted that image artefacts and noisy images can cause false minutiae as a result of the thinning process. As a result, postprocessing is done to deal with false minutiae as follows;

- ***Removing False Minutiae***

  Broken ridge structures, spike structures, triangle, hole and spur are some of the key false minutiae that are caused by the thinning process and can pose a serious problem which affects the performance of the system since it increases the FAR.V P and the FRR. The possible false minutiae are illustrated using Figure 4.20.

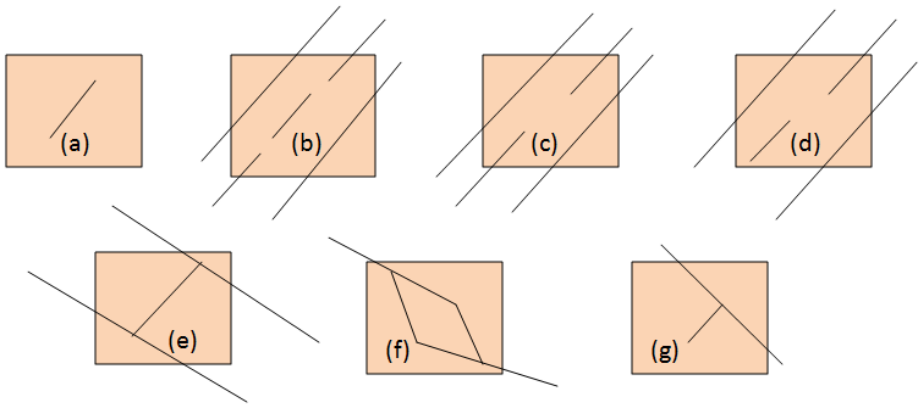


Figure 4.20: possible false minutiae (Jiang & Yau 2000).

- ***Save Minutiae***

  Once the false minutiae have been removed, the only left thing to do is to save according to individual differences in orientation and coordinates. The bifurcation minutiae have three connected lines and angles while the termination minutiae have only one angle.

- ***Matching the Minutiae***

  This involves the use of an alignment-based matching algorithm which separates the minutia matching into:

  a. Alignment Stage.

  b. Match Stage.

- ***Minutiae Matching***

  Given two minutiae sets, L1 and L2 represented by;

  I_1= {m1,m 2,m3…..mm} wheremi=(xi,yi,Θi)

  I_2={m'1,m'2,m'3…..m'n} wherem'i=(x'i,y'i,Θ'i)

  The ridges can be correlated using the following expression;

$$S = \frac{\sum_{i=0}^{m} x_i X_i}{\sqrt{\sum_{i=0}^{m} x_i^2 X_i^2}} \qquad (8).$$

  The selected combination of coordinates that were selected are (Xi….Xn) and (xi….xn). If the obtained score is more than 0.8, then matching is considered to have not taken place. So, the next thing to do is to repeat the process by transforming all the sets based on their reference minutiae and matched together. The reference minutiae will be denoted by M (x,y,Θ) which will be translated but the other minutiae will be rotated in relation to M (x,y,Θ) of the fingerprints using the following expression;

$$\begin{pmatrix} xi\_new \\ yi\_new \\ \theta i\_new \end{pmatrix} = (TM) \times \begin{bmatrix} xi - x \\ yi - y \\ \theta i - \theta \end{bmatrix}$$

$$\text{Where TM} = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (9).$$

- ***Match Stage***

  Minutia can be identical but they can never be the same and this is because inexact quantization and deformations. This requires that a responsive algorithm be used to align the minutia patterns using a restricting box and

minimising the distance between them. The match ratio of the fingerprints is computed using a match score as follows;

$$\text{Match Score} = \frac{number\ of\ total\ matched\ minutiae\ pair}{number\ of\ minutiae\ of\ the\ template\ fingerprint}$$

(10).

The decision is to accept that two fingerprints are of the same finger when the match score exceeds the given threshhold value that given by Maltoni (2009).

4.2.5 Testing and Integration

Testing is done so as to determine if the system is working properly and is no having errors. Testing thus helps to identify errors and possible adjustments that can be made to the system to improve its functionality.

4.2.5.1 Types of Tests

Two major tests were conducted so as to determine the precision and accuracy of the developed system and these tests are;

- **Unit testing:** This involves testing each and every single component of the proposed system. Unit testing involves testing to see how each unit is functioning and whether its functional capabilities will not disturb the functioning of the whole system. 10 experts from the Engineering and Computer Information Systems department were invited to test the units of the system.
- **Integration testing:** This involves the integration of the tested units and testing their interface as a whole system. The integration testing process sought to determine how people would react towards the use of the proposed system and gather their perceptions about;
    1) General opinions about the whole proposed system.
    2) Perceptions about the technical features of the developed system.

Table 4.2: Integration testing summary

Test unit	Test objective	Test case	Expected result	Pass/ fail	Comments
Unit 1: Department information management	Test if the system can add, modify, delete, and display records	Test case for add new department, modify department name, delete department, and show existing departments	Work properly without errors	Pass	The system can add, modify, delete, and display records successfully
Unit 2: Class information management	Test if the system can add, modify, delete, and display records	Test case for add new course, modify course details, delete course, and show existing Courses	Work properly without errors	Pass	The system can add, modify, delete, and display records successfully
Unit 3: Lecturer information management	Test if the system can add, modify, delete, and display records	Test case for add new lecturer details, modify lecturer details, delete lecturer information, and show existing lecturers	Work properly without errors	Pass	The system can add, modify, delete, and display records successfully
Unit 4: Student information management	Test if the system can add, modify, delete, and display records	Test case for add new student details, modify student details, delete student information, and show existing students	Work properly without errors	Pass	The system can add, modify, delete, and display records successfully
Unit 5: Registration management	Test if the system can register/ unregister lecturer/ student for courses	Test case for checking the lecturer and student registration management	Work properly without errors	Pass	The system can register/ unregister lecturer/ students for courses successfully
Unit 6: Display list of registered	Test if the system can display	Test case for display courses which registered in a	Work properly without	Pass	The system displayed list of different

courses in a semester	registered courses in a specified semester	semester	errors		courses which registered in a specified semester successfully
Unit 7: Display list of registered students for a course	Test if the system can display students who registered for a specified course in a semester	Test case for display list of students who registered for a specific course in a semester	Work properly without errors	Pass	The system displayed list of different students who registered for a course in a specified semester successfully
Unit 8: Authentication process 1	Test if the system can check the existing student and verifying him	Test case for authentication process of the system for authorized student	Match the student fingerprint with the existing image in the database	Pass	The system authentication is work properly and the match is done successfully
Unit 9: Send attendance report	Test if the system send attendance report to lecturer via email	Test case for checking attendance report	Destination receive attendance report via email	Pass	The target received attendance report successfully
Unit 10: Authentication process 2	Test if the system can check the unauthorized student and send SMS warning message	Test case for authentication process of the system for unauthorized student	Alert SMS message sent to the destination	Pass	The system authentication is work properly and the SMS message is received by the target

However, after testing the system by the 10 experts, they show their satisfaction about the developed system and the average rating of the system was very good. In addition, they gave some suggestions for the UI of the system.

4.2.6 Maintenance

The maintenance process of the fingerprint system involves what is called programming support which involves making changes to the system to identify and deal with flaws as well as working on improving the system so that it effectively functions quite well. Maintenance thus, seeks to make improvement s on the system and ensure that it is a strong position to meet functional and non-functional needs of the users.

CHAPTER FIVE

DEVELOPED SYSTEM

Once completed, the proposed system will be installed on the systems administration office managed by a system administrator. The fingerprint system will be linked to an internet connection so that it will be able to send or email reports through SMTP.

5.1 Home Screen Window of Exam Attendance System

The execution of the system starts with running the C# application. Figure 5.1 below shows the starting windows form application that contain the list of activities in the menu bar. However, the GUI is designed and implemented in C# platform.

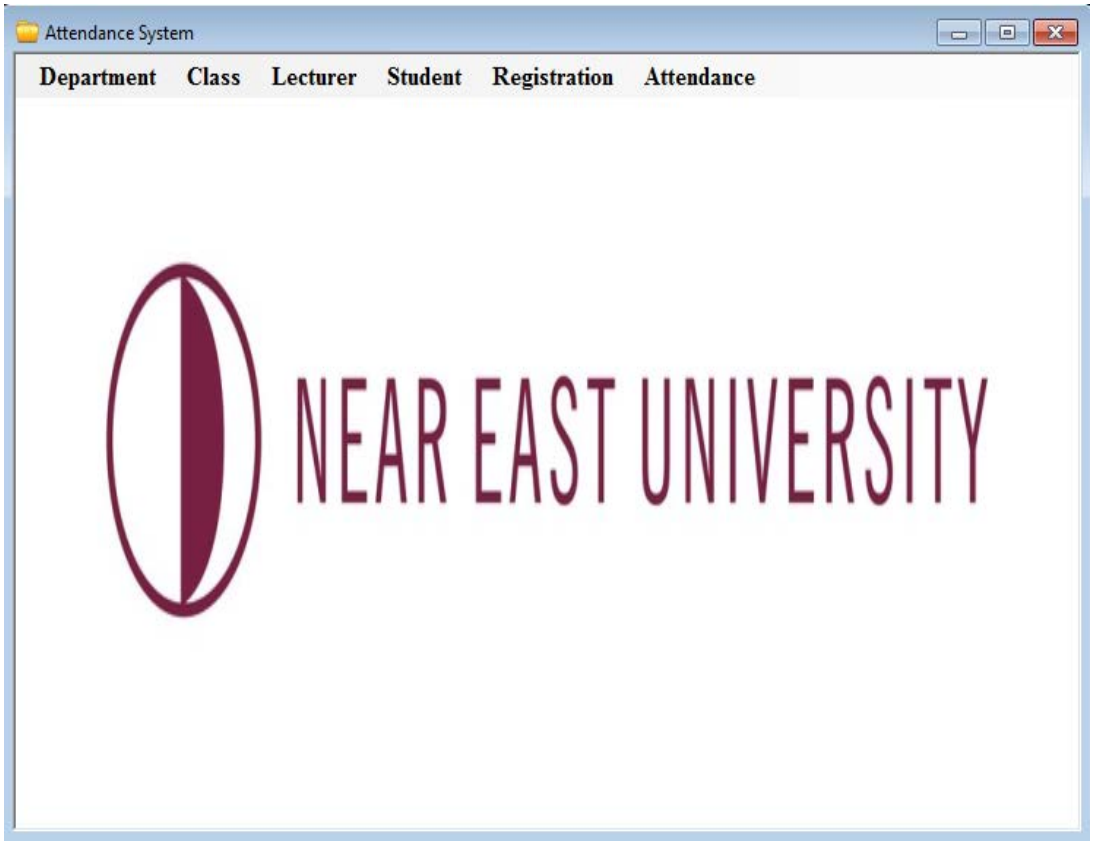


Figure 5.1: The starting form of exam attendance system

However, the execution of the systems GUI as follows:

i. **Department:** Include sub activities that shown in Figure 5.2, this sub activities contains the following;

- ***Add Button*:** When clicking on department option another form will be activated as shown in Figure 5.2, the add process start by typing the department name one per line inside the rich text box, then pressing the Add button to send the new information to the database. However, All the forms contain Home and Exit buttons, the first one returns the user to the main form, while, the second one closing the application.

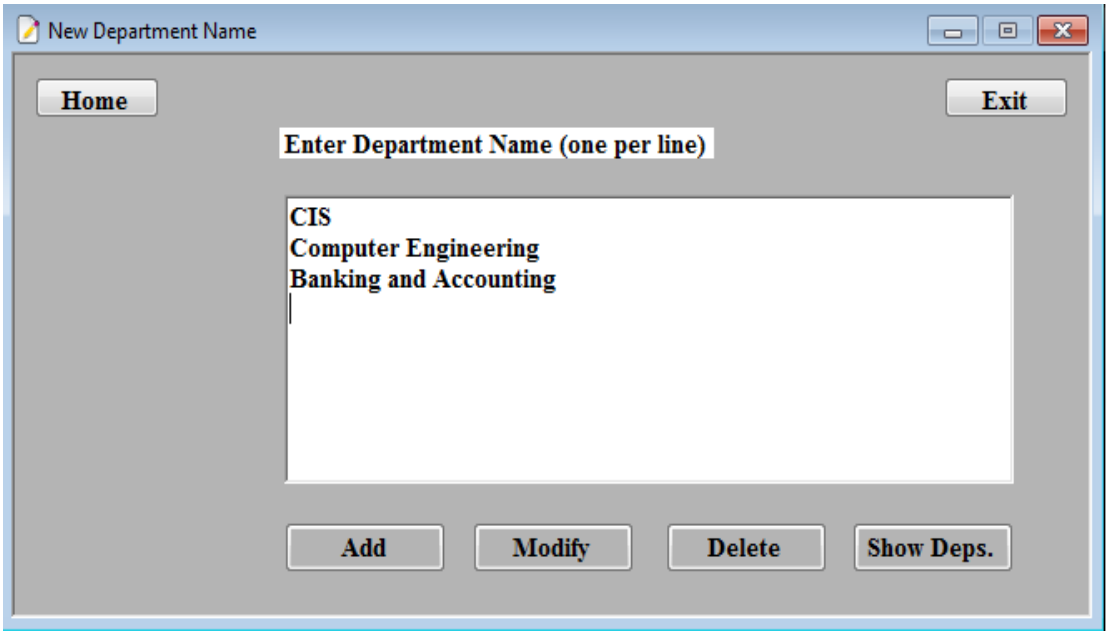


Figure 5.2: Adding new department process

- ***Modify Button*:** First the user has to select the old department name from the combo box then typing the new department name in the text box, to finish editing, the Modify button need to be clicked.

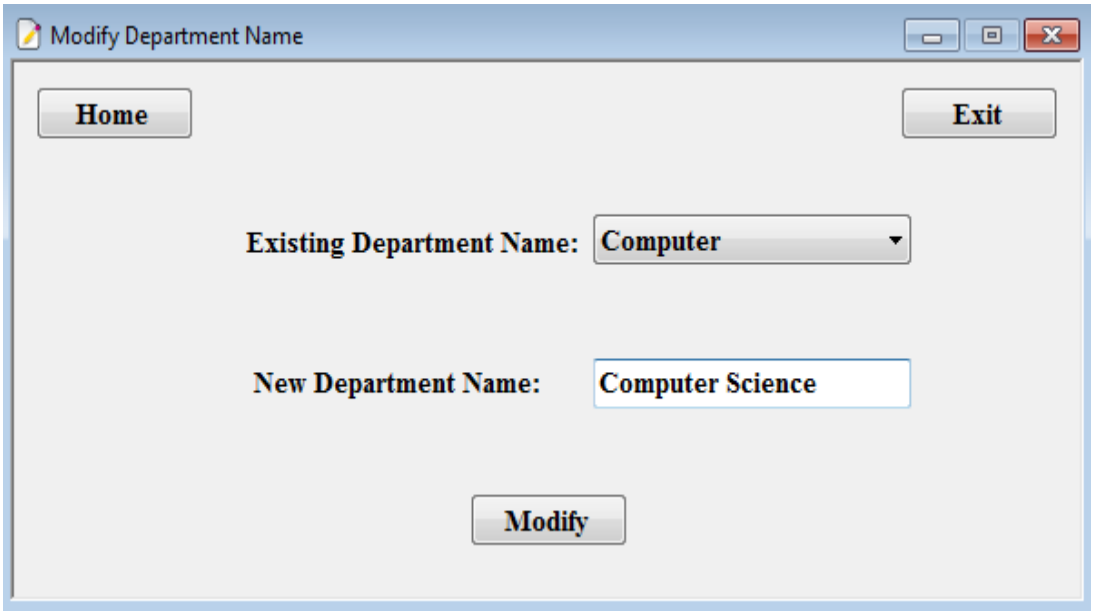


Figure 5.3: Modifying department name form

- ***Deleting Button*:** This is also provided, Figure 5.4, gives a choice to removing department names from the database of the system. By selecting the department name and clicking on the Delete button the name will be deleted.

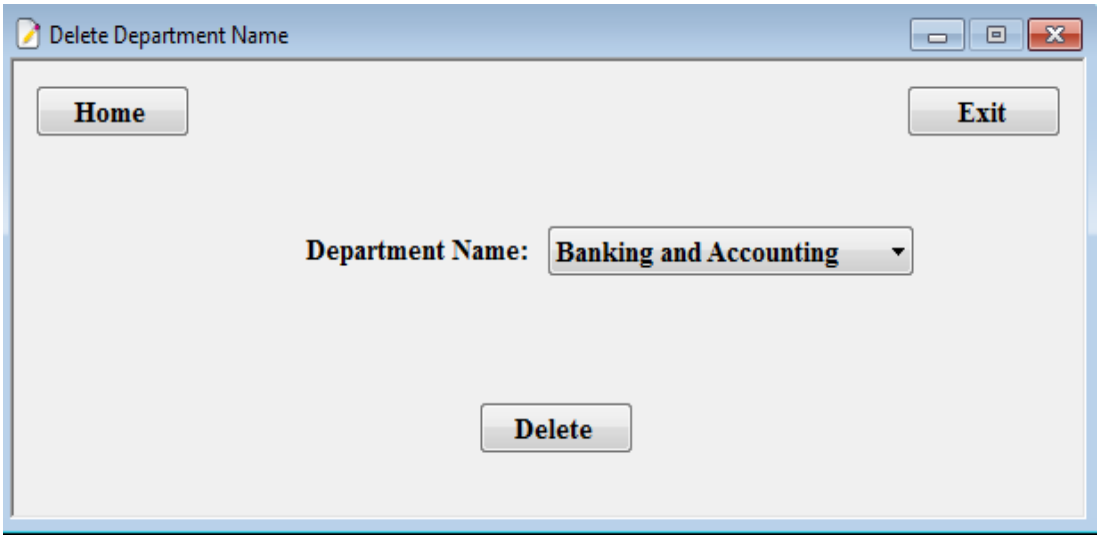


Figure 5.4: Delete department name

- ***Display Department Names Button*:** Provides all the departments that added to the database in a data grid view as shown in Figure 5.5.

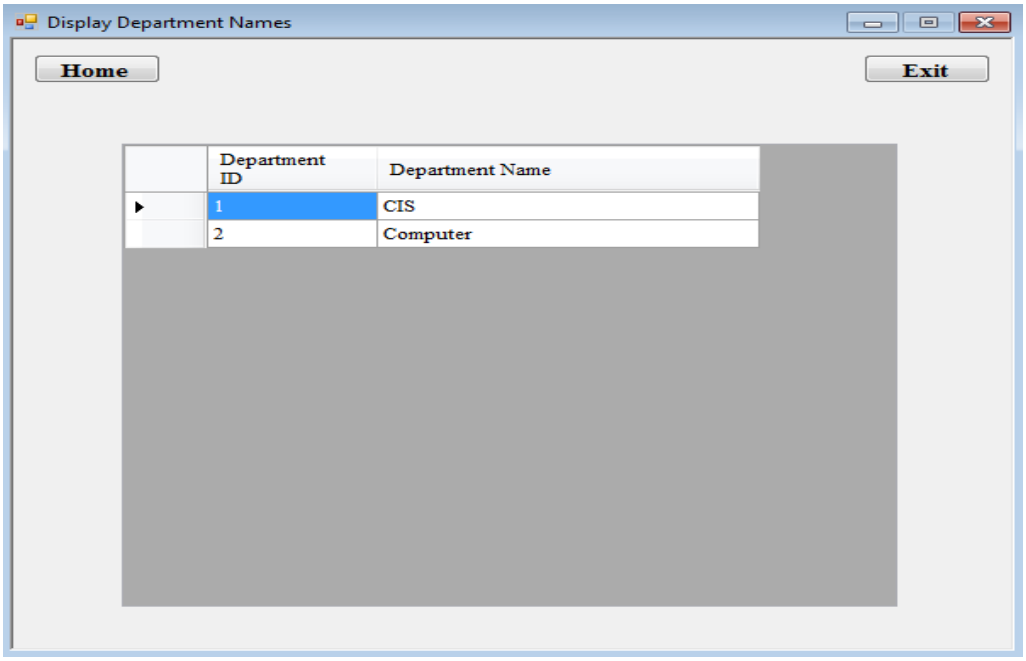


Figure 5.5: Display department names

ii. Class: This option contains adding new class, modify, delete, and display existing classes as demonstrated below.

- ***Add Course Name Button*:** This event allows the admin to add the exam information. It includes inputting the following information: department name that can be selected from the combo box, semester also selected from combo box, course ID, course name, exam date, hall number, exam starting time, and, exam ending time as shown in Figure 5.6. After clicking on Add button the data will be saved in the database.

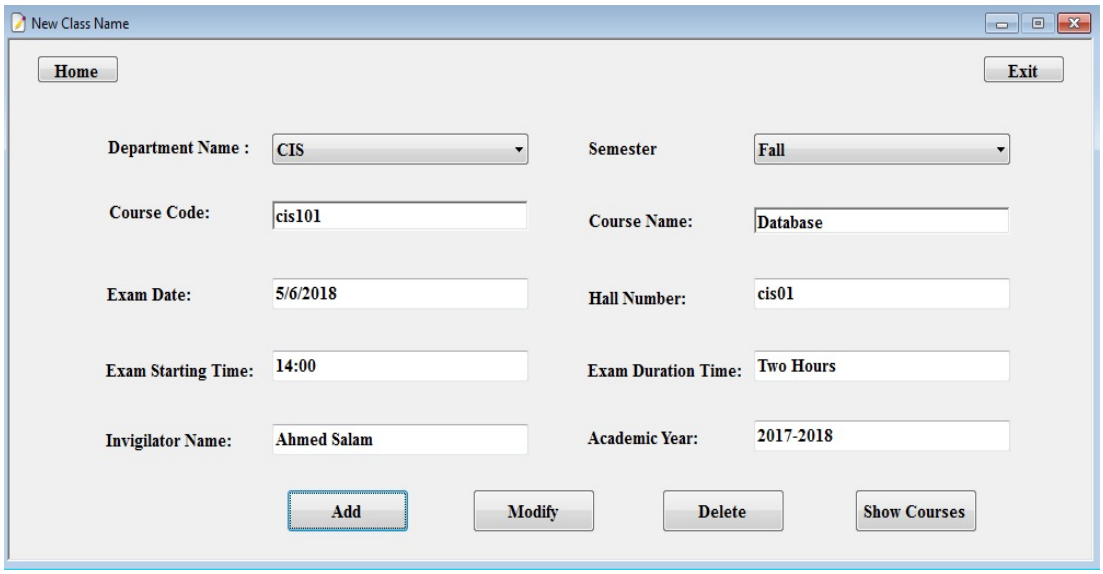


Figure 5.6: Course details

- ***Modify Button*:** This event allows the admin to update the course names by selecting the department name, and, existing course name, then typing the new course name as given in Figure 5.7 after clicking Modify button the information will be changed.

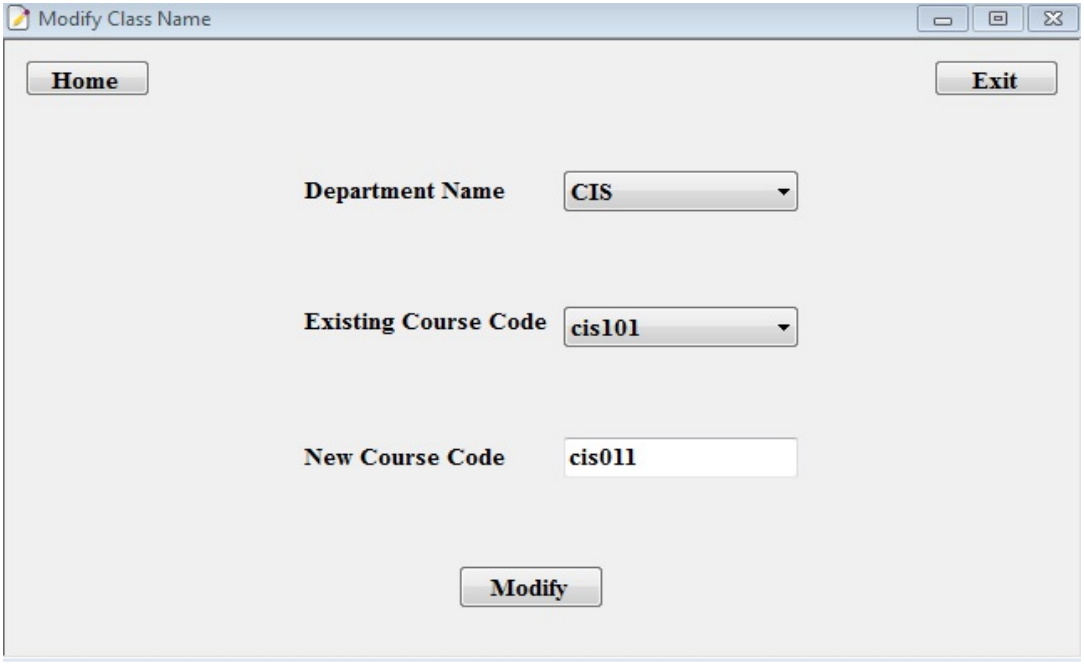


Figure 5.7: Modify course name

- ***Delete Button*:** This event allows the admin to delete course names from the system it's only required selecting department name and course name then clicking on the Delete button as shown in Figure 5.8.

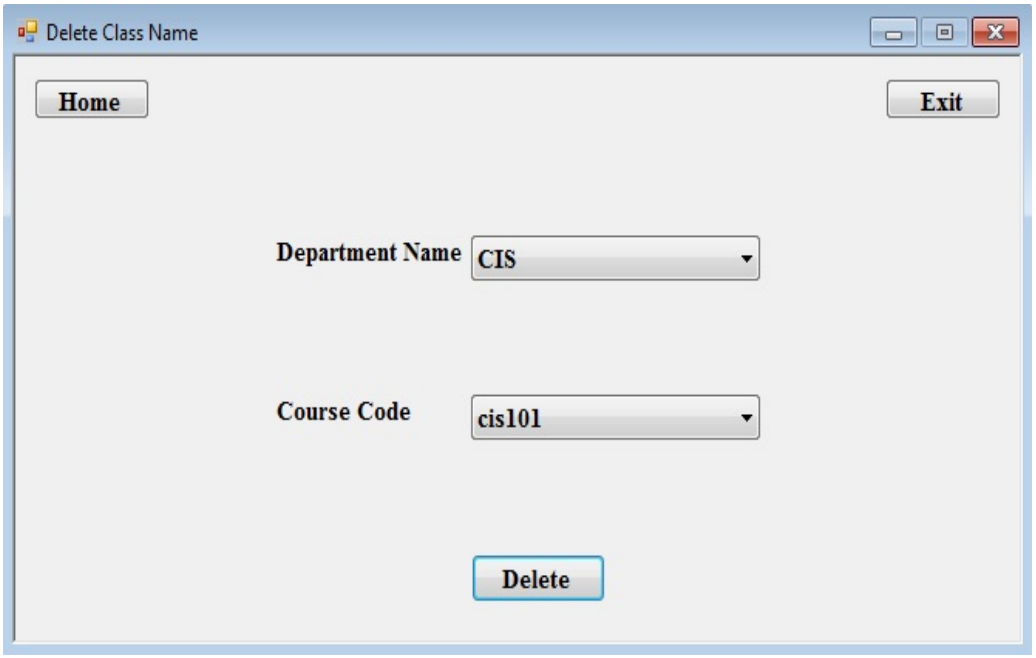


Figure 5.8: Deleting course name

- ***Display Course Names Button*:** As provided in Figure 5.9, this event shows the existing courses in the database by each department.

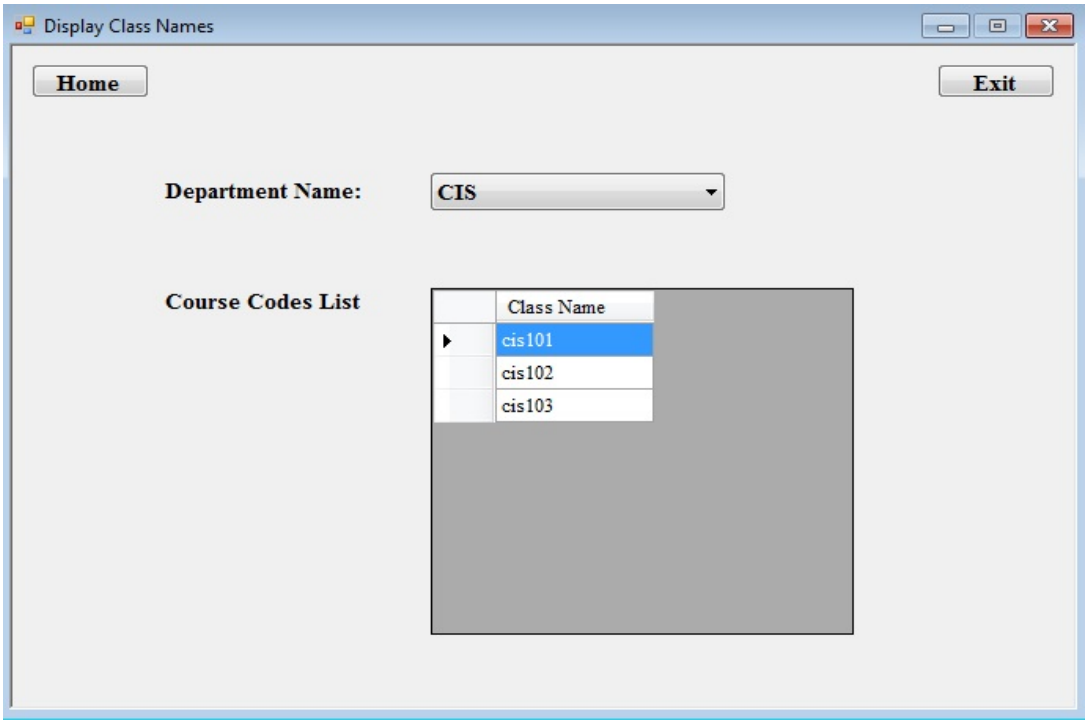


Figure 5.9: Display courses name

- **Lecturer:** This contain the following sub activates: new lecturer name, modify lecturer name, delete, and, display lecturer names.
- ***Add Button*:** By clicking on Add button this window allows the admin to add lecturer name and email for a specific department as given in Figure 5.10.

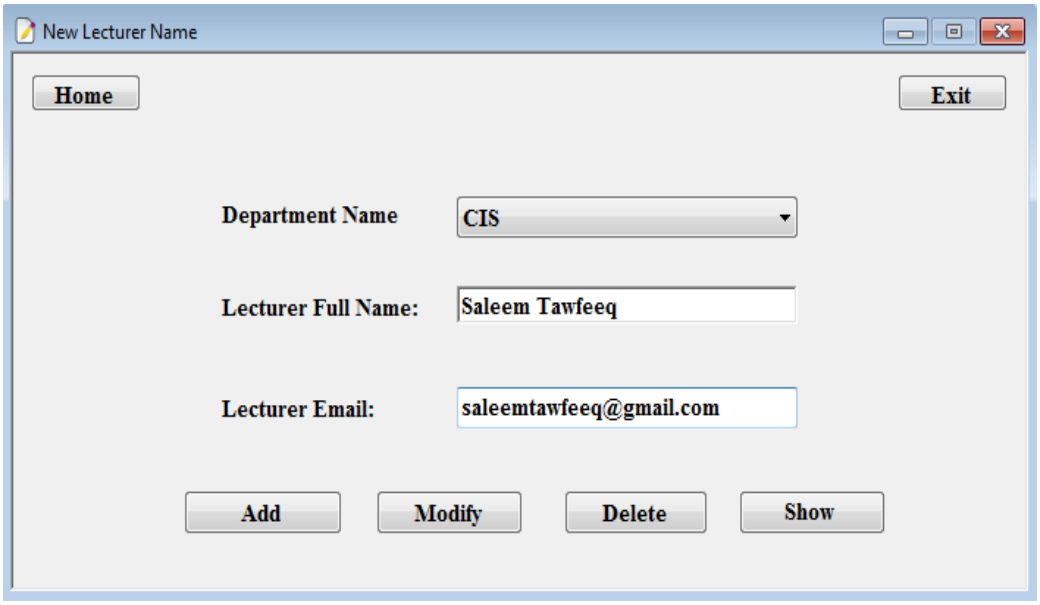


Figure 5.10: New lecturer name window

- ***Modify Button*:** This for is used to updating the lecturer name for a given department as shown in Figure 5.11.

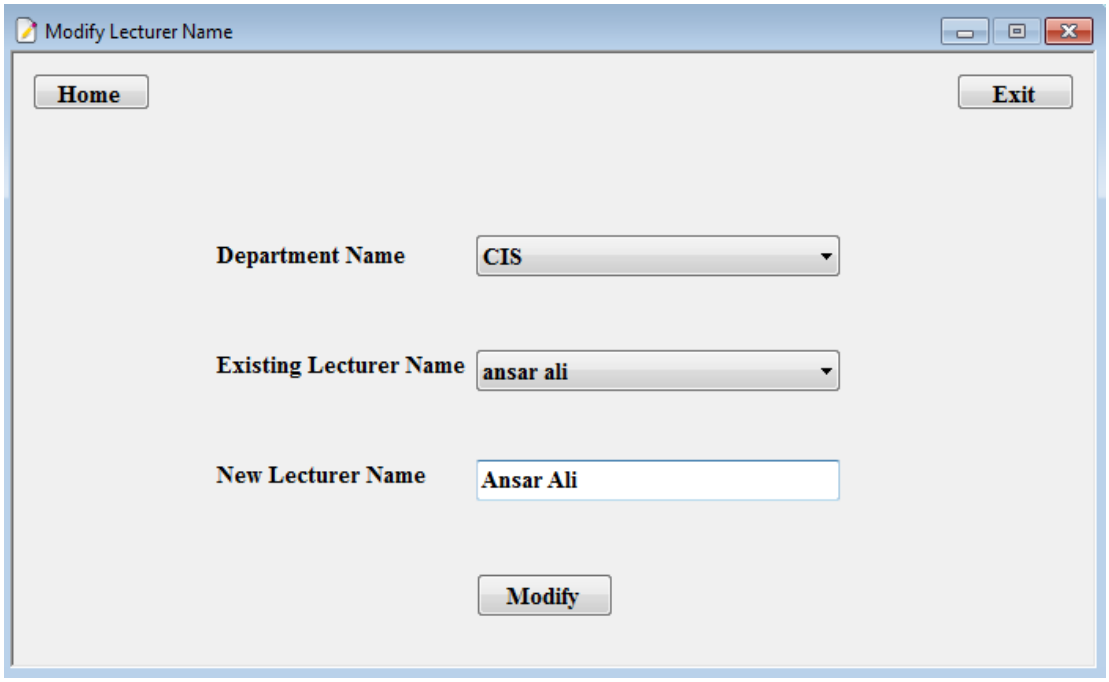


Figure 5.11: Modify lecturer name

- ***Delete Button*:** From this event the admin can delete lecturer name from the system as illustrated in Figure 5.12.

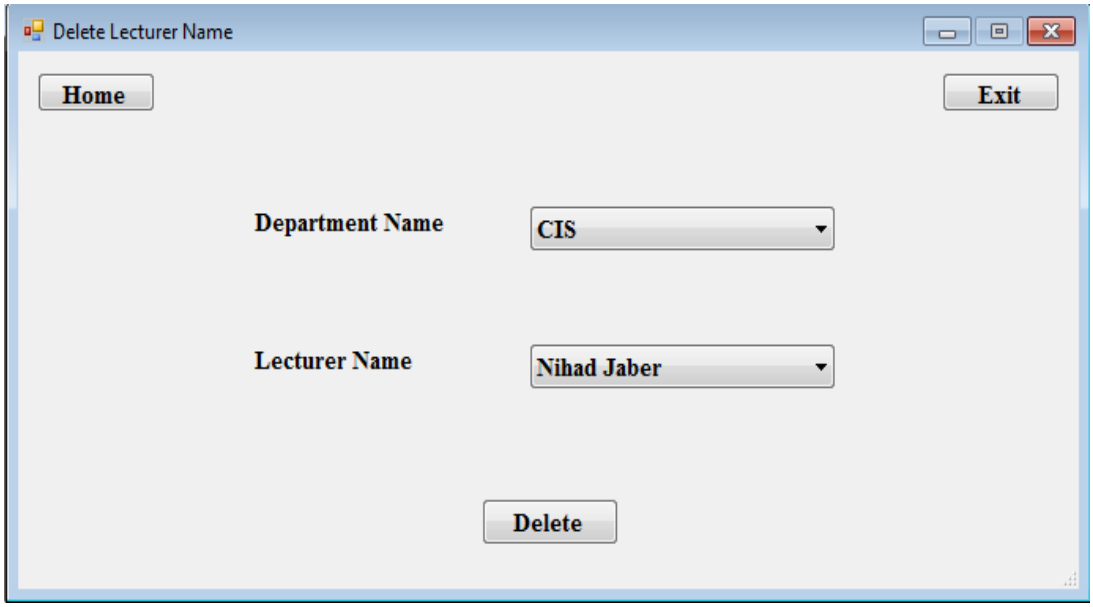


Figure 5.12: Deleting lecturer name

- ***Display Lecturer Names Button*:** This event shows the lecturer names that exist in a selected department as given in the Figure below.

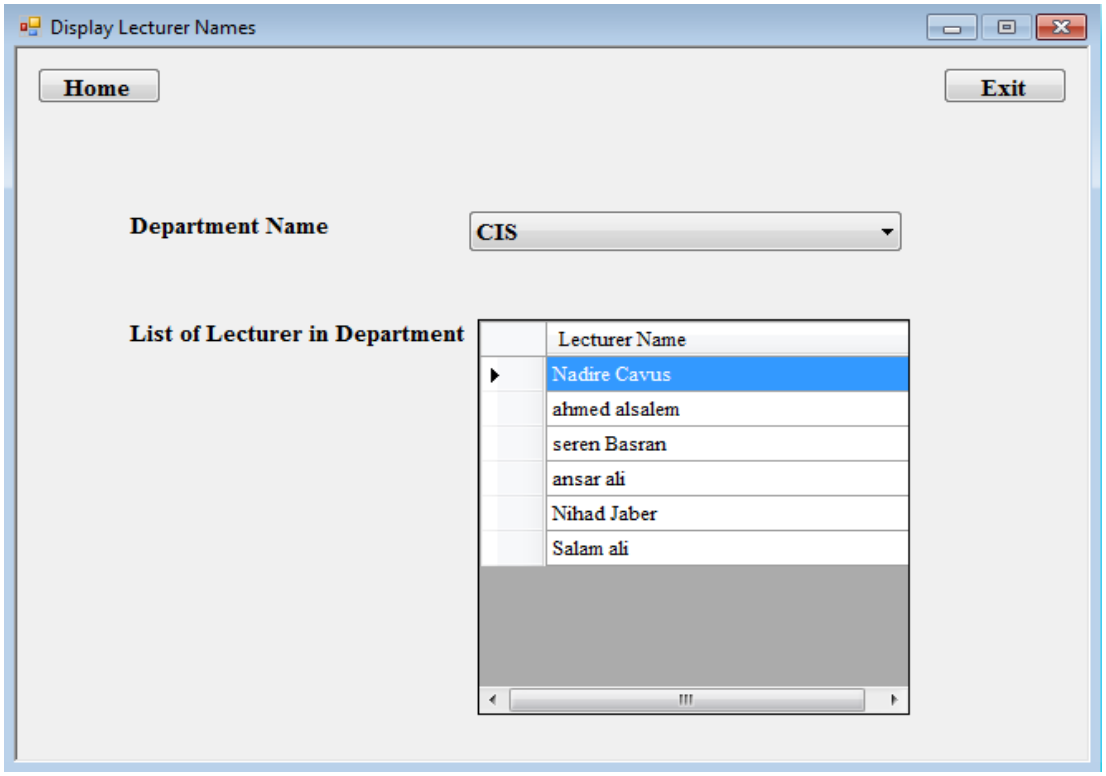


Figure 5.13: Display lecturer names

i. **Student Details:** This window allows admin to enter student information. The department name and course name can be selected directly from its combo boxes, the other information need to be inputted by typing, after that the admin have to select picture for the student by clicking on browse button and selecting picture from the computer. By clicking on Add button the information will be saved in the system. While, the edit button is used to update the student information based on his/her student number. The cancel button used to reset the window and neglecting exist contains of the text boxes. In addition, the delete button is provided to remove all the student information from the system based on student number or student name. Figure 5.14 shows the student details form.

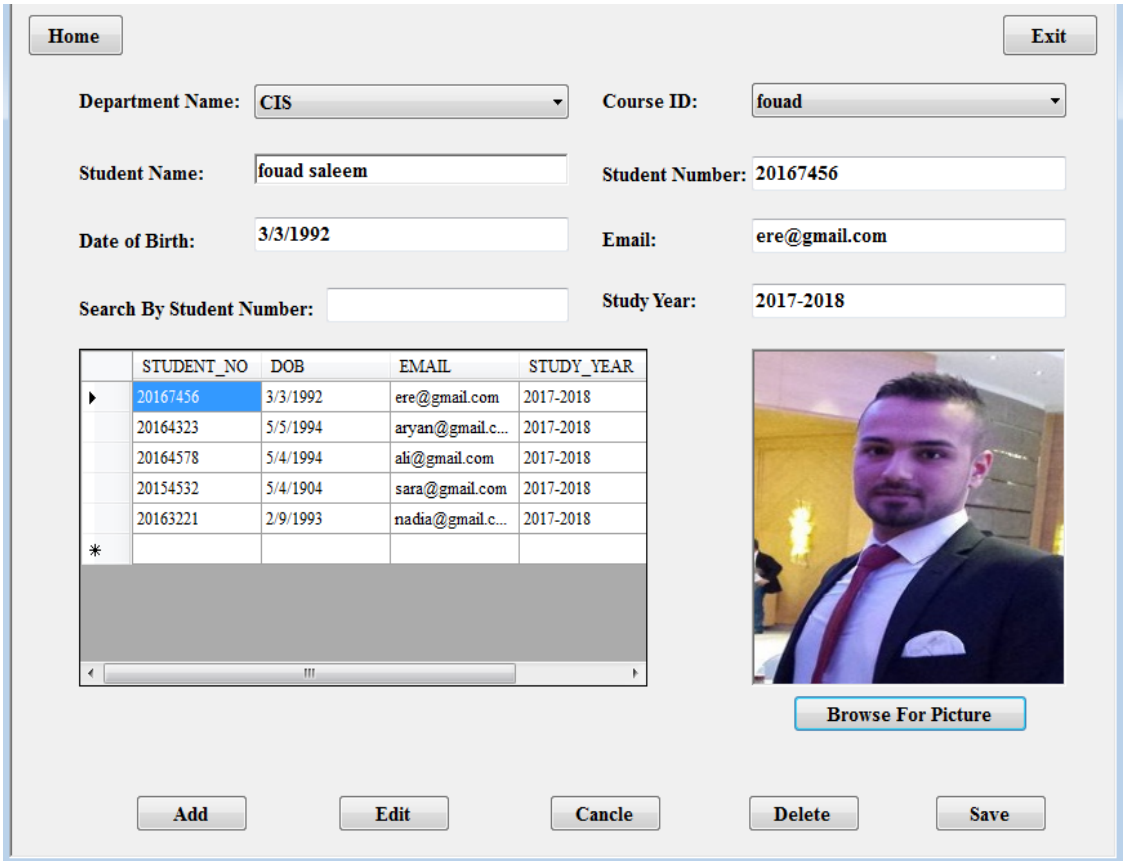


Figure 5.14: Student details form

ii. **Registration:** This is divided into two sub list: lecturer and student registration as demonstrated in Figure 5.15

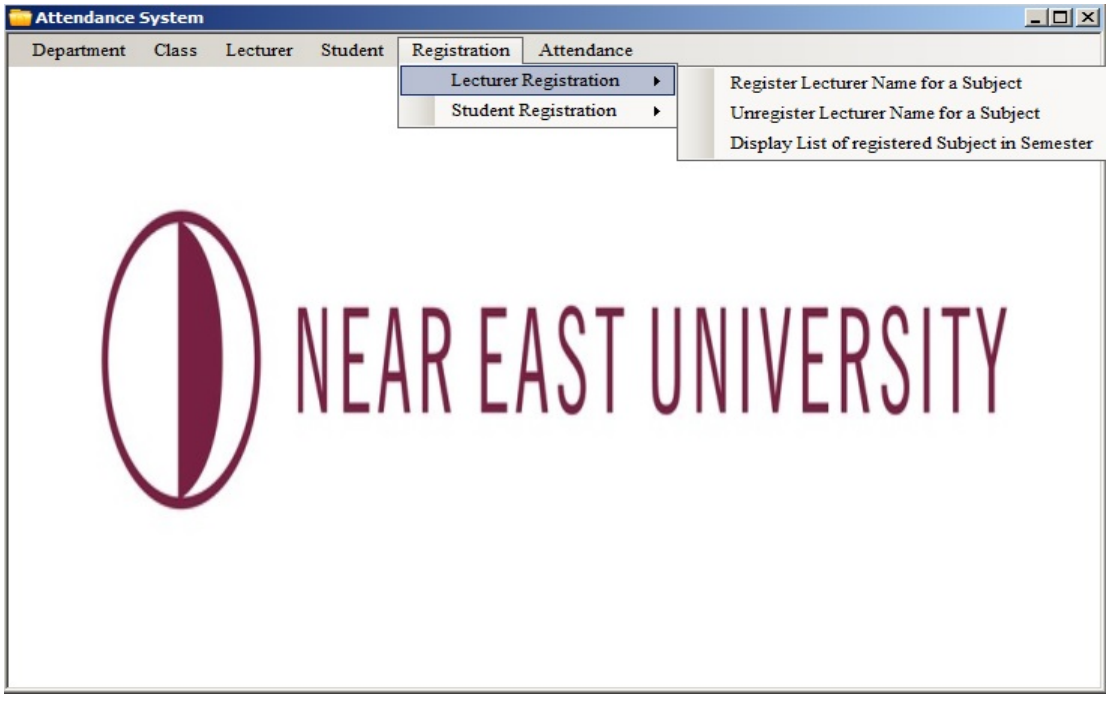


Figure 5.15: Registration option

- ***Register Lecturer Name for a Course*:** This form allow admin to register a lecturer for a specific course, here the admin does not need to typing he/she just select information's from combo boxes then clicking on Register button to complete the event as shown in the Figure below.

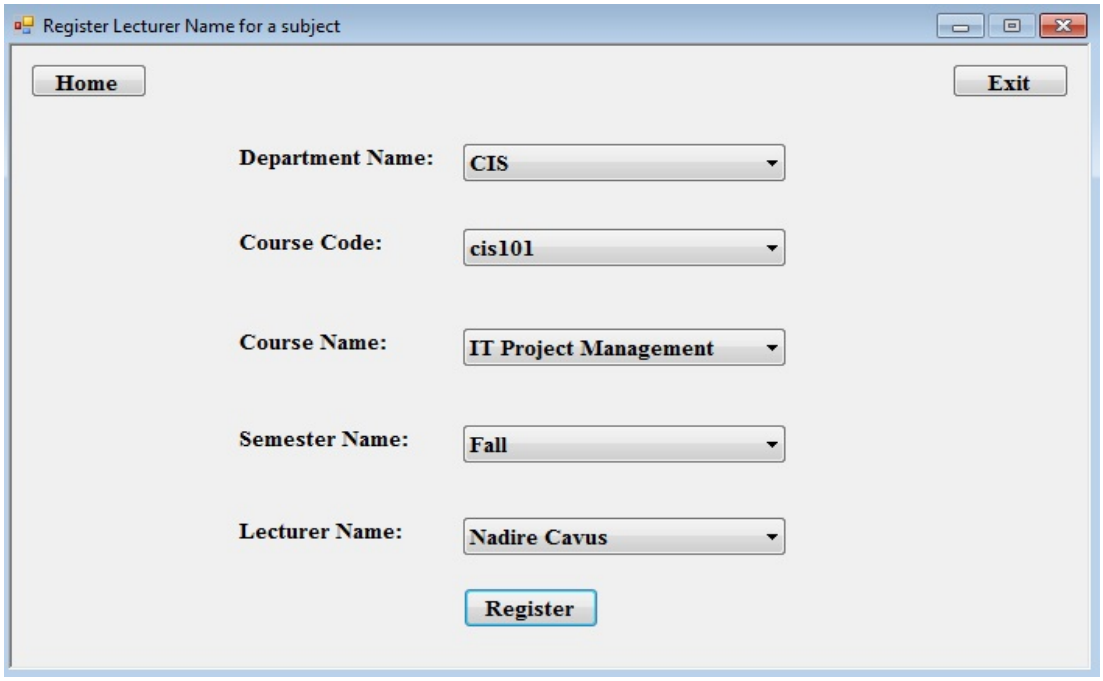


Figure 5.16: Register lecturer for a course form

- ***Unregister Lecturer for a Course*:** This form is same as the previous one, but, with the opposite action as illustrated in the Figure 5.17.

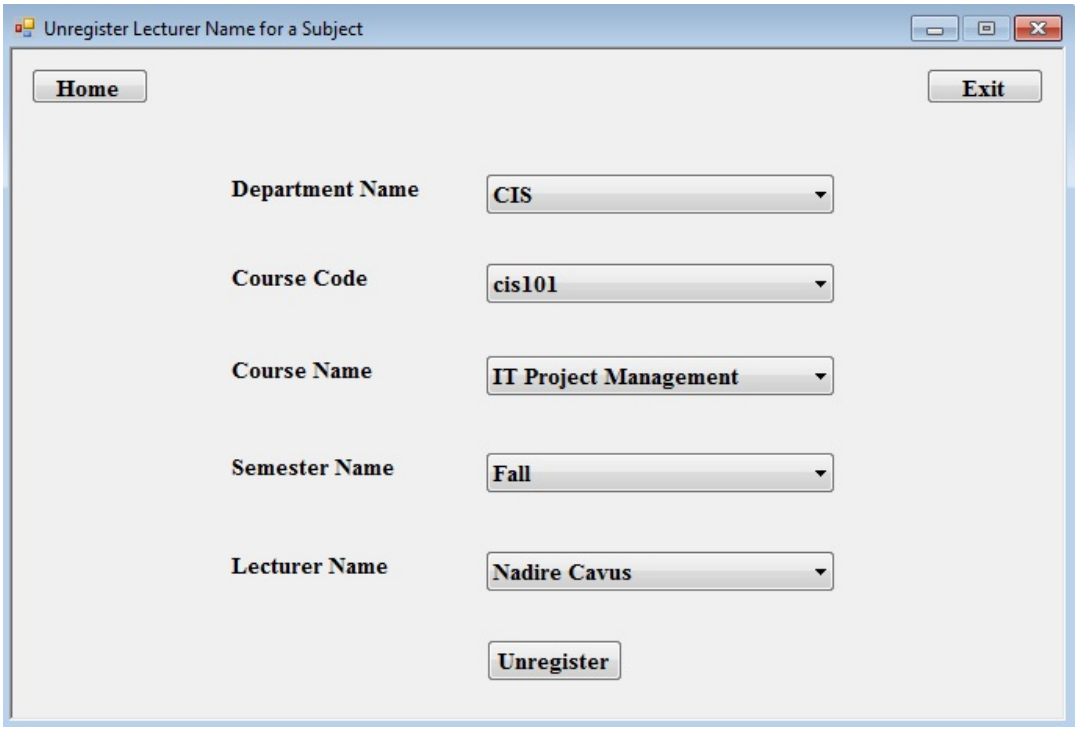


Figure 5.17: Unregister lecturer for a course form

- ***Display List of Registered Courses in a Semester*:** This form contains a data grid view that shows the courses which already registered in the semester. As given in the figure below.

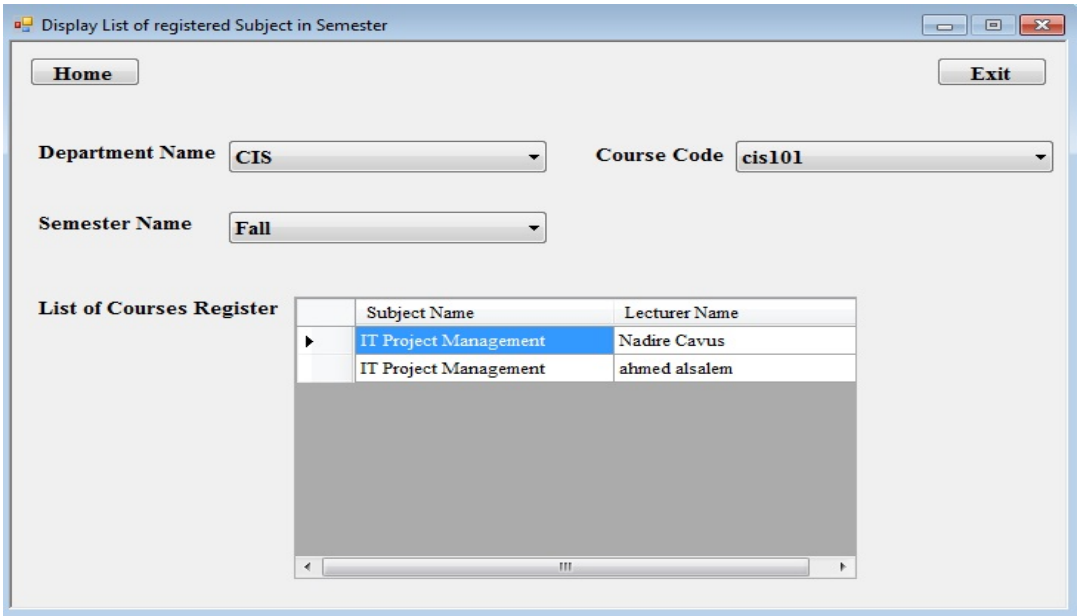


Figure 5.18: List of registered courses

- ***Register Student for a Course***: This form allow admin to register student in two options either by selecting all students who exist in the department as shown in Figure 5.19, or by entering student roll number for each one as shown in Figure 5.20, after selecting one of the options the admin need to click on the Register button to complete the action.

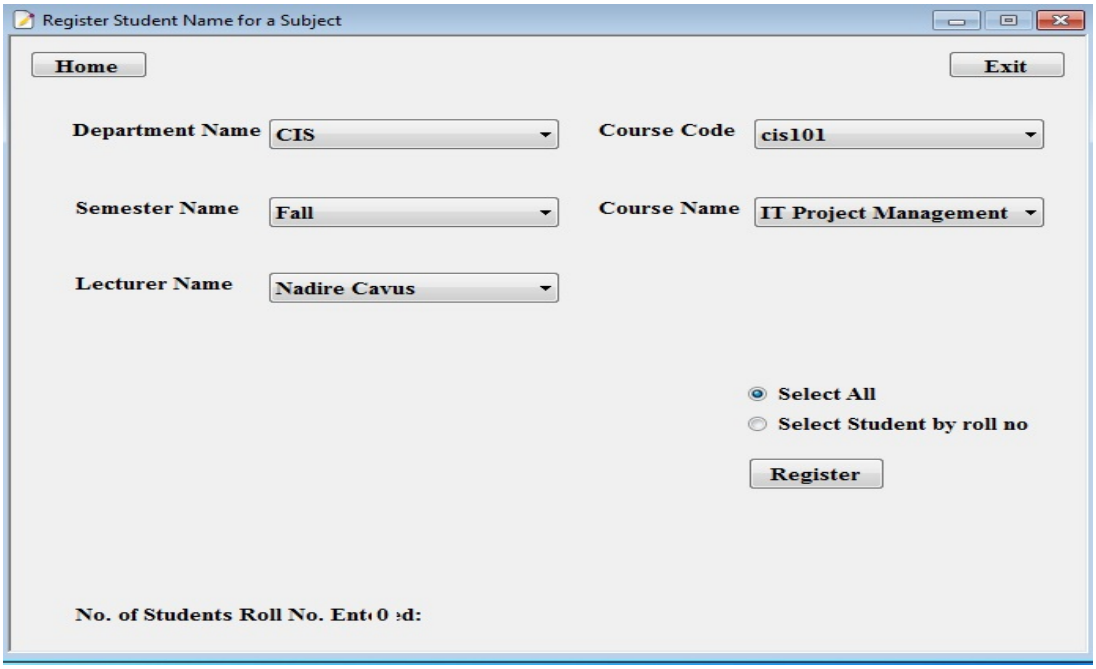


Figure 5.19: Register student for a course by selecting all

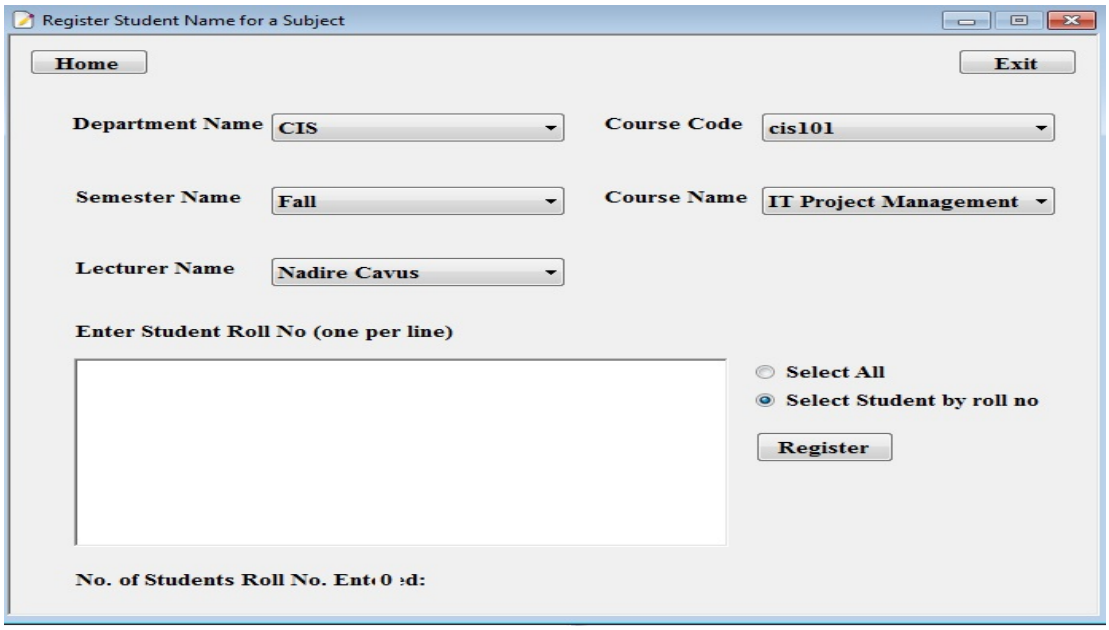


Figure 5.20: Register student for a course by roll number

- ***Unregister Student for a Course*:** This form is same as the previous one, but, with the opposite action as illustrated in the Figure 5.21.

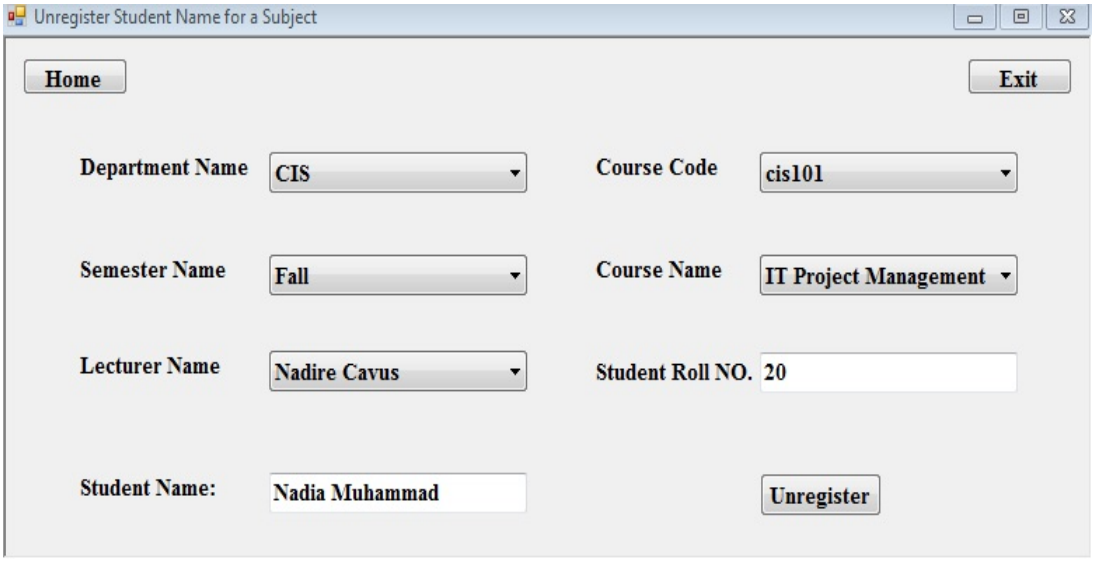


Figure 5.21: Unregister student for a course form

- ***Display List of Registered Students for a Course*:** This form contains a data grid view that shows the students who already registered for courses in the system. As provided in the figure below.

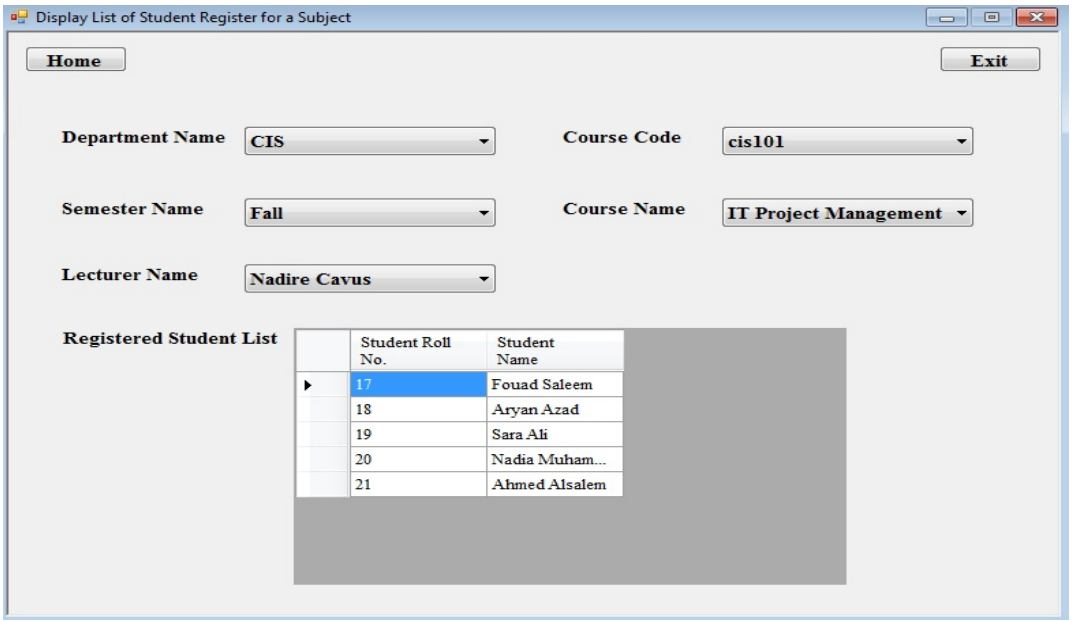


Figure 5.22: List of registered students for a course

iii. Build Attendance Document: In this windows form application the admin should select department name, course name, course ID, semester name, and, lecturer name

to build the attendance document as shown in Figure 5.23. However, the attendance report is designed in a word file that gets the information from the build document form. When clicking on show attendance the data grid view will display the names and attended students, while, when clicking on build document the word file will be generated with the required information that will send to the lecturer after the exam via email. Figure 5.24 shows the screen shot of the report that sent via email from C# application.

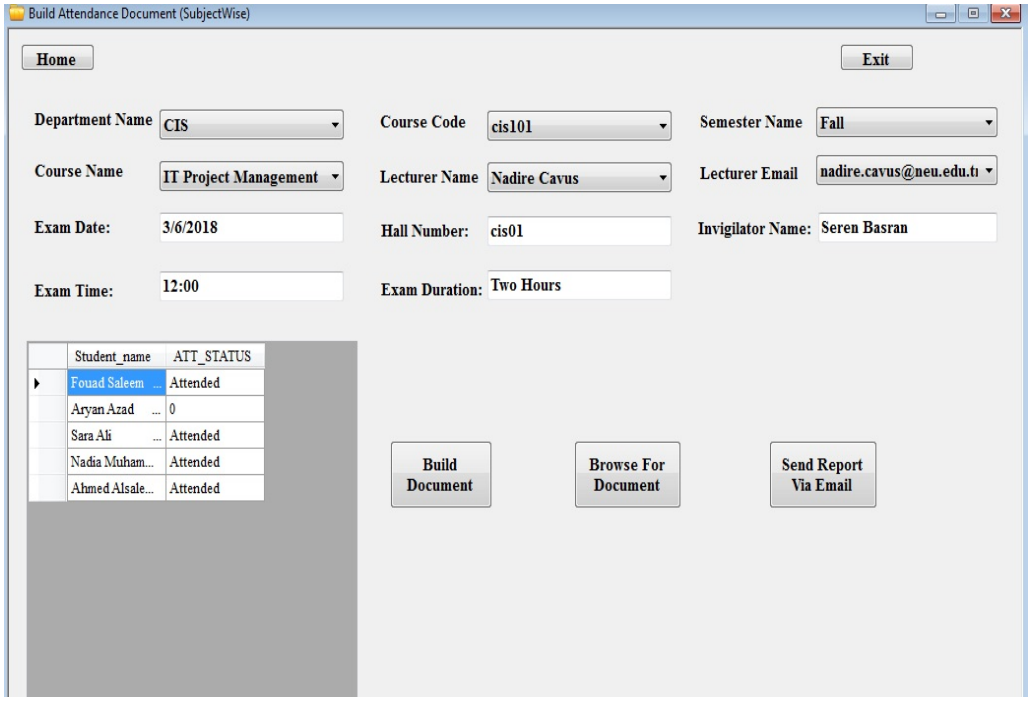


Figure 5.23: Build attendance document form

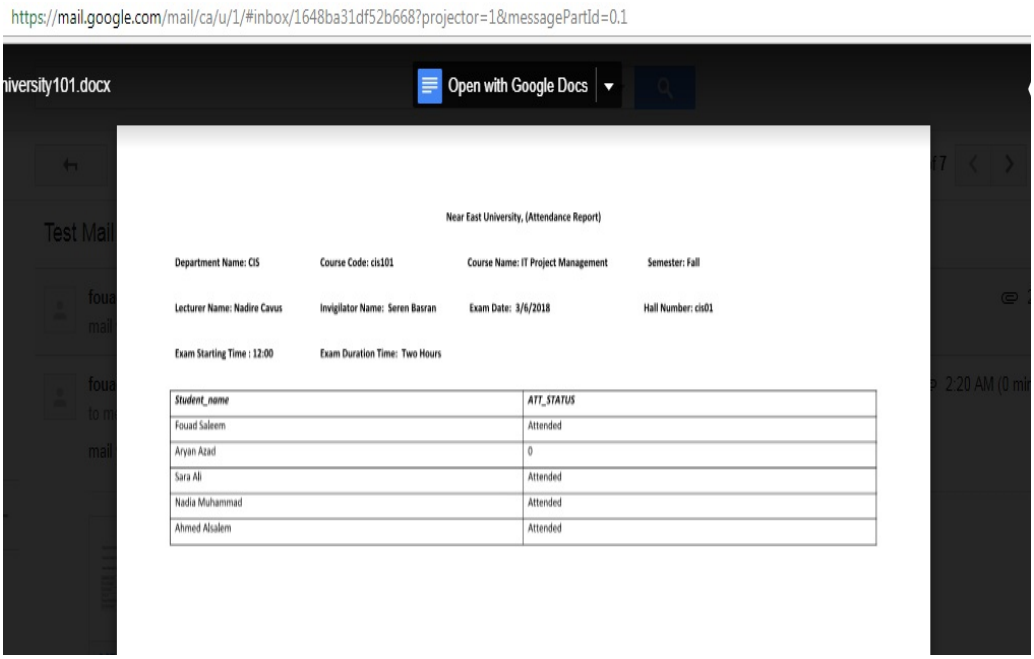


Figure 5.24: Attendance report received via email

i. **Find Student:** As a last form in the design and the first form in the execution is the find student form. In this form first should load the fingerprint image by clicking on the Load Fingerprint Image button and selecting the image from the computer as shown in Figure 5.25, the picture box which located at the bottom right will display the fingerprint image. Moreover, when clicking on the Find Student button the fingerprint will be send to the MATLAB application to identify the entry image, MATLAB in turn after identifying the student, it will send the student ID to the C# and all the student information will be displayed based on the ID that received from the MATLAB program as shown in the Figure below the left picture box contain the fingerprint and the other picture box contain the student image after identification. While, in case of student not found (unauthorized) an SMS message will be send to the advisor inform him\her that there is unauthorized person try to enter the exam as given in Figure 5.26.

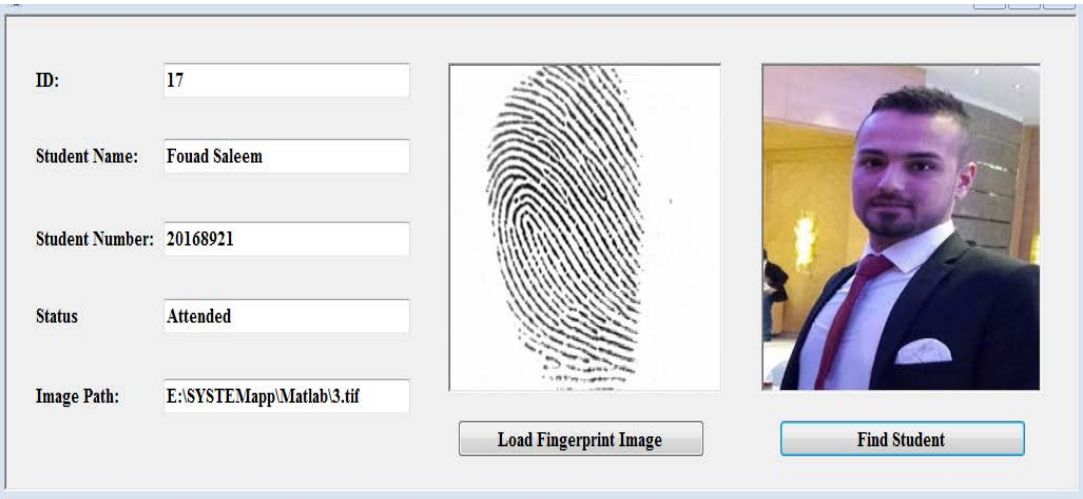


Figure 5.25: Find student form

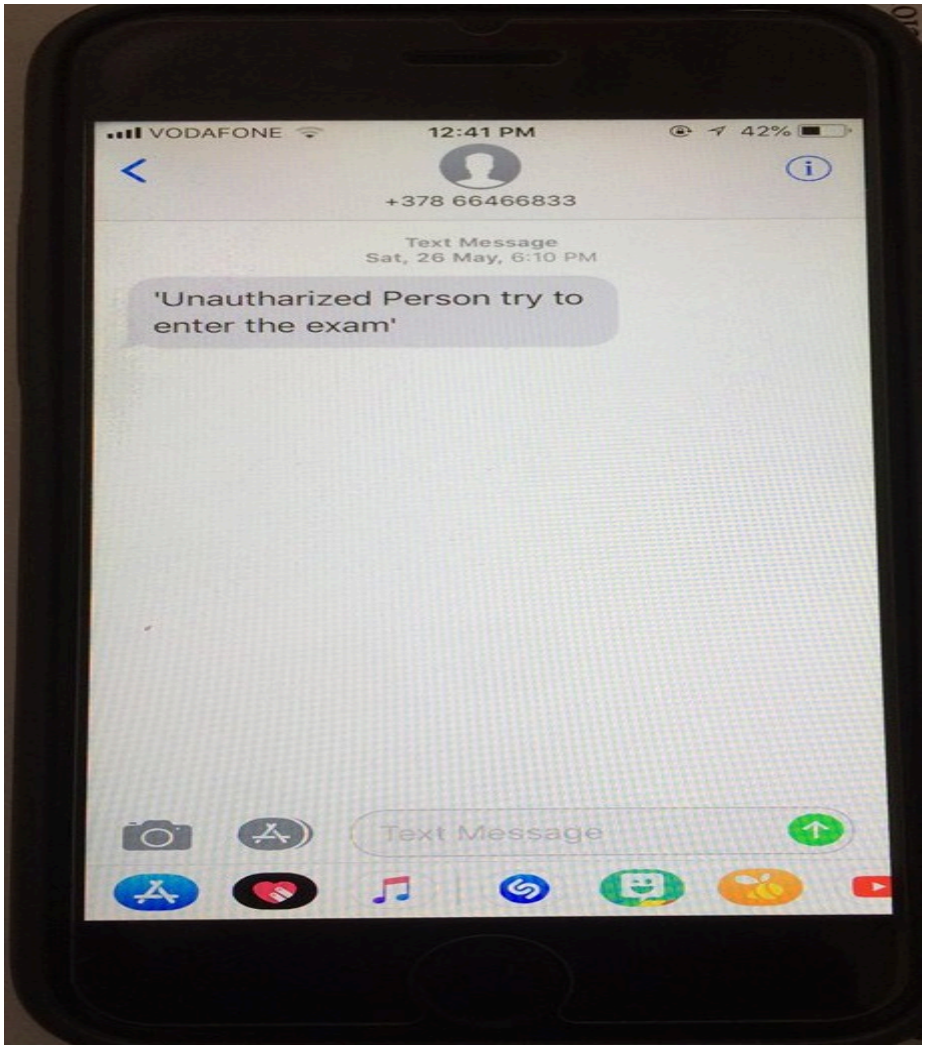


Figure 5.26: Warning SMS message received

CHAPTER SIX

CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

The main aim of this study was to develop an automatic fingerprint attendance recognition system that can be used in exam halls to verify if a student has authentic proof to sit for an exam. As a result, it can be concluded that traditional attendance systems are no longer effective since they involve a lot of manual activities and process as well as a lot of paperwork. Conclusions can also be made that the major challenges that are affecting the use and development of new fingerprint systems are costs and the need to have trained personnel who can manage the system. In addition, based on the observations that have been made about the developed fingerprint system, conclusions can be made that the developed system can effectively send email notifications about the eligibility of a student to sit for an examination as well as the performance of the student. In reference to other attendance recognition systems, the newly developed system can be said to offer a lot of benefits which include among others, ability to combat fraudulent activities, solve the problem of student disruptions during exams, reduce costs, improve effectiveness and efficiency bin recording student attendance and performance information. However, conclusions can also be made that though the proposed fingerprint recognition system is effective and offers a lot of benefits, it remains vulnerable to problems relating to the transmission of diseases and that the system may fail to read when one suffers an injury.

6.2 Recommendations

Based on the above conclusions, recommendations can therefore be made that;

- The biometric system should be linked with a mobile device so as prevent the transmission of diseases.
- A student should have two different fingerprints from his two hands linked to the database so as to curb problems that arise when a student has been injured.

- To improve the performance and the time consuming of the system, Python or any other fast platform can be used instead of MATLAB, or combining all the system process into one faster platform.

REFERENCES

Ahmed, A. O. (2016). A Multifactor Student Attendance Management System Using Fingerprint Biometrics and RFID Techniques. *International Conference on Information and Communication Technology and Its Applications*, 69-74.

Ali, M. M. (march 2016). Overview of fingerprint recognition system. *In Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference* (pp. pp. 1334-1338). mombay: IEEE.

Candela, G. T. (1995). *PCASYS-A pattern-level classification automatic system for fingerprints.* Gaithersburg: National Institute of Standards and Technology.

Cappelli, R. F. (2010). Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(12), 2128-2141.

Cappelli, R. M. (2002). Synthetic fingerprint-database generation. In Pattern Recognition, 2002. Proceedings. *16th International Conference* (pp. (Vol. 3, pp.744-747)). IEEE.

Dastidar, U. G. (2017). Fingerprint Sensor Based Attendance System Using Atmega 328 And ESP8266. *International Journal of Research in Science & Engineering* , 471-475.

Dhanalakshmi, M. B., Banupriya, M., & Janani, T. C. (2018). A parallel and ascendable of erasure writing support in cloud objective storage system. *International Journal for Research Trends and Innovation*, 98-103.

Enciso, L. B.-P.-S. (2018). E-Mail Client Multiplatform for the Transfer of Information Using the SMTP Java Protocol Without Access to a Browser. In L. B.-P.-S. Enciso, *Trends and Advances in Information Systems and Technologies* (pp. 1124-1130). Cham: Springer.

Ezema, L. S.-U. (2015). Fingerprint Based Attendance Management System. *International Journal of Scientific & Engineering Research, 7(6)*, 1623-1628 .

George, J. P. (2002). Development of efficient biometric recognition algorithms based on fingerprint and face. *Doctoral dissertation, Christ University*.

George, J. P. (2012). Transform domain fingerprint identification based on DTCWT. *International Journal of Advanced Computer Science and Applications, 3(1)*, 1-200.

Jain, A. K. (1999). A multichannel approach to fingerprint classification. *IEEE transactions on pattern analysis and machine intelligence, 21(4),*, 348-359.

Jia, Y. S. (2014, November). Caffe: Convolutional architecture for fast feature embedding. *In Proceedings of the 22nd ACM international conference on Multimedia.* (pp. 675-678). Berkeley: ACM.

Jiang, X. &. (2000). Fingerprint minutiae matching based on the local and global structures. *Proceedings of the15th International Conference on Pattern Recognition* (pp. Vol. 2, pp. 1038-1041). Nanyang: IEEE.

Kayaoglu M. Topcu, B. &. (2013). Standard fingerprint databases: Manual minutiae labeling and matcher performance analyses. *arXiv preprint arXiv:1305.1443.*, 1-14.

Kulkarni, R. H. (2017). Investigating Agile Adaptation for Project Development. *International Journal of Electrical and Computer Engineering, 7(3)*, 1278-1285.

Kumar, M. (2018). A Comparative Study of Universally Accepted SDLC Models for Software Development. *International Journal of Scientific Research in Science and Technology*, 1084-1092.

Lavanya, B. N. (2009). Fingerprint verification based on gabor filter enhancement. *International Journal of Computer Science and Information Security, 6(1)*, 138-144.

Le-Phuoc, D., & Hauswirth, M. (2018). *Linked Data for Internet of Everything. In Integration, Interconnection, and Interoperability of IoT Systems* . Cham: Springer.

Maio, D. M. (2002). FVC2002: Second fingerprint verification competition. *Proceedings by 16th international conference on Pattern recognition* (pp. (Vol. 3, pp. 811-814).). San Jose: IEEE.

Maltoni, D. M. (2009). *Handbook of fingerprint recognition.* London: Springer Science & Business Media.

Manickam, A. D. (2018). Score level based latent fingerprint enhancement and matching using SIFT feature. *Multimedia Tools and Applications*, 1-21.

Moreno-Torres, J. G. (2012). Study on the impact of partition-induced dataset shift on $ k $-fold cross-validation. *IEEE Transactions on Neural Networks and Learning Systems*, 23(8), 1304-1312.

Peralta, D. G. (2015). A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation. *Information Sciences*, 315, 67-87.

Raja, K. B. (2010). Fingerprint verification based on fusion of minutiae and ridges using strength factors, 4(1). *International Journal of Computer Applications*, 1-8.

Rani, S. B. (2017). A detailed study of Software Development Life Cycle (SDLC) Models. *International Journal Of Engineering And Computer Science, 6(7)*, 22097-22100.

Ratha, N. K. (2000). Robust fingerprint authentication using local structural similarity. *In Applications of Computer Vision, 2000, Fifth IEEE Workshop on.*, pp. 29-34.

Saraswat, C. &. (2010). An efficient automatic attendance system using fingerprint verification technique. . *International Journal on Computer Science and Engineering*, 2(02), 264-269.

Siddiqui, F. N. (2017). Fingerprint Based Wireless Attendance System. *Imperial Journal of Interdisciplinary Research, 3(2)*, 993-995.

Steinbeck, C., Han, Y., Kuhn, S., Horlacher, O., Luttmann, E., & Willighagen, E. (2003). The Chemistry Development Kit (CDK): An open-source Java library for chemo-and bioinformatics. *Journal of Chemical Information and Computer Sciences, 43(2),* 493-500.

Suryawanshi, V. A. (2017). Attendance System Using Fingerprint Identification with GUI. *International Journal of Engineering Development and Research, 5(2),* 1879-1888.

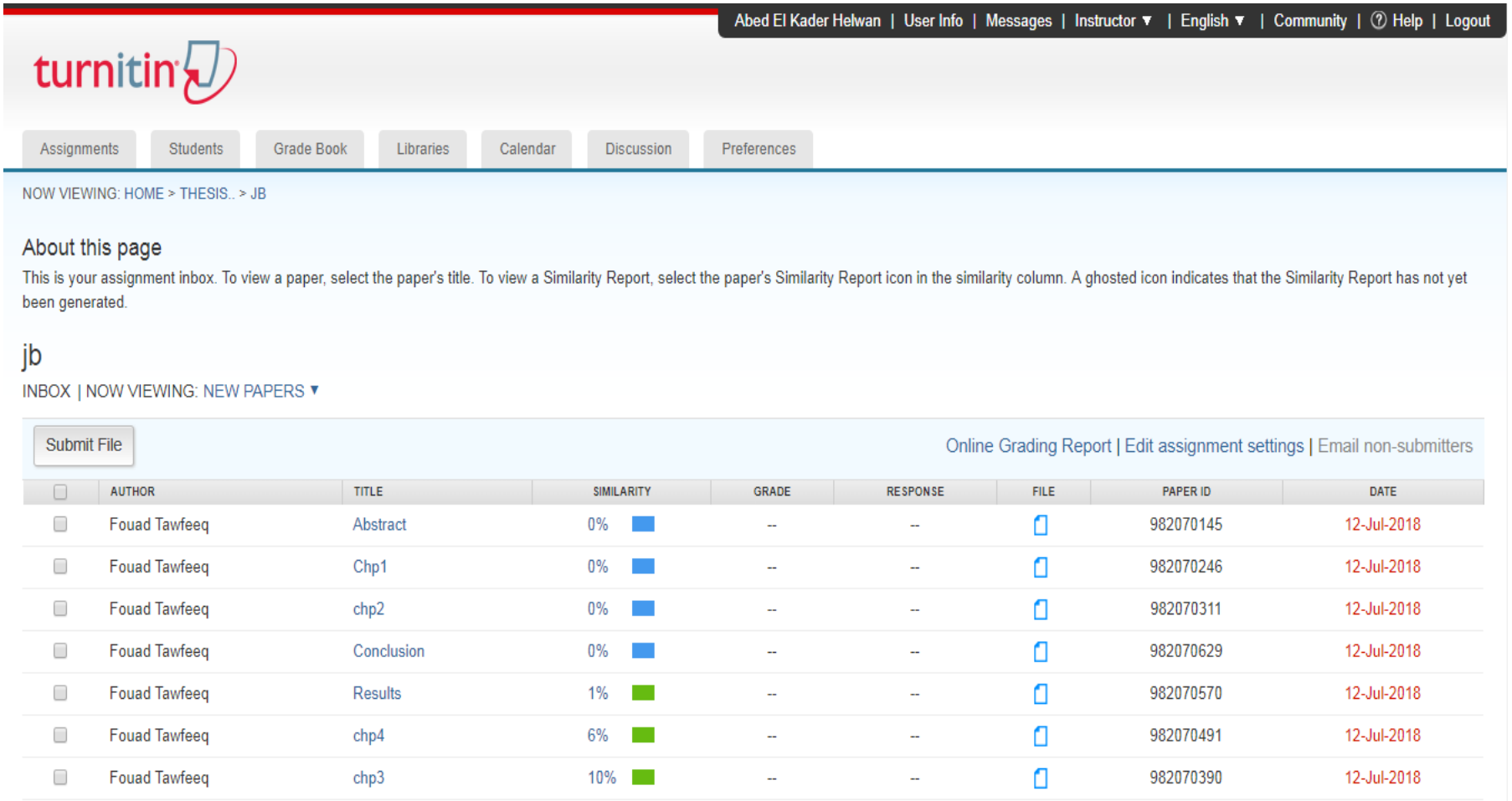
Talaviya, G. R. (2013). Wireless fingerprint based college attendance system using Zigbee technology. *International Journal of Engineering and Advanced Technology, 2(3),* 201-203.

Taylor, S. L., Baumert, J. L., & Boudreau-Romano, S. M. (2017). Allergic reaction from fingerprint kit attributable to unlabeled gluten, probable wheat flour. *The Journal of Allergy and Clinical Immunology: In Practice, 5(2),* 479-481.

Wadhwa, P. (2017). Attendance System Using Android integrated Biometric Fingerprint Recognition. *International Research Journal of Engineering and Technology, Vol. 4(6),* 1069-1073.

Walia, H. &. (2016). Fingerprint Based Attendance Systems-A Review. *International Research Journal of Engineering and Technology, Volume, 3(7),* 1166-1171.

Yadav, D. K. (2015). Fingerprint Based Attendance System Using Microcontroller and LabView. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 4(6),* 5111-5121.


Abed El Kader Helwan | User Info | Messages | Instructor ▼ | English ▼ | Community | Help | Logout
turnitin
Assignments
Students
Grade Book
Libraries
Calendar
Discussion
Preferences
NOW VIEWING: HOME > THESIS.. > JB
About this page
This is your assignment inbox. To view a paper, select the paper's title. To view a Similarity Report, select the paper's Similarity Report icon in the similarity column. A ghosted icon indicates that the Similarity Report has not yet been generated.
jb
INBOX | NOW VIEWING: NEW PAPERS ▼
Submit File
Online Grading Report | Edit assignment settings | Email non-submitters
AUTHOR TITLE SIMILARITY GRADE RESPONSE FILE PAPER ID DATE
Fouad Tawfeeq Abstract 0% -- -- 982070145 12-Jul-2018
Fouad Tawfeeq Chp1 0% -- -- 982070246 12-Jul-2018
Fouad Tawfeeq chp2 0% -- -- 982070311 12-Jul-2018
Fouad Tawfeeq Conclusion 0% -- -- 982070629 12-Jul-2018
Fouad Tawfeeq Results 1% -- -- 982070570 12-Jul-2018
Fouad Tawfeeq chp4 6% -- -- 982070491 12-Jul-2018
Fouad Tawfeeq chp3 10% -- -- 982070390 12-Jul-2018