CLASS ATTENDANCE MANAGEMENT SYSTEM USING BIOMETRIC TECHNOLOGY

BY

IRUAFEMI WISDOM OISEWEMIMI

MAT. NO: ICT/2252060257

BEING A PROJECT WORK SUBMITTED TO THE

DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF

INFORMATION AND COMMUNICATION TECHNOLOGY

AUCHI POLYTECHNIC, AUCHI, EDO STATE.

IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF HIGHER NATIONAL DIPLOMA (HND) IN COMPUTER SCIENCE.

NOVEMBER, 2022

CERTIFICATION

We, the undersigned, hereby certify that the project work was carried out by **IRUAFEMI WISDOM OISEWEMIMI** with the Matriculation Number **ICT/2252060257** of Computer Science Department.

We certify that this work is adequate in scope and quality in partial fulfillment of the requirements for the award of Higher National Diploma (HND) in Computer Science.

________________________ ____________________________

MR. UKOLO JOSEPH **Date**

Project Supervisor

______________________ _____________________________

MR. AKHETUAMEN SYLVESTER **Date**

Head, Department of Computer Science

DEDICATION

This project is dedicated to God Almighty for His love and to our family.

ACKNOWLEDGEMENT

I am most grateful to God Almighty, for His knowledge, wisdom, and mercies throughout the period of the program.

My deep appreciation goes to my supervisor **MR. UKOLO JOSEPH** who gave his time and efforts to make this work achievable.

Also, to my H.O.D **MR. AKHETUAMEN SYLVESTER** for his fatherly advises, encouragement and for imparting knowledge in me for the successful completion of this work. I am most grateful sir.

Also, to my beloved parent **MR. & MRS. IRUAFEMI** for the secret prayers and encouragement. May God continue to preserve you with good health.

To my siblings **EVELYN & FAMOUS IRUAFEMI** thanks for your love toward me during my period of study.

To my friends **OSAS, MATTHEW, WILFRED AND LOVETH** for your friendly advice and support during my period of study.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

CHAPTER TWO

LITERATURE REVIEW

CHAPTER THREE

RESEARCH METHODS

CHAPTER FOUR

SYSTEM IMPLEMENTATION

CHAPTER FIVE

SUMMARY, RECOMMENDATION AND CONCLUSION

ABSTRACT

This project is on the design and implementation of class attendance management system using biometric technology that can be used to monitor attendance of the student. It will eliminate the problems of manual method. The new system utilizes a portable fingerprint scanner as the input to acquire fingerprint images and notebook personal computer as the mobile terminal for the processing of the images and records attendance. It also include database to store student's information and attendance records. Visual Basic.net was used as the programming language to develop this system. The system was tested and found working correctly.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Attendance management of students in institution can be rigorous using the conventional method of paper sheets and old file system method. Every academic institution poses some standards concerning how attendance is to be confirmed for student in classes, laboratory sessions and examination halls. That is why keeping the accurate record of attendance is very important. The approach of using paper sheets and the old file system to confirmed students has been in use for years. There are so many bottlenecks with the conventional method, one of such problem is the difficulty for the management to compute the percentage of student attendance in classes and frequently modify their information. Also in institution, tracking and monitoring student time of attendance could be tedious task, time consuming and as well prone to errors. As an alternative to traditional manual clocking process by students in classes or during examination, an automated system can be used for authenticating students. This research will focus on developing Student Attendance Monitoring System. In the manual signing processes, where lecturer give a sheet of paper to student to write their names and signature as a form of confirming their presence for a particular class session, falsification in student attendance mostly occur a situation where by a student can sign on behalf of his or her colleague as being present in the class when not true can be so difficult to prevent from happening especially for large classes where row count can takes longer time International Journal of Computer Science and Network Security (2009).

The trending concern in this modern world is regarding national security, identifying theft as well as on-line terrorism. Researcher refers to computerization as a solution for detecting user's identity and security challenges emanating in this modern day. Biometric identification is any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identify of an individual. Biometric science utilizes the measurements of a person's behavioral characteristics (keyboard strokes, mouse movement) or biological characteristics (fingerprint, iris, nose, eyes, jaw, voice pattern, etc). It is the features captures that is being transformed digitally into a template. The recognition software can then be used to discover an individual as the person they claim to be. Fingerprint recognition is the most common biometric method adopted in identification of a person (Ismail 2009).

Biometric is a field of technology that uses automated methods for identifying and verifying a person based on physiological and behavioral traits. Because some parts of the human body is use in biometrics, the issue of getting lost is not possible and for password to be easily guess can be easily avoided. Also, utilizing biometrics in most cases can be said to be more efficient when speed is considered and convenient than employing password and ID cards method.

Using a particular person fingerprint as a form of authentication is just like using natural physical data as a password. The benefit of using biometric authentication is that it is absolutely distinct to each person. There are no two different individuals with the same fingerprint, it is difficult and impossible for one another to have the same fingerprint, and fingerprints from different people can never be the same. Also, a fingerprint can never be guess by a criminal, such as a password which imposter can easily predict using a user birth date or any other common password. Infiltration is very hard to come by due to the fact that criminal will not be able to snoop around to steal user password when using ATM with the 4-digit pass code (Valasquez 2013).

Fingerprint can be categorize as one of the most mature biometric traits and is accepted in courts of law as a legitimate proof of evidence. Fingerprints are adopted in forensic analysis globally in investigations of criminal. More recently, there are growing numbers of individuals and commercial users that are currently using or strongly putting into consideration of using fingerprint-based identification for no any other reason other than the matching performance biometric technology has demonstrated as well as a better understanding of fingerprints.

Although there are so many positive impacts for using biometric authentication, however, unlike username and password, biometric data is a physical feature of a person that is fixed and cannot be change. If a person could have access to adequate scan another person fingerprint, that scan has the capability to trick the Touch ID system. In that case, the fingerprint features of a person can’t be change consequently a criminal can’t be prevented from having access to your personal information or files. As fingerprint scanning becomes more widely accepted anywhere anytime, this may become a substantial challenge. A criminal can have access to different accounts because with one fingerprint, a criminal may have access to multiple accounts that implemented authentication using fingerprint.

1.2 Statement of the Problem

The traditional system is still mostly used in lecture room or laboratory session in most institution today. Lecturer or instructor will give out a sheet of paper containing list of student’s name to sign or in some cases, the student will be the ones to write their names, student id and matriculation number to indicate their presence for a particular class. Falsification in student attendance does occur rampantly in the traditional method. For example, another student can easily sign an attendance on behalf of another student. In other to prevent this problem, it is necessary to develop an Authentication System for Students using fingerprint Biometric recognition that will be employed to track and keep the attendance of every student in a particular class. Fingerprint is unique feature for everyone compare to using barcode in smart cards. Therefore, this system designed in this project work is not based on the existing barcode system. Tracking and monitoring student time of attendance could be tedious, time consuming and more susceptible to errors. The security of the existing attendance system that are now use in classroom (signature system) can be easily compromised. Some students can master other student's signature. Thereby, helping their colleague who are absent for a particular class to sign the attendance sheet using the duplicated signature. The Fingerprint Attendance monitoring system designed in this research work for student is a more secure platform where students mark their attendance with their fingerprint.

1.3 Aim and Objectives

The aim of the study is to design and implement a reliable, scalable and cost effective Class attendance management system using biometric technology. This is to be achieved by the following objectives:

(i) To design a System that is able to capture and analysis student finger print

(ii) To implement a system that prevents falsification

(iii) To save student attendance recording properly

1.4 Significance of the Study

The System for Students using fingerprint Biometric will eliminate the use of paper in manual signing processes and all the risk associated with it. One of the risks of using a paper in class attendance is that it can be easily misplaced and students cheat by signing for each other not present in the class thereby defeating the aim of taking the attendance. Tracking and monitoring students time of attendance could be tedious, time consuming and susceptible to error. Thus, the System will drastically reduce time needed to verify attendance data.

The System also allows the institution management to track or investigate student class attendance in a particular course having poor attendance thereby enabling the management to rectify the situation by providing the necessary interventions. The system provide high level of security whereby making it impossible for imposters and impersonators in making their ways to examination halls. The System using fingerprint Biometric will keep historical data making it easy for lecturers to access and grade students.

Class attendance management system using biometric technology is extremely useful in institutions especially during classes, tutorials, laboratory sessions and examination during which heavy security are normally deploy to validate student's identity in order to cob imposters, with the use of Authentication System the number of security personnel will be greatly reduce. Most lecturers' handout sheet of paper for their class attendance, which can easily be misplaced or damaged and poses a lot of stress in cumulating grades for their students. The system allows the lecturer to monitor each student attendance, track down truants and take the appropriate action. Thus, the system eliminates all these downsides. The Authentication system is not only useful to the institutions and lecturers alone, even the students benefit a great deal by reducing the stress in queuing up which result in delay and often time in the damage of the attendance sheet. It also prevents mistakes and anomaly that is associated with manual signing in which student that attend a class are marked as not present thereby losing the mark accorded to the particular attendance due to multiple attendance sheet.

1.5 Scope of the Study

The scope of this work is to develop a Class attendance management system using biometric technology that will improve how attendance management is done by using fingerprint as a form authentication for proof of attending a class. The system will be a window based application developed using Microsoft Visual Basic.net as the preferred programming language for building the user interface and Microsoft SQL Server for database design. It does not cover other aspects of biometric.

1.6 Operational Definition of Terms

Biometrics is physiological or behavioral characteristics unique to individuals, this Include Fingerprint, hand geometry, handwriting, iris, retinal, vein and voice.

PIN personal identification number.

Biometric Verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits.

Scanner a device for examining, reading, or monitoring something in particular..

Fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern.

Rapid Application Development is a concept that products can be developed faster and of higher quality.

Authentication is the process of determining whether someone or something is, in fact, who or what it declared to be.

Use Case Diagram is used to show scenarios used for understanding the requirements of the system and to show the interaction between the user and the system.

Flow chart or Activity Diagram is a Unified Modeling Language that represents the graphical workflows of stepwise activities and actions with support for iteration, choice and concurrency.

CHAPTER TWO

LITERATURE REVIEW

2.1 What is Biometrics?

Biometrics is the science and technology of measuring of measuring and breaking down natural information. In data innovation, biometrics relates to technologies that examine and measure physical human body features, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for validation or authentication purposes (Rouse, 2008).

The process of Biometric validation is way by which an assessing of some spotting biological or traits can be distinctly identified in an individual. These unique identifiers constitute retina, earlobe geometry, iris patterns, fingerprints, hand geometry, voice waves, earlobe geometry DNA, and signatures. The voice waveform recognition method with tape recordings in telephone wiretaps of verification which has been utilized for so many years is now majorly being used in research facilities for access to restrictively databanks. Law enforcement has implemented Facial-recognition technology to fish out people in congregation with significant unwavering quality and reliability. Mostly industries utilize Hand geometry for providing physical access to buildings. For people who try to impersonate another individual, earlobe geometry is utilized to detect their identity. Signature comparison is not referring to as being dependable or reliable in isolation to other method of biometric verification but provides an additional level of check or verification when utilized in together with other biometric verification methods.

In Computer Science, biometric identification or biometric authentication is utilized as a mode of identification and access control and also being implemented to detect individuals in groups that are being watch or under surveillance (Jain, Anil K, Ross, Arun , 2008).

Using biometric verification is turning into a progressively regular for Authentication in corporate and public security systems, consumer electronics and point of sale (POS) applications. In addition to security, the motivation behind biometric verification has been convenience to avert identity theft, biometric data is usually encrypted when it's gathered (Wayman, 2005). The process of biometric verification process starts by using a software application to spot some specific points of human physical characteristics which serves as match point or template. The match point which is stored in the database is then processed using an algorithm that converts the information captured into a numerical format. The input gotten from user input through biometric scanner is now being compared to the numerical value stored, and the authentication process if matches that of the database template is approved or rejected if it differs.

The identification verification process is the same irrespective of the biometric methodology employed. An individual distinct feature is captured, processed by a software application and stored as a template into a database. Subsequently, when there is need for verification of an individual, a new physical feature is captured and compared against the template stored from a data source.

Using biometrics for recognizing users offers some extraordinary favorable circumstances because only biometrics can recognize an individual as himself or herself, biometrics could make keys and combination locks could turn out not to be useful due to biometrics and all data, including biometrics is vulnerable whether in storage or in processing state (Kadry, Smaili, 2010).

2.2 History of Biometrics

The expression "Biometrics" is gotten from the Greek words "bio" (life) and "metrics" (to measure) (Rood and Hornak, 2008). Automated biometric systems have just become useable over the last few decades, because of substantial improvement in the area of image and computer processing. Although biometric technology is a subject of twenty first century, nevertheless the Biometrics has its root as back thousands of years. The ancient Egyptians and the Chinese has a major part in biometrics history. The focus today is on utilizing biometric face recognition, iris recognition, fingerprint, retina recognition and recognizing physical features of human being to put a stop to terrorism predicament and improve security measures. The first recorded systematic capture of hand and finger images for recognizing purposes was during 1858 utilizes by Sir William Herschel, Civil Service of India, who recorded a handprint on the back of a contract for each worker to distinguish employees (Komarinski, 2004). During 1870, Alphonse Bertillon created a technology for recognizing people which is solely dependent on elaborate records of their body measurements, physical descriptions and photographs. This method was termed as "Bertillonage" or anthropometrics and the utilization was terminated in 1903 when it was apparent that some people have same measurements and physical characteristics (State University of New York at Canton, 2003). Sir Francis Galton, in 1892, created a classification system for fingerprints using minutiae characteristics that is utilized by educationalists and researchers in this modern day.

The FBI and West Virginia University in year 1920 established a degree program (Bachelor's Degree) in biometric system that is after consulting some professional associations like International Association for Identification. This serves as the first biometrics based degree program despite some universities having started related courses in biometrics.

In April 2002, a Staff Paper on palm print technology and Integrated Automated Fingerprint Identification System (IAFIS) palm print capabilities was submitted to the Identification Services (IS) Subcommittee, Criminal Justice Information Services Division (CJIS) Advisory Policy Board (APB). The Joint Working Group called "for strong endorsement of the planning, costing, and development of an integrated latent print capability for palms at the CJIS Division of the FBI." As a result of this endorsement and other changing business needs for law enforcement, the FBI announced the Next Generation IAFIS (NGI) initiative. A major component of the NGI initiative is development of the requirements for and deployment of an integrated National Palm Print Service (**2002** Palm Print Staff Paper is submitted to Identification Services Committee).

The National Science & Technology Council, a US Government cabinet-level council, established a Subcommittee on Biometrics to coordinate biometrics R&D, policy, outreach, and international collaboration (2003 Formal US Government coordination of biometric activities begins). On May, 28 2003, The International Civil Aviation Organization (ICAO) adopted a global, harmonized blueprint for the integration of biometric identification information into passports and other Machine Readable Travel Documents (MRTDs) … Facial recognition was selected as the globally interoperable biometric for machine assisted identity confirmation with MRTDs. The European Biometrics Forum is an independent European organization supported by the European Commission whose overall vision is to establish the European Union as the World Leader in Biometrics Excellence by addressing barriers to adoption and fragmentation in the marketplace. The forum also acts as the driving force for coordination, support and strengthening of the national bodies (2003 European Biometrics Forum is established).

The United States Visitor and Immigrant Status Indication Technology (US-VISIT) program is the cornerstone of the DHS visa issuance and entry I exit strategy. The US-VISIT program is a continuum of security measures that begins overseas at the Department of State's visa issuing posts, and continues through arrival to and departure from the US. Using biometrics, such as digital inkless fingerprints and digital photographs, the identity of visitors requiring a visa is now matched at each step to ensure that the person crossing the US border is the same person who received the visa. For visa-waiver travelers, the capture of biometrics first occurs at the port of entry to the US. By checking the biometrics of a traveler against its databases, US-VISIT verifies whether the traveler has previously been determined inadmissible, is a known security risk (including having outstanding wants and warrants), or has previously overstayed the terms of a visa. These entry I exit procedures address the US critical need for tighter security and its ongoing commitment to facilitate travel for the millions of legitimate visitors welcomed each year to conduct business, learn, see family, or tour the country(2004 US-VISIT program becomes operational). The Automated Biometric Identification System (ABIS) is a Department of Defense system implemented to improve the US Government's ability to track and identify national security threats. The associated collection systems include the ability to collect, from enemy combatants, captured insurgents, and other persons of interest, ten rolled fingerprints, up to five mug shots from varying angles, voice samples (utterances), iris images, and an oral swab to collect DNA(2004 DOD implements ABIS).

In 2004, President Bush issued Homeland Security Presidential Directive 12 (HSPD-12) for a mandatory, government-wide personal identification card that all federal government departments and agencies will issue to their employees and contractors requiring access to Federal facilities and systems. Subsequently, Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) for Federal Employees and Contractors, specifies the technical and operational requirements for the PIV system and card. NIST Special Publication 800-76 (Biometric Data Specification for Personal Identity Verification) is a companion document to FIPS 201 describing how the standard will be acquiring, formatting and storing fingerprint images and templates for collecting and formatting facial images; and specifications for biometric devices used to collect and read fingerprint images. The publication specifies that two fingerprints be stored on the card as minutia templates. In 2004, Connecticut, Rhode Island and California established statewide palm print databases that allow law enforcement agencies in each state to submit unidentified latent palm prints to be searched against each other's database of known offenders. The Face Recognition Grand Challenge (FRGC) is a US Government-sponsored challenge problem posed to develop algorithms to improve specific identified areas of interest in face recognition. Participating researchers analyze the provided data, try to solve the problem, and then reconvene to discuss various approaches and their results – an undertaking that is driving technology improvement. Participation in this challenge demonstrates an expansive breadth of knowledge and interest in this biometric modality.

The broad US patent covering the basic concept of iris recognition expired in 2005, providing marketing opportunities for other companies that have developed their own algorithms for iris recognition. However, the patent on the iris Codes implementation of iris recognition developed by Dr. Daugman will not expire until 2011(2005 US patent for iris recognition concept expires). At the 2005 Biometrics Consortium conference, Sarnoff Corporation demonstrated Iris on the Move, a culmination of research and prototype systems sponsored by the Intelligence Technology Innovation Center (ITIC), and previously by the Defense

Advanced Research Projects Agency (DARPA). The system enables the collection of iris images from individuals walking through a portal.

2.3 Types of Biometric Devices Available

There are several types of biometric data use commonly today. Each of these devices has a different mechanism employed to captures data in different form.

The different types of biometric that are frequently in use today are devices that capture data in various formats using different mechanism. The method of production and trait of the biometric data indicates the encroaching of the protocol for enrollment and authentication of users (Woodward, Nicholas 2003). The associated changes in the process of measurement and production can give a vicious person an access and allowing them to alter the security shielded around the biometric system by interfering with the operation of the mechanism for capturing or by changing features of the biometric. There are many types of biometric devices employed today. Some of these biometric devices are generally detected in commonplaces such as movies. Biometrics is essentially the identification of human features that are distinct to each person. The best way to keep your devices safe and ascertain people don’t illegally have access to your personal belongings such as files utilizing is to implement a any biometric technology available in the market.

1. Retina Scanner

These scan are the distinct biometric feature/pattern in each individual’s iris, and compares it with a certain number of distinct recognizing patterns which distinguish each individual separately from other people. In a retinal scan, at the back of the eye, a biometric format is shaped by recording the patterns of capillary blood vessels. Iris scanning can be carried out remotely utilizing a high-resolution camera and formats generated by a technique similar to that of retinal scanning. Iris scanning and retinal scanning are both used to distinguish a person as indicated by their distinct pattern. Despite their efficiency, implementing them is more costly and complex. The retina of human being is a thin tissue constituted by neural cell which is located in the posterior portion of the eye. The composite structure of the capillaries that supply the retina with blood makes the retina of each individual distinct.

Retinal scanners are regularly used for authentication and identification purposes. Retinal scanning has been implemented in several places such as several government agencies, prisons, ATM validation of authentic owners and guiding against fraud, medical application such as transmitted diseases (AIDS, Malaria, Chicken pox and e.t.c). The network of blood vessels in the retina of human being cannot be genetically determined in entirety and for that reason even twins that are identical don’t have same pattern

There are cases where by retinal patterns may be modified for people suffering from of diabetes, glaucoma or retinal degenerative disorders, however, the retina generally is permanent from child birth till death. Considering its distinct and permanence feature, the retina happens to be the most accurate, authentic of all the biometric except DNA. Its accuracy level has been concluded by advocates of retinal scanning that its error rate is estimated one in a million (Homer, Schell, 2012). A biometric identifier known as a retinal scan is used to represent the distinct patterns of a person's retina. The blood vessels in the retina can promptly absorb light more than the subordinate tissue and can be recognized more easily in the presence of lighting. A retinal scan is performed by absorbing an unperceived beam of low-energy infrared light into a person’s eye as they look through the scanner's eyepiece. This beam of light draws a similar pattern like a path on the retina. During the scan process, the total reflection differs due to the absorbent nature of retinal blood vessels of that light than other part of the eye. The format of the variations from the scanner is translated to computer code and stored in a database.

2 Iris Scanner

Iris scanning is an automated method of biometric identification which uses mathematical pattern-recognition techniques on video images of the iris of a person’s eyes, whose complex random patterns are distinct and be spotted from a far range. Digital formats which are referred to as template are converted from these patterns by using mathematical and statistical algorithms which allow the identification of an individual or someone trying to impersonate the legitimate person. Globally, there are millions of individuals in so many countries that have been enrolled into the iris recognition systems for the purpose convenience in passport-free automated border-crossings, and some national ID systems based on this technology are being deployed. The significant benefit of iris recognition, apart from its utmost resistance to false matches and speed, is the stability of the iris as an internal, protected, yet externally visible organ of the eye.

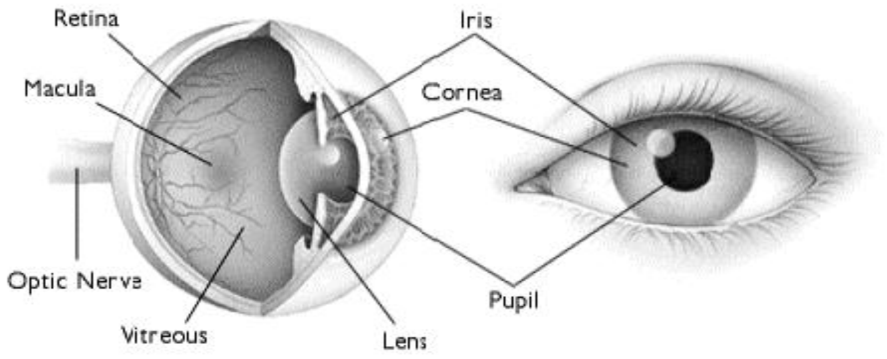


Figure 2.1 Structure of Iris

Figure2.2 Iris scanner

The major feature that depicts iris of the eye as the most ideal and accurate section of human body for biometric recognition is that it is an internal organ which is better guided from damage and wear by extremely sensitive and transparent membrane (cornea). This characteristic makes it more better option to fingerprint, which can be difficult after years of rigorous involvement in some manual labor.

The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae) that control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face. The iris has a fine texture that like fingerprints is determined randomly during embryonic gestation. Like the fingerprint, it is very hard (if not impossible) to prove that the iris is unique (Christine, Modi, 2008).

3 Fingerprint Scanner

When considering the price of biometric identification scanners available in the market today, fingerprint scanning is always on the lower end. There are some fingerprint scanners that can only scan the actual print while the costlier scanners can capture the shape and size of the thumb, presence of blood in the fingerprint and other physical characteristics on a finger. The expensive scanner can capture a 3D image of the fingerprint which in turn makes it more difficult for such fingerprint to be duplicated. The process of acquiring image by the scanner is either though capacitance sensing or optical scanning.

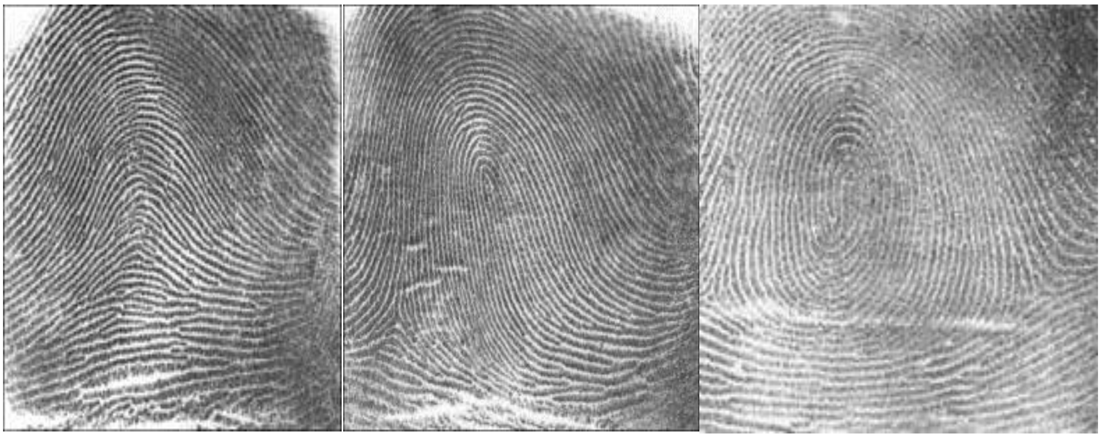
Generation of biometric templates is based on matching minutiae characteristic features in fingerprints. The examining of fingerprints for the purpose of generally requires the comparison of so many features of the print format. These comprise of patterns which are aggregated features of ridges and the minutia points, that are distinct features found within this patterns. Knowing the attributes of human skin and structure is paramount to successfully utilize some of the technologies of imaging.

The three fundamental patterns of fingerprint ridges are presented below.

(i) Arch: In arch, the ridges will enter from one side of the finger then rise in the center forming an arc, and then exit the other side of the finger.

(ii) Loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side.

(iii) Whorl: Ridges form circularly around a central point on the finger.

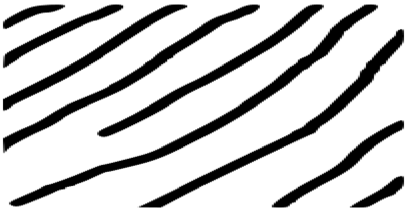


The arch pattern the loop pattern the whorl pattern

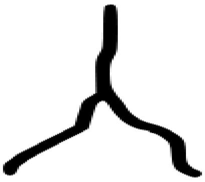
Figure2.3 Fingerprint patterns

Minutia features

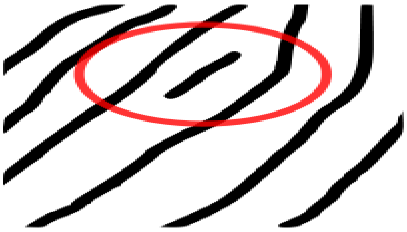
The major minutia features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot). The ridge ending refer to the point at which a ridge terminates. Bifurcations are points whereby a single ridge is divided into two ridges. Short ridges are ridges which are importantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the examining of fingerprints since there has not been any record of two fingerprints proven to be identical.



The ridge ending



Bifurcation



Short ridge (dot)

Fingerprint sensors

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The image captured from the sensor is referred to as a live scan, which in turn is processed digitally to develop an accumulation of extracted features (Biometric Template). This template is stored in a database and utilized for matching. Figure 2.4 presented some fingerprint sensors.

Figure2.4 Scanners

4 Facial Biometrics

The image or video of an individual is generally views by the facial biometrics devices and then compares it to the template stored in database. when matching is being carried out by the facial biometrics, it compares the ratio, shape and structure of the face, the interval between the jaw, top outlines of the eye sockets, the sides of the mouth, eyes, mouth, nose, the region of the cheek bones and the positioning of the nose and eyes. When a user is being enroll in a facial recognition program, various images are captured of the individual at different positions and angles with various facial expressions. In the process of verification and identification the individual will maintain a position facing the camera some seconds, after then the image is verified against the template stored. In other to prevent an individual from putting on a picture or mask when being scanned, some security criteria have been put into place. The user may be asked to smile, nod their hand or blink their eyes during the scanning process. Also as part of the security criteria would be to use facial thermograph to store the heat in the face.

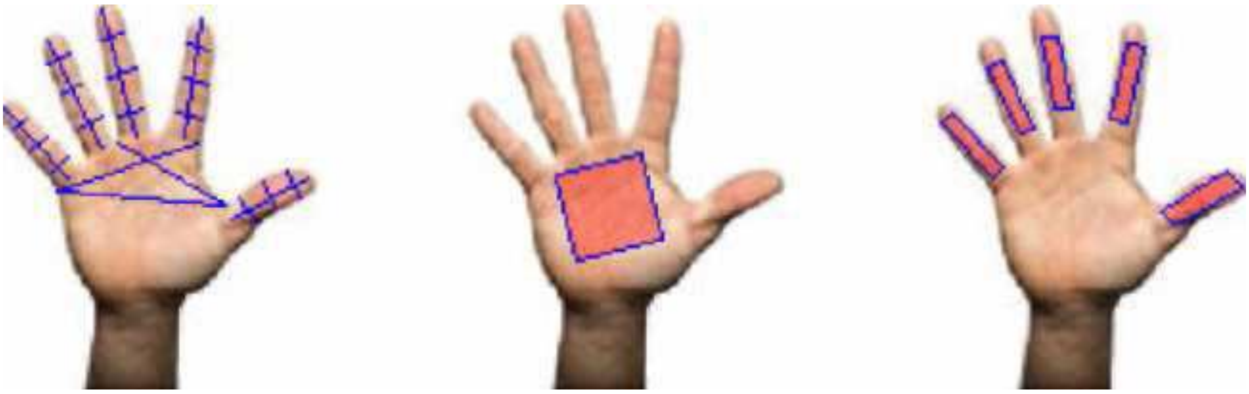
A new method in facial recognition uses the visual details of the skin, which is captured in standard digital or scanned images. This technique is referred to as skin texture analysis, which turns the distinct patterns, lines, and spots obvious in an individual's skin into a mathematical space. Facial biometrics is very good when being utilize for facial authentication than for identification purposes, because of the fact that an individual face can have a physical damage or altered, disguise with a mask, etc. Environment can also affect the camera during the process of capturing. Facial biometrics has been confirmed as a method that can improve validation and authentication of users tremendously.

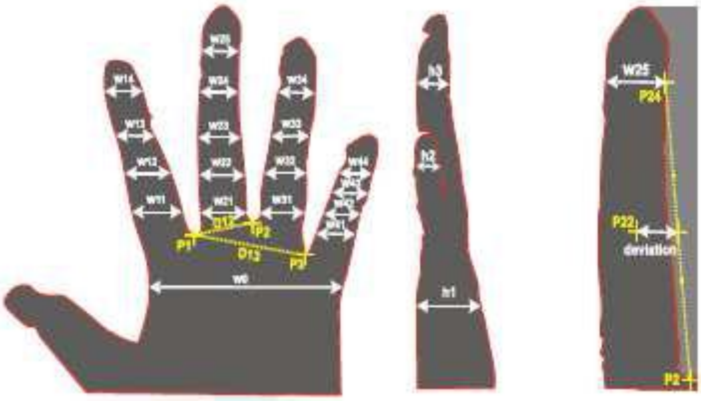
5 Voice Recognition

Every individual on the soil of the earth has a distinct voice pattern. Although the changes can be hardly noticeable to the human hear because it's a slight change. Nevertheless, with the aid of exceptional software for voice recognition, those minute variations in each individual's speech can be spotted, tested, and authenticated to give access only to the person owns the tone, pitch, and volume of speech uttered. Voiceprint recognition performs its operation by comparing the vocal patterns of an individual with template previously stored. This type of biometric has the ability to determine duress through adequate examining of pattern of stress in the input voiceprint. This feature gives voice recognition an advantage over other forms

6 Hand Print Patterns

Similarly to finger print, everybody has distinct handprints. A handprint Biometric Systems scans hand and finger and the captured feature is compared with the specimen stored for the user in the system. The user is given access or rejected based on the result of this verification. Handwriting recognition is the ability of a computer to receive and interpret intelligible handwritten input from sources such as paper documents, photographs, touch-screens and other devices. The image of the written text may be sensed "off line" from a piece of paper by optical scanning (optical character recognition) or intelligent word recognition. Alternatively, the movements of the pen tip may be sensed "on line", for example by a pen-based computer screen surface. Handwriting recognition principally entails optical character recognition. However, a complete handwriting recognition system also handles formatting, performs correct segmentation into characters and finds the most plausible words.





When a person’s hand is place on a scanner, such user will have a distinct fingerprint pattern, as well as the size and shape of the entire hand is also very unique. This is a more complex approach compare to regular fingerprint scanning, and will definitely be more accurate with minimum occurrence of falsification. Templates generated can be said to be very compact, and the method is often sensed by users to be less invasive than other types of biometric devices.

2.4 Application Areas of Biometrics

The areas in which biometrics can be applicable are government, commercial, forensic, institutions, access control, counter tourism, law enforcement agency, airport security and so on. Some of these areas will be briefly discussed below as well as those areas where biometrics is being applied.

1. Government

The application of biometrics in the government sector such as national ID card, correctional facility, driver's license, social security, welfare disbursement, border control, and passport control. Traditionally in the government, they have used token based systems examples ID cards and badges which are been given to people or the workers to put on. The government set up a central database of biometric data, such as fingerprints and digital passport photographs of all foreign nationals who apply for residence or are already residing in their nations. Maintaining a central database would prevent people using another person's identity or using false documents to obtain permission to reside, work or study in their nation. Fingerprints would be used to reliably match immigrants to their personal identification data and documentation. Foreign nationals who apply for a residence permit would be required to provide fingerprints and a passport photograph once, after which their identity could be checked against that data using fingerprint scanning and facial recognition for comparison. The biometric data would be stored in a central databank and on a chip on the residence permit. This way the information could be used by various public authorities, for example, the immigration agency when expelling illegal immigrants and the Custom Agency when incarcerating criminals. The database would also make it easier for the Immigration agency, the Police and embassies to check the identity of foreign nationals and thus prevent identity fraud. Foreign nationals themselves also stand to benefit, as the use of biometrics could prevent their falling victim to identity theft, which can be a serious problem in different nations. The Minister for Immigration, Integration and Asylum Policy sent his bill amending the Aliens Act 2000 to widen the use of biometric data in the immigration system to the House of Representatives on 5 March 2012. Biometric systems work within individual agencies, producing a range of security and facilitation benefits. The utility of biometric systems can be enhanced through the ability, where reasonably necessary, to share biometric data between agencies and to verify data against other agency holdings. Enhancing the interoperability of biometric systems can significantly assist in addressing national security and criminal threats and offer new opportunities for enhanced service delivery. These benefits will be realized through greater opportunities for the lawful sharing of biometric information and biometric capabilities between governments and greater collaboration on biometric system development.

2. Commercial

In this area, biometric is generally applicable for logging in to a computer network, electronic data security, e-commerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, and distance learning. The ability to identify a customer had greatly affected trading, as part of a general group or specifically. Monitoring the attendance of employees becomes a very easy task as employee can clock in and out the time they get or leave the office using iris scan or thumb print. There are some public vehicles’ such as Taxi and Trucks that have devices to determine distance, time, and adequate usage. There are tons of biometric solutions available in the market today and more are still in the course of development. Access control to computer systems (workstations) USB fingerprint readers, voice and face recognition software using standard camera and microphone hardware etc. Time and attendance management in institutions are all biometrics. The problems generally associated with time registration and attendance management are peculiar to those encountered with access control. There are some systems employed today that performs identification through the use of pin code or badge, but this approach can be easily compromise by users. Some employees can misplace their badge or forget their pin code. Also some employees can engage the service of their colleagues who gets to work early to use their pin or badge to the system. Adopting biometric for time registration or attendance management avoids deceiving the system by users and also reduces overhead for engaging security personnel when badges are lost or pin codes forgotten. Biometric is extremely useful in institutions especially during classes, tutorials, laboratory sessions and examination during which heavy security are normally deploy to validate student's identity in order to cob imposters, with the use of biometric System the number of security personnel will be greatly reduce.

3. Forensic

In forensic, biometrics is in use for corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children. The cost of such implementations of biometrics is very high and for existing surveillance systems the success rates vary. The police agencies have used fingerprinting as a means of identifying criminals for well over a hundred years. Police gain the most benefit because a criminal's biometric information such as fingerprints, mugs hot, DNA, etc., may already be held in a database. This enables forensic information collected at a crime scene to be matched against it. An Automated Fingerprint Identification System is designed to enable a fingerprint to be matched extremely quickly against a large number of records in a criminal database. To do this effectively it will always hold encodings of all fingers of criminals that have been saved on the database of the police. Biometrics is also used for security in places like churches where people are been search and take biometrics data before entering in order to prevent tourist, schools for students during examination or their classes and also for investigation where suspects are been examined and collection of evidence, in which the evidence are been matched and identify the deceased using biometrics.

2.5 Related Studies

There are some existing related works on the application of different methods in managing attendance of students. One of the methods proposed for monitoring attendance is embedded computer based lecture attendance management system. In this type of system, a card is reader is interfaced with a digital computer system and an electronic card is provided and personalizes to each user for authentication. Authors in, used a wireless attendance management system that authenticates using the iris of the individual. The system uses an off-line iris recognition management system that can finish all the process including capturing the image of iris recognition, extracting minutiae, storing and matching.

Attendance Management has also been carried out using attendance software that uses passwords for authentication. The authors in designed and implemented a system that authenticates the user based on passwords, this type of system allows for impersonation since the password can be easily fiddled. There are cases where passwords could be forgotten which inturn prevents the user from gain access into the system.

There are attendances software's that are device centric solutions such as RFID-based student attendance system and GSM-GPRS based student attendance system. The GSM-GPRS based systems works by using the position of classroom for marking attendance which is not dynamic. Wrong attendance might be marked if schedule or location of the class changes. One of the problems with RFID based systems is that students will be compelled to always carry RFID cards and also the RFID detectors are needed to be installed. Automated Teller Machine(ATM) system authentication using fingerprint Biometrics in the banking sector is a related study to this Personal Authentication System using fingerprint biometrics of students in institutions, where the students biometrics data are been collected in their various class, laboratory, examination halls and even tutorial by their lecturer, invigilators and even securities personnel in the institution to keep track of each student's attendance performance in various courses. This biometrics authentication can also be used in the banking sector to keeping track of all activities been carried out by each customer that performs transaction through the ATM. With an ATM, a customer or client is able to conduct many banking activities such as cash withdrawal, paying electricity & phone bills, money transfer, beyond official hours and physical interaction with bank staff (Mr. John Mashurano 2013). A newer high-tech method of operating sometimes called card cloning to entangle the installation of a magnetic card reader over the ATM's card slot & the use of a wireless surveillance camera to keep the user's Personal Identification Number. Real Card data are then cloned into a duplicate card & the criminal attempts to cash withdrawal. To overcome this piracy in money transactions, the idea using fingerprints of customers as password along with the traditional pin number (Mr. Wang liqiang 2013).

Another related study to this personal authentication system using fingerprint biometric is the Biometric Voting Machine where voters are been registered and vote using the fingerprint biometric. This machine makes the registration and voting efficient, fast and accurate in order to avoid cheating or imposter voting more than once. The objective of voting is to allow voters to exercise their right to express their choices regarding specific issues, pieces of legislation, citizen initiatives, constitutional amendments, recalls and to choose their government and political representatives. Technology is being used more and more as a tool to assist voters to cast their votes. To allow the exercise of this right, almost all voting systems around the world includes voter identification and authentication, voting and recording of votes cast, vote counting, publication of election results and these are achieved using the Biometric Authentication system using fingerprint. Voter identification is required during two phases of the electoral process: first for voter registration in order to establish the right to vote and afterwards, at voting time, to allow a citizen to exercise their right to vote by verifying if the person satisfies all the requirements needed to vote (authentication). Another important reason fingerprint scanners are used is, they provide a quick, easy, efficient, and secure measure through which, an individual with the proper access privileges can authenticate. The fingerprint of an employee for example, is stored in a database that the scanner queries every time it is used. There are two basic Boolean conditions the scanner then goes through when an individual's print is scanned. First, the print is usually searched for in a database of fingerprints, once it is found it then looks at the print to see what access privileges are associated with the print and compares them to the access they are trying to gain (Karthik, 2010).

2.6 Summary of Review

In summary Biometrics is a distinct step to identity management that offers user convenience, increased security, cost-effective provisioning and a non-repudiated, compliant audit trail for the system user and operator. The tokens an password cannot ascertain an individual using a system is the legitimate individual except if natural features such as fingerprints, facial recognition, irises, retinas, voice recognition and other characteristics possible. The method of validating users using biometrics can be so frustrating for users and expensive for system operators however the users just have to do it because it helps in personal authentication in order to reject imposters or frauds. Using biometrics for identifying human beings offers some distinct benefits because only biometrics can identify you as you, biometrics could make keys and combination locks obsolete and all data, including biometrics is vulnerable whether in storage or in processing state. Biometric have devices, such as fingerprint scanners, retina scanner, iris scanner, voice recognition that are been used in the authentication of a person's confidential or getting a person's real data. Also Biometric consist of a reader or scanning device, Software that converts the scanned information into digital form and compares match points and a database that stores the biometric data for comparison.

Biometrics are applicable in several areas or almost all areas now, areas like commercial as a whole that in terms of banking sectors, buying and selling, airport etc. the government areas as in law enforcement agencies, immigration agency, custom agency etc. and in forensic areas for criminal investigation, terrorist identification, parenthood determination and missing children.

CHAPTER THREE

SYSTEM ANALYSIS AND DESIGN

3.1 Analysis of the Existing System

Attendance is an important aspect in institutions, regular attendance will not only ensure full exposure to the scope of majors and opportunities available at institution, and it is also one of the criteria used in determining your final grade. Tracking and monitoring student time of attendance using the manual attendance in colleges and universities could be tedious, time consuming and more prone to errors. The manual attendance system that is use in classroom (signature system) is not too secure because some students can copy other student’s signature. For manual attendance signing process, the most common problem is the lecturer need to take student daily attendance and manually filled the record in attendance sheet or book for every lecture. If the attendance sheet is missing or misplace, it could lead to big problem because the lecturer need the attendance record to make analysis and generate an attendance report. Another problem is the lecturer will need more time to analyze and generate the attendance report because the lecturer needs to search and refer the old attendance record first. Besides that, an error could happen when the teacher make the calculations to generate the attendance report by themselves. Even though the attendance record is hassle to keep by the lecturer, management report is required in urgent basis. Analyzed attendance record is required by the school management for future actions is normally being delay because of the lack of precise. Moreover, delay analyzes would leads to prolong the time to inform the parents about the truancy students.

3.2 Justifications of the New System

The new system is going to deal with the limitations of the existing system by; keeping historical data that makes it easy for lecturers to access and grade students, providing high level of security whereby making it impossible for imposters and impersonators in making their ways to examination halls. The system will allow the lecturer to monitor each student attendance, track down truants and take the appropriate action and reduces the stress in queuing up which result in delay and often time in the damage of the attendance sheet. The new system will provide user friendly interface which will help to guide each user to use it correctly without any specialized training.

3.3 Methodology

Top-down model was adopted in designing the Class attendance management system using biometric technology. The result of the analysis was broken down into different components where the design is started from the main component down to the elementary components. The System was categorized into three (3) major subsystems which are; admin subsystem, and lecturer subsystem and student subsystem. Each of the listed subsystems above has a different user privileges to use the system.

Admin subsystem, here the user of this subsystem has the following privileges; add/delete/update records and information of the entire system. This subsystem is further broken down into; add Course, assign course, fingerprint enrollment, enroll student, enroll lecturer and report. In the listed subsystems the administrator can delete, add, and update the subsystem information.

Lecturer subsystem, unlike the admin subsystem here most privileges are taken away, the user can only activate attendance, view a student record or marked attendance or the courses he/she was assign to lecture on. The subsystem is further broken down into; (I) course (II) lecture taken (III) activation duration and (IV) profile.

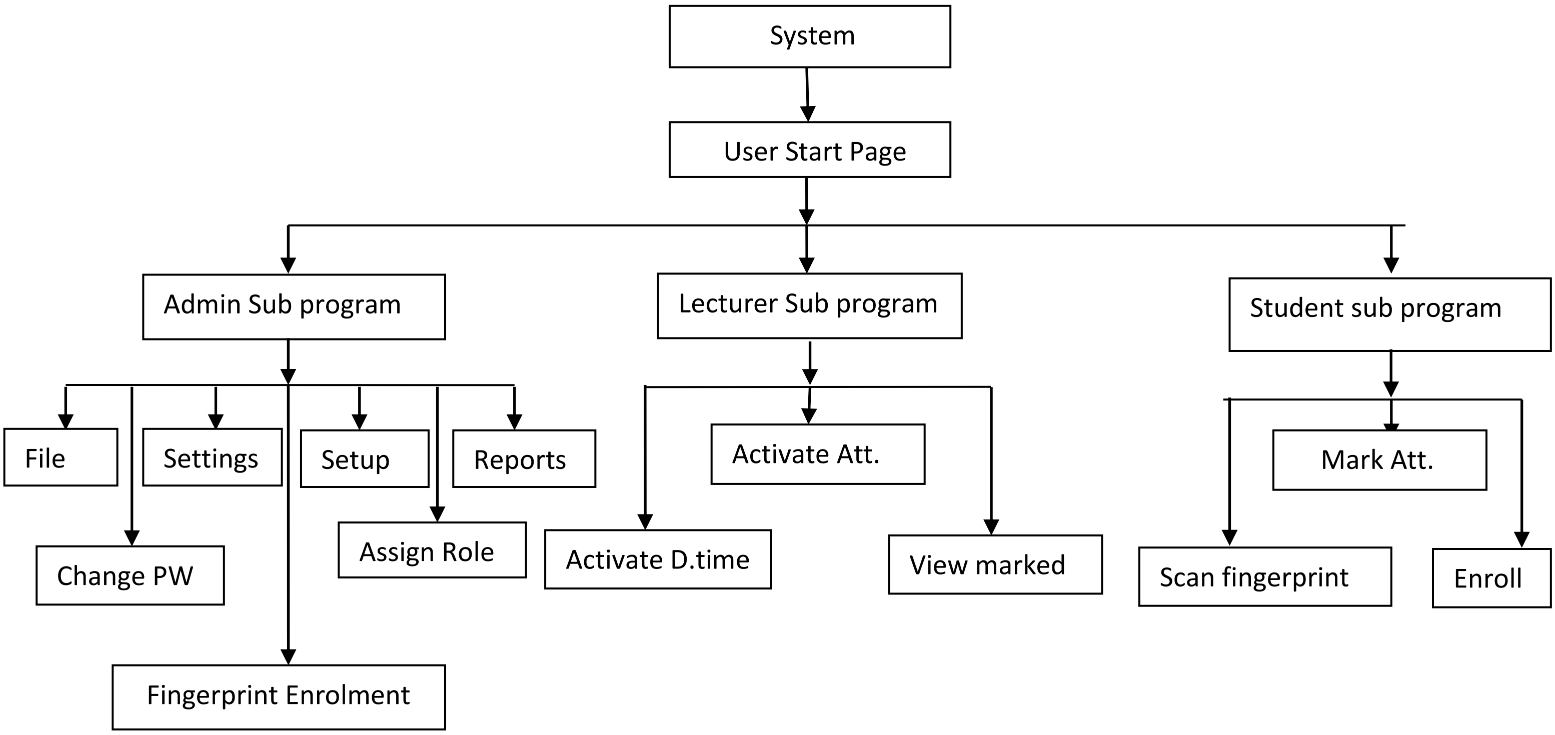
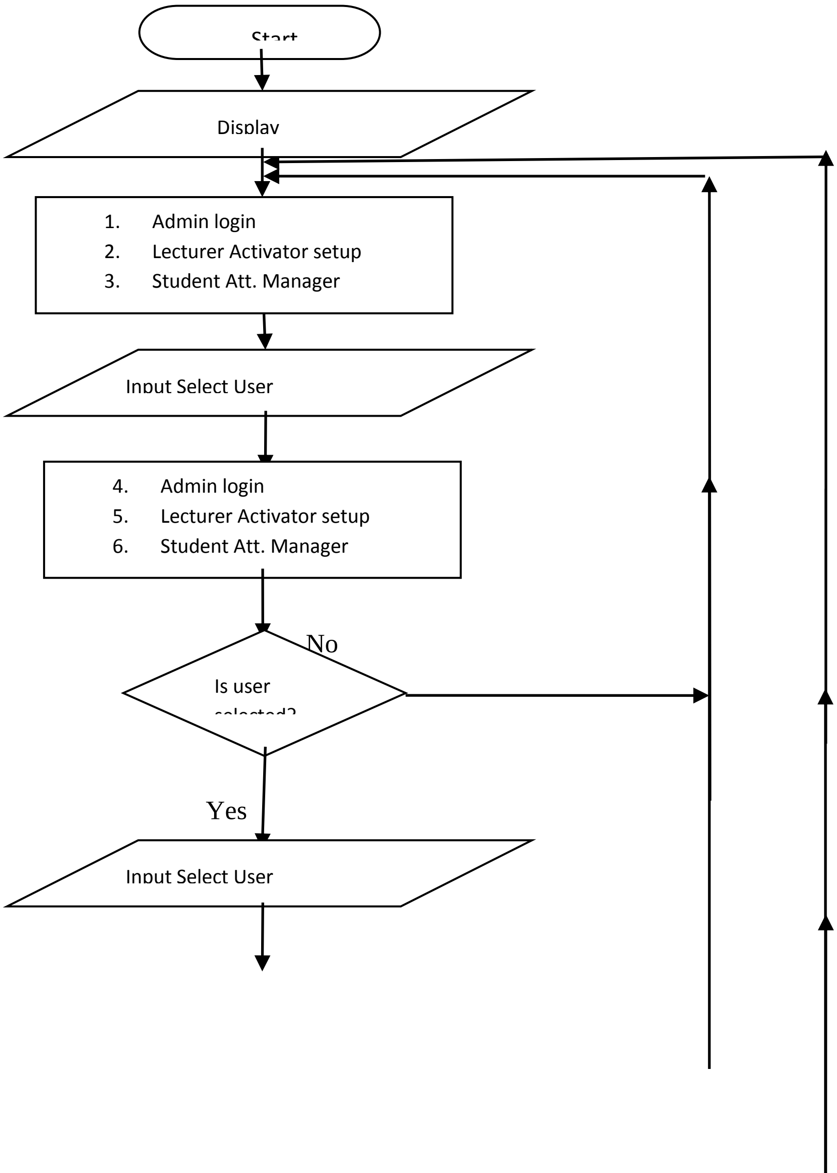


Figure 3.1: Top Down Design approach for the system

3.4 Data Collection

The major purpose of this work is to eliminate the use of paper in manual signing processes and all the risk associated with it and carry out the analysis of manual processes involved in class attendance and examination attendance of students with the aid of Class attendance management system using biometric technology. For these I met with lecturers and departments, and asked them to tell me the information that they need from students for the assessment of their class attendance in order to assign marks. Then they mentioned; student ID, matriculation number, student name, department, level, gender and fingerprint template. All the information listed will be the main information to be collected from each student. Then also ask departments to tell me the information they also need from the lecturers in order to assign courses to them. Then they mentioned; lecturer ID, courses taken for the semester/session, name, and fingerprint template etc. these information listed will be the primary information to be collected from each lecturer and so also the administrator.

3.5 The Proposed New System



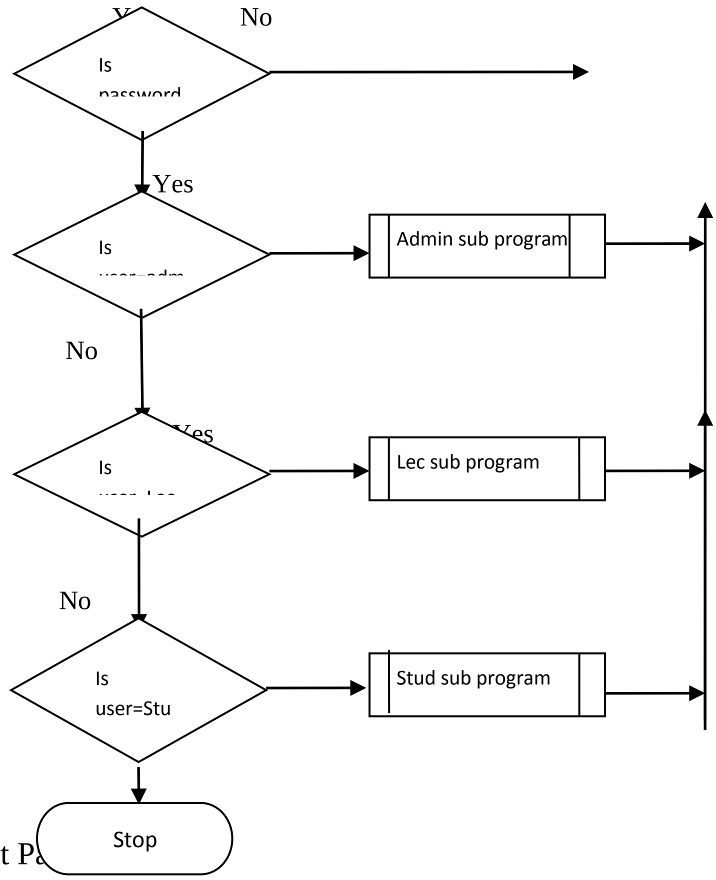
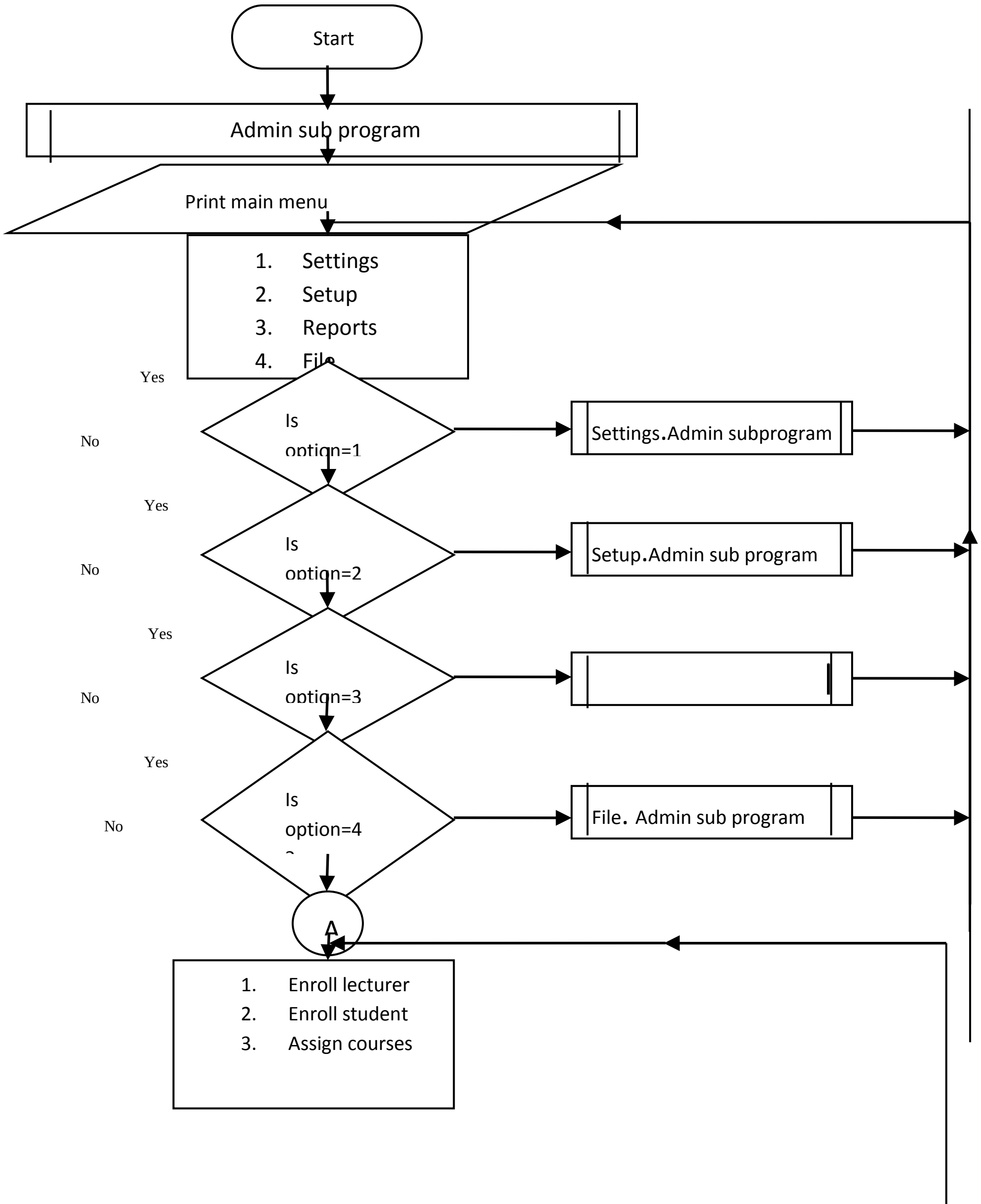


Fig3.2 Flow Chart for User Start Pa

Figure 3.2 showed the User Start page the new system in a flowchart format. The User Start page is used as the landing page of the system then and each user base on their role will select the module they have the privilege to access.


Start
Admin sub program
Print main menu
1. Settings
2. Setup
3. Reports
4. File
Yes
No
Is option=1
Settings.Admin subprogram
Yes
No
Is option=2
Setup.Admin sub program
Yes
No
Is option=3
Yes
No
Is option=4
File. Admin sub program
A
1. Enroll lecturer
2. Enroll student
3. Assign courses

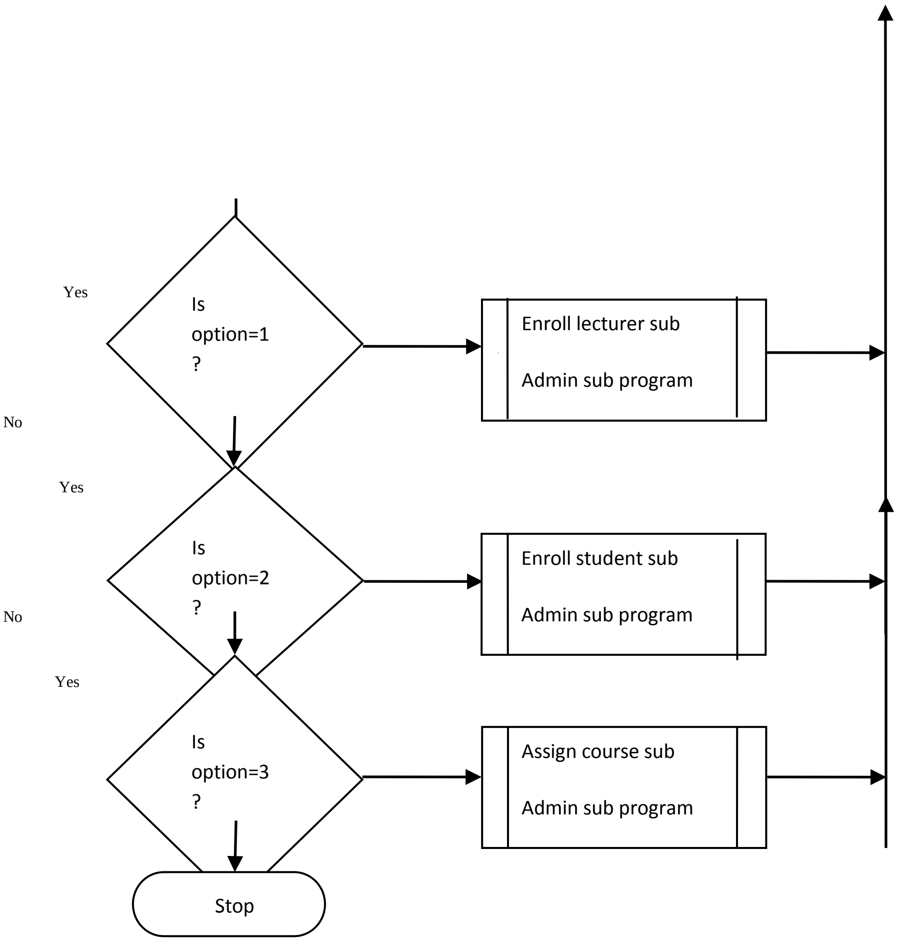
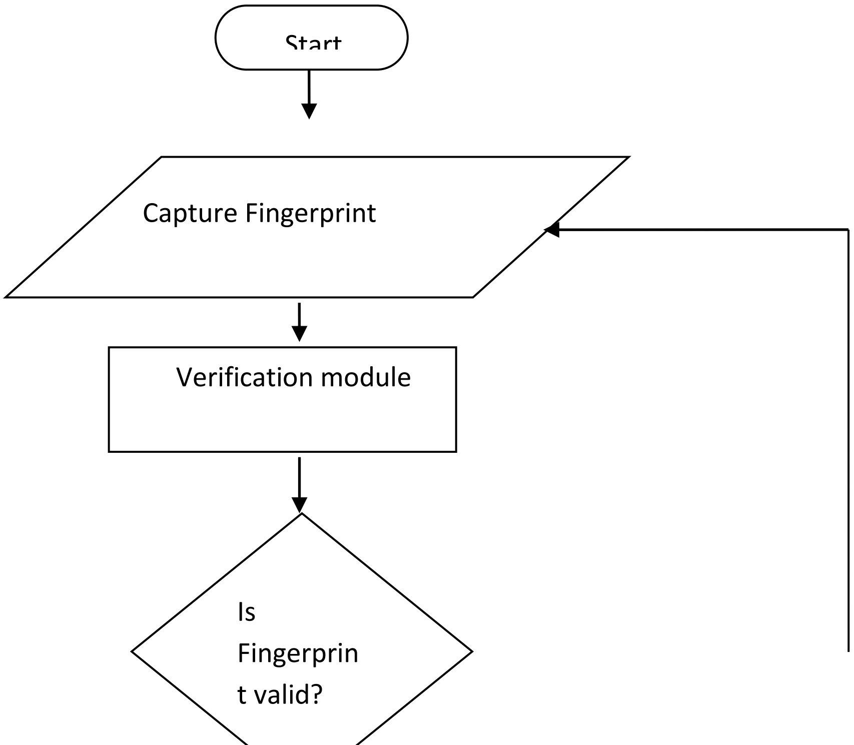


Fig3.3 Flow Chart for Admin Sub Program

Figure 3.3 represents the admin sub-system. Here is where users who logged in as admin are redirected to. The user of this sub-system maintains the entire system by performing actions such as; enrolling lecturers and students, assigning courses to lecturers and change password etc.



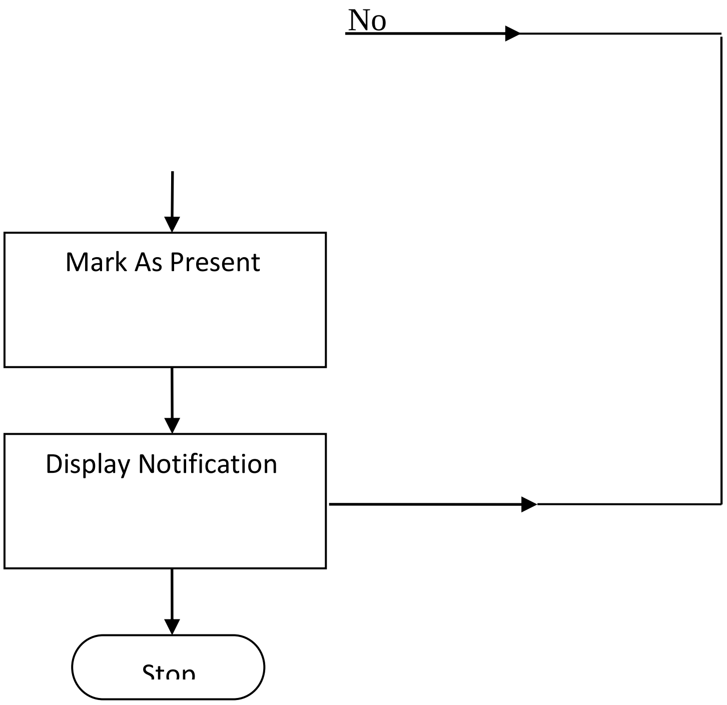
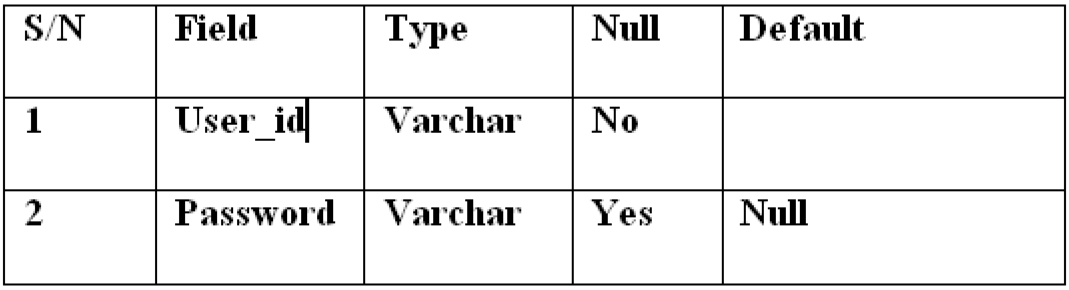


Fig3.4 Flow Chart for Student Sub Program

Figure 3.4 represents the student sub-system. Here is where users which are the student take their attendance for a particular class after the lecturer must have activated it with the duration of time the lecturer wants the attendance marking to last.

3.6 Database Structure

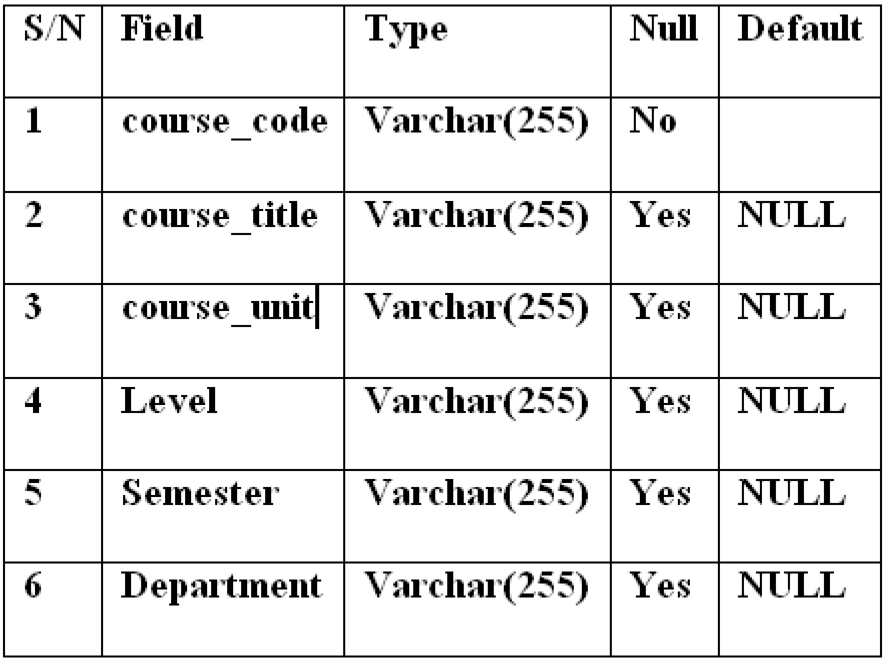
Table 3.1 Administrator database



S/N	Field	Type	Null	Default
1	User_id	Varchar	No	
2	Password	Varchar	Yes	Null

Table3.1 represents the table structure of admin database. Here all admin personal records are stored and access.

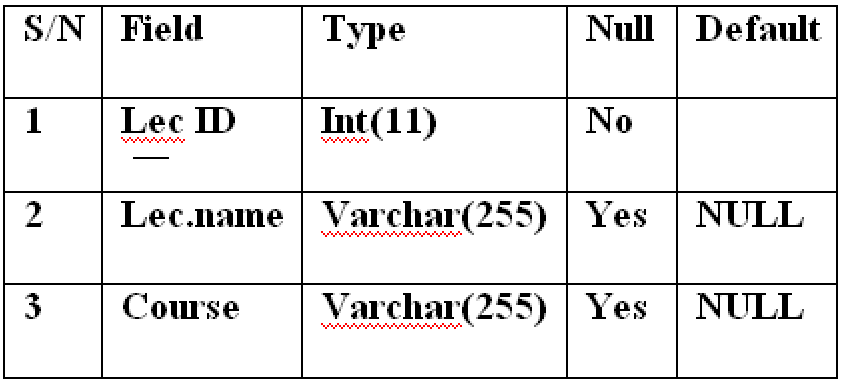
Table 3.2 Course database



S/N	Field	Type	Null	Default
1	course_code	Varchar(255)	No	
2	course_title	Varchar(255)	Yes	NULL
3	course_unit	Varchar(255)	Yes	NULL
4	Level	Varchar(255)	Yes	NULL
5	Semester	Varchar(255)	Yes	NULL
6	Department	Varchar(255)	Yes	NULL

Table 3.2 represents the table structure of course database. All courses that students are to offer and take attendance are stored and accessed here. The courses sub-system uses this database to manage courses.

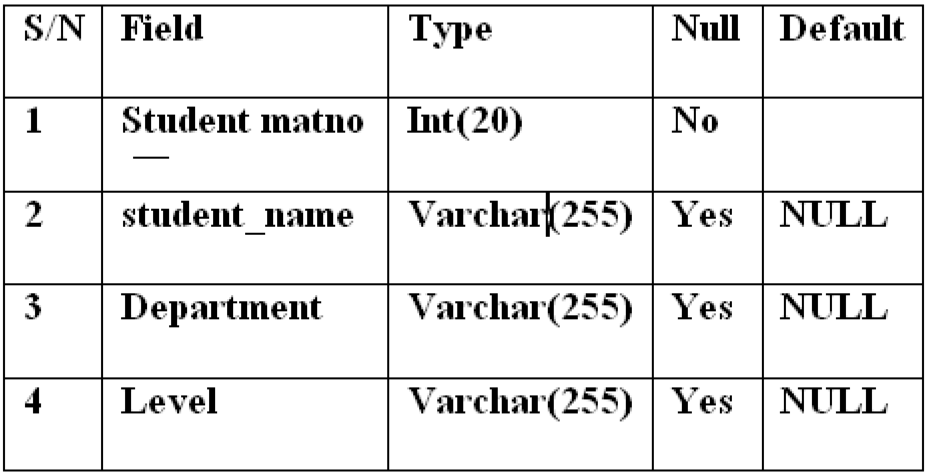
Table 3.3: Lecturer database



S/N	Field	Type	Null	Default
1	Lec ID	Int(11)	No	
2	Lec.name	Varchar(255)	Yes	NULL
3	Course	Varchar(255)	Yes	NULL

Table 3.3 represents the table structure of lecturer database. The lecturer database is where the information needed from a particular lec. This database is only accessed by view lecturer sub-system.

Table 3.4 Student database



S/N	Field	Type	Null	Default
1	Student matno —	Int(20)	No	
2	student_name	Varchar(255)	Yes	NULL
3	Department	Varchar(255)	Yes	NULL
4	Level	Varchar(255)	Yes	NULL

Table 3.4 represents the table structure of student database. The student database is where the information needed from all students is been stored and accessed by the administrator for updates.

CHAPTER FOUR

SYSTEM IMPLEMENTATION, TESTING AND INTEGRATION

4.1 Choice of Programming Language

The system was designed using common and popular window development technology which includes Microsoft Visual Basic.net 2010 and MSSQL Server 2008 R2.

- **VB.NET:** Vb.net is used to implement the server side logic of the design. The reason for using this language is because of its fastness and easy way in creating web applications. It is an object oriented programming language which allows objects to be manipulated easily and also an event driven programming language.
- **.NET Framework:** Visual basic programs run on the .Net Framework which is an integral component of Windows that includes a virtual execution system called the Common Language Runtime (CLR) and a unified set of class libraries. Source code written in VISUAL BASIC.NET is compiled into an Intermediate Language (IL) that conforms to the Common Language Infrastructure (CLI) specification.
- **Microsoft SQL Server:** MSSQL server is used to implement the back end of the new system. The server uses relational database management system that offers a variety of administrative tools to ease the burdens of database development, maintenance and

administrations. It also allows the use of stored procedure which is used to implement some of the business logic directly from the database.

- **T-SQL:** Transaction Structured Query Language is used to write stored procedures embedded in the Microsoft SQL server.

4.2 The System Main Menu Implementation

This refers to how the main menu in the system is being implemented. There are several interfaces that make up the entire system. They are described below:

4.2.1 Main Menu

Figure 4.1 shows the administrator login, lecturer activator setup and student attendant manager. Here the administrator can login by clicking on the Admin login and then proceeds to other settings or updates, settings in terms of inputing of administrator username and password. The lecturer and students so also can proceed to other action by clicking on their various options on the main menu.

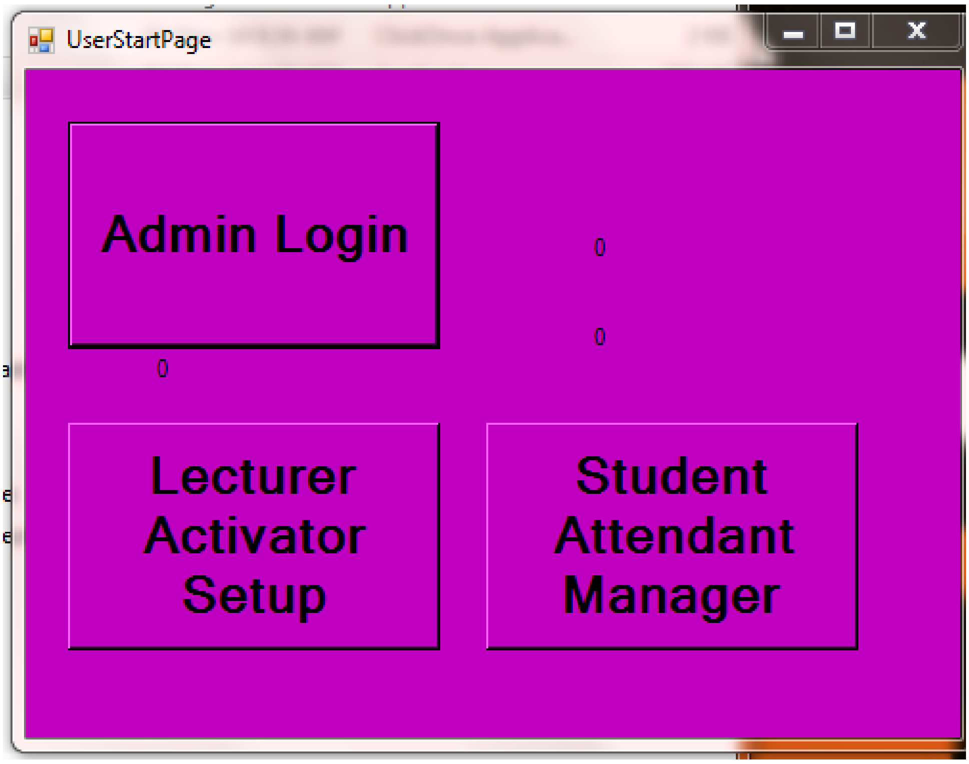


Figure 4.1: User Start Page

4.2.2 Admin Login Page

Figure 4.2 shows the login page of administrator. The administrator types in his/her user name and password in order for them to navigate to the main page where he/she to perform enrollment, updates and settings.

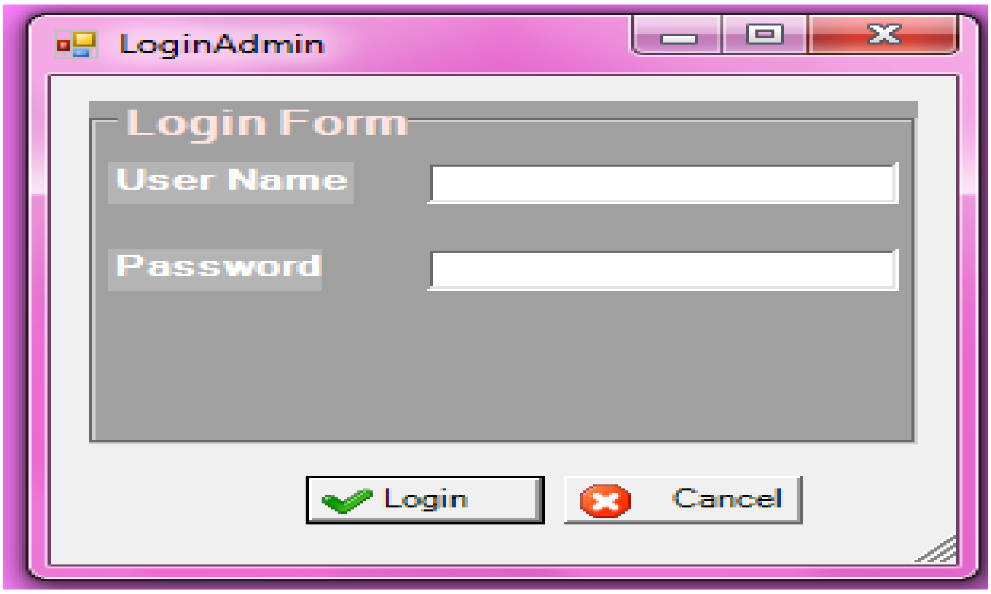


Figure 4.2: Admin Login Implementation

4.2.3 Lecturer Activator Setup Page

Figure4.3 shows the attendance activator for the lecturer in any particular class. The lecturer will have to login, input fingerprint for verification and activate a particular session of class and the duration of time it will take for the attendance marking session of the student. Students cannot take attendance without the lecturer activating.

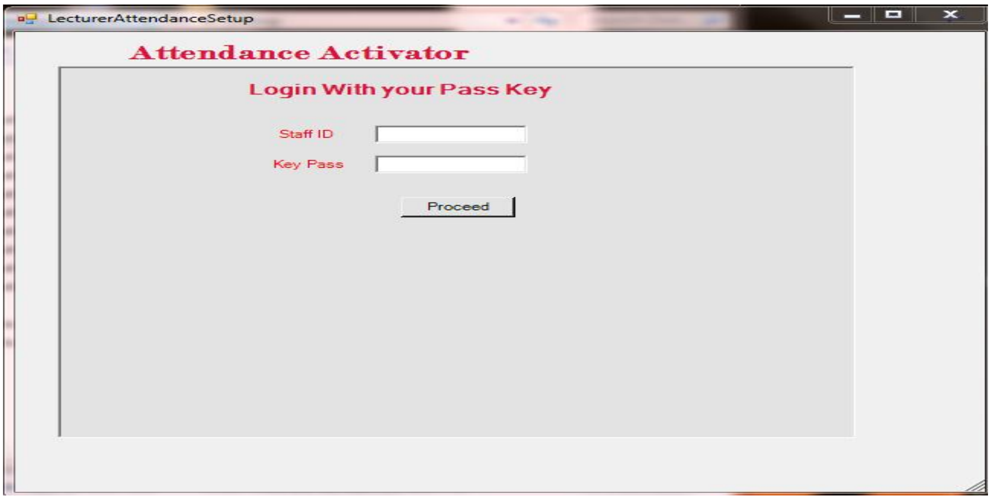


Figure 4.3: Lecturer Attendance Setup

4.3 Implementation of the Sub-system

Selecting the administrator (Admin) login option from the main menu results in a display of Login form, after providing a valid username and password, access is then granted to the administrator who can also be the lecturer, which then leads to the administrator sub-menu, which have the file menu, settings menu, setup menu and report menu. The administrator can enroll fingerprint of the lecturers and students, change password etc from the settings menu in the administrator's sub-menu.

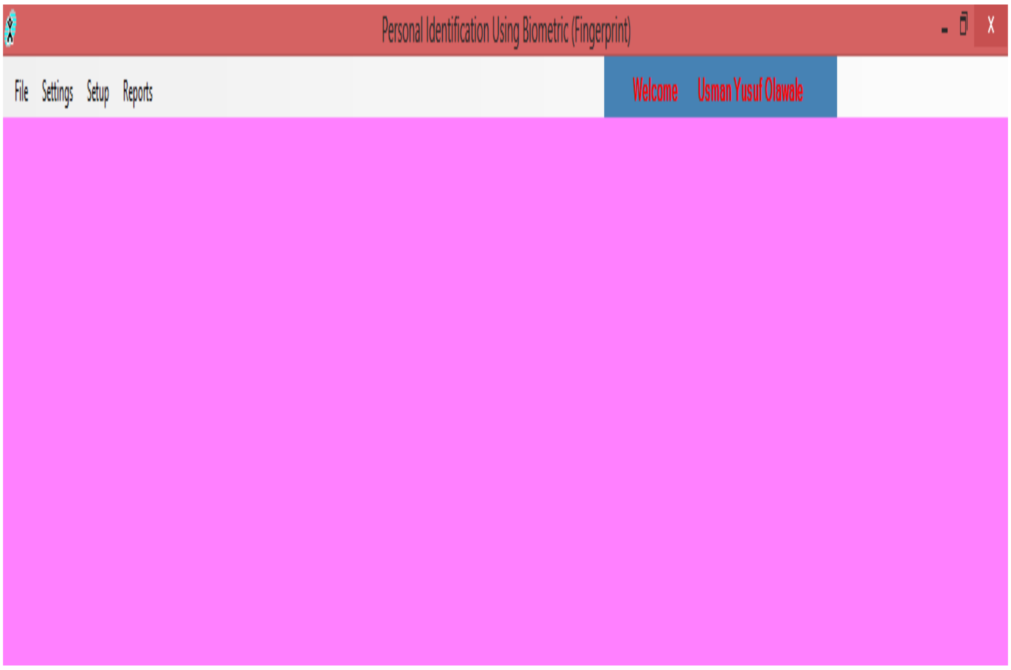
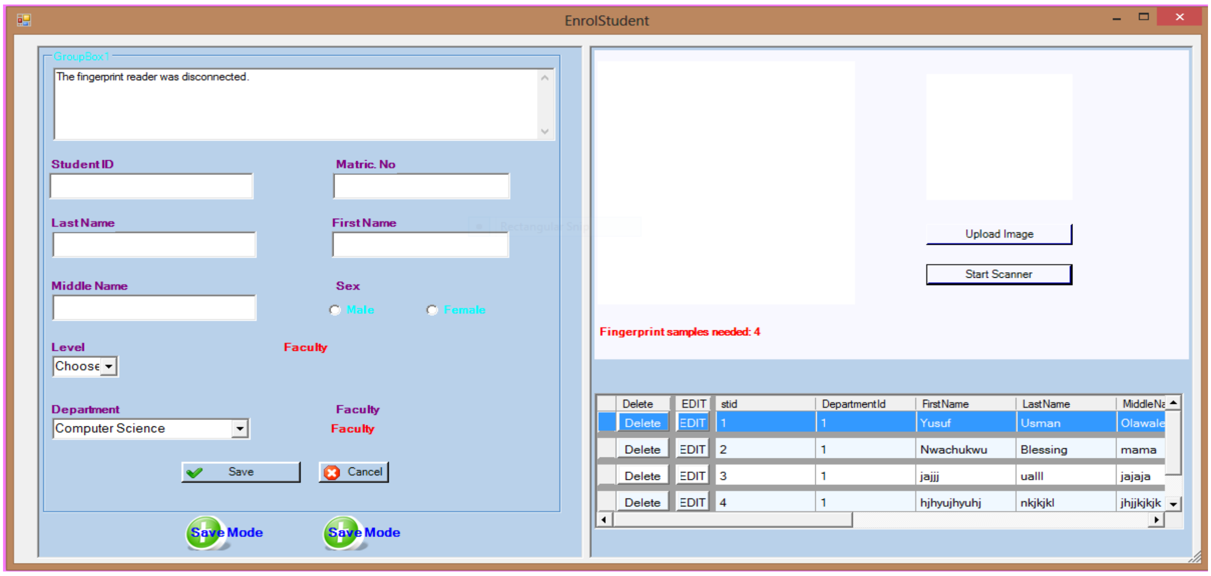


Figure 4.4: Administrator Sub-menu

In figure4.5, the students are been enrolled by the administrator or lecturer. The students bio data is been registered and the fingerprint of each student is been captured for authentication of the attendance.



The fingerprint reader was disconnected.

Level: Choose

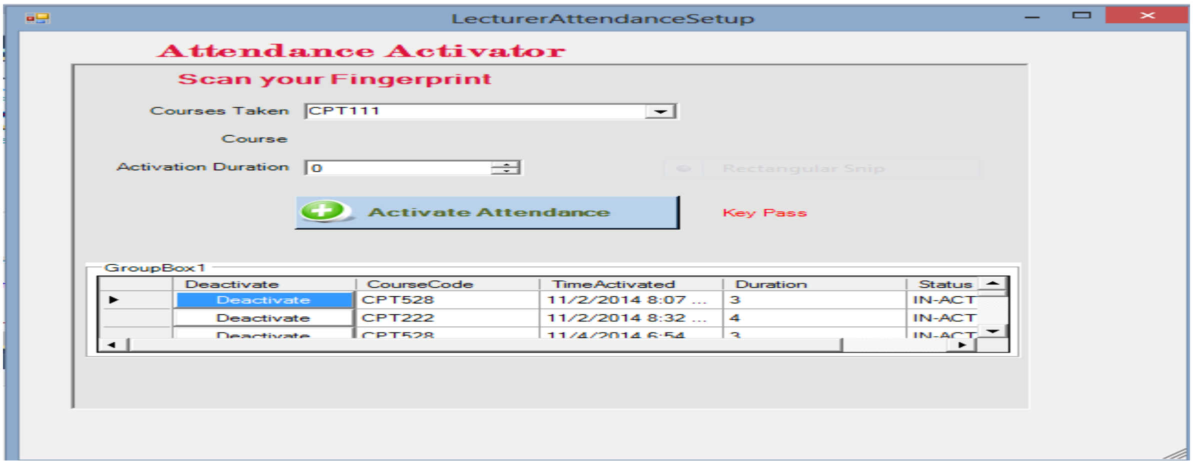
Department: Computer Science

Fingerprint samples needed: 4

	Delete	EDIT	stid	DepartmentId	FirstName	LastName	MiddleNa
	Delete	EDIT	1	1	Yusuf	Usman	Olawale
	Delete	EDIT	2	1	Nwachukwu	Blessing	mama
	Delete	EDIT	3	1	jajjj	ualll	jajaja
	Delete	EDIT	4	1	hjhyujhyuhj	nkjkjkl	jhjjkjkjk

Figure4.5: Student Enrollment submenu

Figure4.6, the lecturer activates the system for each session before student marks attendance. The lecturer inputs his/her course for the session and the duration for the attendance marking.



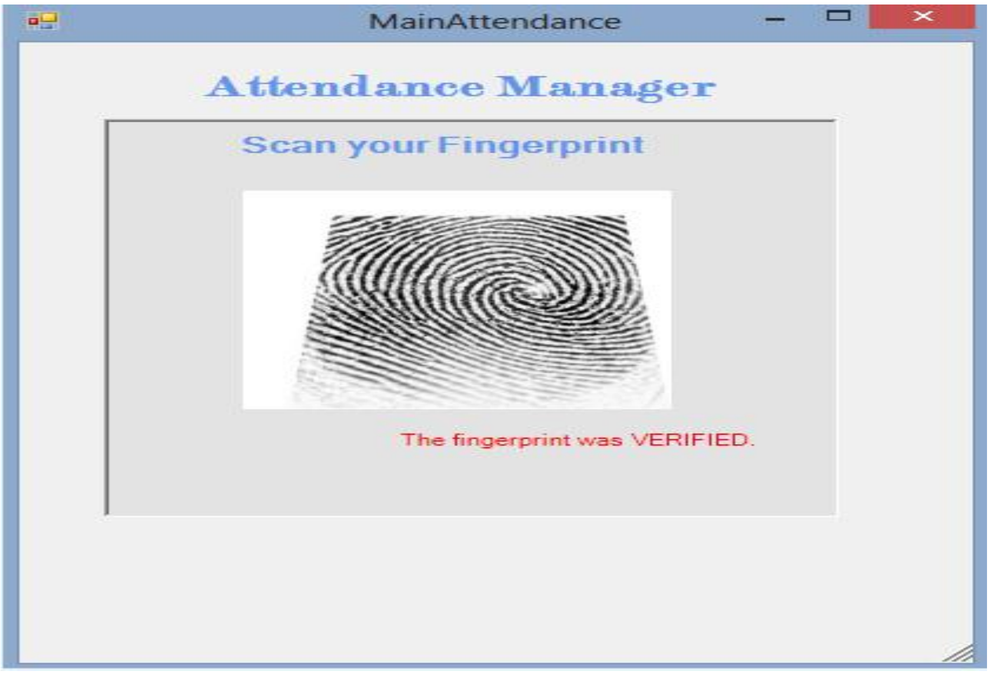
Courses Taken: CPT111

Activation Duration: 0

	Deactivate	CourseCode	TimeActivated	Duration	Status
▶	Deactivate	CPT528	11/2/2014 8:07 ...	3	IN-ACT
	Deactivate	CPT222	11/2/2014 8:32 ...	4	IN-ACT
	Deactivate	CPT528	11/4/2014 6:54	3	IN-ACT

Figure4.6: lecturer attendance activator

The figure4.7 shows the fingerprint verified of the student for a particular session of class. At this time the duration time that the lecturer set is still on, if any student comes after the duration time the attendance manager shows session not activated.



The fingerprint was VERIFIED.

Figure4.7: Student fingerprint verified

4.4 Query Sub-system Implementation.

The MSSQL Server 2008 R2 which setup the relational database of is very important because it provides the authentication system with efficiency, consistency and reliability. However, after the administrator must have input the information's of all the students for a particular session, the administrator can therefore query a particular department to know how many student is in that particular department from the database and also how many student had being enrolled and authenticated for a particular course. The lecturer can also query the attendance update from the database to know how many students were present in class for a particular lecturer in order to assign marks for attendance to the present students.

4.5 System Testing and Integration

This is a formal process of soliciting feedback on or from a system that is being developed. It is used to determine the effectiveness, the correctness, efficiency, reliability and robustness of the proposed system. Unit testing was carried out on individual components of different layers in the application to verify and ensure all different components such as classes are at the required minimal functional level. Also, integration test was carried out, where all the independent components or modules are then integrated together to further verify the functionality of the interfaces of each components so as to spot defects in various interfaces and the behavior or responsiveness of each components when interacting together.

4.6 Test Plan

It involves a stage-by-stage assessment of all the subsystems which are carried out to determine the performance and efficiency on the authentication system and comparing the result to the over-all desired result. This verifies that the system elements have been properly integrated.

4.7 Test Data

The data needed for the testing comprises of all student information such as student ID, mat no, name, level, department and sex and the lecturer personal information such as staff ID, name and department which is to be filled when administrator is enrolling students or lecturers. The course details so also such as course code, course title, course description, add course and course unit which is to be filled by administrator after the students and the lecturers have been rolled and authenticated.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

This project is focused on the protection of student manual attendance system using fingerprint biometric. The fingerprint Biometrics is one of the most successful applications of biometric technology was used in this Class attendance management system using biometric technology which serves as an alternate for traditional manual signing processes involved in class attendance and examination attendance. Reviewing and assessing the authentication system for student class attendance follows a hierarchical flow from policies down through the specific actions taken to enforce them.

Attendance is usually noted using paper sheets and the old file system, this approach has been in use for a long time. It becomes difficult for the management to regularly update the record and manually calculate the percentage of classes attended. For any growing institution, tracking and monitoring student time of attendance could be tedious, time consuming and more prone to errors. There are many concepts to understand and the technological solutions can be complex. Dynamic institution driven solutions continue to tout a silver bullet but none ever really exists. Keeping up with security threats and countermeasures requires a continuous education and understanding.

This project covers the basic concepts so one's knowledge can be outfitted and applied to the situations that you will face as a certified IS auditor, however diverse they may be. Again for this project, the focus is not only on the technical details of how this fingerprint biometric works under the hood. Rather, it assumes that you have some base knowledge of these issues and is geared more towards identifying the risk and control points of the authentication system. The system's inner workings and the exact technology used to secure them will change over time, probably in the time it takes you another researcher to work on it.

In chapter four, the programming languages that was chosen were Microsoft Visual Basic.net 2010 and MSSQL Server 2008 R2 those languages was discussed briefly. The implementation of all the components were tested and integrated for proper performance and evaluation of the system. This verifies that the system elements have been properly integrated.

5.2 Recommendations

Through analysis of the data and research conducted for this study, the school district maintain or develop strict guidelines for student attendance and monitor factors that could hinder a student from attending school on a regular basis. The use of encryption for files in the database transit is an area of protection that should be visited. I strongly believe in protection. Window based authentication system is an important management tool which reduces the lecturers/teachers work load of colleges and university. Therefore, is highly recommended that all schools should adopt it.

The system was designed to ease the lecturer work and also allow lecturer and students to use the system without taking special training for it. Should any modification or upgrading arises it should be done with the idea of making it a user friendly so as to make it easily accessible to users, efficient and readily available to specified user.

5.3 Conclusion

It can be concluded from the above discussion that a reliable, secure, fast and an efficient system has been developed replacing a manual and unreliable system. Results have shown that this system can be implemented in academic institutes for better results regarding the management of attendance. This system will save time, reduce the amount of work the administration has to do and will replace the stationery material with electronic apparatus. Hence a system with expected results has been developed but there is still some room for improvement. Having presented a biometric identity based fingerprint scheme. I have utilized, extended and implemented ideas in the areas of error corrected string construction from biometric data, key generation, and pairing based fingerprint schemes to form the components of the system. The research presented the application of such a scheme to repudiation situations. Discussion on advantage of using the biometric data in the public key and described the utility of using biometric evidence in disputes that may arise. This work has been an insight into the hidden problems; the manual attendance system tends within daily activities. The problems are fair and need computerized authentication system to replace the manual student attendance system.

REFERENCES

Books

1. Introducing Microsoft .NET, Second Edition author David S. Platt.

2. Joe Mayo, “Microsoft Visual Studio 2010: A Beginner's Guide”, Tata McGraw Hill, 2010.

3. Alex Mackey, “Introducing .NET 4.0: With Visual Studio 2010”, Press, USA, 2010.

WEBSITES

1. http://www.msdn.net/
2. http://msdn.microsoft.com/en-us/library/orm-9780596518455-02.aspx
3. http://www.w3schools.com/asp.net/
4. http://www.cramerz.com/aspdotnet
5. http://www.dotnetspider.net/
6. http://www.stackoverflow.com
7. http://www.codeproject.com

APPENDIX I (SOURCE CODE

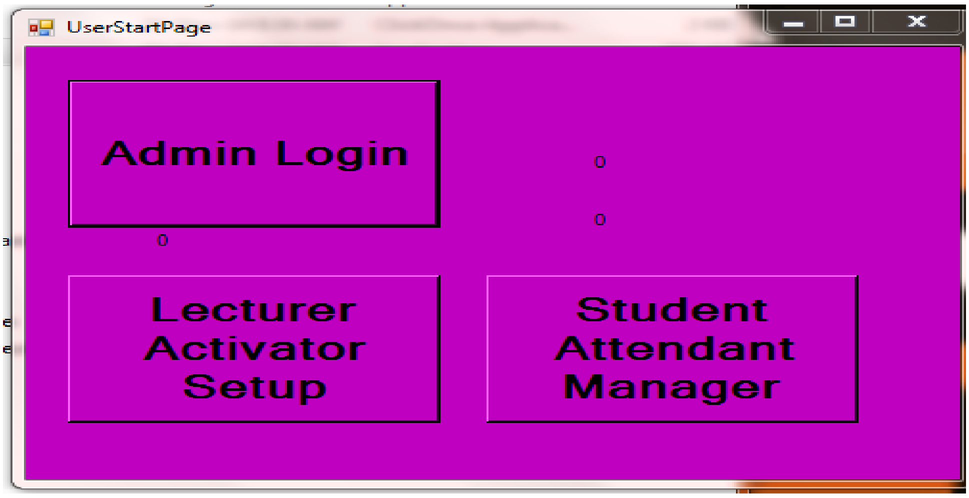
```
sconn = "DRIVER=Microsoft Excel Driver (*.xls);" & "DBQ=" & sFile
Set CnXls = New ADODB.Connection
CnXls.ConnectionString = sconn
CnXls.Open
OpenXLS = 0
```

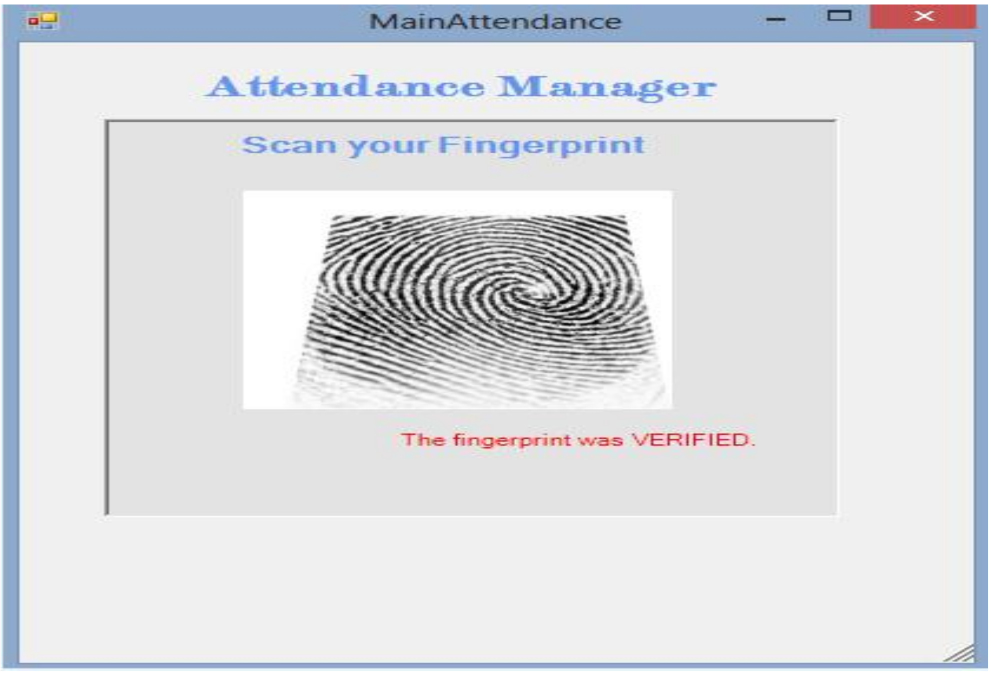
```
      Exit Function
fix_err:
      OpenXLS = Err.Number
End Function
Public Sub ExecuteQuery(qstring As String)
    Cn.Execute qstring
End Sub
Public Function OpenRS(strSql As String) As ADODB.Recordset
Dim rs As ADODB.Recordset
        Set rs = New ADODB.Recordset
        rs.CursorLocation = adUseClient
        rs.CursorType = adOpenDynamic
        If IsNull(Cn) = False Then
            rs.Open strSql, Cn, adOpenKeyset, adLockPessimistic
        End If
        Set OpenRS = rs
End Function
Public Function OpenRSXLS(strSql As String) As ADODB.Recordset
Dim rs As ADODB.Recordset
        Set rs = New ADODB.Recordset
        rs.CursorLocation = adUseClient
        rs.CursorType = adOpenDynamic
        If IsNull(CnXls) = False Then
            rs.Open strSql, CnXls, adOpenKeyset, adLockPessimistic
        End If
        Set OpenRSXLS = rs
End Function

Public Function QuoteReplace(s As String) As String
Dim tmpstr As String
    'find if the string contains qoutes
    If InStr(s, "'") Then
        tmpstr = Replace(s, "'", "\'")
        QuoteReplace = tmpstr
    ElseIf InStr(s, "\") Then
        tmpstr = Replace(s, "\", "\\")
        QuoteReplace = tmpstr
    Else
        QuoteReplace = s
    End If
End Function
Public Function ClsSql(str As String) As String
    Dim tmpstr As String
    Dim s As String
    s = str
    tmpstr = Replace(s, "'", "''")
    'tmpstr = Replace(s, "\", "\\")
    ClsSql = tmpstr
End Function
Private Sub cmdCancel_Click()
    IMPORTINFO.accesspassword = ""
    Unload Me
End Sub

Private Sub cmdDone_Click()
    IMPORTINFO.accesspassword = txtPassword.Text
    Unload Me
End Sub
Private Sub Form_Load()

End Sub

Private Sub txtPassword_KeyPress(KeyAscii As Integer)
    If KeyAscii = 13 Then cmdDone_Click
End Sub Dim tblList As ADODB.Recordset
Dim tblListxls As ADODB.Recordset
Dim fldlst As ADODB.Recordset
Dim fldlstxls As ADODB.Recordset
Dim rs_source As ADODB.Recordset

Private Sub cmbSheets_Click()
    ShowExcelFields
End Sub

Private Sub cmbTables_Click()
    ShowFields
End Sub

Private Sub cmdBack_Click()
    Form1.Show
    Unload Me
End Sub

Private Sub cmdBackup_Click()
    Dim bakcnt As Integer
    Dim bakfilename As String
```

```
AGAIN1:
   bakcnt = bakcnt + 1
   bakfilename = Left$(IMPORTINFO.accessfile,
Len(IMPORTINFO.accessfile) - 4)
   bakfilename = bakfilename & "_BAK" & bakcnt & ".mdb"

   'ops file already exist increment back count again
   If FileExists(bakfilename) = True Then GoTo AGAIN1

   'now copy anyway
   CopyFileWindowsWay IMPORTINFO.accessfile, bakfilename

   MsgBox "Backing up succeded!", vbOKOnly, "Backup"
End Sub

Private Sub cmdclose_Click()
Unload Me
End Sub

Private Sub ShowTables()
   Set tblList = New ADODB.Recordset
   Set tblList = Cn.OpenSchema(adSchemaTables)

   Me.MousePointer = vbHourglass
   'list all the table from the database
   Do While Not tblList.EOF
      If tblList.Fields(3) = "TABLE" Then
      cmbTables.AddItem tblList.Fields(2)
      End If
      tblList.MoveNext
   Loop
   Me.MousePointer = vbNormal
End Sub

Private Sub ShowExcelSheets()
   Set tblListxls = New ADODB.Recordset
   Set tblListxls = CnXls.OpenSchema(adSchemaTables)

   Me.MousePointer = vbHourglass
   'list all the table from the database
   Do While Not tblListxls.EOF
      'If tblListxls.Fields(3) = "TABLE" Then
```

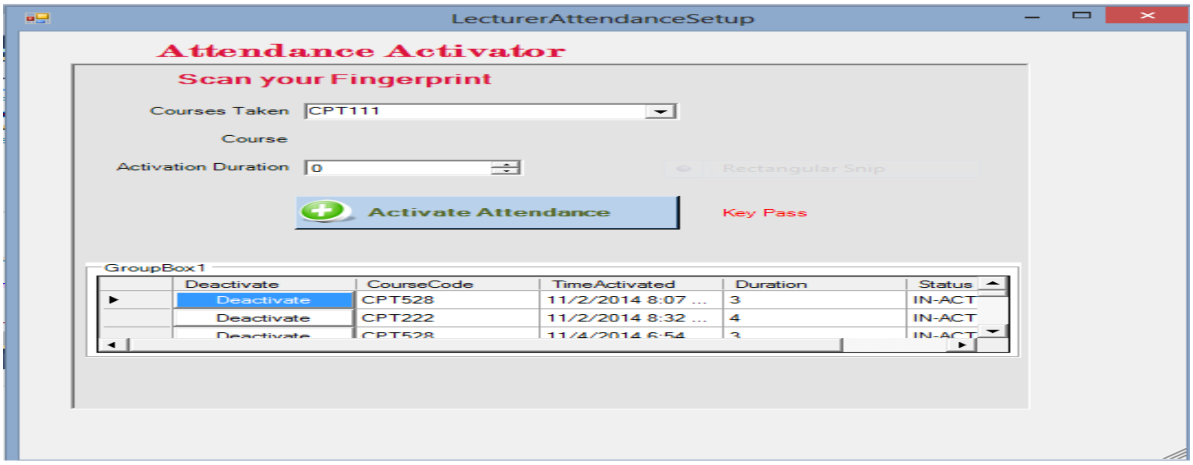
```
        cmbSheets.AddItem tblListxls.Fields(2)
        'End If
        tblListxls.MoveNext
    Loop
    Me.MousePointer = vbNormal
End Sub

Private Sub cmdImport_Click()
    Dim destinationtble As String
    Dim sourcetble As String
    Dim selflds As String
    Dim i As Integer
    Dim defval As String
    Dim qSTRUCT() As QUERYSTRUCT
    Dim fldCount As Integer
    Dim sqltxt1 As String
    Dim sqltxt2 As String
    Dim retval As String
    Dim notnull As Boolean
    Dim cnt As Integer


    If MsgBox(" W   A   R   N   I   N   G  !" & vbCrLf & "You are about to
make changes to Access Database file, be sure to BACKUP first the
database before doing this!. Continue anyway?", vbYesNo, "Import Data
Warning!") = vbNo Then Exit Sub

    If ListView1.ListItems.Count = 0 Then
        MsgBox "There are no table selected from Access Database",
vbOKOnly, "Import Error!"
        Exit Sub
    End If
```

APPENDIX II (INTERFACE SCREENSHOT)





The fingerprint was VERIFIED.

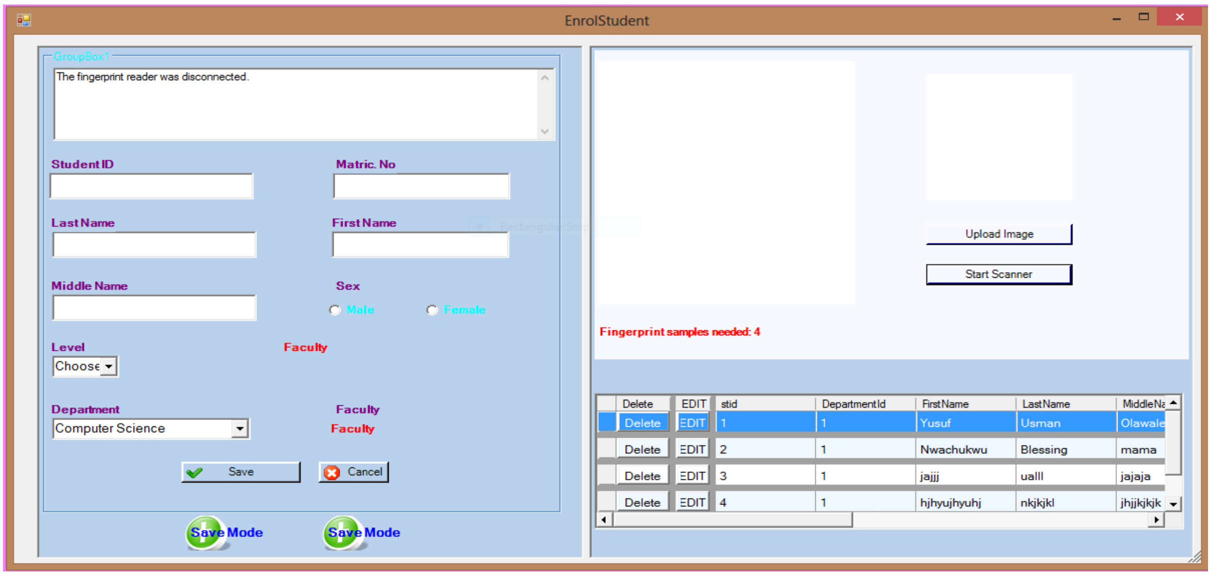


Courses Taken CPT111

Course

Activation Duration 0

	Deactivate	CourseCode	TimeActivated	Duration	Status
▶	Deactivate	CPT528	11/2/2014 8:07 ...	3	IN-ACT
	Deactivate	CPT222	11/2/2014 8:32 ...	4	IN-ACT
	Deactivate	CPT528	11/4/2014 6:54	3	IN-ACT



The fingerprint reader was disconnected.

Student ID

Matric. No

Last Name

First Name

Middle Name

Sex ○ Male ○ Female

Level Choose

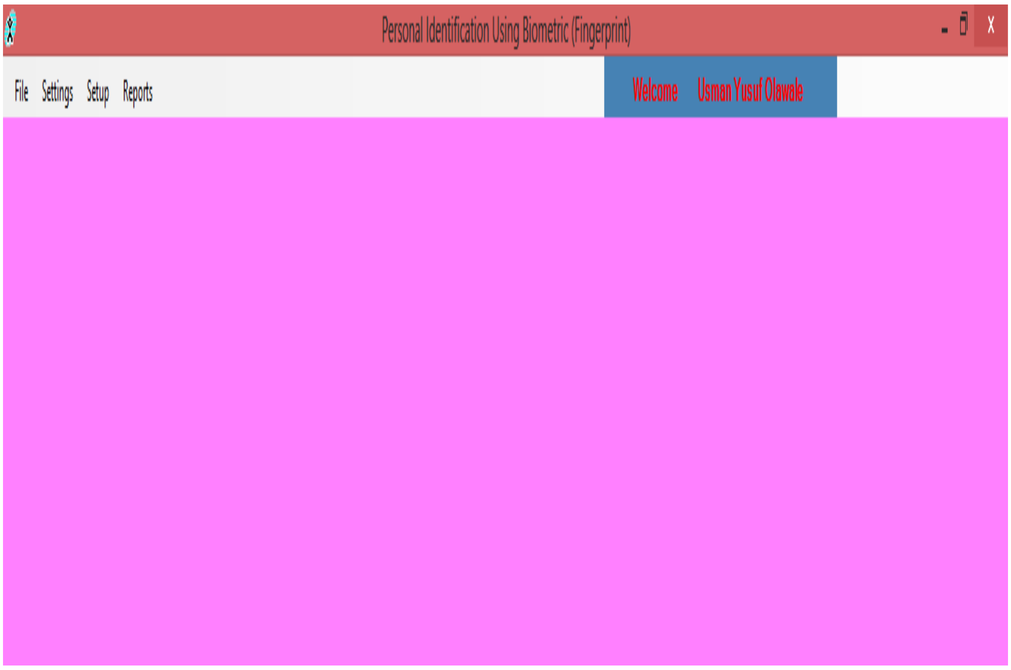
Faculty

Department Computer Science

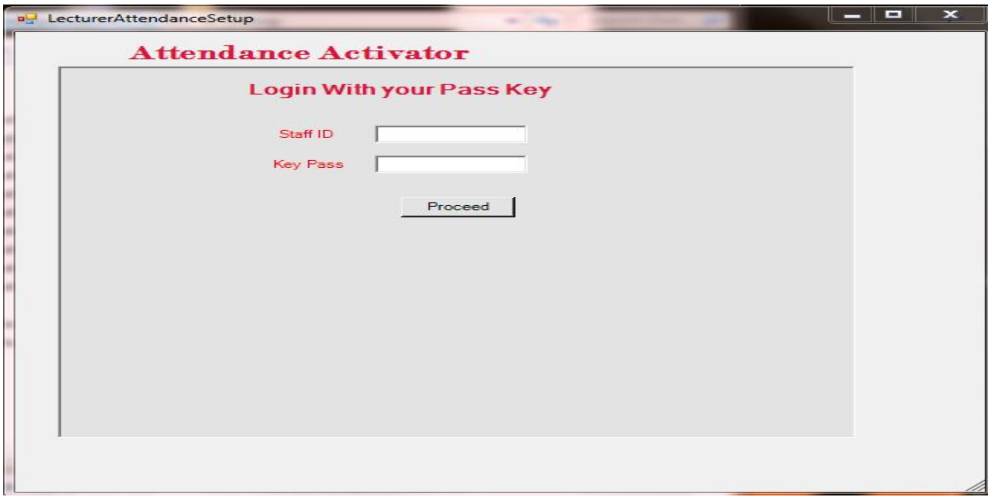
Faculty Faculty

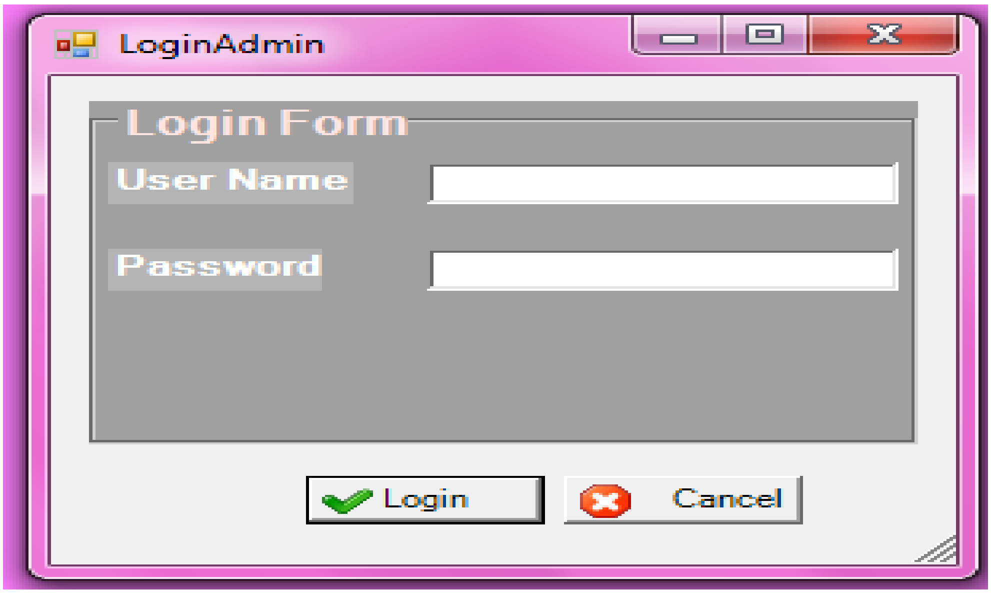
Fingerprint samples needed: 4

	Delete	EDIT	stid	DepartmentId	FirstName	LastName	MiddleNa
	Delete	EDIT	1	1	Yusuf	Usman	Olawale
	Delete	EDIT	2	1	Nwachukwu	Blessing	mama
	Delete	EDIT	3	1	jajjj	ualll	jajaja
	Delete	EDIT	4	1	hjhyujhyuhj	nkjkjkl	jhjjkjkjk



Welcome Usman Yusuf Olawale


LecturerAttendanceSetup
Attendance Activator
Login With your Pass Key
Staff ID
Key Pass
Proceed


LoginAdmin
Login Form
User Name
Password
Login
Cancel