DESIGN AND IMPLEMENTATION OF STUDENTS ATTENDANCE MANAGEMENT SYSTEM USING FINGERPRINT BIOMETRIC CAPTURING

BY

ENOLULUMONLEN HOPE JEROME	**ICT/2252070058**
EKHORUTOMWEN OSARUGUE GLORY	**ICT/225200355**

BEING A PROJECT WORK SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY, AUCHI POLYTECHNIC, AUCHI, EDO STATE

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF HIGHER NATIONAL DIPLOMA (HND) IN COMPUTER SCIENCE, AUCHI POLYTECHNIC, AUCHI, EDO STATE.

SUPERVISED BY:

DR. (MRS.) E. B. ODUNTAN

NOVEMBER, 2022

CERTIFICATION

We, the undersigned hereby certify that this project was carried out by;

ENOLULUMONLEN HOPE JEROME	**ICT/2252070058**
EKHORUTOMWEN OSARUGUE GLORY	**ICT/225200355**

in the department of Computer Science, School of Information and Communication Technology.

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

______________________________ ______________________

DR. (MRS.) E. B. ODUNTAN **DATE**

(Project Supervisor)

______________________________ ______________________

MR. SYLVESTER O. AKHETUAMEN **DATE**

(Head, Department of Computer Science)

DEDICATION

This project work is dedicated to God almighty for his mercies and strength throughout our educational pursuit.

ACKNOWLEDGEMENT

Firstly, our profound gratitude goes to the Almighty God, the Father of wisdom whose wisdom has been our guide. This project would not have been completed without the valuable contribution of our supervisor, colleagues, friends and family.

We owe our deep appreciation to our supervisor; **DR. (MRS.) E. B. ODUNTAN** for her encouragement, assistance and thorough supervision during the course of our research. We appreciate her devotion for helping us achieved our goal. Thank you for the attention you gave to us even with your busy schedule.

We would like to also express our sincere gratitude to the Head of department of computer science, **MR. SYLVESTER O. AKHETUAMEN** for his support and invaluable advice.

We would like to express our deepest gratitude and respect to our parents and siblings for their financial support, moral teaching, love, care and motivation.

Others in the trend are the departmental lecturers and a lot of friends in the computer science field; we say a very big thank you for all your support.

God bless you all.

TABLE OF CONTENTS

CHAPTER FOUR: PROGRAM IMPLEMENTATION AND TESTING

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

ABSTRACT

This project focuses on the design and implementation Automated Examination Attendance System Based on Fingerprint Recognition that can be used to monitor attendance of the student and can assist in curtailing examination impersonation. The research methodology adopted in this work is design science approach. Initial investigation was carried out through interaction and enquiries with technology users and domain experts to establish the existence of real problems that require technical solutions by way of deploying available I.T appliances. It will eliminate the problems of manual method. Up till now, the Federal Polytechnic, Auchi is not using fingerprint as mode of identification during examination, this has resulted in people sitting for examinations for others. With the adoption of the new system, the problem of examination impersonation will be eliminated. 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 includes database to store student's information and attendance records. To achieve more reliable verification or identification we should use something that really characterizes the given person. Main objective is to eliminate any form impersonation during exam by employing a more secured means of fingerprint biometrics. Automated biometrics in general, and fingerprint technology in particular, can provide a much more accurate and reliable user authentication method. More importantly, this system should be used in various tertiary institutions to curb examination impersonation.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Attendance management of students in institutions 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.

In era of Information technology (IT), biometrics refers to technology for measuring and analyzing human physiological traits along with fingerprints, eye retinas and irises, voice patterns, facial styles, and hand measurements, specially for authentication functions (Olaniyi, Omotosho, Oluwatosin, Adegoke, and Akinmukomi, 2012).

Biometrics is the science of measuring physical and/or behavioural characteristics that are specific to each character and they verify that a person is who she or he claims to be (Pankaj 2014).

Reliable user authentication is becoming an increasingly important task in the Web- enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer enhanced security.

The prevailing techniques of user authentication, which involve the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. The relevance of biometrics in modern society has been reinforced by the need for large-scale identity management systems whose functionality relies on the accurate determination of an individual’s identity in the context of several different applications. Biometric method has come to be a prominent alternative and secured means of authentication able to sustaining the emerging popular computing.

All academic institutions have certain criteria for admitting students into examination hall; that is why preserving the correct file of attendance and fees payments are very critical. In nearly all institutions in the growing countries, clearance is generally finished manually using paper sheets and antique report gadget method, but this method is prone to impersonation. Biometric identity of a person is fast, easy-to-use, specific, truthful and cost effective over traditional understanding-based totally and manual techniques. A biometric gadget includes mainly a photograph taking pictures module, a feature extraction module and a sample matching module. A photograph shooting module acquires the raw biometric facts of a person using a sensor, making use of appropriate set of rules characteristic extraction module that improves the exceptional of the captured picture. Database module shops the biometric template information of enrolled folks. Sample matching module compares the extracted features with the saved templates, which in-flip generates fit score. This technique discourages fraud, impersonation at some stage in the examination in contrast to the paper clearance strategies which inspire fraud, impersonation etc.

The rate of problems encountered in conducting higher institutions examination is too high and the approach used is too poor. Some of these problems include: student impersonation, unsecured authentication of students, manual verification of students, time consumption etc. Hence, this research study focuses on the design and implementation of automated examination attendance system based on fingerprint recognition to curb impersonation in examination conduct in higher institutions.

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, biometrics characteristics can be used for authenticating students. This research will focus on developing Fingerprint based Biometric Student Attendance Monitoring System. The fingerprint Biometrics is adopted in this research work for the fact it is one of the most successful applications of biometric technology. 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).

1.2 Statement of the Problem

The traditional system is still mostly used in most of the tertiary institutions today. Lecturer or instructor will give out a sheet of paper containing list of student's names to sign or in some cases, the student will be the ones to write their names, matriculation number and signature to indicate their presence for a particular class or examination. 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 or examination. Other problems which are encountered in the manual system are student impersonation, unsecured authentication of students, stress and time-consuming (because the student has to go through a long process so as to just obtain an examination slip which is used to prove that he or she is eligible to sit for an exam. This 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 examination. Hence, propositions have been made that fingerprint recognition will help in dealing with these problems.

1.3 Aim and Objectives of the study

The aim of the study is to design and develop a reliable, scalable and cost-effective Students Attendance Management System using Biometric capturing. The system will be designed and implemented using HTML, CSS, PHP, Mysql, C# and JavaScript.

1.4 Significance of the study

With the increasing rate of examination malpractices in the educational sectors the school management deserves to inculcate tight security means to ensure that these activities of exam impersonators stop. The system uses fingerprint biometrics; this would help ensure that only registered students during registration with their fingerprints are allowed into the examination hall. The system would contribute in the area of stopping any activity of corruption in the educational sector among students, and students to invigilators. Hard work would be encouraged as every registered student knows he/she is going to write the exam by himself or herself. The impersonation which has eaten the educational system thereby encouraging laziness among students would be eliminated and the standard of student educational performance would be increased.

1.5 Scope of the study

The scope of this work is to develop a Examination Attendance Management System Based on Fingerprint Recognition that will improve how attendance management is done by using fingerprint as a form authentication for proof in examination hall and which will be more accurate, easier and faster.

1.6 Limitations of the Study

The efficiency of the scanner can be reduced due to the roughages in the captured images which are often caused by worn-out or cut or dirt’s found on fingerprint. Therefore, there is every possibility that enrolled users can be rejected by the system.

Other factors that limit this research work are; time, finance and inaccessibility to the relevant materials.

1.7 Definition of Terms

Biometrics: This refers to technology for measuring and analyzing human physiological traits along with fingerprints, eye retinas and irises, voice patterns, facial styles, and hand measurements, especially for authentication functions.

Examination: is a set of questions or exercises evaluating skill or knowledge

Examination malpractice: unethical or misconduct in an Examination Hall

Examination Impersonation: Examination impersonation is act by which an individual who is not registered as a candidate for a particular examination takes the place of one that is registered

Software: Written programs or procedures or rules and associated documentation pertaining to the operation of a computer system and that are stored in read/write memory.

Fingerprint Scanner: A fingerprint scanner is an electronic device used to capture a digital image of the fingerprint pattern

Fingerprint: Analyzing fingertip patterns.

Facial Recognition: Facial recognition is a way of identifying or confirming an individual’s identity using their face. Facial recognition systems can be used to identify people in photos, videos, or in real-time.

CHAPTER TWO

LITERATURE REVIEW

In today's world, biometric recognition is a common and reliable way to authenticate the identity of a living persons based on physiological or physical make up of such an individual. As services and technologies have developed in the modern world, human activities and transactions have proliferated in which rapid and reliable personal identification is required. Examples of applications include logging on to computers, pass through airport, access control in laboratories, factories and homes, people need to verify their identities, bank Automatic Teller Machines (ATMs), and other transactions authorization, premises access control, and in general security systems (Sabarigiri, B. et al., 2012). All such identification efforts share the common goals of speed, reliability and in previous, the most popular methods of keeping information and resources secure are to use password and User ID/PIN protection. These schemes require the users to authenticate themselves by entering a -secret- password that they had previously created or were assigned (Afsana Ahamed *et al.*, 2012). These systems are prone to hacking, either from an attempt to crack the password or from passwords, which were not unique. However, password can be forgotten, and identification cards can be lost or stolen (Penny K., 2014). A Biometric Identification system is one in which the user's "body" becomes the password/PIN. Biometric characteristics of an individual are unique and therefore can be used to authenticate students' allowance to examination halls.

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 (Wayman, 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 *et al.*, 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 and 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. This entry and 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.

2.3.1 Retina Scanner

This scans 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 and 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.

2.3.2 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.

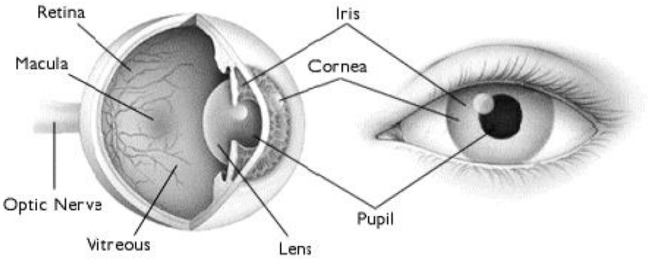


Figure2.1 Structure of Iris. ***Source: (https://studymafia.org/biometrics)***

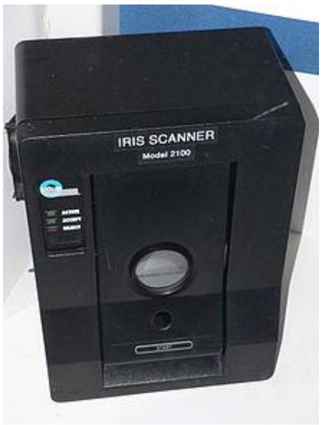


Figure 2.2: Iris scanner. ***Source: (https://studymafia.org/biometrics)***

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 and Modi, 2008).

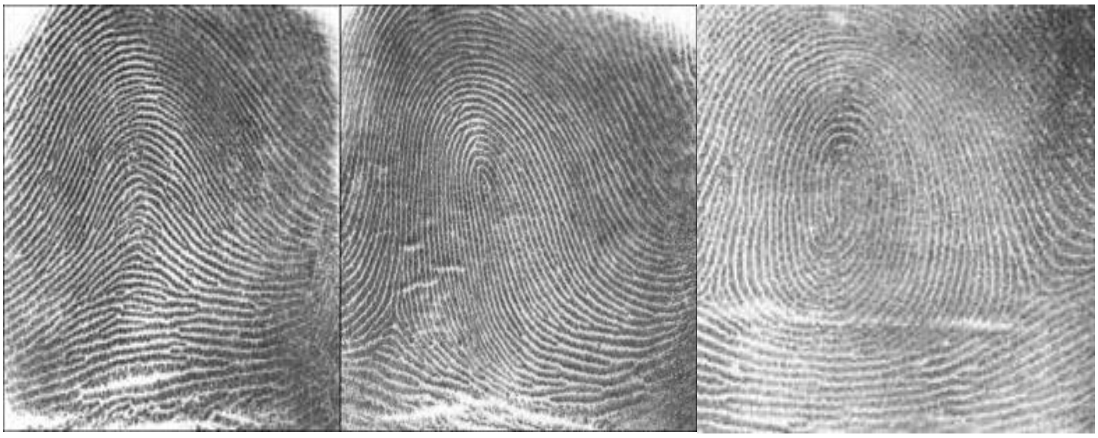
2.3.3 Fingerprint Scanner

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 pattern. 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.

- **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.
- **Loop:** The ridges enter from one side of a finger, form a curve, and then exit on that same side.
- **Whorl:** Ridges form circularly around a central point on the finger.

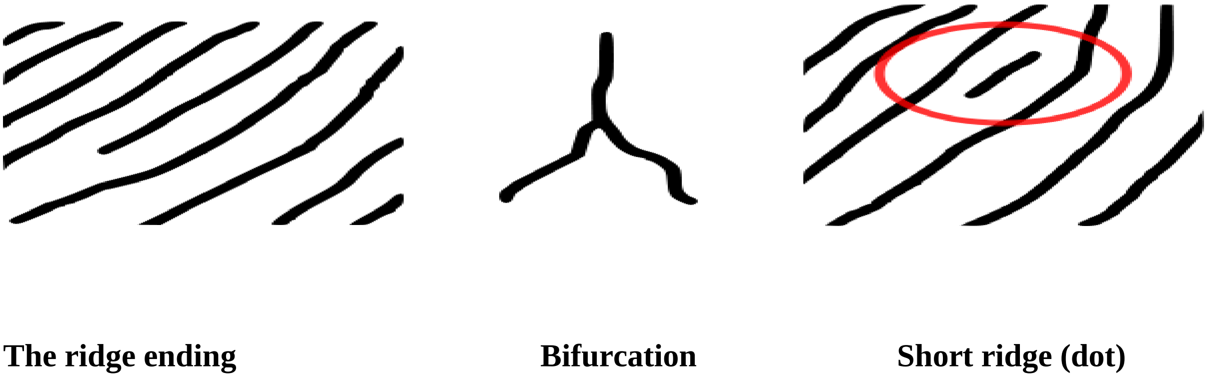


The arch pattern the loop pattern the whorl pattern

Figure 2.3: Fingerprint patterns *Source: (https://studymafia.org/biometrics)*

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)**

Figure 2.4: Minutia features. ***Source: (https://studymafia.org/biometrics)***

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.

Figure 2.4: Scanners. ***Source: (https://studymafia.org/biometrics)***

2.3.4 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.

2.3.5 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

2.3.6 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.

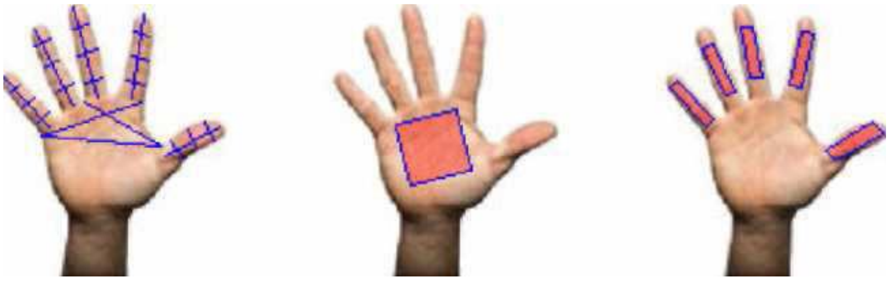


Figure 2.4: Hand Print Patterns. ***Source: (https://studymafia.org/biometrics)***

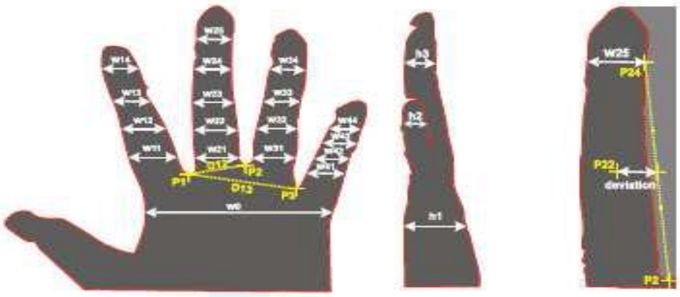


Figure 2.4: Hand Print Patterns. ***Source: (https://studymafia.org/biometrics)***

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.

2.3.7 DNA Fingerprint

This method works by taking a tissue sample from an individual and then sequencing and comparing short segments of DNA. DNA technique has a very low acceptance rate because samples have to be taken from human body and also the speed at which these samples are processed

2.3.8 Deep Tissue Illumination

A relatively new method that involves illumination of human tissue by specific lighting conditions and the identification of deep tissue patterns based on light reflection. This method is claimed to be less prone to falsification than other forms of biometric techniques, b it is very complex to imitate the process of light reflection (Nixon, 2003).

2.3.9 Voice Print Keystroke Pattern

This method works by discovering patterns while an individual is typing on a keyboard and these patterns are then compared against previous patterns stored. Biometrics that has to do with keystroke have been utilized to make password entry more complex, to provide certainty that a password was inputted by the same person that saved it by comparing the speed at which it was typed.

Some of these products are tend to be expensive than others simply because they employ technology that is much more complex. Nevertheless, when considering the level of security level required the amount of to acquire different types of biometric devices will be almost the same. The features derived from the biometric are then converted into a biometric template.

The process of retrieving features from the captured data and converting it into a template are usually important. These templates are then used as the foundation for verification during authentication. The process by which biometric template are acquired, transmitted and stored are important aspects of biometric security systems, because risks can surface from these are areas and spurious attacks can be made which will compromise the integrity of the system.

2.4 Applications Areas of Biometric

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.

2.4.1 Forensic

The use of biometric in the law enforcement and forensic is more known and from long date, it is used mainly for identification of criminals. In particular, the AFIS (automatic fingerprint identification system) has been used for this purpose.

Lately the facial-scan technology (mug shots) is being also used for identification of suspects. Another possible application is the verification of persons of home arrest, a voice-scan is an attractive solution for this problem. The typical applications are:

- Identification of criminals
- Surveillance
- Corrections
- Probation and home arrest

2.4.2 Government

There are many applications of the biometry in the government sector. An AFIS is the primary system used for locating duplicates enroll in benefits systems, electronic voting for local or national elections, driver's license emission, etc. The typical applications are:

- National Identification Cards
- Voter ID and Elections
- Driver's licenses
- Benefits Distribution (social service)
- Employee authentication
- Military programs

2.4.3 Commercial

Banking and financial services represent enormous growth areas for biometric technology, with many deployments currently functioning and pilot project announced frequently. Some applications in this sector are:

- Account control
- ATMS
- Expanded service kiosks
- Online banking
- Telephony transaction
- PC/Network access
- Physical access
- E-commerce
- Time and attendance monitoring

2.4.4 Health Care

The applications in this sector includes the use of biometrics to identify or verify the identity of individuals interacting with a health-care entity or acting in the capacity of health-care employee or professional. The main aim of biometrics is to prevent fraud, protect the patient information and control the sale of pharmaceutical products. Some typical applications are:

- PC/Network Access

- Access to personal information
- Patient identification

2.4.5 Travel and Immigration

The application in this sector includes the use of biometrics to identify or verify the identity of individual interacting during the course of travel, with a travel or immigration entity or acting in the capacity of travel or immigration employee. Typical applications are:

- Air
- Border
- Employee
- Passports

2.5 Biometric Modality

There is no single biometric modality that is best for all implementations. Commonly implemented or studied biometric modalities include: Fingerprint, face, iris, voice, signature and hand geometry. Many other modalities are in various stages of development and assessment. Many factors must be taken into account when implementing a biometric system, including but not limited to: physical location, security risks, task (identification or verification), expected number of end users, user circumstances. Each biometric modality has its own strengths and weaknesses that must be evaluated in relation to the application before implementation. The effectiveness of a particular implementation of biometric technology is dependent on how and where the technology is used.

Key decision factors for selecting a particular biometric technology for a specific application includes but is not limited to:

- The environment
- Throughput needs (the required speed of the transaction)
- Costs associated with obtaining and storing templates and conducting biometric

recognition

- Population size and demographics
- Ergonomics
- Interoperability with existing systems
- Other user considerations — for instance, an access control system to a coal mine, where individuals might have very worn and/or dirty fingerprints, will not be a suitable environment for a fingerprint reader.

2.6 Advantages Of Biometric Security

- Increase security **-** Provide a convenient and low-cost additional tier of security.
- Reduce fraud by employing hard-to-forge technologies and materials. e.g. minimize the opportunity for ID fraud, buddy punching.
- Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For e.g. prevent unauthorized use of lost, stolen or "borrowed" ID cards.
- Reduce password administration costs.
- Replace hard-to-remember passwords which may be shared or observed.
- Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access.
- Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN!
- Offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time & Attendance.
- Unequivocally link an individual to a transaction or event.

2.7 Challenges of Biometric Usage

According to ***www.ovic.com***, while biometric solutions have many advantages, they also present four major biometric authentication challenges that must be considered:

- **Privacy and Data Breach**

  Biological characteristics are unique and nearly impossible to replicate, making biometrics a secure access solution. Passwords on the other hand can be shared and easily stolen by hackers because “people” manage their passwords. Biometrics poses the challenge of privacy since the key features of recognition is exposed to the world. For example, others can record your voice, use your image without consent in facial recognition or copy your fingerprints from an object surface you have held. If the identity management systems get compromised, hackers can leak or steal your biometric data. Since your biometric information is irreplaceable, malicious people can perpetuate criminal activities as long as they possess your data.

- **Errors**

  Biometric equipment is subject to two common mistakes, False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR is the likelihood that the system will accept an unauthorized person, while FRR is the measure of times the system rejects attempts by an authorized user. The biometric technology works on the theory that authorized users have a high pattern score than imposters who are denied access accordingly. It implies that as the FAR declines, then the FRR rises, and the vice-versa is true. Should an imposter’s score exceed the minimum identification threshold, then access is authorized. The reverse is also true. If the authorized user scores below the maximum acceptable score, then no permission is granted.

- **Failure to enroll**

  This occurs when a template for biometric information cannot be successfully created. This may be due to a number of factors, such as low-quality reference information (for example, due to sensors or poor environmental conditions – such as lighting – at the time of enrolment), or a person may have a physical or medical condition that prevents them from enrolling into the system.

- **Compromised biometrics**

  Another limitation of biometric systems is that unlike passwords or ID tokens, biometric characteristics cannot be reissued or cancelled. If a person’s fingerprint or other physiological biometric is compromised, it can be extremely difficult – if not impossible – to change that feature. This can be problematic when using that biometric characteristic for future authentication.

CHAPTER THREE

SYSTEM ANALYSIS AND DESIGN

3.1 System Study

I went through literature on biometrics, and also, I visited different schools such as the School of Engineering, School of art and design, School of Information and Communication Technology etc. of the Federal Polytechnic Auchi to investigate the way examination authentication is carried out. I discovered that the way of capturing attendance information and verifying if a student is eligible to sit for an examination is taken manually by using an attendance sheet. Problems such as student impersonation, stress (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), and unsecured authentication of students are encountered in the manual authentication system. Hence, it is time-consuming.

3.2 System Analysis

In the manual examination authentication system, student will first of all register their courses which they will take in a semester. After the registration process, when examination is approaching, students are grouped, and every student is given an examination permit (ID card) which is brought to the examination hall, and students are verified with the permit. But this is still not a strong measure or security because the eyes are used in this case to check for the occurred passport and the physically occurring human. When it is time of exams student are expected to arrive at the examination hall with their exam permit (photo card or id card), this exam permit serves as an authorization for them to gain access to the exam hall and participate fully in the examination. Since the process use is what you have and not what you are, impersonator can simply make black and white photocopy of the photo card making his picture to be dark so when check during the exam or even swap the photo on the exam permit to his own photo. Certain student who is not capable of writing the proposed course due to laziness in studies might pay people to come and write the courses for him. Using the eye, a physical matching is now taken between the passport that has been printed and the physically present human to check if the student that has register is actually the one writing the exam and if not, he/she is apprehended. But this has proven to be very inefficient. Several problems tend to exist within the use of the system and as such include:

- Inefficient in its usage and comprehend the act of exam impersonation
- The process of authorization is based on a concept of what you have; which can be manipulated at any time.
- Matching to establish security measures occurs through the physical eye and this is a very big problem and requires great power of recognition, hence an impersonator can be present with recognition.

3.2.1 Flow Chart of the Current System

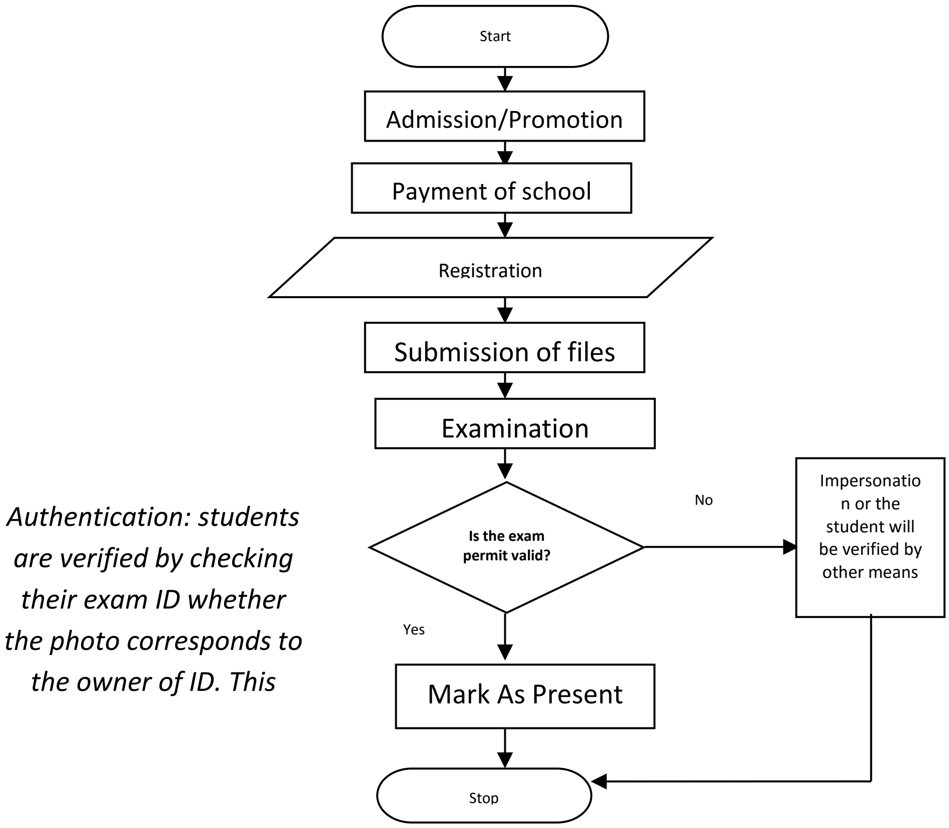

Start
Admission/Promotion
Payment of school
Registration
Submission of files
Examination
Authentication: students are verified by checking their exam ID whether the photo corresponds to the owner of ID. This
Is the exam permit valid?
No
Impersonation or the student will be verified by other means
Yes
Mark As Present
Stop

Figure 3.1: Flowchart of the existing system

The Admission/Promotion:

At the stage, the student is admitted into the institution or promoted from one level to another.

Payment of school fees:

The school fees payment made by the student is processed and acknowledged at this stage.

Registration:

At this stage, the student login to the school portal and carries out all the steps required for the registration and prints out the necessary documents.

Submission of files:

The printed documents are filed and submitted to the departmental administrator by the student.

Examination attendance (Authentication):

When it is time for examination, the student is expected to arrive at the examination hall with his/her exam permit (photo card or id card), this exam permit serves as an authorization for them to gain access to the exam hall and participate fully in the examination. The student is verified with the permit. But this is still not a strong measure or security because the eyes are used in this case to check for the occurred passport and the physically occurring human. Several problems tend to exist within the use of the system and as such include:

- Inefficient in its usage and comprehend the act of exam impersonation
- The process of authorization is based on a concept of what you have; which can be manipulated at any time.
- Matching to establish security measures occurs through the physical eye and this is a very big problem and requires great power of recognition, hence an impersonator can be present with recognition.

Hence this system needs to be corrected by deploying a biometric attendance system based on fingerprint recognition.

3.3 Design of the proposed system

The proposed system provides solution to examination impersonation problems through the use of interacting software that is interfaced to a fingerprint device. The student bio-data (Matriculation number, Name, Gender and Date of Birth) and the fingerprint are enrolled first into the database. The fingerprint is captured using a fingerprint device. For examination, the student places his/ her finger over the fingerprint device and the attendance is taken by comparing a single fingerprint image with the fingerprint images previously stored in a database during the registration process. During the exam the school management is expected to come with system containing the student's database of information for those exams and each student is expected to thumb print before entering for the exams. During the process of thumb printing, if a student that has not registered for the exams wants to impersonates, a matching template will fail and the student will be apprehended as impersonator. The system is meant to permit only users verified by their fingerprint scan and doesn't allow non verified users. This system will add more security measures to the examination processes using finger print biometrics and eliminates the possibility of an imposter appearing in an exam.

3.3.1 Flowchart Of The Proposed System

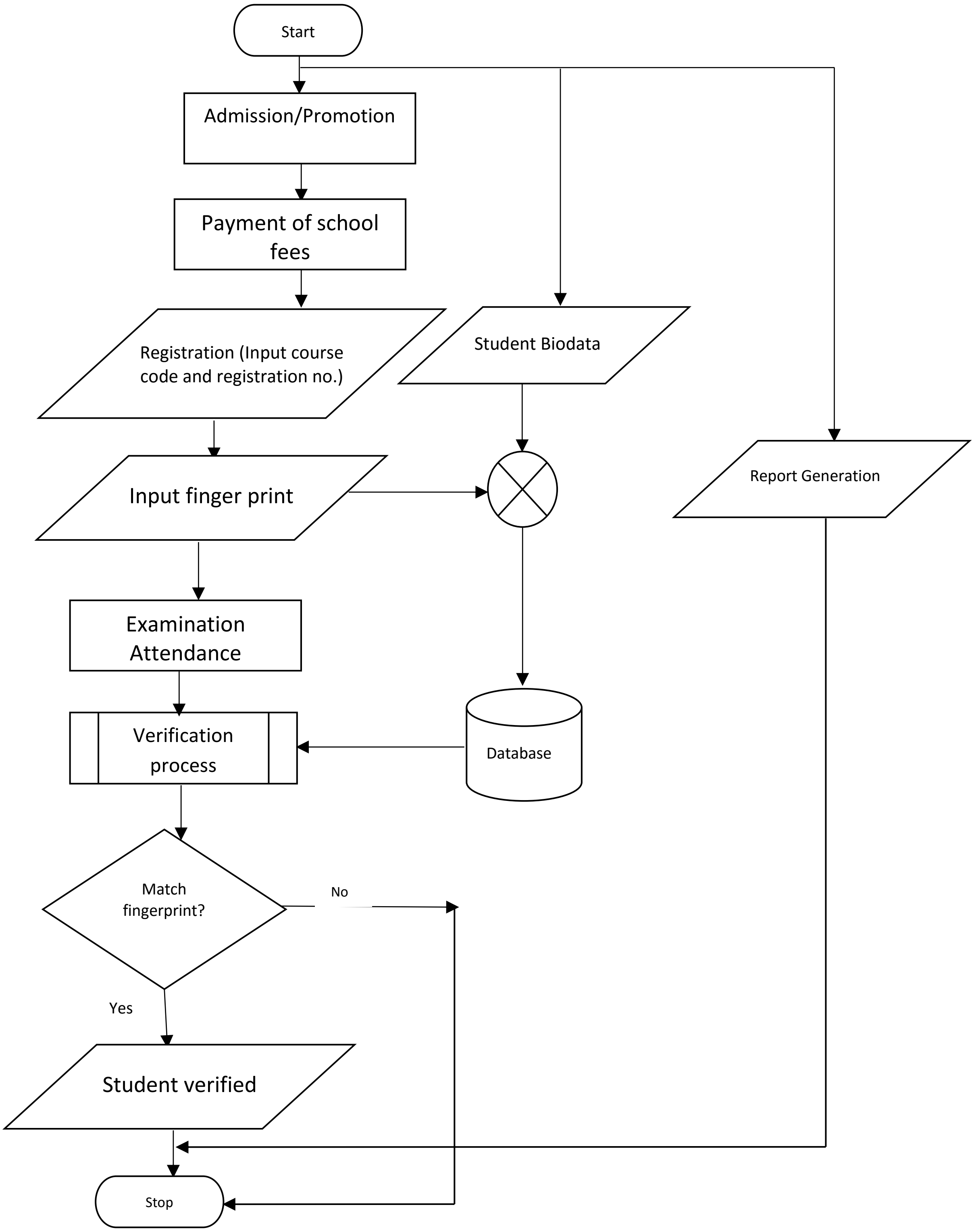


Figure 3.2: Flowchart of the proposed system.

3.4 PROGRAM FLOWCHART

3.4.1 Admin Login

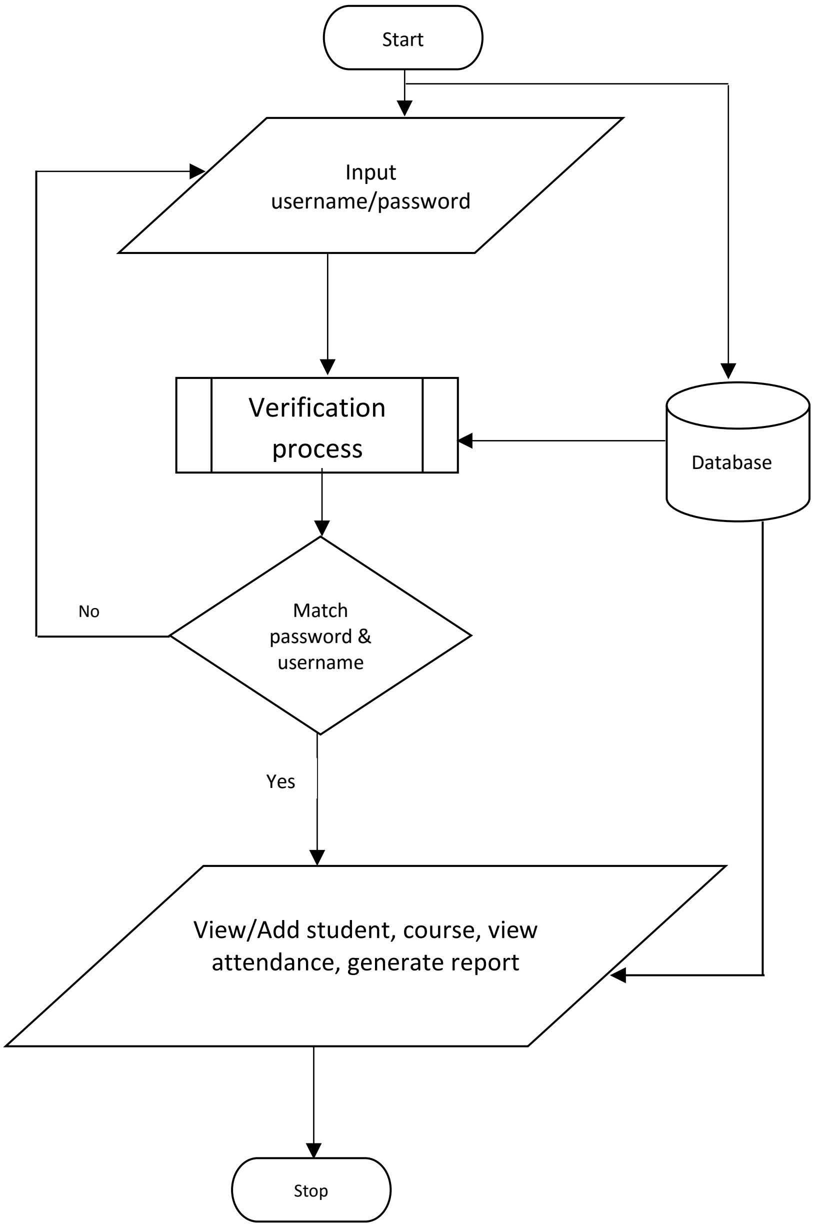

Start
Input username/password
Verification process
Database
No
Match password & username
Yes
View/Add student, course, view attendance, generate report
Stop

Figure 3.3: Admin login flowchart

3.4.2 Student Fingerprint verification (Time-In/Time-out) flowchart

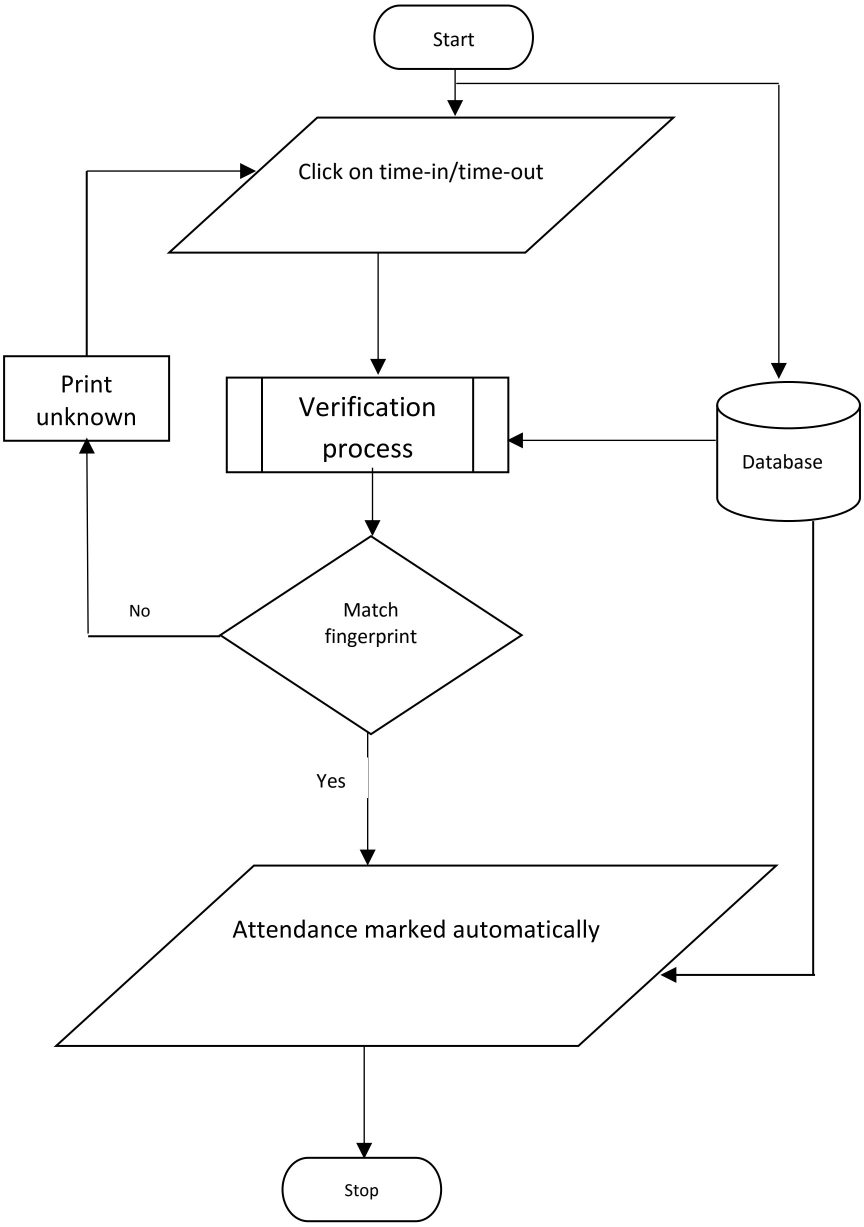


Figure 3.4: Student Time-in/Time-out Flowchart

3.4.3 Input Form Design

3.4.3.1 Add New Student

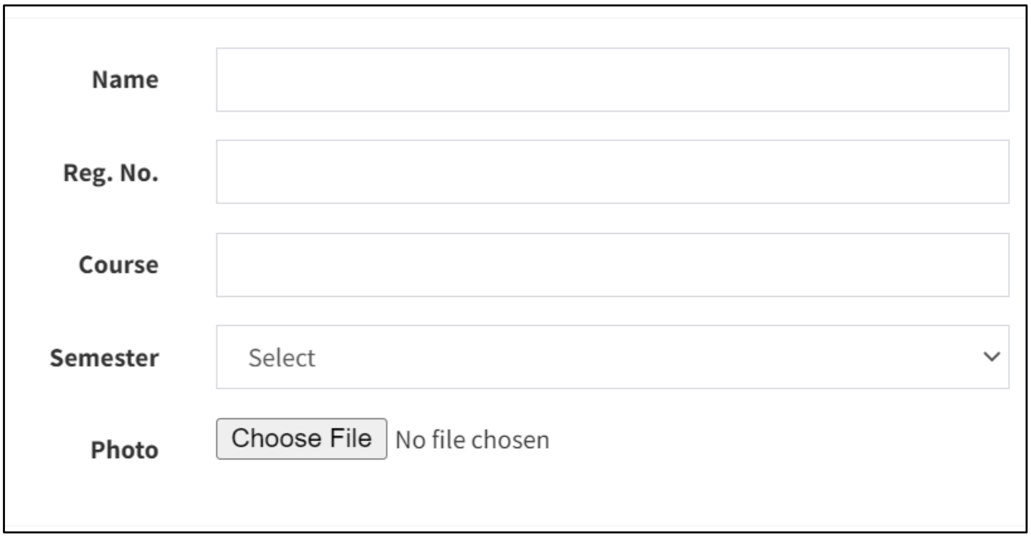


Figure 3.5: Add new student input form

3.4.3.2 Add New Course

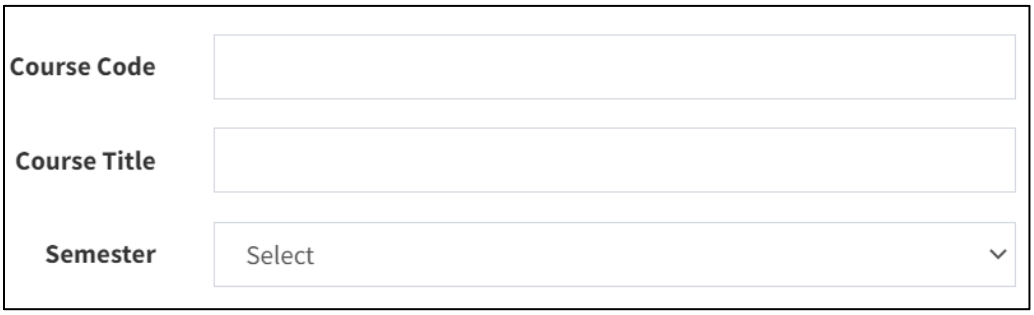


Figure 3.6: Add new course input form

3.4.3.2 Add New Lecturer

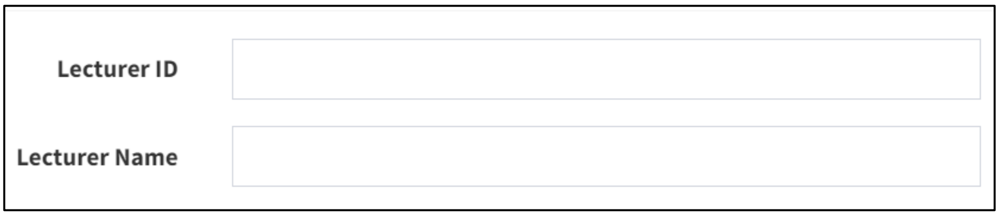
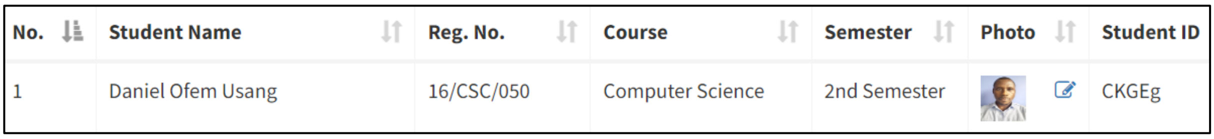


Figure 3.7: Add new Lecturer input form

3.4.4 Output Form Design

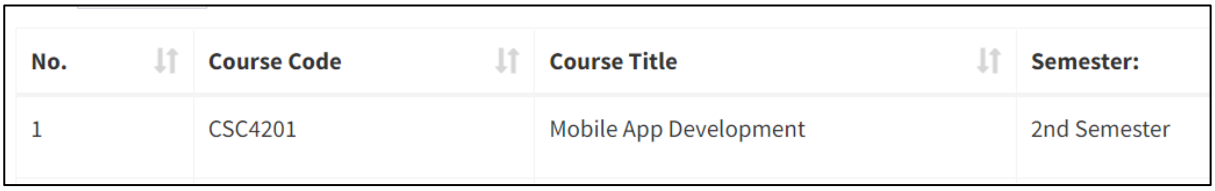
3.4.4.1 Student output form



No.	Student Name	Reg. No.	Course	Semester	Photo	Student ID
1	Daniel Ofem Usang	16/CSC/050	Computer Science	2nd Semester	✎	CKGEg

Figure 3.8: Add new student output form

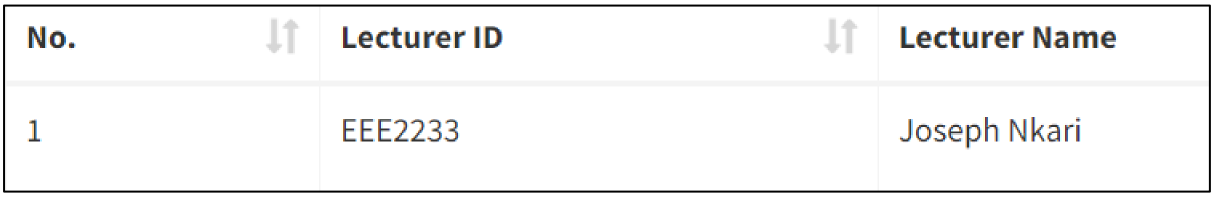
3.4.4.1 Course output form



No.	Course Code	Course Title	Semester:
1	CSC4201	Mobile App Development	2nd Semester

Figure 3.9: Add new course output form

3.4.4.1 Lecturer output form

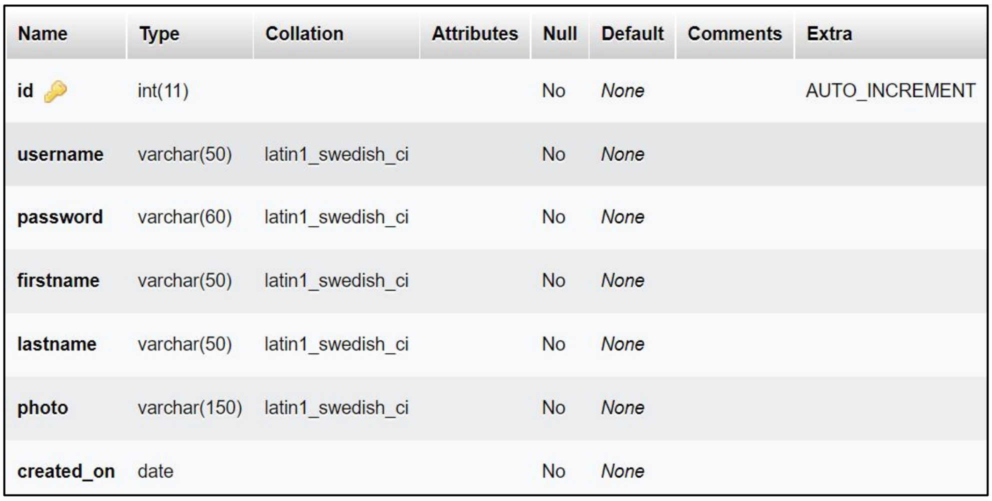


No.	Lecturer ID	Lecturer Name
1	EEE2233	Joseph Nkari

Figure 3.10: Add new Lecturer output form

3.5.3 Database Design

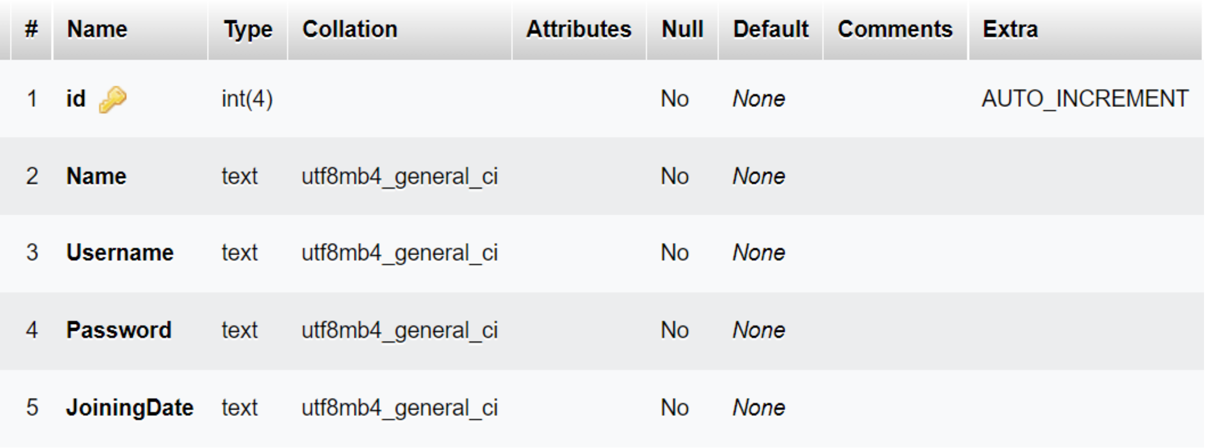
3.5.3.1: Admin Database



Name	Type	Collation	Attributes	Null	Default	Comments	Extra
id 🔑	int(11)			No	*None*		AUTO_INCREMENT
username	varchar(50)	latin1_swedish_ci		No	*None*		
password	varchar(60)	latin1_swedish_ci		No	*None*		
firstname	varchar(50)	latin1_swedish_ci		No	*None*		
lastname	varchar(50)	latin1_swedish_ci		No	*None*		
photo	varchar(150)	latin1_swedish_ci		No	*None*		
created_on	date			No	*None*		

Table 3.1: Admin Database

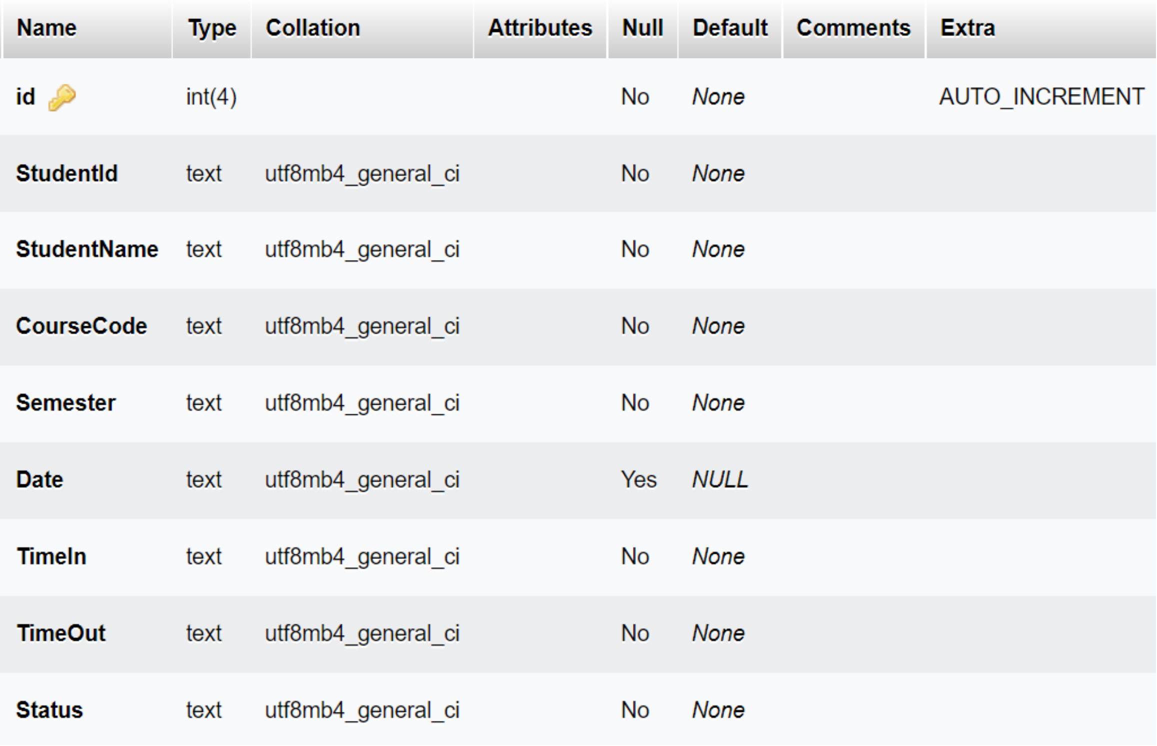
3.5.3.2: Admin Registration Database



#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra
1	**id** 🔑	int(4)			No	*None*		AUTO_INCREMENT
2	**Name**	text	utf8mb4_general_ci		No	*None*		
3	**Username**	text	utf8mb4_general_ci		No	*None*		
4	**Password**	text	utf8mb4_general_ci		No	*None*		
5	**JoiningDate**	text	utf8mb4_general_ci		No	*None*		

Table 3.2: Admin Registration Database

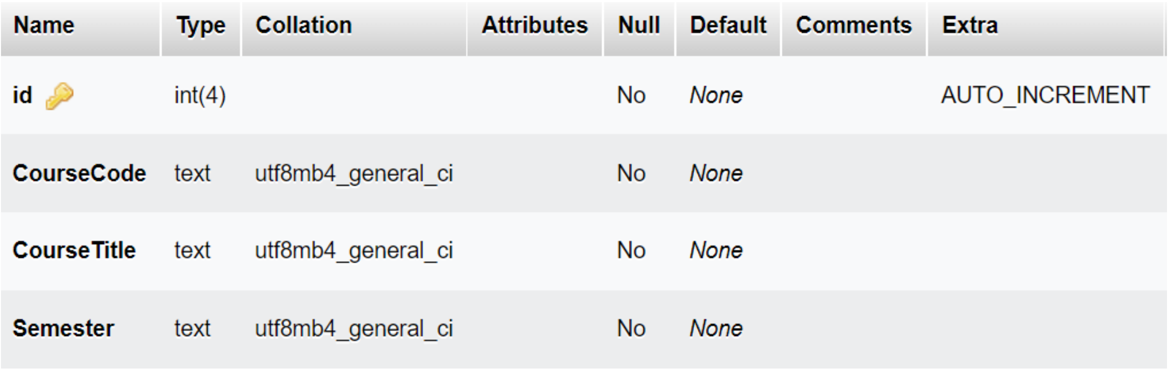
3.5.3.3: Student Attendance Database



Name	Type	Collation	Attributes	Null	Default	Comments	Extra
id 🔑	int(4)			No	*None*		AUTO_INCREMENT
StudentId	text	utf8mb4_general_ci		No	*None*		
StudentName	text	utf8mb4_general_ci		No	*None*		
CourseCode	text	utf8mb4_general_ci		No	*None*		
Semester	text	utf8mb4_general_ci		No	*None*		
Date	text	utf8mb4_general_ci		Yes	*NULL*		
TimeIn	text	utf8mb4_general_ci		No	*None*		
TimeOut	text	utf8mb4_general_ci		No	*None*		
Status	text	utf8mb4_general_ci		No	*None*		

Table 3.3: Student Attendance Database

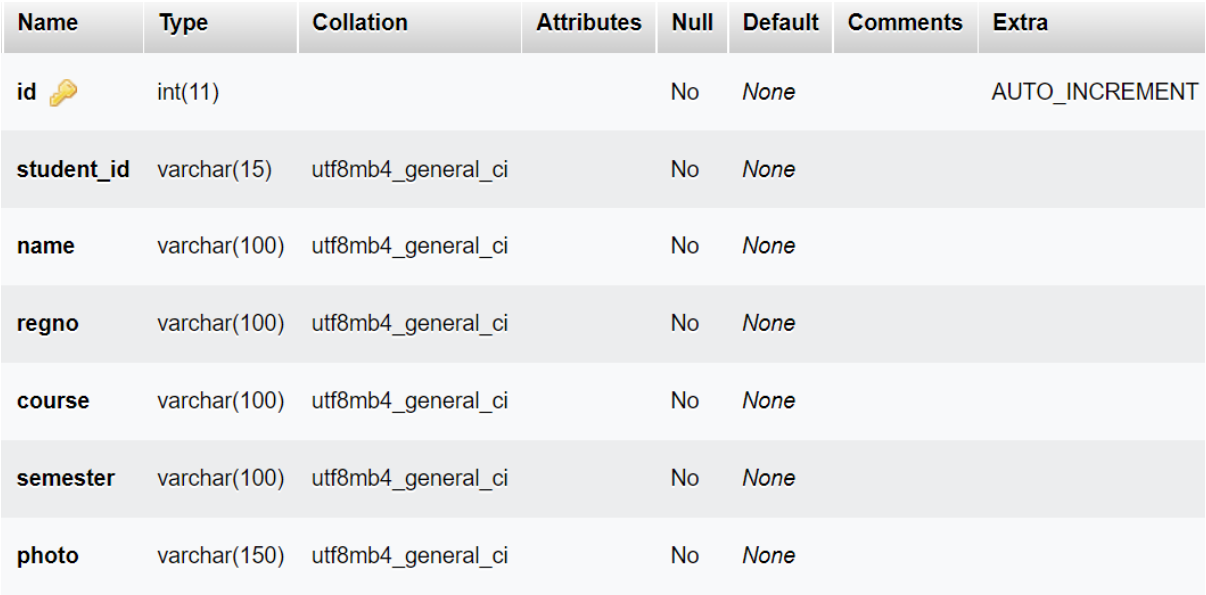
3.5.3.4: Course Registration Database



Name	Type	Collation	Attributes	Null	Default	Comments	Extra
id 🔑	int(4)			No	*None*		AUTO_INCREMENT
CourseCode	text	utf8mb4_general_ci		No	*None*		
CourseTitle	text	utf8mb4_general_ci		No	*None*		
Semester	text	utf8mb4_general_ci		No	*None*		

Table 3.4: Course Registration Database

3.5.3.5: Student Registration Database



Name	Type	Collation	Attributes	Null	Default	Comments	Extra
id 🔑	int(11)			No	*None*		AUTO_INCREMENT
student_id	varchar(15)	utf8mb4_general_ci		No	*None*		
name	varchar(100)	utf8mb4_general_ci		No	*None*		
regno	varchar(100)	utf8mb4_general_ci		No	*None*		
course	varchar(100)	utf8mb4_general_ci		No	*None*		
semester	varchar(100)	utf8mb4_general_ci		No	*None*		
photo	varchar(150)	utf8mb4_general_ci		No	*None*		

Table 3.4: Student Registration Database

CHAPTER FOUR

IMPLEMENTATION AND TESTING

This chapter describes and shows how this standalone system is implemented, developed and tested, using the appropriate necessary programming languages, tools and technology.

4.1 IMPLEMENTATION

System or Software Implementation is the conversion of the System Requirements into an executable and working system.

4.1.1 Implementation tools

The Automated Examination Attendance System based on Fingerprint Recognition works as web-based and offline application system. It was implemented using PHP, C++ and MySQL was used for the database and the Integrated Development Environment (IDE) used was Bracket text editor, Visual Studio 2017 and XAMPP was used as the offline local server.

1. PHP

PHP is a general-purpose programming language originally designed for web development. It was originally created by Rasmus Lerdorf in 1994; the PHP reference implementation is now produced by The PHP Group. PHP originally stood for Personal Home Page, but it now stands for the recursive initialism PHP: Hypertext Preprocessor.

PHP code may be executed with a command line interface (CLI), embedded into HTML code, or it can be used in combination with various web template systems, web content management systems, and web frameworks. PHP code is usually processed by a PHP interpreter implemented as a module in a web server or as a Common Gateway Interface (CGI) executable. The web server combines the results of the interpreted and executed PHP code, which may be any type of data, including images, with the generated web page. PHP can be used for many programming tasks outside of the web context, such as standalone graphical applications and robotic drone control.

2. MySQL

MySQL is an Oracle-backed open-source relational database management system (RDBMS) based on Structured Query Language (SQL). MySQL runs on virtually all platforms, including Linux, UNIX and Windows. Although it can be used in a wide range of applications. MySQL is most often associated with web applications and online publishing.

3. XAMPP

XAMPP is a software distribution which provides the Apache web server, MySQL database (actually MariaDB), Php and Perl (as command-line executables and Apache modules) all in one package. It is available for Windows, MAC and Linux systems. No configuration is necessary to integrate PHP with MySQL. It is a great fit for this course and provides a relatively stress-free installation and way to manage the configuration changes. Also provided is PhpMyAdmin which gives a graphical user interface (GUI) tool for managing MySQL databases.

4. C++

C++ (pronounced "See Plus Plus") is a modern, object-oriented, component-oriented and type-safe programming language. C++ enables developers to build many types of secure and robust applications that run in .NET. C# has its roots in the C family of languages and will be immediately familiar to C, C#, and JavaScript programmers. C++ provides language constructs to directly support these concepts, making C++ a natural language in which to create and use software components. Several C++ features help create robust and durable applications.

5. Visual Studio

Visual Studio is a complete set of development tool for windows application, web applications and mobile applications. Visual Basic, Visual C#, Visual C++, Visual F# and many other languages are supported in Visual Studio. Programmers or developers like to develop software using Visual Studio. It is very user friendly.

4.2 System Requirements

The system requirements are the software and hardware requirements. The software requires a set of instructions that controls a computer's action. It is a computer program that accomplishes some specific applications or tasks. This software can be purchased or a user can develop the software from software developers.

The hardware requirements unlike the software refer to the physical components of the computer i.e. the peripherals in this design. The hardware and software requirements for this system are listed below.

4.2.1 Software Requirements

• Operating System	Windows 2007/2010/later versions\
• Browser	Chrome
• Web/Application Server	XAMPP
• Database Server	MySQL
• Database Connectivity	PHP
• IDE	Visual Studio 2017, Bracket

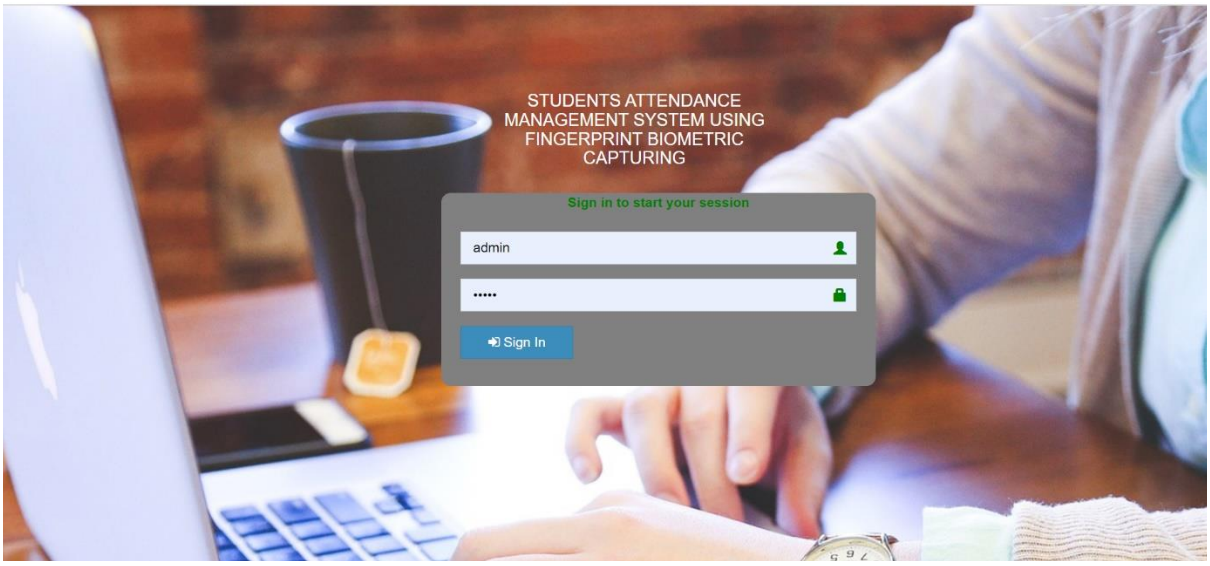
4.2.2 Hardware Requirements

• Computer	Desktop/laptop
• Intel Core i3 and above	1.6 GHZ or above
• RAM Capacity	4GB or above
• Hard Disk	120GB or above
• Fingerprint scanner	Digital Persona U and U 4500

4.3 SAMPLE INTERFACES

4.3.1 Admin Panel

Login: The admin will insert his/her username and password in the provided spaces and click on the LOGIN button to access the admin panel.



STUDENTS ATTENDANCE MANAGEMENT SYSTEM USING FINGERPRINT BIOMETRIC CAPTURING

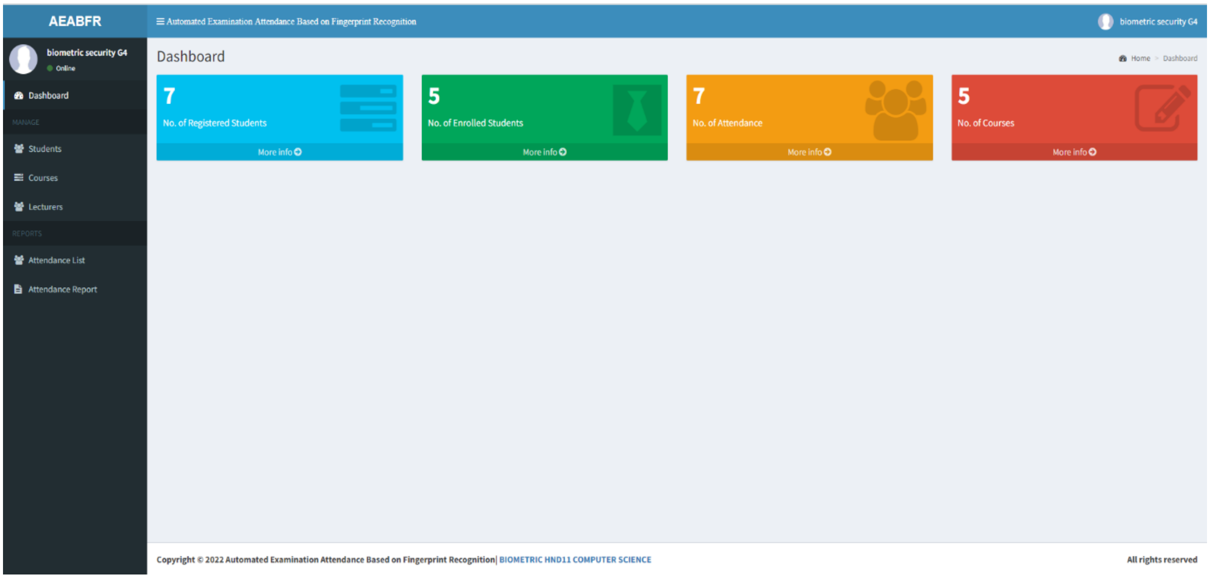
Sign in to start your session

admin

•••••

Figure 4.1: Admin Login Page

1. ***Admin Home Page:*** After Login, the admin homepage will open which will allow admin to navigate to his/her dashboard.



AEABFR

Automated Examination Attendance Based on Fingerprint Recognition

biometric security G4

Dashboard

7 No. of Registered Students

5 No. of Enrolled Students

7 No. of Attendance

5 No. of Courses

Copyright © 2022 Automated Examination Attendance Based on Fingerprint Recognition| BIOMETRIC HND11 COMPUTER SCIENCE

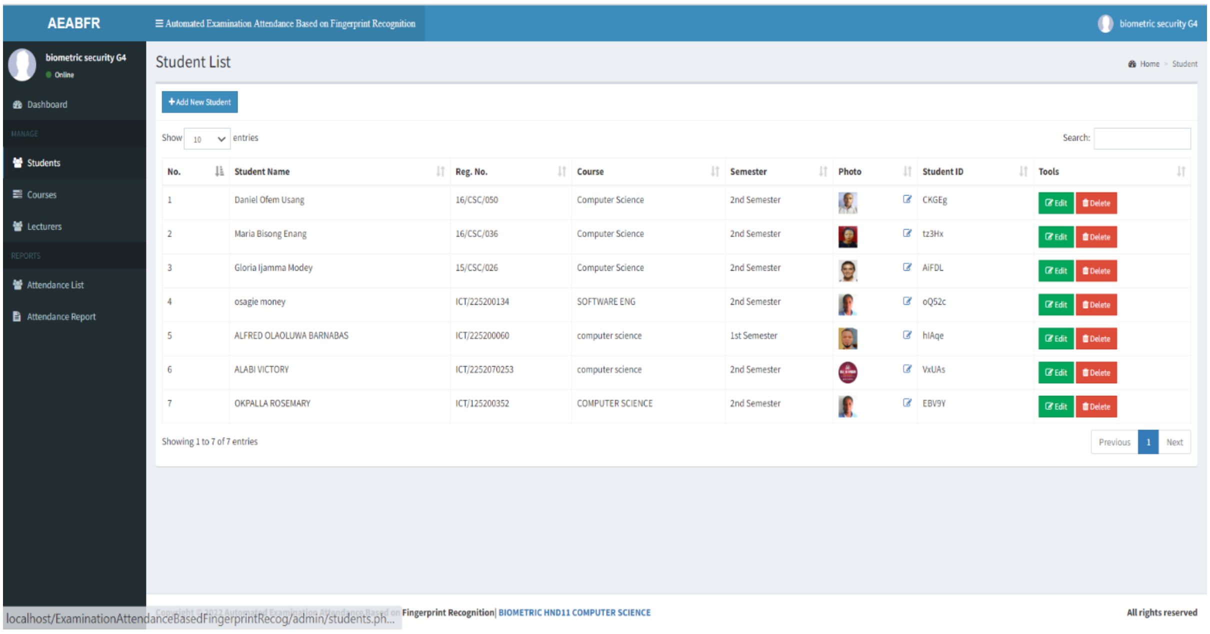
All rights reserved

Figure 4.2: Admin Home Page

2. *Admin Dashboard:* The window (fig 4.2) that allows admin to

- Add Student
- Add Lecturers
- Add Courses
- View Attendance list
- View Attendance Report
- View Number of registered students
- View Number of Courses etc.

3. *Add Student:* This window (fig 4.3) allows admin to add student, view student or edit his profile if needed.



Student List

Show 10 entries

Search:

No.	Student Name	Reg. No.	Course	Semester	Photo	Student ID	Tools
1	Daniel Ofem Usang	16/CSC/050	Computer Science	2nd Semester		CKGEg	Edit Delete
2	Maria Bisong Enang	16/CSC/036	Computer Science	2nd Semester		tz3Hx	Edit Delete
3	Gloria Ijamma Modey	15/CSC/026	Computer Science	2nd Semester		AiFDL	Edit Delete
4	osagie money	ICT/225200134	SOFTWARE ENG	2nd Semester		oQ52c	Edit Delete
5	ALFRED OLAOLUWA BARNABAS	ICT/225200060	computer science	1st Semester		hlAqe	Edit Delete
6	ALABI VICTORY	ICT/2252070253	computer science	2nd Semester		VxUAs	Edit Delete
7	OKPALLA ROSEMARY	ICT/125200352	COMPUTER SCIENCE	2nd Semester		EBV9Y	Edit Delete

Showing 1 to 7 of 7 entries

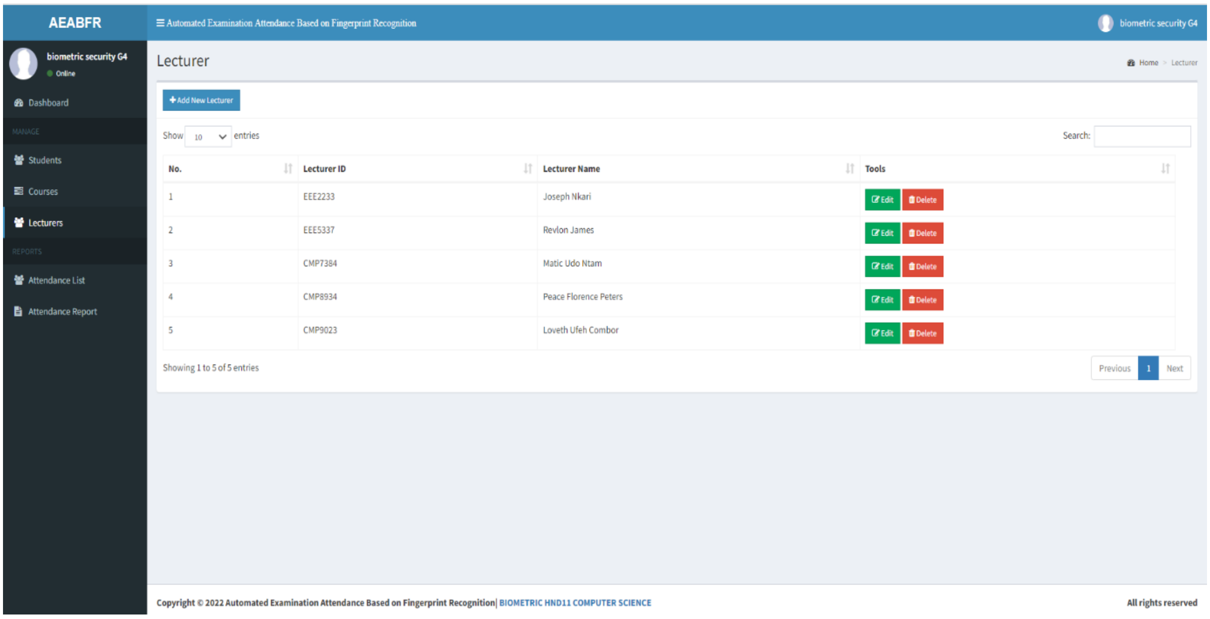
Copyright © 2022 Automated Examination Attendance Based on Fingerprint Recognition| BIOMETRIC HND11 COMPUTER SCIENCE

All rights reserved

localhost/ExaminationAttendanceBasedFingerprintRecog/admin/students.ph...

Figure 4.3: Admin Dashboard – Add/Delete/Edit Student Detail

4. ***Add Lecturers:*** This window (fig 4.4) enables the admin to add lecturers, view or edit lecturer profile if necessary.



Lecturer

Show 10 entries   Search:

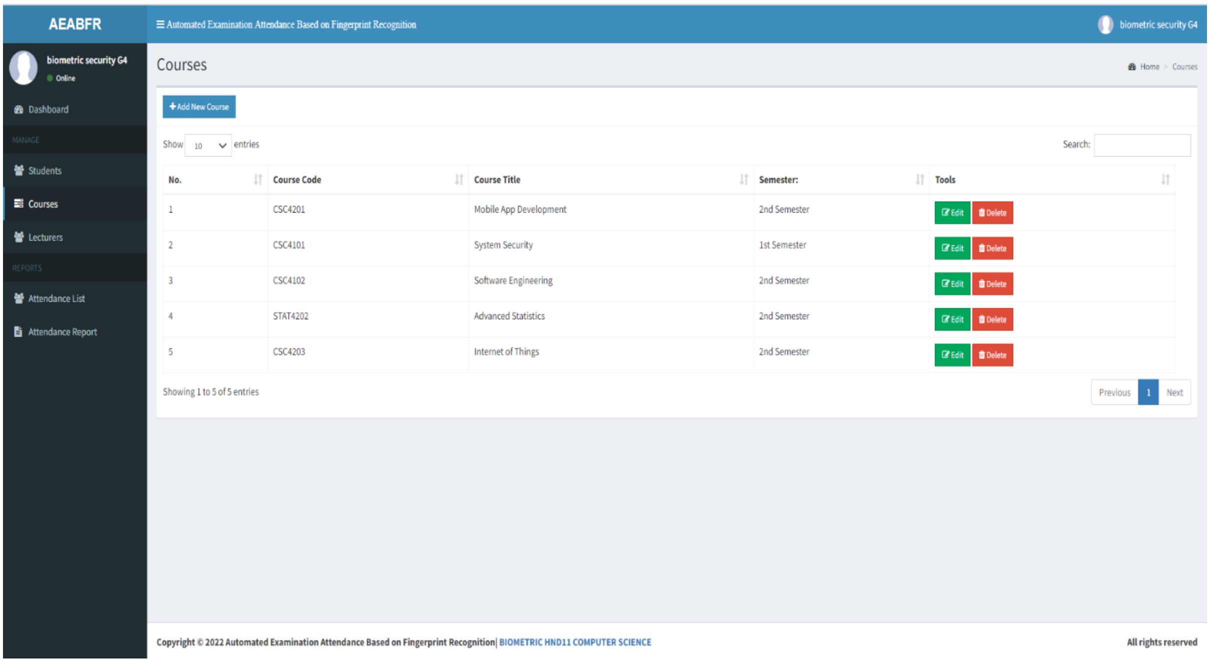
No.	Lecturer ID	Lecturer Name	Tools
1	EEE2233	Joseph Nkari	Edit Delete
2	EEE5337	Revlon James	Edit Delete
3	CMP7384	Matic Udo Ntam	Edit Delete
4	CMP8934	Peace Florence Peters	Edit Delete
5	CMP9023	Loveth Ufeh Combor	Edit Delete

Showing 1 to 5 of 5 entries

Copyright © 2022 Automated Examination Attendance Based on Fingerprint Recognition| BIOMETRIC HND11 COMPUTER SCIENCE   All rights reserved

Figure 4.4: Admin Dashboard – Add/Delete/Edit Lecturer Detail

5. ***Add Courses:*** This window (fig 4.5) allows admin to add/remove courses.



Courses

Show 10 entries   Search:

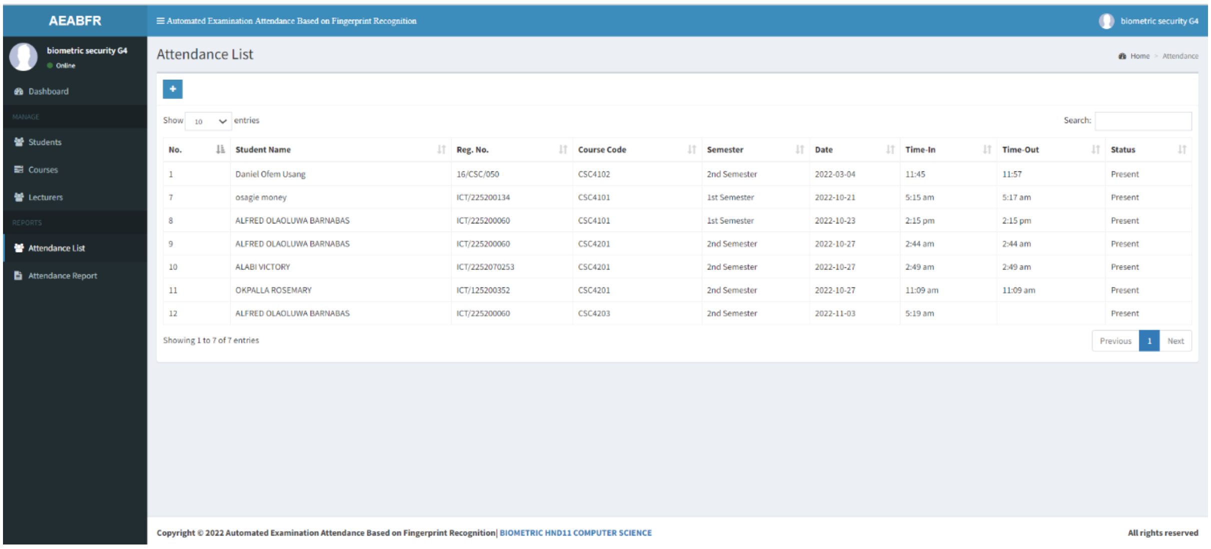
No.	Course Code	Course Title	Semester:	Tools
1	CSC4201	Mobile App Development	2nd Semester	Edit Delete
2	CSC4101	System Security	1st Semester	Edit Delete
3	CSC4102	Software Engineering	2nd Semester	Edit Delete
4	STAT4202	Advanced Statistics	2nd Semester	Edit Delete
5	CSC4203	Internet of Things	2nd Semester	Edit Delete

Showing 1 to 5 of 5 entries

Copyright © 2022 Automated Examination Attendance Based on Fingerprint Recognition| BIOMETRIC HND11 COMPUTER SCIENCE   All rights reserved

Figure 4.5: Admin Dashboard – Add/Delete/Edit Course Detail

6. *View Attendance list:* This window (fig 4.6) enables the admin to view attendance list of students that participated in the examination.



Attendance List

Show 10 entries

Search:

No.	Student Name	Reg. No.	Course Code	Semester	Date	Time-In	Time-Out	Status
1	Daniel Ofem Usang	16/CSC/050	CSC4102	2nd Semester	2022-03-04	11:45	11:57	Present
7	osagie money	ICT/225200134	CSC4101	1st Semester	2022-10-21	5:15 am	5:17 am	Present
8	ALFRED OLAOLUWA BARNABAS	ICT/225200060	CSC4101	1st Semester	2022-10-23	2:15 pm	2:15 pm	Present
9	ALFRED OLAOLUWA BARNABAS	ICT/225200060	CSC4201	2nd Semester	2022-10-27	2:44 am	2:44 am	Present
10	ALABI VICTORY	ICT/2252070253	CSC4201	2nd Semester	2022-10-27	2:49 am	2:49 am	Present
11	OKPALLA ROSEMARY	ICT/125200352	CSC4201	2nd Semester	2022-10-27	11:09 am	11:09 am	Present
12	ALFRED OLAOLUWA BARNABAS	ICT/225200060	CSC4203	2nd Semester	2022-11-03	5:19 am		Present

Showing 1 to 7 of 7 entries

Copyright © 2022 Automated Examination Attendance Based on Fingerprint Recognition| BIOMETRIC HND11 COMPUTER SCIENCE

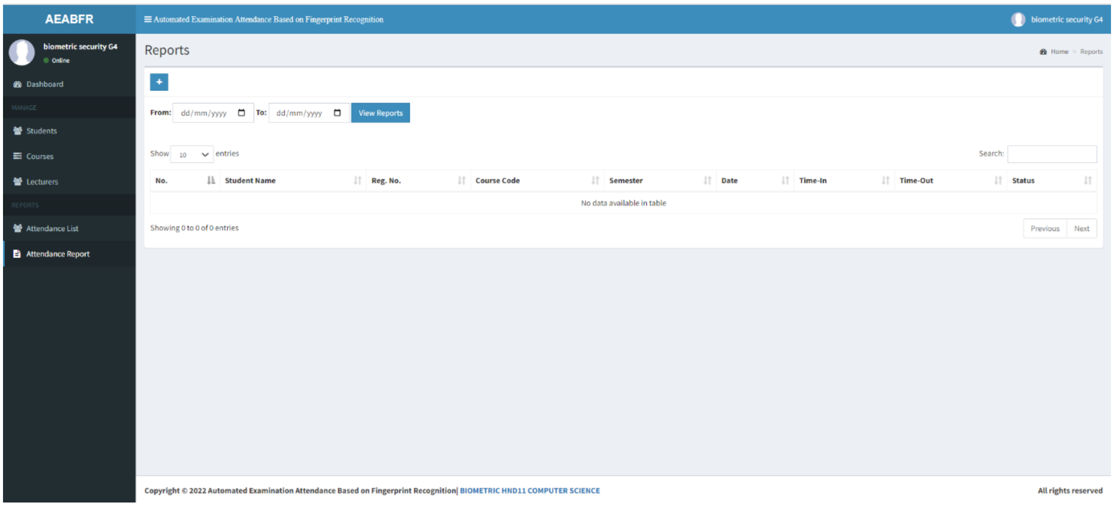
All rights reserved

Figure 4.6: Admin Dashboard – View Attendance List

7. *View Number of registered students:* Enables the admin to view the total number of registered students to participate in the examination.

8. *View Number of Courses:* Enables the admin to view the total number of student courses.

9. *View Attendance Report:* This enables the admin to generate both old and recent attendance reports.



Reports

From: dd/mm/yyyy To: dd/mm/yyyy

Show 10 entries

Search:

No.	Student Name	Reg. No.	Course Code	Semester	Date	Time-In	Time-Out	Status
No data available in table								

Showing 0 to 0 of 0 entries

Copyright © 2022 Automated Examination Attendance Based on Fingerprint Recognition| BIOMETRIC HND11 COMPUTER SCIENCE

All rights reserved

Figure 4.7: Admin Dashboard – View Attendance Report

4.3.2 User Interface

This interface consists of the following:

1. ***Capture Fingerprint:*** This captures the student fingerprint.

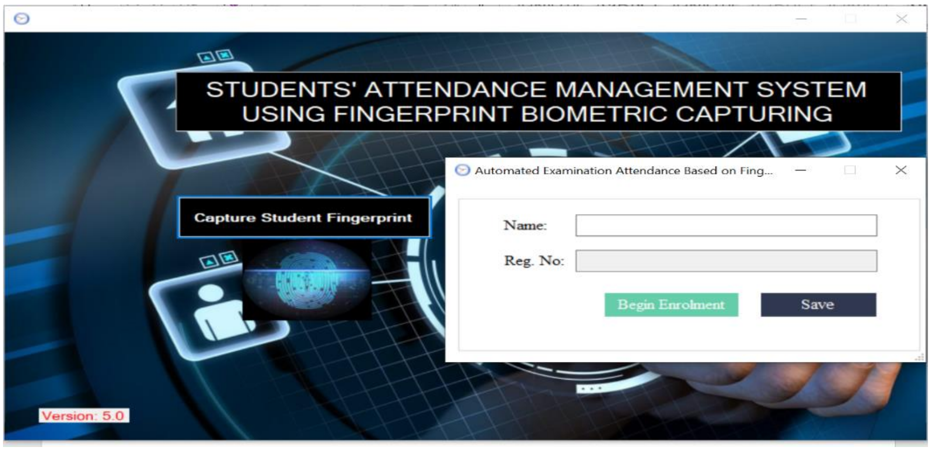
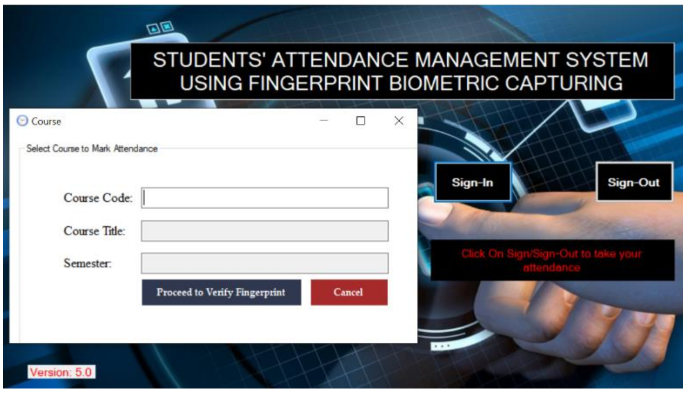

STUDENTS' ATTENDANCE MANAGEMENT SYSTEM
USING FINGERPRINT BIOMETRIC CAPTURING
Capture Student Fingerprint
Automated Examination Attendance Based on Fing...
Name:
Reg. No:
Begin Enrolment
Save
Version: 5.0

Figure 4.8: User Interface – Capture Student Fingerprint

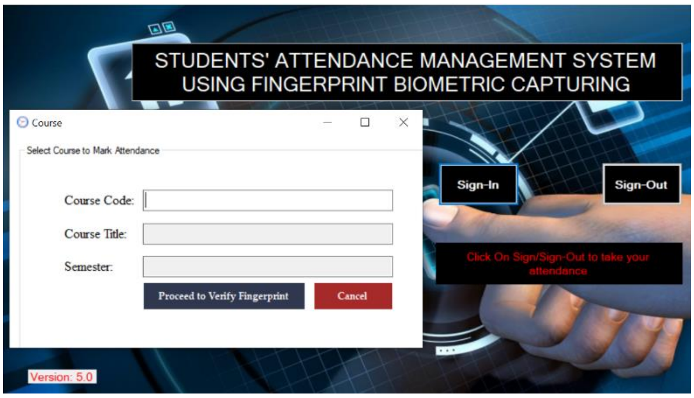
2. ***Sign-In:*** This enables the student to sign in and also verify the student eligibility to sit for the examination.


STUDENTS' ATTENDANCE MANAGEMENT SYSTEM
USING FINGERPRINT BIOMETRIC CAPTURING
Course
Select Course to Mark Attendance
Course Code:
Course Title:
Semester:
Proceed to Verify Fingerprint
Cancel
Sign-In
Sign-Out
Version: 5.0

Click On Sign/Sign-Out to take your attendance

Figure 4.9: User Interface – Sign-In

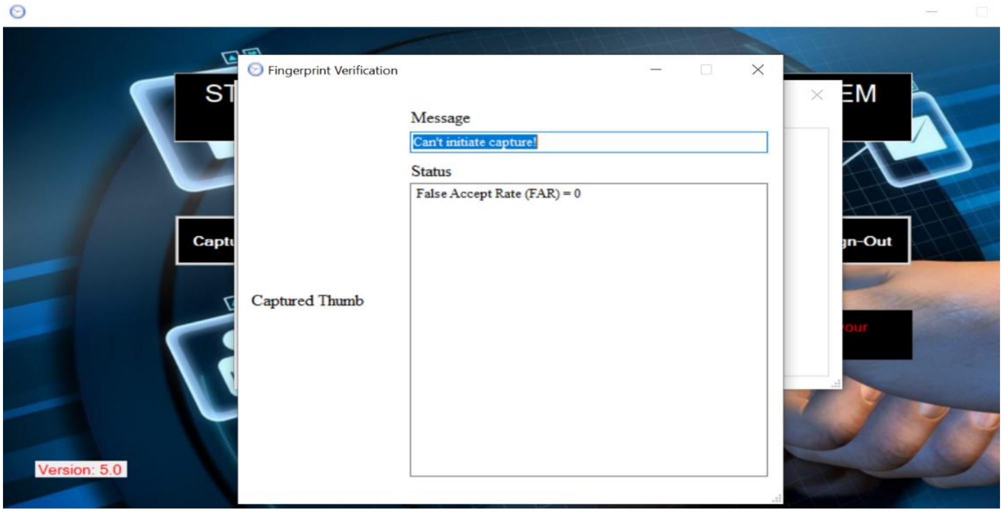
3. ***Sign-Out:*** This verify that the student participated in the exam.


STUDENTS' ATTENDANCE MANAGEMENT SYSTEM
USING FINGERPRINT BIOMETRIC CAPTURING
Course
Select Course to Mark Attendance
Course Code:
Course Title:
Semester:
Proceed to Verify Fingerprint
Cancel
Sign-In
Sign-Out
Version: 5.0

Click On Sign/Sign-Out to take your attendance

Figure 4.10: User Interface – Sign-Out

4. ***Fingerprint Capture Interface***

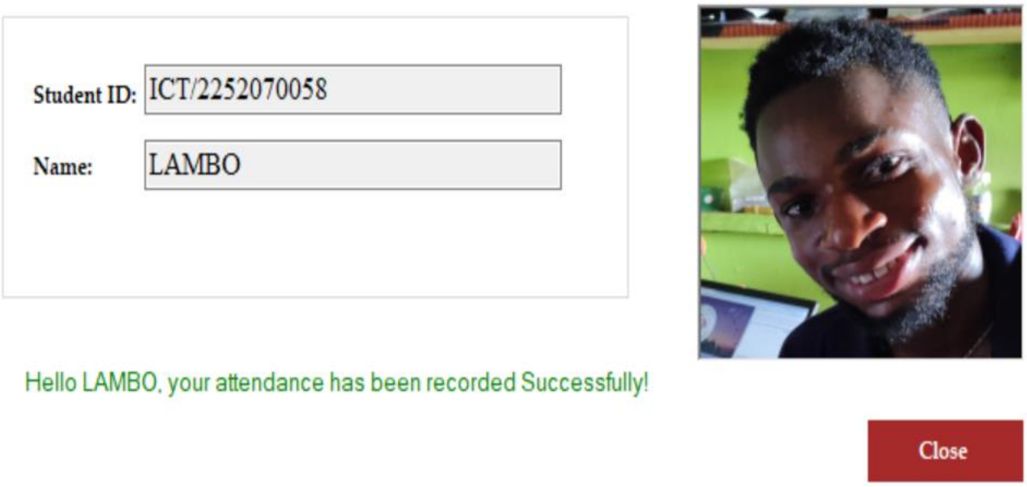


Message: Can't initiate capture!

Status: False Accept Rate (FAR) = 0

Captured Thumb

Figure 4.11: User Interface – Fingerprint Capture



Student ID: ICT/2252070058

Name: LAMBO

Hello LAMBO, your attendance has been recorded Successfully!

Figure 4.12: User Interface – Output of a Successful Sign-in/Sign-out

4.4 System Maintenance

The process of modifying an information system to meet changing needs is known as system maintenance. System maintenance is a primary task or obligation any computerized organization must take up in order to ensure efficiency and continuity of the developed system. It is a routine activity, which is to say that the maintenance of the system is very essential to the smooth running of the system.

The following practices and measure must be taken to ensure that the new system does not breakdown and achieve its proposed aim and objectives:

i. Information Management: Each student is required to provide all the necessary and accurate information during registration; this enhances this integrity of the data in the database. For maximum security, each Admin must protect their password.

ii. Regular Database Backup: This involves the creating duplicates of data which acts as an insurance copy should in case the active copy is damaged or destroyed. The backup is usually stored in an external storage device. Recovery involves the use of specialized utility programs to rebuild or replace damaged files. The best way to recover a file or program is to restore it from a backup copy.

iii. Virus Protection: A virus is a program that infects a computer and could damage a system depending on its nature. Because new viruses must be analyzed as they appear, the antivirus must be updated regularly to be effective.

iv. Training End Users: In order for the new system to work properly, proper training has to be provided by the institution on the use of the new system. Training the users is necessary so as to acquaint them with the working of the system before it is fully developed.

v. Proper use of the system: These include starting (booting) and shutting down the system in the right manner to prevent the system from hanging or data corruption and file loss.

vi. Regular servicing of the computer hardware and peripherals when due to prevent unforeseen breakdown.

4.5 Documentation

Documentation involves all the function performed by the system and how the system is to be used. Documentation describes how the program is used and it also clarifies any obscurities in the design. Documentation usually shows how to use the system, how to install and operate the system, system implementation and test procedure so that it may be maintained.

To initiate the program execution, we launch xampp, create a database and import the sql file to enable the application runs on local server. Then launch the browser (Google Chrome or Mozilla Firefox) then browse the file index. At this point, the content displays the admin login interface. On entering all the necessary detail, the browser takes him/her to corresponding web page. With the way the site is organized, one browses through all the available links without any hitch. And in order to capture and verify students, the admin has to launch the window-based version which was designed with C#.

To capture student fingerprint, the admin will enter the student’s name, the system automatically searches the database to know if the student’s name is valid. Then, the student will return the name and matriculation number of the student if name is found and then student fingerprint will be enrolled by placing his or her finger on the fingerprint scanner.

To verify and take student attendance, the admin will launch the windows-based version, then click on Time-in to verify and takes the student attendance while entering into the examination hall. The same procedure is applicable to Time-out.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary

This project; a software for Examination Attendance is developed after reviewing and analyzing the existing manual system at the investigation stage. The design is implemented using PHP, C# and MySQL was used for the database and the Integrated Development Environment (IDE) used was Bracket text editor, Visual Studio 2017 and XAMPP was used as the offline local server. The web application starts with login which contains Admin login, then the Home Page where Admin can click to view the various menus on the Dashboard.

5.2 Conclusion

The Automated Examination Attendance System based on fingerprint recognition is developed and tested using the appropriate necessary programming languages, tools and technology that fully meets the objectives of the system which has been developed. The system has reached a steady state where all bugs have been eliminated. The system is operated at a high level of efficiency, the admin and students associated with the system understands its advantage. The system solves the problem it was intended to solve as requirement specification.

5.3 Recommendations

As a result of the findings made during the analysis and design stages of this research work, in order to improve the effectiveness of the system to its greater height and full potential, it is recommended that the following features should be added for future expansion of this project.

- E- Learning (Virtual Classes)
- A website for student forums
- Online Tutorial Classes
- Online Quiz/Exams
- Admin should be able to generate report for both absentees and students present in class

- Admin should be able to generate report for each course

For the effective usage of this system and to have good management of it, it is necessary to provide computer to the various registration/examination centers and staff should be trained to acquire knowledge on how to use the computer and new system to meet global standard and modern challenges of information technology. More importantly, this system should be used in various tertiary institutions to curb examination impersonation.

REFERENCE

Afsana, A., Mohammed I. and Hassan B., (2012) “Low Complexity Iris Recognition Using Curvelet Transform” in the preceding of International Conference on informatics, Electronics & Vision held in the year 2012, pp.548-553.

Penny K. (2002) *“Iris Recognition Technology for Improved Authentication”* SANS Security Essentials Practical Assignment, version 1.3 SANS Institute.

Sabarigiri, B., and Karthikeyan T. (2012) “Acquisition Of Iris Images, Iris Localization, Normalization, And Quality Enhancement For Personal Identification” *in the International Journal of Emerging Trends & Technology in Computer Science,* ISSN 2278-6856, pp 274-275, Volume 1.

Jain S., Bhadauria S.S, Jadon R.S (2008). Biometric: Case Study, *Journal of Global Research in Computer Science, (JGRCS) ISSN -2229-371X, Volume 2, No. 10.*

R00d J and Hormak, U (2008). Addressing Impersonation Threats in Online Assessment Environment Using Temporal Information and System. *Interactions Merit Research Journal of Education and Review, Vol. 3(6), pp.215-220.*

Sachin T, Miss. Pranjali B, Miss. Pooja G, Miss. Priyanka S, Miss. Rutuja W. (2015). Direct Indirect Human Computer Interaction Based Biometrics. *International Journal of Emerging Engineering Research and Technology Volume 3, Issue 3, March 2015.*

Hevner, A. R. (2005). A three-cycle view of design science research. *Scandinavian journal of information systems*, *19*(2), 4.

https://arcjournal.com (October, 2022)

https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/

https://studymafia.org/biometrics-seminar-and-ppt-with-pdf-report-2/ (July 13, 2022)

Recfaces W. (2021). What Is Biometric Security and Why Does It Matter Today? https://recfaces.com/articles/biometric-security.

Wayman, U. J (2004). "An FPGA-based architecture for real time image feature extraction,", Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference, Print ISBN: 0- 7695-2128-2, pp. 801-804 Vol. 1, 23-26.

Christine, K. and Modi, V.K. (2008). *“Reconfigurable computing systems.",* Proceedings of the IEEE, ISSN: 0018-9219, vol. 90, issue.7, pp.1201-1217.

Kadry, D. and Smaili S. (2010) “An Iris Matching Algorithm for Reliable Person Identification Optimized Level of Decomposition” in the preceding of International Conference on Computing, Electronics and Electrical Technologies held in the year 2012, pp. 1073-1076.

Hormer, A. J and Schell B.A (2012) “Accurate Iris Location Based on Region of Interest” in the preceding of IEEE International Conference on Biomedical Engineering and Biotechnology held in the year 2012, pp 704-707, volume 12.

APPENDIX I: BACKEND SOURCE CODE

```
<?php include 'includes/session.php'; ?>
<?php include 'includes/slugify.php'; ?>
```

```
<?php include 'includes/header.php'; ?>
<body class="hold-transition skin-blue sidebar-mini">
<div class="wrapper">

  <?php include 'includes/navbar.php'; ?>
  <?php include 'includes/menubar.php'; ?>

  <!-- Content Wrapper. Contains page content -->
  <div class="content-wrapper">
    <!-- Content Header (Page header) -->
    <section class="content-header">
      <h1>
        Dashboard
      </h1>
      <ol class="breadcrumb">
        <li><a href="#"><i class="fa fa-dashboard"></i> Home</a></li>
        <li class="active">Dashboard</li>
      </ol>
    </section>

    <!-- Main content -->
    <section class="content">
      <?php
        if(isset($_SESSION['error'])){
          echo "
            <div class='alert alert-danger alert-dismissible'>
              <button type='button' class='close' data-dismiss='alert' aria-hidden='true'>&times;</button>
              <h4><i class='icon fa fa-warning'></i> Error!</h4>
              ".$_SESSION['error']."
            </div>
          ";
          unset($_SESSION['error']);
        }
        if(isset($_SESSION['success'])){
          echo "
            <div class='alert alert-success alert-dismissible'>
              <button type='button' class='close' data-dismiss='alert' aria-hidden='true'>&times;</button>
              <h4><i class='icon fa fa-check'></i> Success!</h4>
              ".$_SESSION['success']."
            </div>
          ";
          unset($_SESSION['success']);
        }
      ?>
      <!-- Small boxes (Stat box) -->
      <div class="row">
        <div class="col-lg-3 col-xs-6">
          <!-- small box -->
          <div class="small-box bg-aqua">
            <div class="inner">
               <?php
                $sql = "SELECT * FROM students";
                $query = $conn->query($sql);

                echo "<h3>".$query->num_rows."</h3>";
              ?>

              <p>No. of Registered Students</p>
            </div>
            <div class="icon">
              <i class="fa fa-tasks"></i>
            </div>
            <a href="students.php" class="small-box-footer">More info <i class="fa fa-arrow-circle-right"></i></a>
          </div>
        </div>
        <!-- ./col -->
        <div class="col-lg-3 col-xs-6">
          <!-- small box -->
          <div class="small-box bg-green">
            <div class="inner">
             <?php
                $sql = "SELECT DISTINCT EmpCNIC FROM finger";
                $query = $conn->query($sql);

                echo "<h3>".$query->num_rows."</h3>";
              ?>
```

APPENDIX II: USER INTERFACE SOURCE CODE

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using MySql.Data.MySqlClient;
using System.IO;

namespace ExamAttenBasedFingerprintRecog
{
    public partial class Clock_In : Form
    {
        //MySqlDataReader rdr = null;
        DataTable dtable = new DataTable();
        //MySqlConnection con = null;
        //MySqlCommand cmd = null;
        DataTable dt = new DataTable();
        MySqlConnection con = new MySqlConnection("SERVER=localhost; DATABASE=biostudent_attendance;
userid=root; PASSWORD=; PORT=3306;");
        MySqlConnection con3 = new MySqlConnection("SERVER=localhost; DATABASE=biostudent_attendance;
userid=root; PASSWORD=; PORT=3306;");
        MySqlConnection con2 = new MySqlConnection("SERVER=localhost; DATABASE=biostudent_attendance;
userid=root; PASSWORD=; PORT=3306;");
        MySqlConnection con4 = new MySqlConnection("SERVER=localhost; DATABASE=biostudent_attendance;
userid=root; PASSWORD=; PORT=3306;");

        public Clock_In()
        {
            InitializeComponent();
        }

        //private void Clock_In_Shown(object sender, EventArgs e)
        //{
        //    ClockIn();
        //    gridView();
        //}

        #region fill to Datagrid view
        //public void gridView()
        //{
        //    MySqlCommand cmd = new MySqlCommand("select StudentName as'Student Name', CourseCode as'Course
Code', Semester as'Semester',Date,TimeIn,TimeOut,Status From Attendance", con4);
        //    try
        //    {
        //        con4.Open();
        //        MySqlDataAdapter da = new MySqlDataAdapter();
        //        da.SelectCommand = cmd;
        //        DataTable dt = new DataTable();
        //        da.Fill(dt);
        //        BindingSource bs = new BindingSource();
        //        bs.DataSource = dt;
        //        dataGridAttendance.DataSource = dt;
        //        da.Update(dt);
        //        con4.Close();
        //    }
        //    catch (Exception ex)
        //    {
        //        MessageBox.Show(ex.Message);
        //    }
        //}
        #endregion

        private void Clock_In_Load(object sender, EventArgs e)
        {
            //Get Data from GetCourse form
            txtCourseCode.Text = GetCourse.GetCourseCode;
            txtCourseTitle.Text = GetCourse.GetCourseTitle;
            txtSemester.Text = GetCourse.GetSemester;

            try
            {

                if (!(txtStaff_ID.Text.Equals("")))
                {
                    MySqlConnection con = new MySqlConnection("SERVER=localhost; DATABASE=biostudent_attendance;
userid=root; PASSWORD=; PORT=3306;");
                    con.Open();

                    string strcom = "select name, photo from students where regno='" + txtStaff_ID.Text + "'";
                    MySqlDataAdapter daDetails = new MySqlDataAdapter(strcom, con);
                    DataSet dsDetails = new DataSet();
                    daDetails.Fill(dsDetails);

                    if (dsDetails.Tables[0].Rows.Count > 0)
                    {
                        txtStaff_Name.Text = dsDetails.Tables[0].Rows[0][0].ToString();
                        //txtJobTitle.Text = dsDetails.Tables[0].Rows[0][1].ToString();


                        //MemoryStream ms = new MemoryStream((byte[])dsDetails.Tables[0].Rows[0]["Picture"]);
                        //pix.Image = new Bitmap(ms);

                    }

                    MySqlDataAdapter dpt = new MySqlDataAdapter(strcom, con);
                    DataSet ds = new DataSet();
                    dpt.Fill(ds);
                    if (ds.Tables[0].Rows.Count > 0)
                    {
                        string imagePath = @"C:\xampp\htdocs\ExaminationAttendanceBasedFingerprintRecog\images\" +
dsDetails.Tables[0].Rows[0]["photo"].ToString();

                        txtImg.Text = imagePath;

                        pix.Image = new Bitmap(txtImg.Text);

                    }

                    con.Close();

                }
                else
                {

                    MessageBox.Show("ID can't be Empty!", "Fingerprint Enrollment", MessageBoxButtons.OK,
MessageBoxIcon.Warning);
                }

                ClockIn();
                //gridView();
            }
            catch (Exception ex)
            {
                MessageBox.Show(ex.Message);

            }

        }
```