DESIGN AND IMPLEMENTATION OF ACCESS CONTROL EXAMINATION ATTENDANCE SYSTEM BASED ON FACE RECOGNITION

BY

OGUNBODELE PATRICK	**ICT/2252070395**
BAMIDELE ADESUWA	**ICT/2252070626**
IDUYE LUCKY MARCUS	**ICT/2252070348**
BELLO PEDRO	**ICT/2252560043**

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. IGBAPE E.M.

NOVEMBER, 2022

CERTIFICATION

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

OGUNBODELE PATRICK	**ICT/2252070395**
BAMIDELE ADESUWA	**ICT/2252070626**
IDUYE LUCKY MARCUS	**ICT/2252070348**
BELLO PEDRO	**ICT/2252560043**

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. IGBAPE E.M. **DATE**
(Project Supervisor)

_____ _____

MR. SYLVESTER 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

Our sincere gratitude goes to God almighty for seeing us through the course of this work may His name be praise forever more.

Our profound gratitude to our amiable and intelligent supervisor **Dr. Igbape E.M.** for his guidance and encouragement to this research work, may God bless you richly bless you sir.

Our sincere gratitude goes to our Head of Department Mr. **Mr. Sylvester akhetuamen** for his unwavering advice to improve our learning and also special thanks goes to every lecturers in the Department of Computer Science, Federal Polytechnic, Auchi – Dr. Chette F.C., Mr. Okumagbe S.E., Mr. Bayo Adedeji, Mr. Omoregie K.O., Mr. Abass Aliu and the entire academic staff of this great Department.

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

TABLE OF CONTENTS

ABSTRACT

The main purpose of this project is to build a face recognition-based access control attendance management system for educational institution to enhance and upgrade the current attendance system into more efficient and effective as compared to before. The current old system has a lot of ambiguity that caused inaccurate and inefficient way of taking attendance and granting students access into examination hall. Many problems arise when the authority is unable to enforce the regulation that exist in the old system. The technology working behind will be the face recognition system. The human face is one of the natural traits that can uniquely identify an individual. Therefore, it is used to trace identity as the possibilities for a face to deviate or being duplicated is low. In this project, face databases will be created to pump data into the recognizer algorithm. Then, during the attendance taking session, faces will be compared against the database to seek for identity. When a student is identified, access will be granted and its attendance will be taken down automatically saving necessary information into an excel sheet. More significantly, this system should be used in various tertiary institutions to curtail examination impersonation.

Keywords- Examination, Face Recognition, OpenCV, Numpy, Access Control

CHAPTER ONE

INTRODUCTION

1.1 Background of the study

According to Advance learners' Dictionary, access is the right to obtain or make use of or take advantage of something (as services or membership) or a code (a series of characters or digits) that must be entered in some way (typed or dialed or spoken) to get the use of something (a telephone line or a computer or a local area network etc.)

Generally, access is seen as the ability to use, alter, or display something through a computer resource(s). A Control According to Advance learners' Dictionary, a standard against which other conditions can be compared in a scientific experiment or lessen the intensity of; temper; hold in restraint; hold or keep within limits. A system is a group of independent but interrelated elements comprising a unified whole or a complex of methods or rules governing behavior.

Therefore, Access Control System using the Face recognition is a kind of system created to manage, control, monitor, and sanitize the usage of a resource either physically or technologically (digitally).

Access controls guarantee all complete access to objects which is allowed, by managing data and programs such as reading, modifying and deleting, Access control protects against malicious attacks to privacy, authenticity and availability of the system. Computer security and the likes have been, and will continue to be the biggest issue in the IT (Information technology) world (Ezenma A.A. et al., 2014). Access control has continued to adapt to growing IT-system applications. Access control was initially developed in multi-user and multi-level protected systems to protect sensitive data. This is to avoid unauthorized usage by unlawful users of machine resources and protect legal use the resources of the system. Access control system is intended to monitor

technical and technological tools using the Face Recognition in order to avoid unauthorized and improper disclosure of confidential resource(s) and malicious changes thus preserving access to control entities (users). Access control is defined as an essential security requirement in the IT sector (Adigwe P.K and Okoye P.V.C, 1998). Company has its own information management system that determines a collection of policies based on circumstances where customers are able to access all or some of the program's resources. Achieving these Resources security policies are important. Access control focuses on authentication and potency, password-based securities, potentialities and access control list (ACLs), multilateral and multi-level securities. In this proposed work we try to introduce solution, help life to be easier and smarter. The home accessing one of the main Jobs we do every day even as people may forget their keys or forget to lock their homes and many security issues are related to who want to access the home. Our contribution is to propose a solution to enable the homeowners to do many Jobs related to the home Door using their mobile Application called smart access control system. The solution utilizes the face recognition system to identify the authorized people face in order to allow them to access their home like young people or home owners who forget their keys.

It is an established fact that every resource(s) needs or requires an access, but the challenge over time has grown to become unauthorized persons still gaining access to such resource even at the presence of some manual security checks and off course it is harmful and constitutes threat to data security, confidentiality and integrity of such resources. The insecurity breaches are constantly on the increase, especially in the cyber space form the background of this research in order to assuage this very important challenging issues which is a threat to the information and technology world. We there look forward to creating a system that will take over access controlling

through granting and denier of individuals using Face Recognition based on the stored instruction and data.

1.2 Statement of the problem

Research carried out in Federal Polytechnic, Auchi shows that manual access granting to homes, offices, cyber space, etc. is threat to resource security as unauthorized access is gained by malicious individual thereby leading to destruction(s) of valuable items. The conventional manual method of granting access to students into examination hall is seen to lead to various problems which include unauthorized persons gaining access to examination hall (examination impersonation), unsecured authentication of students, stress and the system is also time consuming.

1.3 Aim and Objectives of the study

The main aim of this study is to develop an Access Control system for examination attendance based on face recognition that can be used in exam halls to verify or differentiate between a registered student and an imposter before entering the examination hall.

The study seeks to achieve the following objectives;

- To create a system that will enable the administrator to fetch out impersonators in the examination system using the methodology of face recognition biometrics.
- To reduce time-consumption, stress and rate of corruption in the educational sector.
- To show the possibility of computer technology in the satisfaction of human needs and also enforce strict security measures that ensure unregistered students do not write exams for other registered students.

1.4 Significance of the study

It is an established fact that every resource(s) needs or requires an access, but the challenge over time has grown to become unauthorized persons still gaining access to such resource even at the presence of some manual security checks. The significance of this study is to design and implement an Access Control System Based on Face Recognition for taking examination attendance. The study will strengthen both physical and cyber security and ensures that the integrity of files and attendance is achieved without any form of compromised. Also, it will be highly informative, protective and defensive as possible being able to recognize and the registered students of the institution and reject or deny unrecognized impersonated students through the generation (capturing) of students' face and matching them for decision through the face recognition device and stored instructions. Hence, impersonation which has eaten the educational system thereby encouraging laziness among students would be eliminated.

1.5 Scope of the study

The main scope of this project is to replace the manual current method of granting students access into examination hall and taking attendance by an Access Control Examination Attendance System Based on Face Recognition which will be more efficient.

1.6 Research Methodology

Good systems engineering begins with a clear understanding of the context, the world view and then progressively narrows until technical detail is achieve (Pressman, R. 2005).

The research methodology adopted in this work is design science approach (Hevner et. al, 2004; March and Smith, 1995). In this approach, the first step is to identify the existence of a problem that requires viable solution.

- 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.
- A review of related literature was carried out on the established research domain of interest such as research journals, product manuals, books and related technical materials.
- Key concepts were identified, defined, and research objectives written
- Thereafter, a case study was selected using Examination Centre to establish the technical feasibility of the deployment of biometric attendance system based on face recognition to provide solution to the established real-life problem.

1.7 Definition of Terms

Access Control: Access control is a security technique that regulates who or what can view or use resources in a computing environment.

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

Facial Recognition: This 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 Biometric

The word 'Biometric' is a two sections terminology, is taken from the Greek word, of which 'Bio' means life and 'Metric', mean measure. By combining these two words, 'Biometric' can be defined as the measure (study) of life, which includes humans, animals, and plants "Biometric

technologies” defined as an automated methods of verifying or recognizing the identity of a living by definition, there are two key words in it: “automated” and “person”. The word “automated” differentiates biometrics from the larger field of human identification science. Biometric authentication techniques are done completely by machine, generally (but not always) a digital computer. The second key word is “person”. Statistical techniques, particularly using fingerprint patterns, have been used to differentiate or connect groups of people or to probabilistically link persons to groups, but biometrics is interested only in recognizing people as individuals. All of the measures used contain both physiological and behavioral components, both of which can vary widely or be quite similar across a population of individuals (Sambita D. & Tapasmini S., 2012). No technology is purely one or the other, although some measures seem to be more behaviorally influenced and some more physiologically influenced.

A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic" (Bondalapati K. & Prasanna V.K. 2002). A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below:

Identification - One to Many: Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database.

Verification - One to One: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans Iris recognition or can grant access to a bank account at an ATM by using retinal scan.

Biometric authentication requires to compare a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (Capture, Process, Enroll) followed by a Verification or Identification process.

During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner or video camera. The second phase of processing is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed biometric identifier record (sometimes called biometric sample or biometric template) (Yan Li *et al.*, 2012). Next phase does the process of enrollment. Here the processed sample (a mathematical representation of the biometric - not the original biometric sample) is stored / registered in a storage medium for future comparison during an authentication. In many commercial applications, there is a need to store the processed biometric sample only. The original biometric sample cannot be reconstructed from this identifier. Due to the reliability and nearly perfect recognition rates of Biometric methods; it becomes reliable and secure identification of people. Many biometric-based identification systems have been proposed such as: fingerprint, face recognition, facial expressions, voice, iris recognition, etc. as shown in Fig. 2.1. For this purpose, these methods based on physical or behavioral characteristics are of interest because people cannot forget or lose their physical characteristics.

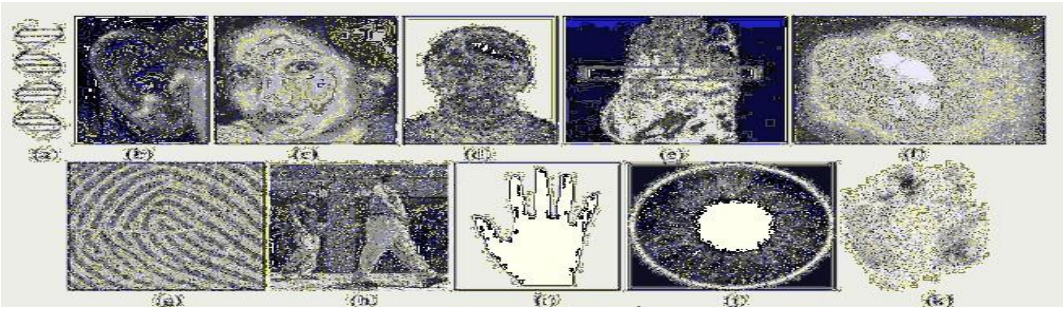


Figure 2.1: Showing Biometric Characteristics
(A_project_report_on_iris_recognition_sys%20(1) By MOHD NASRULLAH KAZMI (14DET50) MOHD FAIZ (12ET77),pp(10))

2.2 Biometric History

The science of using humans for the purpose of identification dates back to the 1875 and the measurement system of Alphonse Bertillon. Bertillon's system of body measurements, including skull diameter and arm and foot length, was used in the USA to identify prisoners until the 1925. Before that William Herschel and Sir Francis Galton proposed quantitative identification through fingerprint and facial measurements in the 1880s. The development of digital signal processing techniques in the 1960s led immediately to work in automating human identification. Speaker and fingerprint recognition systems were among the first to be applied. The potential for application of this technology to high-security access control, personal locks and financial transactions was recognized in the early 1960s. The 1970s saw development and deployment of hand geometry systems, the start of large-scale testing and increasing interest in government use of these automated personal identification technologies. Then, Retinal and signature verification systems came in the 1980s, followed by face systems. Lastly, Iris recognition systems were developed in the 1990s.

2.3 Biometric Concepts

A number of biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires that the biometric characteristics satisfy the following characteristics.

Universal: Every person must possess the characteristic/attribute. The attribute must be one that is universal and seldom lost to accident or disease.

Invariance of properties: They should be constant over a long period of time. The attribute should not be subject to significant differences based on age either episodic or chronic disease.

Measurability: The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.

Singularity: Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are all attributes that are unique assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.

Acceptance: The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body.

Reducibility: The captured data should be capable of being reduced to a file which is easy to handle.

Reliability and tamper-resistance: The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.

Privacy: The process should not violate the privacy of the person.

Comparable: Should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.

Inimitable: The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

2.3.1 Operating Mode

Depending on the application context, a biometric system may operate in two modes: verification mode or identification mode. In the verification mode, the system verifies the identity by comparing the presented biometric trait by a stored biometric template in the system (one-to-one). If the similarity is sufficient according to some similarity measure, the user is accepted by the

system. In such a system, an individual who desires to be recognized claims an identity, usually via a Personal Identification Number (PIN), a user name, or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "Does this biometric data belong to this person (x)?"). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

In the identification mode, database search is crucial and needed. A user presents a not necessarily known sample of his/her biometrics to the system. This sample is then compared with existing samples in a – central - database (one-to-many). Identification is a critical component in negative recognition applications, where the system establishes whether the person is who he/she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

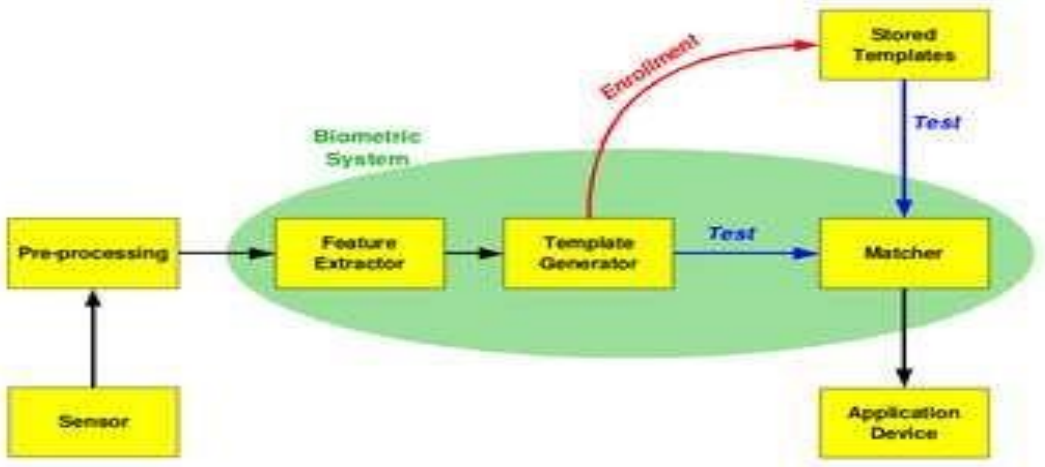


Figure: 2.2 Components of Biometric System

(A_project_report_on_iris_recognition_sys%20(1) By MOHD NASRULLAH KAZMI(14DET50) MOHD FAIZ (12ET77), pp13)

2.4 Commonly Used Biometrics Characteristic

A number of biometric characteristics exist and in use each biometric has its strengths and weaknesses, and the choice depends on the application. In other words, no biometric is "optimal" however the iris recognition is seen as a more secured biometric authentication verification system, a brief introduction to the commonly used biometrics is given below.

2.4.1 Physiological Characteristic Biometrics

- Facial, hand, and hand vein infrared thermogram, A pattern of radiated heat from human body considers a characteristic of an individual. These samples of patterns can be captured by an infrared camera in an unobtrusive manner like a regular (visible spectrum) photograph. The technology could be used for covert recognition.
- Ear many researchers suggested that the shape of the ear to be a characteristic. Studying the structure of the approaches is based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.
- Fingerprint, A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal creation. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high.
- Retina, since the retina is protected in an eye itself, and since it is not easy to change or replicate the retinal vasculature; this is one of the most secure biometric. Retinal recognition creates an eye signature from the vascular configuration of the retina, which is

supposed to be a characteristic of each individual and each eye, respectively (Jang-Hee Yoo *et al.*, 2014).

2.4.2 Behavioral Characteristic Biometrics

- Gait, Basically, gait is the peculiar way one walks and it is complex spatio-temporal biometrics. This is one of the newer technologies and is yet to be researched in more detail. Gait is a behavioral biometric and may not remain the same over a long period of time, due to change in body weight or serious brain damage. Acquisition of gait is similar to acquiring a facial picture and may be an acceptable biometric.
- Keystroke, it is noticed that each person types on a keyboard in a characteristic way. Keystroke dynamics is a behavioral biometric for some individuals, one may expect to observe large variations in typical typing patterns

Technology	Accuracy	Cost	Social Acceptability	Devices
DNA	High	High	High	Lab Test Equipment
Iris	High	High	Medium-Low	Camera
Face	Medium-Low	Medium	Low	Camera
Voice	Medium	Medium	Medium	Microphone
Finger Print	High	Medium	High	Scanner
Hand Gesture	Medium-Low	Low	Medium	Scanner
Signature	Low	Medium	High	Optical Pen

Figure 2.3: Comparison of Different Biometric Technique
(a_project_report_on_iris_recognition_sys%20(1), by MOHD NASRULLAH KAZMI (14DET50) MOHD FAIZ (12ET77), pp14).

2.5 Biometric Technology

A biometric framework gives automatic recognition of an individual based on certain unique characteristics or feature possessed by them. Biometric frameworks have been developed based on fingerprints, facial elements, voice, hand geometry, handwriting, the retina, and the iris. The biometric framework works by:

- Capturing a specimen of unique feature
- Transforming the specimen using couple of numerical models into biometric layout.
- This biometric format will provide a standardized, efficient and profoundly segregating portrayal of feature.
- Comparison with other layouts to determine identity.

A decent biometric is described by utilization of an element that is; thoroughly unique – so that the possibility of any two individual having a similar characteristic will be insignificant, immutable so that the feature remains unfluctuating over the period of time, and be adequately obtained so as to provide suitability to the user, and avert dispersion of the feature (Jang-Hee Yoo *et al.*, 2007).

2.5.1 The Human Iris

Iris is the pigmented region of the eye. It is a circular sinewy diaphragm separating the two regions of the eye. It extends from ciliary muscle across the eyeball in front of the lens. It has a small circular aperture in the middle through which the light enters the eye, which is called pupil. The iris controls the amount of light entering the eye by contracting or relaxing the eye muscle, and hence contracting or dilating the pupil.

2.5.2 Iris

The particular pattern in the iris region is formed during the elementary term of life, and stromal pigmentation occurs in the following couple of years. The incidental process of formation of the

unique patterns of the iris is not related to any genetic factors. The only characteristic that depends on ancestral genes is the pigmentation of the iris, giving eye its color. As a result, leading to an autonomously independent pattern of the two eyes of an individual (Bariamis D. et al., 2004). Furthermore, identical twins acquire non-germane iris patterns.

Image processing frameworks can be used unique feature and pattern extraction along with converting it into the biometric template from the digital image of the eye, which can be later stored in the database. This biometric template contains a physical-mathematical representation of the unique information stored in the iris and allows comparisons to be made between models (Sambita D. & Tapasmini S. 2012). When a client prefers to be distinguished and identified by an

2.8 Levels of Access Controls

Access controls at different levels in a system. Access control works at a number of levels, as described in the following:

- The access control mechanisms, which the user sees at the application level, may express a very rich and complex security policy. A modern online business could assign staff to one of dozens of different roles, each of which could initiate some subset of several hundred possible transactions in the system. Some of these (such as credit card transactions with customers) might require online authorization from a third party while others (such as refunds) might require dual control.
- The applications may be written on top of middleware, such as a database management system or bookkeeping package, which enforces a number of protection properties. For example, bookkeeping software may ensure that a transaction that debits one ledger for a certain amount must credit another ledger for the same amount.

- The middleware will use facilities provided by the underlying operating system. As this construct's resources such as files and communications ports from lower-level components, it acquires the responsibility for providing ways to control access to them.
- Finally, the operating system access controls will usually rely on hardware features provided by the processor or by associated memory management hardware. These control which memory addresses a given process can access. As we work up from the hardware through the operating system and middleware to the application layer, the controls become progressively more complex and less reliable. Most actual computer frauds involve staff accidentally discovering features of the application code that they can exploit in an opportunistic way, or just abusing features of the application that they were trusted not to. But in this chapter, we will focus on the fundamentals: access control at the hardware and operating system level. Access control makes sense only in the context of a protection goal, typically expressed as a security policy. This puts us at a slight disadvantage when discussing PCs running single-user operating systems such as DOS and Win95/98, which have no overt security policy: any process can modify any data. People do have implicit protection goals, though; you don't expect a Security Engineering: A Guide to Building Dependable Distributed Systems 53 shrink-wrap program to trash your hard disk. So an explicit security policy is a good idea, especially when products support some features that appear to provide protection, such as login IDs. I mention one protection technique-sandboxing-later, but leave off a substantial discussion of viruses. In what follows, the focus will be on protection mechanisms for systems that support the isolation of multiple processes.

CHAPTER THREE

SYSTEM DESIGN AND ANALYSIS

3.1 System Study

We went through literature on biometrics, and also, we visited the various schools in Auchi Polytechnic 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 of accessing students into examination hall. We 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 permit which he or she can use to prove that he or she is eligible to sit for an exam), and unsecured method of accessing students are encountered in the manual authentication system. Hence, it is time-consuming.

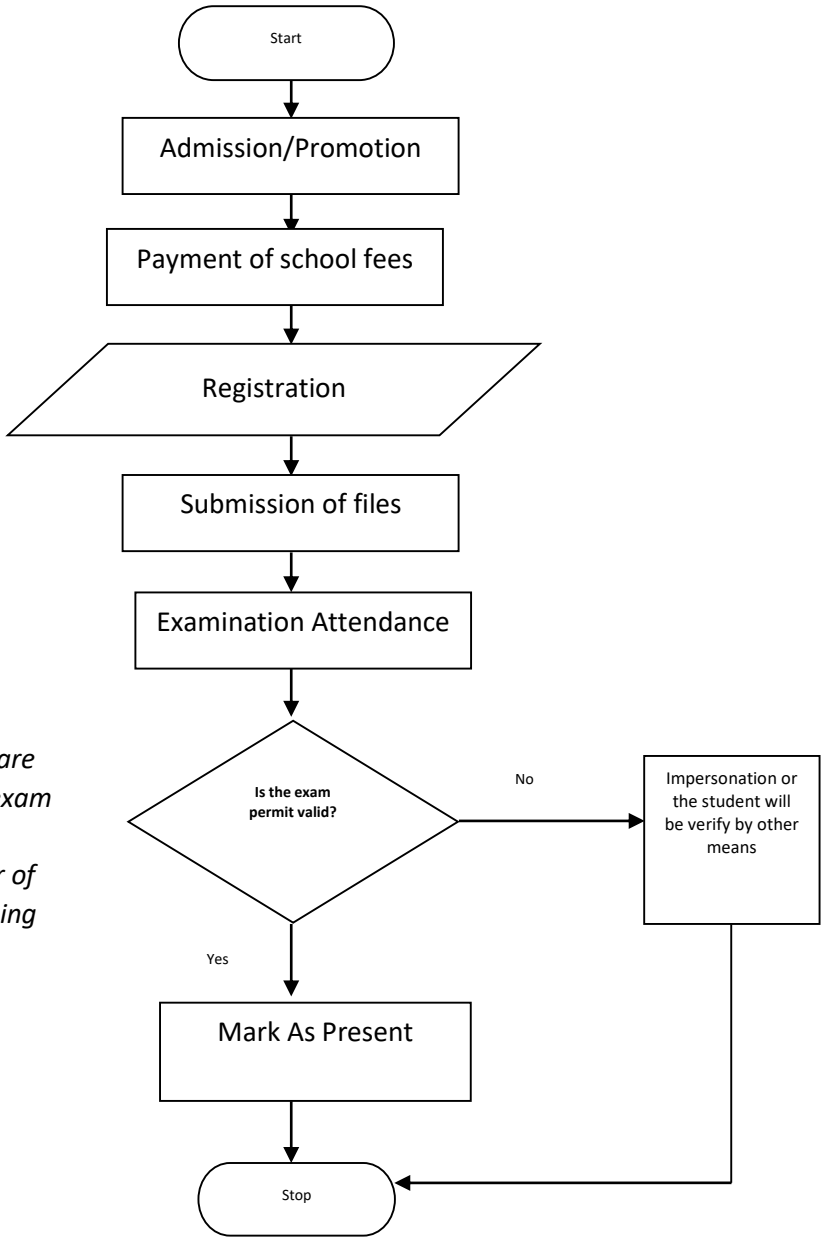
3.2 System Analysis

In the manual method of accessing students into examination hall, 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 in order to gain access into the exam hall. 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 examination impersonation
- The process of assessment 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



Access Control: students are verified by checking their exam ID whether the photo corresponds to the owner of ID. This method of accessing students is prone to impersonation

Access Control for Examination attendance:

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.

3.3 Design of the proposed system

This proposed system shall be use to handle the problems encountered in the current control mechanism of access control into examination hall using Manual student's identity card (ID card) check with the face recognition technology as it seeks to present more security trust. The system will help reduced the security bridges in the current access control methods with a replacement with the face technology. The proposed system provides solution to examination impersonation problems through the use of interacting software that is interfaced to a face recognition device. The student bio-data (Matriculation number, Name, Gender and Date of Birth) and the face are enrolled first into the database. The face is captured using a face recognition device. For examination, the student will look directly to the face recognition device and the attendance is

taken by comparing the face with the previously stored and trained images 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 be facially by the system before entering for the exams. During the process of recognition, if a student that has not registered for the exams wants to impersonates, a matching template will show unknown and the student will be apprehended as impersonator. The system is meant to permit only recognized students by their face recognition and doesn't allow non verified students.

3.3.1 Flowchart of the proposed system

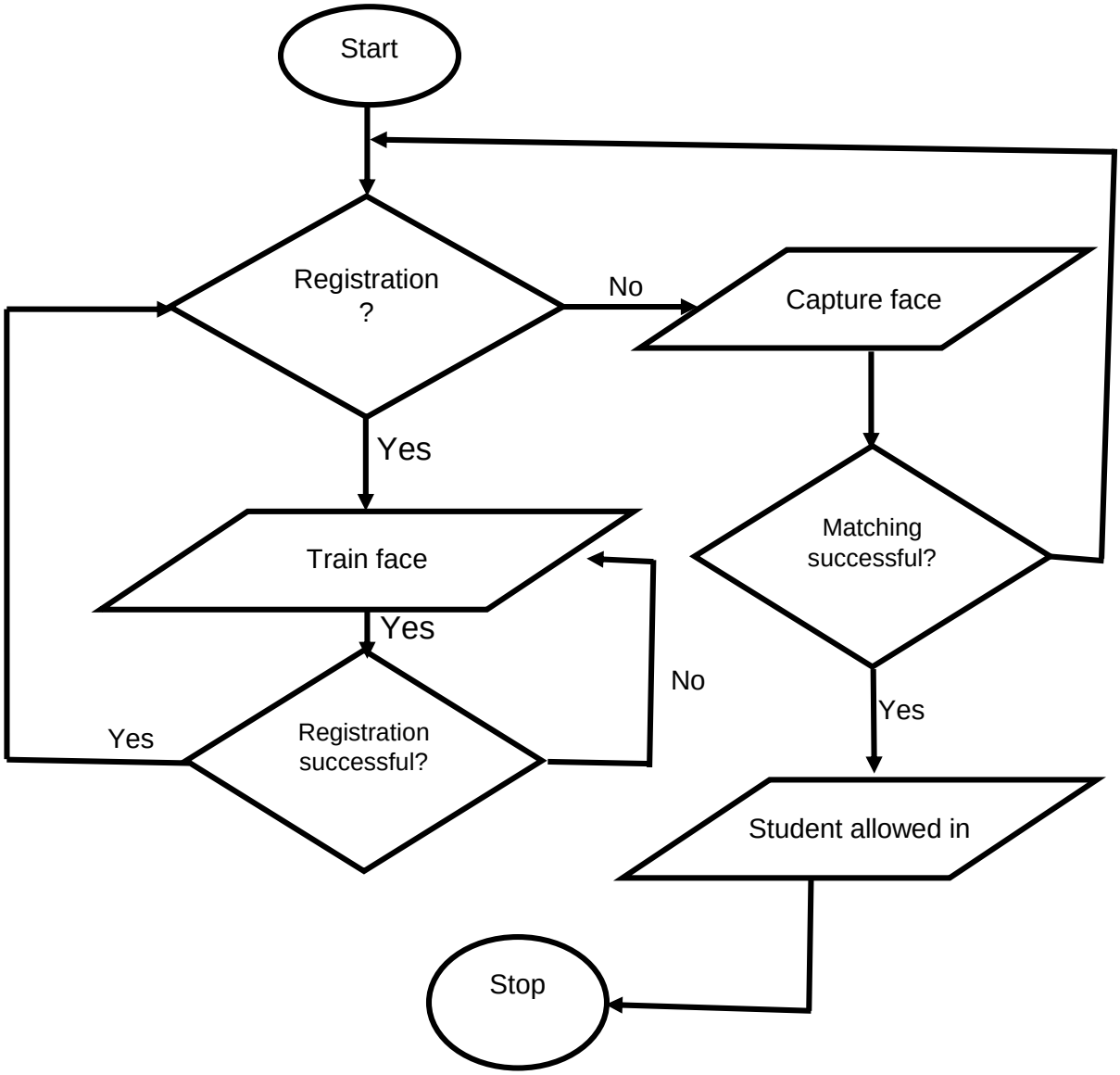


Figure 3.2: Flowchart of the proposed system

CHAPTER FOUR

IMPLEMENTATION AND TESTING

4.1 IMPLEMENTATION

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

4.1.1 Implementation Choices

The Access Control System for examination attendance based on face Recognition works as offline application system. It was implemented using Python, OpenCv and MySQL was integrated in the program for the database and the Integrated Development Environment (IDE) used was Visual Studio Code, Jupyter and Python IDE.

4.1.1.1 Python

Python is a popular programming language. It was created by Guido van Rossum, and released in 1991. Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation. Python is dynamically-typed and garbage-collected. It supports multiple programming paradigms, including structured, object-oriented and functional programming.

4.1.1.2 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.

4.1.1.3 OpenCV

OpenCV (Open Source Computer Vision Library) is an open source computer vision and machine learning software library. OpenCV was built to provide a common infrastructure for computer vision applications and to accelerate the use of machine perception in the commercial products. Being an Apache 2 licensed product, OpenCV makes it easy for businesses to utilize and modify the code. The OpenCV project was initially an Intel Research initiative to advance CPU-intensive applications, part of a series of projects including real-time raytracing and 3Ddisplay walls. The main contributors to the project included several optimization experts in Intel Russia, as well as Intel's Performance Library Team.

4.1.1.4 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.

Software Requirements

- Operating System — Windows 2007/2010/later versions\
- Database Server — MySQL
- IDE — Visual Studio code, Jupyter, Python IDLE
- Plugins (Extensions) — Numpy, OpenCV, Tkinter, Pandas, Flask

Hardware Requirements

- Computer — Desktop/laptop
- Intel Core i3 and above — 1.6 GHZ or above
- RAM Capacity — 8GB or above
- Hard Disk/SSD — 120GB or above
- Web Camera — Face Recognition

4.3 SAMPLE INTERFACES

Home Page: After launching the application, homepage will open which will allow admin to register students, check students' identity and navigate to his/her dashboard to check the number of registered students.

The home page window allows admin to

- Enroll new students into the system
- Captures students faces
- Train the captured images
- Check students' identity
- Manually fill attendance when necessary
- check the number of registered students in the database

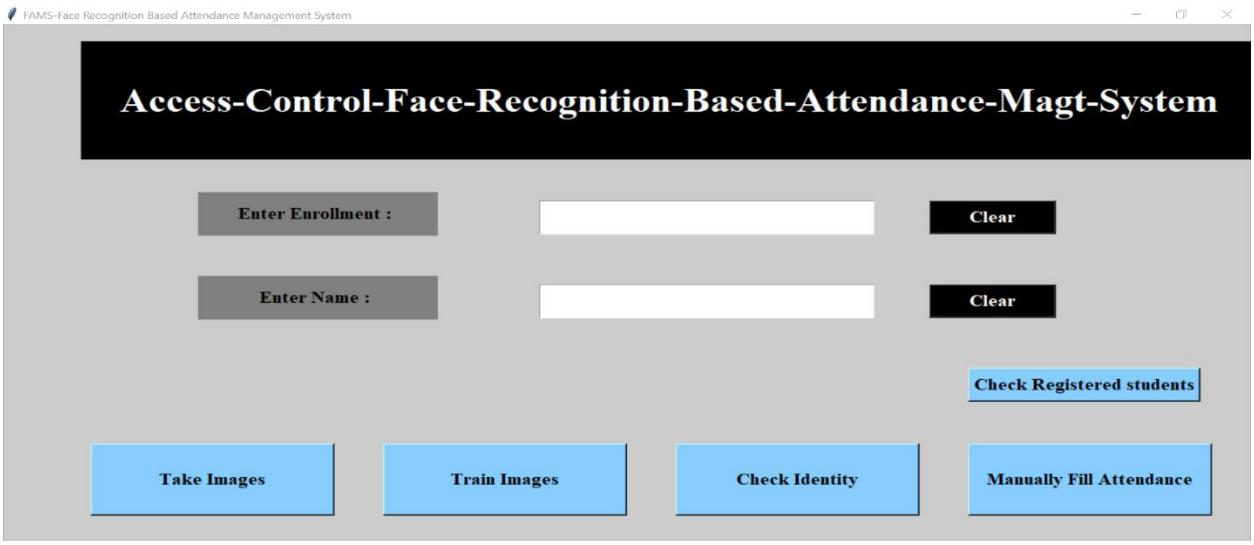


Figure 4.1: Program home page

Take Images: This enables the admin to captures student face during registration using the built-in camera of the laptop or through an external camera.

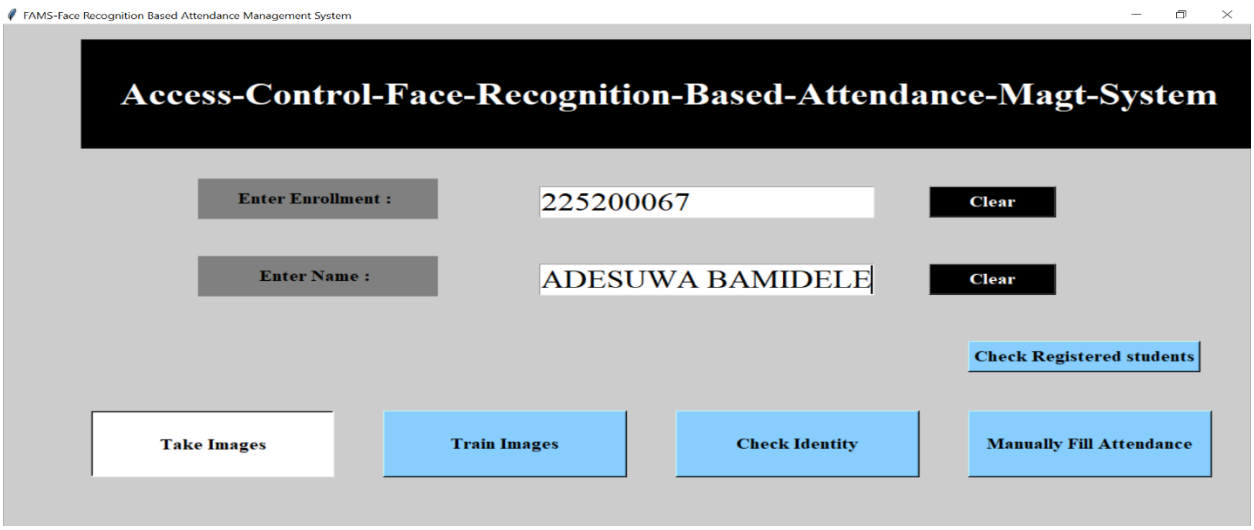


Figure 4.2: Take Image page

Train Images: This enables the admin to train the captured face to enhance easy identification. During registration, the admin will register a student by entering the digit in the matriculation number of the student and also enters the student's name, then captures his/her face.

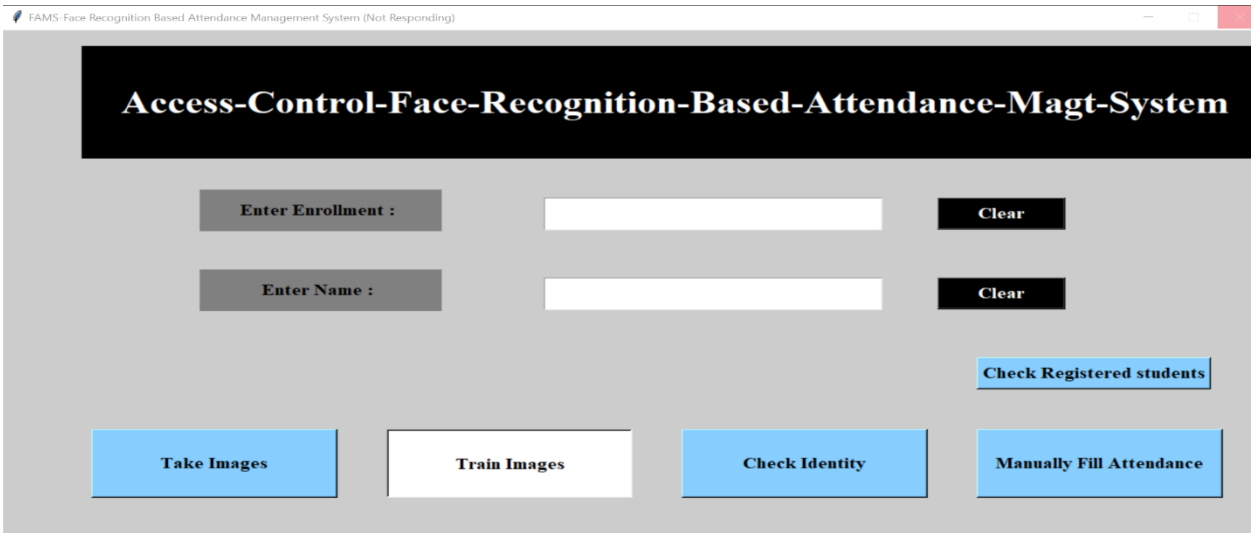


Figure 4.3: Train Image

Check Identity: With this, the admin can check and verify student identity before they are granted access into the examination hall to sit for an exam. In order to check student identity, the admin is expected to click on “check Identity” button, from the display window, enter the title of the course the student is to write and then click on “verify student identity” and wait while the system identifies the student. During identification, the student is expected to look directly to the camera, if the face matches with any of the faces stored and trained in the system, the student attendance will be taken automatically and he/she will be granted access to write the exam.

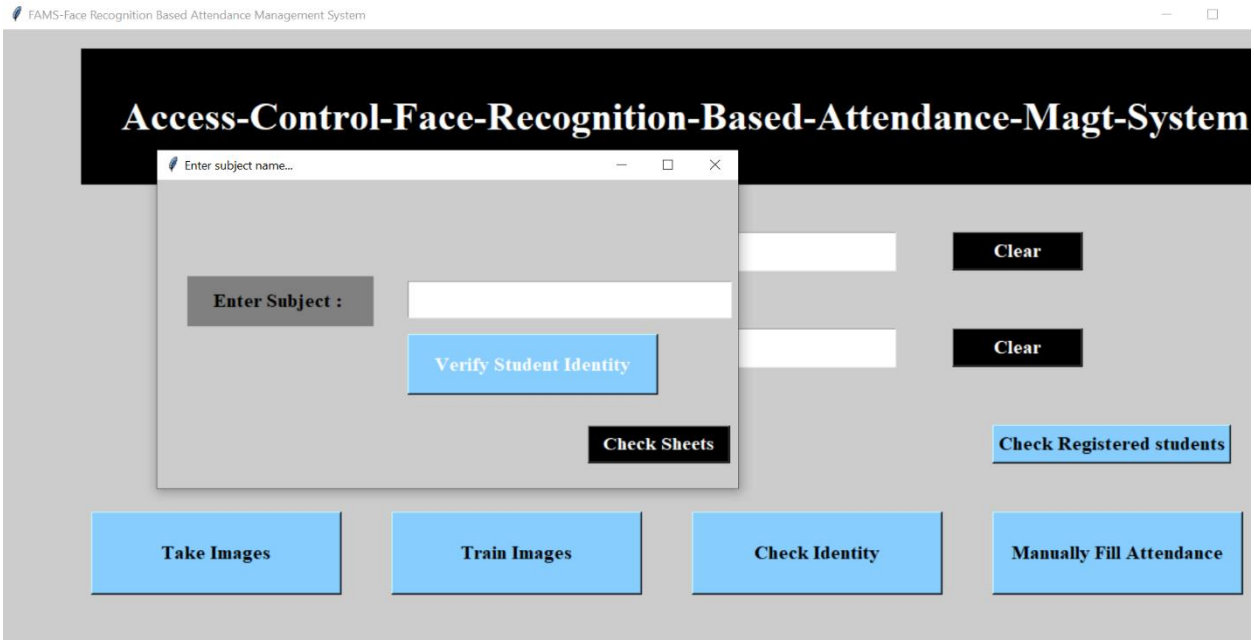


Figure 4.4: Check Identity

Manually Fill attendance: This enables the admin to fill attendance for a student manually when necessary.

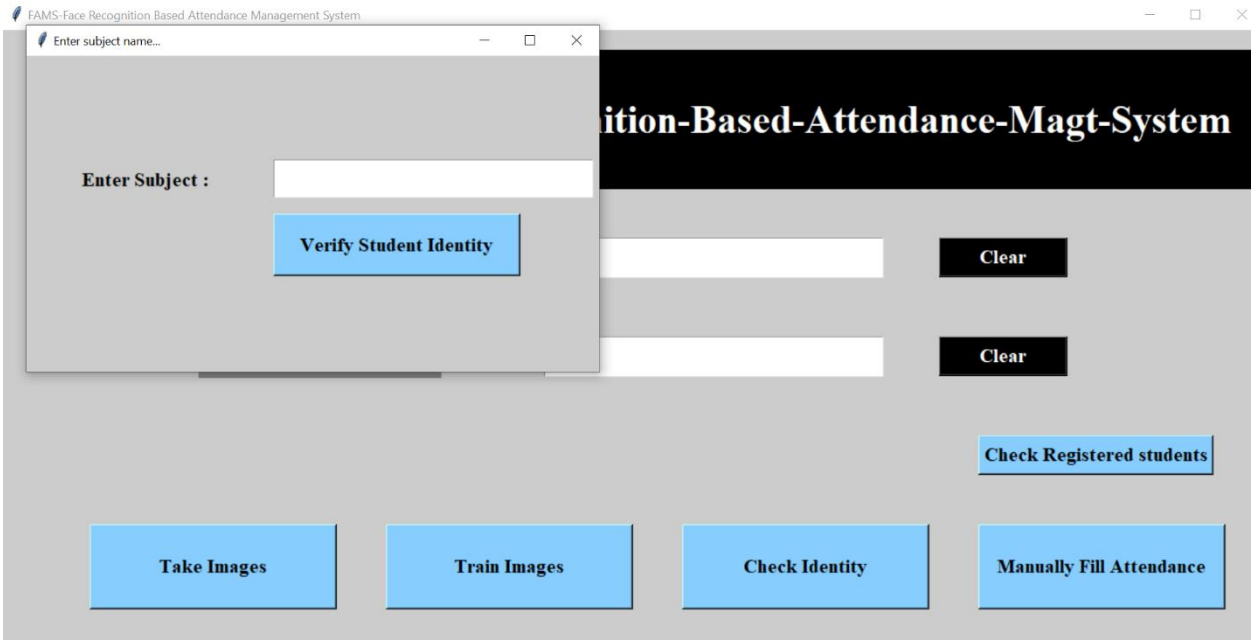


Figure 4.5: Manually fill attendance

Check Registered students: This allows the admin to view the total number of registered students and their information in the database. Here, the admin is expected to enter his/her username and password before he can gain access to the database.

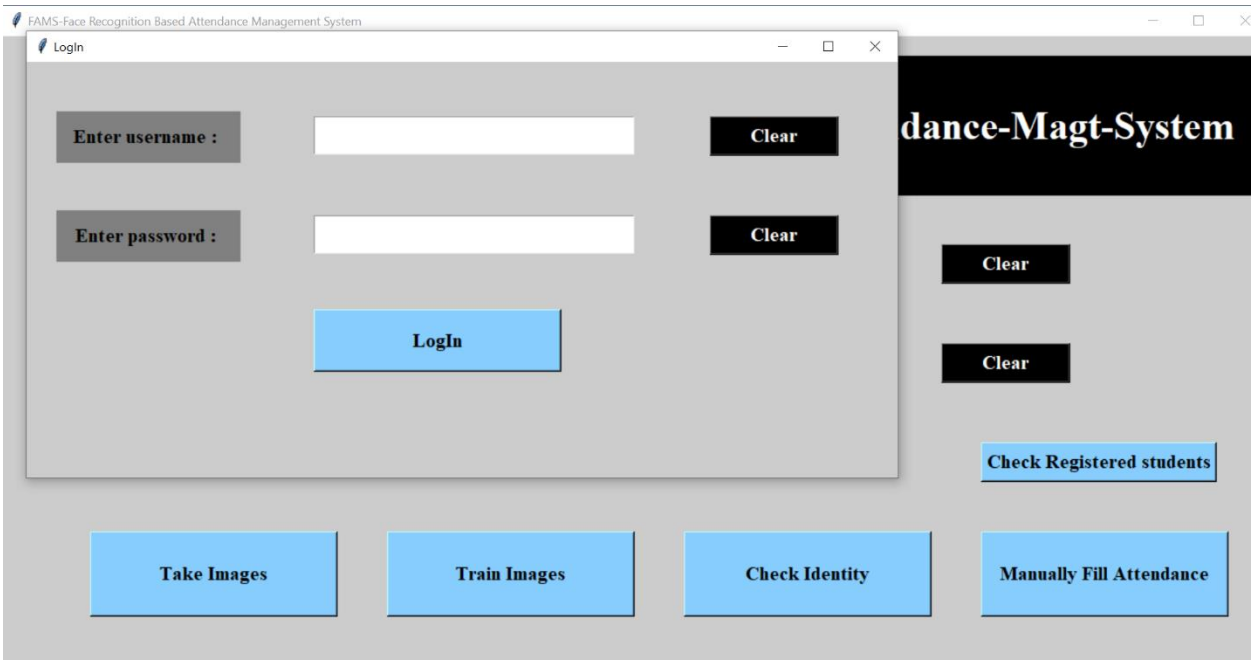


Figure 4.6: Check Registered students

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 SUMMARY

This paper studied an access control system using facial recognition. This project; a software for Examination Attendance is developed after reviewing and analyzing the existing manual system. The computational models, which were implemented in this project, were chosen after extensive research, and the successful testing results confirm that the choices made by the researcher were reliable. The design is implemented using Python and MySQL was integrated in the system for the database and the Integrated Development Environment (IDE) used was Jupyter, Visual Studio Code and Python IDLE.

5.2 CONCLUSION

Before the development of this project. There are many loopholes in the process of granting students access into examination hall and taking attendance using the manual method which caused many troubles to most of the institutions. Therefore, the facial recognition feature embedded in the attendance management system cannot only ensure attendance to be taken accurately and also eliminated the flaws in the previous system. By using technology to conquer the defects cannot merely save resources but also reduces human intervention in the whole process by handling all the complicated task to the machine. In this project, the face database is successfully built. Apart from that, the face recognizing system is also working well. At the end, the system not only resolve troubles that exist in the old model but also provide convenience to the user to access the information collected easily.

5.3 RECOMMENDATION

Through analysis of the data and research conducted for this study, in order to improve the efficacy of the system to its greater height and full potential, its recommended that the following features should be added for future expansion of this project.

- E- Learning (Virtual Classes)
- A website for student forums
- Online Quiz/Exams

More also, the system can be extended to a greater number of students with freedom to change list of students according to class changes, the system can be made more flexible to allow updating of templates in case student incurs significant amount of change in his facial features and the system can also be extended to allow better face recognition algorithm in which even rotational features of face can be detected efficiently. More significantly, this system should be used in various tertiary institutions to curtail examination impersonation.

REFERENCE

Adigwe P.K. and Okoye P.V.C (1998). Data Processing and Technique, (vol. 1) New York: Hafarier Publishing Co.

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.

Bariamis, D., Iakovidis, D. and Maroulis, D. (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.

Bondalapati, K. and Prasanna, V.K. (2002). *"Reconfigurable computing systems."*, Proceedings of the IEEE, ISSN: 0018-9219, vol. 90, issue.7, pp.1201-1217.

Ezenma, A.A, Emmanuel, B. and Choji D.N. (2014).Design and Implementation of Secured Result Processing System for Publish Secondary School in Nigeria". *Internal Journal of Computer and Information Technology,* Vol. 3(1).

Hevner, A.R., March, S.T., Park J. and Ram S. (2004). Design Science in Information Systems Research. MIS Quarter 28:75-105.

Jang-Hee Y., Jong-Gook K., Sung-Uk, J., Yun-Su C., Ki-Hyun K., Ki-Young M. and Kyoil C. (2007) "Design of an Embedded Multimodal Biometric System", Signal-Image Technologies and Internet- Based System, 2007. SITIS '07. Third International IEEE Conference on Shanghai, Print ISBN: 978-0- 7695-3122-9, pp. 1058 – 1062.

March, S.T. and Smith G. (1995). Design and Natural Science Research on Information Technology. *Desci. Support System,* 15:251-266.

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

Pressman, R. (2005). Software Engineering: A Practitioner's Approach, New York: McGraw-Hill.

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.

Sambita D. and Tapasmini S. (2012) "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.

Yan, L., Wen, L., Yide M. (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: SOURCE CODE

```
import tkinter as tk
from tkinter import *
import cv2
import csv
import os
import numpy as np
from PIL import Image, ImageTk
import pandas as pd
import datetime
import time

# Window is our Main frame of system
window = tk.Tk()
window.title("FAMS-Face Recognition Based Attendance Management System")

window.geometry('1280x720')
window.configure(background='grey80')

# GUI for manually fill attendance

def manually_fill():
    global sb
    sb = tk.Tk()
    # sb.iconbitmap('AMS.ico')
    sb.title("Enter subject name...")
    sb.geometry('580x320')
    sb.configure(background='grey80')
```

```
    def err_screen_for_subject():


        def ec_delete():
            ec.destroy()
        global ec
        ec = tk.Tk()
        ec.geometry('300x100')
        # ec.iconbitmap('AMS.ico')
        ec.title('Warning!!')
        ec.configure(background='snow')
        Label(ec, text='Please enter your subject name!!!', fg='red',
              bg='white', font=('times', 16, ' bold ')).pack()
        Button(ec, text='OK', command=ec_delete, fg="black", bg="lawn green", width=9,
height=1, activebackground="Red",
               font=('times', 15, ' bold ')).place(x=90, y=50)


    def fill_attendance():
        ts = time.time()
        Date = datetime.datetime.fromtimestamp(ts).strftime('%Y_%m_%d')
        timeStamp = datetime.datetime.fromtimestamp(ts).strftime('%H:%M:%S')
        Time = datetime.datetime.fromtimestamp(ts).strftime('%H:%M:%S')
        Hour, Minute, Second = timeStamp.split(":")
        # Creatting csv of attendance


        # Create table for Attendance
        date_for_DB = datetime.datetime.fromtimestamp(ts).strftime('%Y_%m_%d')
        global subb
        subb = SUB_ENTRY.get()
```

```
DB_table_name = str(subb + "_" + Date + "_Time_" +
                    Hour + "_" + Minute + "_" + Second)

import pymysql.connections

# Connect to the database
try:
    global cursor
    connection = pymysql.connect(
        host='localhost', user='root', password='', db='manually_fill_attendance')
    cursor = connection.cursor()
except Exception as e:
    print(e)

sql = "CREATE TABLE " + DB_table_name + """
              (ID INT NOT NULL AUTO_INCREMENT,
               ENROLLMENT varchar(100) NOT NULL,
               NAME VARCHAR(50) NOT NULL,
               DATE VARCHAR(20) NOT NULL,
               TIME VARCHAR(20) NOT NULL,
                  PRIMARY KEY (ID)
                  );
             """

try:
    cursor.execute(sql)  # for create a table
except Exception as ex:
    print(ex)  #
```