**AUTOMATED DOOR ACCESS SYSTEM WITH FACIAL RECOGNITION**

**BY**

**ADEUGA DANIEL ADEWUMI**

**13CJ015264**

**COMPUTER ENGINEERING**

**A PROJECT SUBMITTED TO THE DEPARTMENT OF ELECTRICAL AND INFORMATION ENGINEERING, COLLEGE OF ENGINEERING, COVENENT UNIVERSITY**

**IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE BACHELOR OF ENGINEERING DEGREE (COMPUTER ENGINEERING)**

**PROJECT SUPERVISOR: DR. JOSEPH OLOWOLENI**

**MAY 2019**

# **DECLARATION**

I hereby declare that the work done and reported in this project was carried out in the department of Electrical and Information Engineering, Covenant University, under the supervision of Dr. Joseph Olowoleni. I also declare that to the best of my knowledge; no part of this report has been submitted here or elsewhere in a previous application for the award of a degree. All sources of knowledge have been referenced and acknowledge.

------------------------------------------------------------

ADEUGA DANIEL

13CJ015264

# **CERTIFICATION**

This is to certify that the project titled “Automated door access system with facial recognition” by ADEUGA DANIEL ADEWUMI, meets the requirements and regulations governing the award of the Bachelor in Engineering, B.Eng. (Computer Engineering) degree in Covenant University and its approved for its contribution to knowledge and literary presentation.

**Supervisor:** Sign: …………………….. ………………………..

Name: Dr. Joseph Olowoleni Date:

**Internal Examiner:** Sign: …………………….. ………………………..

Name: …………………………... Date:

**Head of Department:** Sign: …………………….. ………………………..

Name: Prof. Adoghe Anthony. U Date:

# **DEDICATION**

I dedicate this project first to God almighty the one whom I depended on throughout my stay in Covenant University and who never failed me once. To my parents Prince Adeuga Franklin Adedoyin and Princess Adeuga Francisca Adefolake whose prayers, support, love and words of encouragement has brought me to this level. Finally, to my sister Adeuga God’s Promise Adeola who restored my hope when all hope was lost. May God bless you and keep you all for me Amen.

# **ACKNOWLEDGEMENT**

I am most grateful to God Almighty for the grace He made available for me to work on this project.

I am also very grateful to my project supervisor, Dr. Joseph Olowoleni for the love, support, encouragement I received from him and constantly monitoring the progress my project work.

I also want to apricate the management and staff of Covenant University under the leadership of Bishop David Oyedepo for providing a conducive learning environment for me.

Finally, a hearty appreciation goes to my parents, my sister Adeuga God’s-promise Adeola for their financial and moral support I enjoyed from them.

# **ABSTRACT**

Security remains one of the major areas of concern in the world we live in. It is a very important need in our society. The level of crime activities has been on the increase over the years. Our society today is faced with many security threats and challenges. One of it is unauthorized access to building by criminals. This issue raises the need to create a more reliable and a more technologically advanced system to guide against unauthorized access. This project is aimed at automating the process of authenticating and authorizing the access of an individual to a building through the door using facial recognition as the means of identifying and authenticating an individual. The facial recognition software has the ability to identify and recognize the face of the individual it has been trained to recognize. So, when an individual approach the door, the system runs a facial scan on the individual to identify the individual. If the person is identified, the door will open on its own accord to the individual but remain closed if the individual is not identified. This will eliminate unauthorized access to a building through the door there by guiding against crime and insecurity.

**CONTENTS**

[**DECLARATION** ii](#_Toc10269750)

[**CERTIFICATION** iii](#_Toc10269751)

[**DEDICATION** iv](#_Toc10269752)

[**ACKNOWLEDGEMENT** v](#_Toc10269753)

[**ABSTRACT** vi](#_Toc10269754)

[**LIST OF FIGURES** ix](#_Toc10269755)

[**LIST OF TABLES** x](#_Toc10269756)

[CHAPTER ONE 1](#_Toc10269757)

[INTRODUCTION 1](#_Toc10269758)

[1.1 INTRODUCTION 1](#_Toc10269759)

[1.2 PROJECT SIGNIFICANCE 1](#_Toc10269760)

[1.3 PROBLEM STATEMENT 2](#_Toc10269761)

[1.4 MOTIVATION 2](#_Toc10269762)

[1.5 AIM 3](#_Toc10269763)

[1.6 OBJECTIVES 3](#_Toc10269764)

[1.7 METHODOLOGY 3](#_Toc10269765)

[1.8 PROJECT ORGANIZATION 4](#_Toc10269766)

[**CHAPTER TWO** 6](#_Toc10269767)

[**LITERATURE REVIEW** 6](#_Toc10269768)

[2.1 BIOMETRICS 6](#_Toc10269769)

[2.1.1 FINGERPRINT BIOMETRICS 8](#_Toc10269770)

[2.1.2 HAND GEOMETRY 10](#_Toc10269771)

[2.1.3 VOICE BIOMETRICS 11](#_Toc10269772)

[2.1.4 IRIS BIOMETRICS 12](#_Toc10269773)

[2.1.5 SIGNATURE RECOGNITION SYSTEM 14](#_Toc10269774)

[2.2 FACIAL RECOGNITION 15](#_Toc10269775)

[2.2.1 FACIAL RECOGNITION ALGORITHMS 16](#_Toc10269776)

[2.2.2 FACIAL RECOGNITION APPROACH 21](#_Toc10269777)

[2.2.3 APPLICATION OF FACIAL RECOGNITION 22](#_Toc10269778)

[2.2.4 ADVANTAGES OF FACIAL RECOGNITION 24](#_Toc10269779)

[2.2.5 DISADVANTAGES OF FACIAL RECOGNITION 24](#_Toc10269780)

[2.3 SETBACKS OF BIOMETRICS 25](#_Toc10269781)

[2.4 FUTURE FEATURES OF BIOMETRICS 27](#_Toc10269782)

[2.5 ELECTRONIC LOCKS 28](#_Toc10269783)

[2.5.1 ELECTROMAGNETIC LOCKS 28](#_Toc10269784)

[2.5.2 ELECTRONIC DEADBOLTS AND LATCHES 28](#_Toc10269785)

[2.5.3 ELECTRONIC STRIKES 29](#_Toc10269786)

[2.6 REVIEW ON RELATED WORKS 30](#_Toc10269787)

[2.6.1 AUTHENTICATION FOR MOBILE BANKING USING FACIAL RECOGNITION 30](#_Toc10269788)

[2.6.2 FINGERPRINT BASED LOCKING SYSTEM 31](#_Toc10269789)

[2.6.3 AUTOMATIC ATTENDANCE SYSTEM USING FACE RECOGNITION 31](#_Toc10269790)

[**CHAPTER THREE** 32](#_Toc10269791)

[**METHODOLOGY** 32](#_Toc10269792)

[**3.1 INTRODUCTION** 32](#_Toc10269793)

[**3.2 PRINCIPAL HARDWARE AND COMPONENTS** 32](#_Toc10269794)

[3.2.1 MICROCONTROLLER 33](#_Toc10269795)

[3.2.2 FT232RL FTDI CABLE 34](#_Toc10269796)

[3.2.3 SERVO MOTOR 35](#_Toc10269797)

[**3.3 SOFTWARE DESIGN** 36](#_Toc10269798)

[**3.4 SYSTEM OPERATION** 37](#_Toc10269799)

[3.4.1 THE ENROLMENT STAGE 37](#_Toc10269800)

[3.4.2 THE IDENTIFICATION AND AUTHENTICATION STAGE 38](#_Toc10269801)

[**CHAPTER FOUR** 40](#_Toc10269802)

[**CONSTRUCTION, IMPLEMENTATION, TESTING AND RESULT ANALYSIS** 40](#_Toc10269803)

[**4.1 CONSTRUCTION OF THE AUTOMATED DOOR ACCESS SYSTEM WITH FACIAL RECOGNITION** 40](#_Toc10269804)

[4.1.1 CIRCUIT DIAGRAM 40](#_Toc10269805)

[**4.1.2 CONNECTION OF THE COMPONENTS ON A BREADBOARD** **42**](#_Toc10269806)

[4.1.3 FINAL CONNECTION OF THE COMPONENT ON A VERO BOARD AND SOLDERING OF THE COMPONENTS 43](#_Toc10269807)

[4.1.4 PACKAGING 44](#_Toc10269808)

[4.1.5 SOFTWARE IMPLEMENTATION 44](#_Toc10269809)

[**4.2 TESTING OF THE AUTOMATED DOOR ACCESS SYSTEM WITH FACIAL RECOGNITION** 45](#_Toc10269810)

[**4.3 OBSERVATIONS AND RESULT OF THE TEST** 45](#_Toc10269811)

[**4.4 BILL OF ENGINEERING MEASUREMENT AND EVALUATION (BEME)** 47](#_Toc10269812)

[**CHAPTER FIVE** 50](#_Toc10269813)

[**SUMMARY, RECOMMENDATION AND CONCLUSION** 50](#_Toc10269814)

[**5.1 SUMMARY OF THE WORK DONE** 50](#_Toc10269815)

[**5.2 ACHIEVEMENT** 50](#_Toc10269816)

[**5.3 CHALLENGES ENCOUNTERED** 50](#_Toc10269817)

[**5.4 RECOMMENDATION** 51](#_Toc10269818)

[**5.5 CONCLUSION** 52](#_Toc10269819)

[**REFERENCES** 53](#_Toc10269820)

[**Appendix A** 54](#_Toc10269821)

# **LIST OF FIGURES**

[Figure 2.1: STEPS IN BIOMETRICS 6](#_Toc5287455)

[Figure 2.2: A BIOMETRIC SYSTEM DESIGN 8](#_Toc5287456)

[Figure 2.3: FINGERPRINT FEATURES 9](#_Toc5287457)

[Figure 2.4: HAND GEOMETRY 10](#_Toc5287458)

[Figure 2.5: IRIS 13](#_Toc5287459)

[Figure 2.6: FACIAL RECOGNITION 13](#_Toc5287459)

[Figure 2.7: A TRAINING SET CONSISTING OF TOTAL M IMAGES 13](#_Toc5287459)

[Figure 2.8: FACE IMAGE CONVERTED TO FACE VECTOR 13](#_Toc5287459)

[Figure 2.9: GENERATED EIGENFACES 13](#_Toc5287459)

[Figure 2.10:THE FLOWCHART OF PCA 13](#_Toc5287459)

[Figure 2.11: FACE IMAGES TO VECTORS 20](#_Toc5287459)

[Figure 2.12: ELECTROMAGNETIC LOCK 28](#_Toc5287459)

[Figure 2.13: ELECTRONIC DEADBOLT AND LATCHES 29](#_Toc5287459)

[Figure 2.14: ELECTRONIC STRIKES 30](#_Toc5287459)

[Figure 3.1: BLOCK DIAGRAM OF THE SYSTEM 32](#_Toc5287459)

[Figure 3.2: ATMEL ATMEGA168 MICROCONTROLLER 34](#_Toc5287459)

[Figure 3.3: FT232RL FTDI CABLE 34](#_Toc5287459)

[Figure 3.4: PINS OF FTDI AND THEIR COLOR CODE 35](#_Toc5287459)

[Figure 3.5: 180 DEGREE ROTATION SERVO MOTOR 36](#_Toc5287459)

[Figure 3.6: ENROLLMENT STAGE FLOWCHART 38](#_Toc5287459)

[Figure 3.7: IDENTIFICATION AND AUTHENTICATION FLOWCHART 39](#_Toc5287459)

[Figure 4.1: THE CIRCUIT DIAGRAM 42](#_Toc5287459)

[Figure 4.2: BREAD BOARDING OF THE COMPONENTS 43](#_Toc5287459)

[Figure 4.3: SOLDERING OF THE COMPONENTS TO VERO BOARD 43](#_Toc5287459)

[Figure 4.4: SCREEN SHOT OF THE MICROCONTROLLER CODE 45](#_Toc5287459)

[Figure 4.5: THE DATASET 46](#_Toc5287459)

[Figure 4.6: RECOGNIZING A FACE 47](#_Toc5287459)

# **LIST OF TABLES**

[Table 4.1: BILL OF ENGINEERING MEASUREMENT AND EVALUATION 48](#_Toc5287459)

**CHAPTER ONE**

**INTRODUCTION**

**1.1 INTRODUCTION**

Today, technology has improved our ways of life in various aspects, including security. In the past, we have seen the shift from the use of key to lock doors to automated door lock with keypad to automated door lock with RFID locks. These methods boosted the level of security but still have some setbacks. The automated keypad lock is prone to shoulder surfing especially with the use of cameras to record the process of inputting a pin. Also, users sometimes forget the pin combination. This system can also be easily hacked. The RFID cards can be misplaced, forgotten or stolen and used for an unauthorized access. With these stated problems the need for a better system arises.

This project topic is targeted at addressing these problems by creating a new system of automated door access system. The Automated door access system with facial recognition basically employs biometrics for authentication and identification with the human face to open and close a door.

**1.2 PROJECT SIGNIFICANCE**

This system will foster security at homes, offices, organizations, banks and other places where security is paramount. The project will create an automated door access system which will be very difficult for intruders to break or hack. This system eliminates the risk of shoulder surfing and password blank out posed by the keypad door lock. This system will eliminate the risk of duplicating, stealing or loosing of RFID cards posed by the RFID automated lock. The system has a high level of accuracy, very effective, efficient and simple to use. The system is economically efficient compared to other types of automated door lock. The technology can be modified to various other forms of authentication system.

**1.3 PROBLEM STATEMENT**

Over the years the rate of security breach has been alarming. Keylocks do not really guide against hoodlums and thieves anymore, because the key can be stolen and duplicated. The keylock system can be picked using an ordinary pin. The keylock can also be destroyed by heating it with a candle. Hence, does not really offer protection against the real trouble. To solve these problems, technology brought about the keypad door lock. This uses a combination of pin known only by the user to open the door, but the keypad lock is prone to attacks such as hacking shoulder surfing and so on. The RFID locks evolved, but this RFID locks has similar problems with the traditional keylocks. The RFID tags can be stolen duplicated or misplaced just as the key to a keylock.

**1.4 MOTIVATION**

The major motivation was to create an automated door access system, that will be very difficult (almost impossible) to hack or break into. Over the years hackers and criminals have deduced various method to beat the two major types of automated locks, which is the RFID lock and the keypad lock. They break the keypad lock either by pin trial and error, brute forcing or by shoulder surfing. And the RFID cards is almost as vulnerable as the manual keylock. So, looking at this issue I was motivated to create a better system that would eradicate all these problems with a new door lock system.

**1.5 AIM**

This project is aimed at creating an automated door access system with facial recognition that will foster public security, guide against intruders and criminals, and eliminate the problems posed by the current existing forms of automated lock i.e. the RFID lock and the keypad lock.

**1.6 OBJECTIVES**

* To create an automated lock system that uses a biometrics property (face) has a means of identification and authentication
* To create a more reliable, accurate, efficient and effective system of computer authentication and identification
* To create a new system of automated lock that would solve the problems posed by the keypad lock and RFID lock.
* To foster security by creating an automated lock system that is difficult to hack into or breach thereby preventing unauthorized access.
* To create an automated door that opens to an authorized individual without human intervention

**1.7 METHODOLOGY**

This project involves the use of different technologies to create an automated door access system that uses a biometric property (the face) as a means of identification and authentication.

The project is divided into two major aspect, the hardware design aspect and the software design aspect. The hardware consists of a microcontroller (Ateml Atmega168) that controls the system, a camera to take the face image of an individual (I used the webcam of my pc for this project), an FT232RL FTDI cable used for data transmission between the PC and the microcontroller, a 180º rotary servo motor. The servo motor was used to open and close the Door. The software was written in python programming language and we used OpenCV framework as the computer vision for face recognition. Other frameworks used include Haar cascade classifier, python imaging library (PIL) a python library that adds support for opening, manipulating and saving many different image file formats, PySerial this is a module that interfaces python software with the microcontroller. The software is used for enrollment, a process where an individual’s details and faceprint is registered and saved to the database. Identification, the process where the computer is able to recognize an individual using his facial properties. Authentication the process of giving access to a recognized and authorized individual. and denying access to a non-recognized and unauthorized individual.

**1.8 PROJECT ORGANIZATION**

Chapter One includes the general overview, project significance, motivation, aim, objective, scope of project methodology, principal components and project report

Chapter Two includes the literature review, review of previous project done on biometrics, and face recognition authentication system and the working principles of face recognition, advantages and setbacks of biometrics, algorithms of facial recognition, facial recognition approaches, applications of biometrics and future features of biometrics and face recognition.

Chapter Three explains in details the system design and construction.

Chapter four covers implementation, Testing and Analysis of project to get required result.

Chapter Five includes the achievements, challenges encountered, recommendation and conclusion.

**CHAPTER TWO**

**LITERATURE REVIEW**

**2.1 BIOMETRICS**

The term biometrics refers to the use of human physical or behavior properties for identification. These properties are unique to an individual hence can be used to distinguish human beings from one another. Biometrics physical properties include face shape, fingerprint, hand geometry, retina, iris, etc. while the behavioral properties include, voice pattern, keystroke, dynamics, gait, etc.

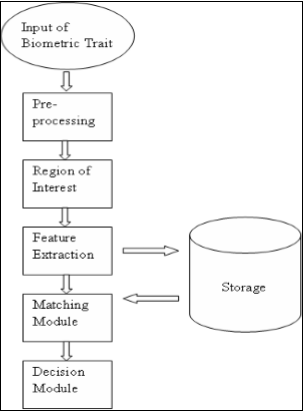


Figure 2.1: STEPS IN BIOMETRICS

In the ICT world, biometrics method of identification has been a useful and reliable method for human identification and authentication. The process involved in biometrics identification are of two phases: The enrollment phase and the authentication phase.

**The enrollment phase: -** In the enrollment phase we have two different stages:

* **The Capturing stage:** - This process involves the collection of biometrics data using a sensor device such as fingerprint scanner, iris scanner etc. to capture the biometric data and convert it to electronic or digital format that can be read by a computer.
* **The extraction stage**: - This is the process of extracting and analyzing the unique details and features in a biometrics data using an algorithm and then saving the extracted information and features as a template for point of reference in the database.

**The comparison Phase**: - This is phase where identification of an individual takes place. This is done by matching an inputted biometrics data with the saved templates to find a match. if there is a match, authentication takes place.

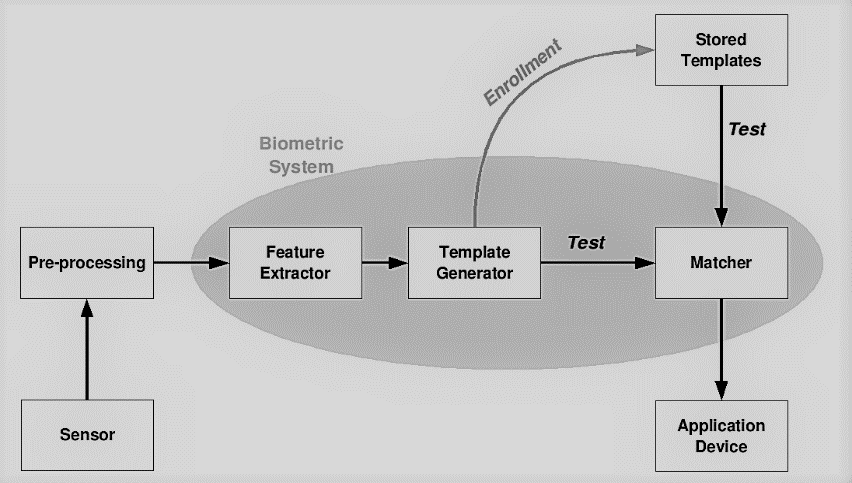


Figure 2.2: A BIOMETRIC SYSTEM DESIGN

The major types of biometric method used in computing for identification include:

* Fingerprint
* Hand geometry
* Voice recognition
* iris recognition
* Signature Verification Technique.
* Face recognition

## 2.1.1 FINGERPRINT BIOMETRICS

Fingerprint is one of the oldest form of biometrics method of identification. Fingerprint is the pattern formed from the impression of the ridges on the skin of a finger. The arrangement of this ridges on the human finger is unique. No two individuals have been found to have the same fingerprint. Fingerprint also remains constant throughout a life time it does not change due to growth hence this makes it a very viable tool for identification. Fingerprint consist of two or more ridge connecting ridge unit of the ridge skin to form a unique pattern called fingerprint. These pattern or outline are of three major types; the arches, the loop and the whorls. A fingerprint scanner is used to capture the fingerprint. These scanners are of three major types: the optical scanner, the capacitive scanner and the ultrasonic scanner (the best of the three). The captured data is then converted to a digital form and an algorithm is applied to it to extract unique features then it is stored in a database as a template for reference point



Figure 2.3: FINGERPRINT FEATURES

**ADVANTAGES OF FINGERPRINT BIOMETRICS**

* The fingerprint remains constant for a life time and hence can be used and referenced to at any point in time unlike face that changes with the growth of an individual
* The fingerprint scanners are very portable and dynamic hence can stand alone as an embedded system or be integrated to any device
* High level of accuracy
* One of the most significantly unique form of biometrics
* Easy to use
* Fosters security
* It is economically efficient compared to other forms of biometrics
* Very difficult (almost impossible) to compromise

**DISADVANTAGES OF FINGERPRINT BIOMETRICS**

* Some skin diseases, burnt wound, acid attack etc. can destroy the structure of the fingerprint making it impossible to be recognized.
* Error rate: - Although fingerprint a high level of accuracy rate, it is not a perfect system hence error can occur and could sometimes be catastrophic
* Data Storage: - Digital image consumes large memory hence creating a problem of data storage in the system

## 2.1.2 HAND GEOMETRY

This has been in use for over 20 years. The Hand geometrics is a biometrics method that identifies an individual using physical characteristic on the finger and palm these characteristics could be shape of the palm, the thickness, length of fingers, width and surface area on the palm. The hand geometry reader measures a user’s hands along various dimensions then compares those measurement with the templates stored in a database to detect a match. Hand geometry is similar to fingerprints. The flow of papillae, shape and size are all measured and minutiae are the main features that are extracted and used in the identification process.

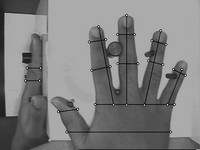


Figure 2.4: HAND GEOMETRY

**ADVANTAGES OF HAND GEOMETRY RECOGNITION**

* They are user friendly because they are easy to use.
* Unlike fingerprint, hand geometry is not affected by the moisture condition of the skin.
* The data for hand geometry is easy to collect compared to fingerprint that require a sophisticated imaging system or iris data that require a special lighting condition.

**DISADVANTAGES OF HAND GEOMETRY RECOGNITION**

* Hand geometry is not totally unique to an individual
* It is not advisable to use for growing children because it changes with growth.
* The data collected by hand geometry are large and pose problem of storage hence places a limitation on its usage e.g. cannot be used for an embedded system

## 2.1.3 VOICE BIOMETRICS

Voice biometrics is the process where voice patterns are inputted to a computer to recognize and identity the individual with the voice. There are to main approaches to voice recognition. The feature analysis and the template matching. The template matching is commonly used because it is cheap, simple to implement and it is more accurate than feature analysis. Notwithstanding the method used, the first step for voice biometrics is that the individual speaks into a microphone. Then the voice is converted first to analogue signals then to digital signals using an analogue to digital converter (ADC). The digital signal is stored to the memory. The procedure is repeated several times then the computer statically computes the average of the multiple sample. The average sample is then stored in the database and used as bases for comparison.

**Advantages of voice biometrics**

* High level of accuracy
* High level of social acceptability

**Disadvantages of voice biometrics**

* The voice could be recorded and used for an unauthorised authentication
* It requires high computing power to perform the task
* Some illness such as cough, sore throat, crack voice or loss of voice can make voice recognition very difficult or impossible.

**2.1.4 IRIS BIOMETRICS**

Iris is one of the unique biometrics’ property used to identify an individual. It is done by using a sophisticated pattern recognition technique on the image of either one or both iris in the eye of an individual for identification. The iris is the coloured part in the eye that surrounds the pupil. The pupil is the black part of the eye. The pattern is very complex to analyse but they are unique to an individual and just like fingerprint, it is not affected by growth of the individual i.e. it is constant for a life time.The iris biometrics is captured with an iris scanner which comprises of a charged coupled device (C.C.D) digital camera. The camera makes use of both visible and near-infrared light to take pictures of the individual’s iris. The near-infrared light makes the pupil very black and easily separated from the iris by an image processing software. When an individual stand in front of the iris scanner, the picture of the eyes is captured and then uses the center of the pupil, the edge of the pupil, the edge of the iris and the eye lid to analyse the pattern in the iris and then compares it with images in the database to find a match.



Figure 2.5: IRIS

**Advantages of iris biometrics**

* Eye glasses or contact lens do not interfere or cause inaccuracy in the result.
* The iris pattern of an individual is unique and constant throughout a life time.
* It takes into consideration and compares about 200 nodes or point of reference making it more accurate than fingerprint biometrics which compares about 70 to 80 nodes.
* It has high level of accuracy apparently it is considered to be the most accurate method of biometric that is currently existing.
* The iris capture can be done from a distance.
* It is user friendly and easy to use.

**Disadvantages of iris biometrics**

* It is expensive. It is by far more expensive to implement compared to other forms biometrics method
* The presence of reflection can easily compromise the result of the biometrics
* The individual has to be steady in front of the camera because it is hard to perform the scan in presence of movement
* It is obscured by eye latches.
* A lot of memory is required to store the data
* Infrared light can do some damage to the eye if constantly exposed to infrared light

## 2.1.5 SIGNATURE RECOGNITION SYSTEM

Signature recognition is a behavioral biometric method that identifies the signature of an individual. In this method, the signature of an individual is inputted with the aids of an electronic signatory pad and then converted to a digital image. The speed, velocity and pressure are considered are also part of the features considered. The image is then compared to the one in a database to determine if there is a match. This method has been adopted in banks, and law enforcement agencies and top organization to validate the identify of an individual. Just like every other biometric system the signature is first captured to a database either by scanning the signature with a normal scanner or by using an electronic signatory pad which converts the signature to a digital image and saved to database then for identity verification, the signature is inputted into the electronic signatory pad and then compared with the images in a database for a perfect match using an image processing algorithm.

**Advantages of signature recognition**

* High level of accuracy.
* The software can Automatic detect, crop, and enhance the signature from a digital image.
* Verification of two or more signature can be done at the same time thereby increasing efficiency.
* It is user friendly and easy to use

**Disadvantages of signature verification**

* Some individuals do not have a constant signature.
* Some fraudsters can effectively master their victims’ signature pattern and use it to impersonate them
* Not as accurate as other forms of biometrics listed above

**2.2 FACIAL RECOGNITION**

Face recognition is a biometric method designed for identify an individual in a digital image or a video frame by extracting and analysing patterns of the individual’s facial texture and shape and stores the extracted data as a template called faceprint in a database. Nowadays facial recognition software is equipped with 3D-modelling to guide against being spoofed by photos or masks. This type of software compares over 30,000 variables. Facial recognition is used in automated security system for authentication and it is also used in crime investigation to identify individuals in footage form a CCTV or from any other source.



Figure 2.6: FACIAL RECOGNITION

## 2.2.1 FACIAL RECOGNITION ALGORITHMS

There are currently three major facial recognition algorithm they include the Principal Component Analysis (PAC), the Linear Discriminant Analysis (LDA) and Elastic Bunch Graph Matching (EBGM).

**THE PRINCIPAL COMPONENT ANALYSIS (PCA):** This method is used more than the other two facial algorithm methods. The PCA was invented in 1901 by karl pearson. The PCA is used mostly as a tool in exploratory data analysis and for making predictive models and it is also used to reveal the internal structure of the data in a way which best depicts the major features and directions in a data (i.e. variance). PCA is the simplest of the true eigenvector based multivariable analysis

**HOW PCA IS USED FOR FACIAL RECOGNITION**

Given a training set of M images and unknown face all of the same size in width and height, the PCA represents a face image as a linear combination of a set of eigenvectors. These eigenfaces (eigenvectors) are the PCA of the trained set of images generated after reducing the dimensionality of the training set. PCA eigenfaces method considers each pixel in an image as a separate dimension so an sized image will have dimensions. Example for a = . For recognition, all face images must be of the same exact dimension. PCA eigenfaces method does not work on the images directly, it first converts them to matrix (vector) form. Here are the major steps involved in PCA

Step 1: - a training set each of these images must be of the same size is created. Considering the training set where N = the size of each of the image 1.e the width = height=N and M= the total number of images in the training set.



Figure 2.7: A TRAINING SET CONSISTING OF TOTAL M IMAGES

Step 2: - convert face images in training set to face vectors. The vectors will contain values.

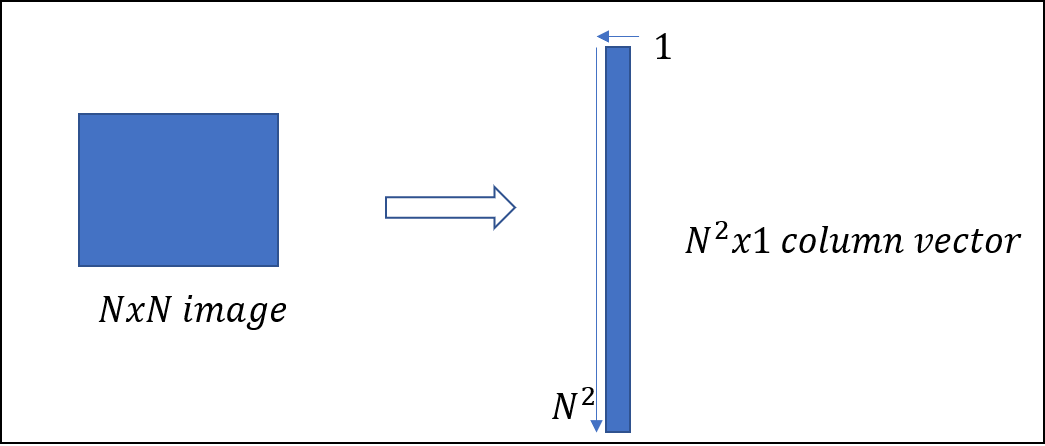


Figure 2.8: FACE IMAGE CONVERTED TO FACE VECTOR

Step 3: - The next step is a process referred to as normalization. This simply means normalizing the face vectors i.e. removing common features present in all the images of the training set. this is done by calculating the average face vector of all images in the training set and then subtracting the average face vector from each of the face vector to give the normalized face vectors denoted by

Step 4: - calculate the eigen vector. This is done by calculating the covariance matrix C

where and is the transpose of matrix 1

There fore But calculating the eigenface this way gives a very large data to work with which can sometimes affect and slowdown the CPU. A solution to this problem is known as dimensionality reduction. The formula for the covariance of reduced dimensionality is given by



Figure 2.9: GENERATED EIGENFACES

The figure above shows the generated eigenfaces with the total number of K. The number of eigenfaces (K) is always less than or equal to the total number of images (M)

STEP 5: - Select K best eigenfaces such that can represent the whole training set. The

Step 6: - A weight Vector which is used to represent each face from the training set is generated by adding the mean face to the sum of . The weight vector is denoted by and each of this weight vectors is stored. Now for an unknown face to be recognized, the procedures shown in the flowchart below is followed.

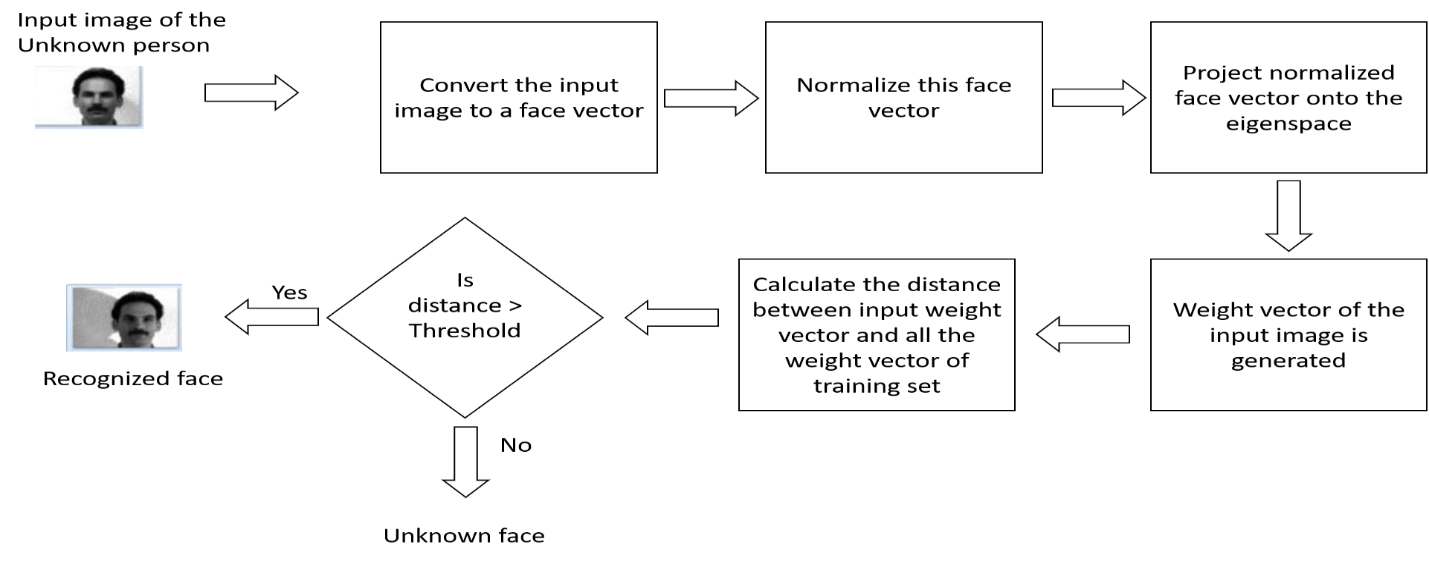


Figure 2.10: THE FLOWCHART OF PCA

**LINEAR DISCRIMINANT ANALYSIS (LDA):** - This is a classification method developed by R.A. Fisher. It is a simple mathematical technique used to produce models whose accuracy is as good as more complex techniques such as PCA. It was developed as an enhancement of the PCA hence very similar to the PCA. The major difference is that the LDA uses the concept of classes but both PCA and LDA do dimensionality reduction and they transform images as a vector to new space with new axes It was developed based on the concept of searching for a linear combination of variables that best separate two classes. It is exceptionally valuable for decrease of dimensionality and feature reaction. It is used in pattern, face recognition, object recognition and machine learning to find a linear combination of features that isolates at least two classes of object or item.

**ALGORITHMS**

Assuming a square image with the is the number of images in the database and P to be the number of persons in the database, Then the data base structure will look like this

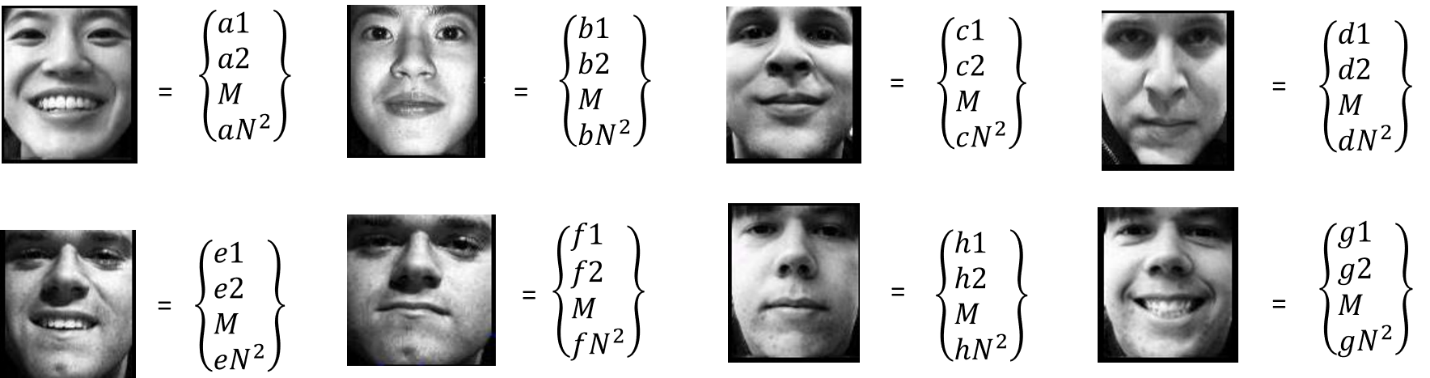


Figure 2.11: FACE IMAGES CONVERTED TO VECTORS

The face images are converted to face vectors then the next step is to compute the average of all faces is as shown in the equation below

The next step is to compute the average face of each person as shown in the equation below

The next step is to subtract the average face of each person from the training faces. Then the next step is to build the scatter matrices

And the within-class Scatter matrix

The between-class scatter matrix is expressed by the equation below

We are searching the matrix maximizing

**THE ELASTIC BUNCH GRAPH MATCHING**: - This technique was created by Wiskott et al. The algorithm is a 2D based model utilized for object detection and recognition in computer vision. Visual objects in EGM are represented as labeled graphs, nodes are used to represent local textures based on Gabor wavelets while edges are used to represent distances between the node locations on an image. Thus, an image of an object is represented as a collection of local textures in a certain spatial arrangement.

## 2.2.2 FACIAL RECOGNITION APPROACH

**HOLISTIC MATCHING APPROACH: -** This method uses feeds the recognition system with the entire face region as the input to. One of the most commonly used representations of the face region is eigen pictures, which works based on principal component analysis. it uses the entire face and ignores other features like the mouth the nose the eye etc. this method can be classified into two: the statistical method which uses the density of the face image and the artificial method that uses neural network technique.

**FEATURE BASED (STRUCTURAL) MATCHING APPROACH: -** This method is the complete opposite of the holistic method. In this method, local features such as the eyes, nose, and mouth are considered. Leaving out the details from the whole face.

**HYBRID MATCHING APPROACH: -** This method is recognized as the best method among all the methods listed. Just as the name implies, it combines both the holistic and the feature-based technique i.e. it uses both the whole face and the other features like the eyes the nose and the mouth for recognition.

**2.2.3 APPLICATION OF FACIAL RECOGNITION**

There is no doubt that facial recognition has advanced our security and identification system in various ways. We take a look at some of the areas where the facial recognition is applicable

**Crime Investigation**: - Biometric identification especially face and fingerprint have been useful to law enforcement agencies who have the difficult task of figuring out perpetrators of crime. Most time this law enforcement agents most times, do not witness the crime. They rely on evidences, eye witnesses and clues gotten from the crime scene. Biometrics has proven to be very useful in this area. It helps the law enforcement agents to identify criminals by running a face recognition on the faces of individual in the footage gotten from any closed-circuit television CCTV around the crime scene to identify who the suspect in the footage is. They can also recover fingerprints and footprints from the crime scene or crime weapon and use it to detect whoever used the weapon to commit a crime or who was present in the crime scene when the crime was committed.

**Security**: - Security has been a major aspect where face recognition has been very useful ranging from domestic level security to industrial level security. There has been emergence of various devices that enhances the use of facial biometrics in the aspect of security some are listed below

* Security of buildings, offices, industries laboratories, etc. The emergence of face recognition lock system has been useful for the securities of homes, offices, industries, organisations factories etc. The face recognition system only opens to whose ever has his or faceprint saved to the database. This has prevented access of unauthorised individuals into their target buildings thereby fostering security in the society
* Guide against cybercrime. Most smartphones, smart devices, laptops and many other computers have adopted facial recognition authentication system as against the pattern, pin or password which can easily be guessed, spoofed or surfed by cyber attackers. Hence making digital information stored in these devices more secure than ever.
* E-commerce. Many online marketing platform and online payment platform have also adopted the use of face recognition and fingerprint biometrics for authentication. E commerce sites and online payment platforms no longer demand only user name and password but also a facial and fingerprint authentication before authorizing a transaction. This has reduced the reports of fraudulent activities.
* In developed and developing countries, there is Closed-Circuit Television in major places, blind spot, buildings, street, and many other places. The awareness of this CCTV around has created fear in the hearts of many and restricted them form perpetrating crimes in certain places because the know someone somewhere is watching.
* Many organizations now use facial organization to take attendance of their employees as against the paper signing

**2.2.4 ADVANTAGES OF FACIAL RECOGNITION**

* It is easy and convenient to use.
* It helps to foster security in various aspect.
* It is flexible your face is always part of you.
* It is highly accurate and reliable.
* It is economical as no special camera or vision sensor is needed.

**2.2.5 DISADVANTAGES OF FACIAL RECOGNITION**

* Error rate: - Although facial recognition a high accuracy rate. It is not a perfect system hence error can occur and could sometimes be grievous
* High cost: - The cost of implementing a facial recognition system is relatively high
* Data Storage: - Digital image and video consumes large memory hence creating a problem of data storage in the system
* Physical Disability: - An individual face geometry can be altered due to some disabilities such as acid attack, burnt, diseases, scald or severe injuries sustained in accident hence making it difficult for their current image to match their previous faceprints.
* Additional Hardware Integration: - Sometimes a software may not be enough to handle the task hence some special hardware or embedded systems must be integrated to the system which makes it more complicated and more expensive.
* Face alteration: - with the aid of plastic surgery an individual can totally reconstruct the shape and structure of his or her face making him look totally different from the formal self hence rendering the face recognition software ineffective.

**2.3 SETBACKS OF BIOMETRICS**

* Biometric hack has greater consequences: - This is one major setback of biometrics. If an attacker successfully steals a password, the password can be changed but if an attacker steals a biometric data e.g. fingerprint the attacker has it forever it cannot be changed. The only solution is to stop using fingerprint as a means of identification. Which is a tough one.
* Biometrics are not totally hack proof: - Biometric devices are difficult to hack but they are just difficult not impossible to hack. We have had instances of hacking into iris scanner, fingerprint scanner, facial recognition system, etc to either by-pass it or steal information from it. Ethical hackers and researchers have proven this often.
* Biometrics are not private: - Biometrics are unique to an individual but are not private, for pins or password, it is only known by the individual and hackers need to use some technical methods to get the password. But the case is different for biometrics. Our faces are always visible and they are also in numerous pictures we have taken. We leave fingerprint on anything we touch. (that’s how crime investigation with fingerprint is possible). We talk every time and our voices can easily be recorded without our knowledge and all this information can be used to hack into biometrics system.
* Human physical properties could be damaged: - The structure of the human physical properties could be damaged due to many reasons. Example the fingerprint can be damaged by skin diseases, burnt, injury, etc. the eyes structure to can be damaged. The face can be damaged by injuries burns, acid attacks and skin diseases. The voice could also be damaged or cracked (this is common among musicians). The damage of the human physical structure makes it difficult or impossible for an individual to be identified using biometrics.
* Error in identification and authentication: - biometric system sometimes commit error in identification and authentication. This is more common with low cost devices. Although the error rate in biometrics is minimal, it is still not 100% error free.
* Expensive to implement: - Biometrics systems are expensive to implement, manage and maintain. The high cost of implementation and maintenance is the reason why many companies and organization have refused to implement it.
* Large storage needed: - The data generated from biometrics are very large thus pose the problem of storage when implementing. Some biometric system has not been able to function as a system on its own (embedded system) because of the problem of storage. The cost of large memory also increases the cost of implementation and maintenance.

**2.4 FUTURE FEATURES OF BIOMETRICS**

As time goes on, we would expect biometrics technology to have gone further and should have had more advancement. Some of the likely features we would see in biometrics include:

* Multifactor biometrics which will use more than one biometric property for identification and authentication. This would increase the stability and efficiency thereby enhance security.
* Biometrics security for internet of things: - In the nearest future where everything electronics would be able to connect to the internet, biometrics would be the only reliable security method to solve the security issues evolving from the internet of things.
* DNA Recognition: - Biometrics DNA has been proven to be the most unique physical qualities of all physical qualities. But as advanced as technology is today, it still takes at least 24hrs to get the result of a DNA test. But in the future, we will see a biometric system that is DNA based. It will be able to process DNA data and store the result electronically all in real-time to be used for identification and authentication.
* Biometrics For medical Evaluation: - In the future we should be hoping for a biometric system that can give the breakdown of one’s health status without having to pierce the body or take liquid samples like urine and blood. The emergence of this technology will see a great revolution in the medical industry.
* Biometric authentication as part of human life: By 2020 experts predict that the only form of computer identification and authentication will be biometrics the use of cumbersome username and passwords will be eradicated. Also, the use of RFID tags and identity cards will also be eradicated. Biometrics will take over all aspect of life, the banking, transportation, e-commerce, Medical organizations, government and private organization, offices, tourist centers, institutions, library, event centers, car parks, laboratory, museums, legal institutions, etc. all will depend on biometrics for identification and authentication.

**2.5 ELECTRONIC LOCKS**

**2.5.1 ELECTROMAGNETIC LOCKS**

This is the most essential kind of electronic lock. A huge electro-magnet is fixed on the door frame and an equivalent armature is mounted on the door. when the magnetic is powered and the door is shut, the armature holds fast to the magnetic. One setback is that study reveals that it is very difficult to breakdown or force entry and it has caused a lot of fire accident to escalate



Figure 2.12: ELECTROMAGNETIC LOCK

**2.5.2 ELECTRONIC DEADBOLTS AND LATCHES**

Electric mortise and cylindrical locks are exchanged for mechanical locks which are fixed to the door. An extra hole must be penetrated in the entryway for electric power wires. Likewise, a power exchange pivot transfers electrical power from the door frame to the door. Electric mortise and cylindrical locks permit mechanical free exit, and can either come up short opened or fizzle bolted. A very good features is that it is equipped with a flame detector and will open on its own accord once flame is detected for emergency exit. The major setback of this lock is that it is very difficult to install so it requires a lot of skills to be able to install the lock.



Figure 2.13: ELECTRONIC DEADBOLTS AND LATCHES

**2.5.3 ELECTRONIC STRIKES**

An electric strike is an access control gadget used for doors. It swaps fixed strike faceplate often used with a latchbar. Similar to fixed strikes, it typically presents a ramped surface to the locking latch permitting the door to lock. But an electric strike can be controlled automatically making it possible for an automated locking and unlocking process. It does not need to be mechanically turned by a key before it would unlock or lock



Figure 2.14: ELECTRONIC STRIKES

**2.6 REVIEW ON RELATED WORKS**

**2.6.1 AUTHENTICATION FOR MOBILE BANKING USING FACIAL RECOGNITION**

This work identified the two major forms of authentication used by mobile banking applications which is the username and the password, their setbacks and the need for a safer method of authentication using facial recognition. The work was about creating a more secure authentication for mobile banking applications using facial recognition as a means of authentication thereby improving on the existing system, and also assisting in the actualization of cashless policy in our society. A review and difficulties of the present system were also highlighted. The design of the proposed system was presented. A prototype of the system which was developed using java programming language and tested using simulated databases of Nigeria communication commissions (NCC) and the facilitating bank. The result showed that the system performed with a maximum response time of seven minutes and false acceptance rate (FAR) of 3%. A conclusion that merging the system with one or more other forms of biometric technologies such as finger vein, iris among others will surely produce a fraud proof and a less vulnerable platform for mobile banking application was drawn.

**2.6.2 FINGERPRINT BASED LOCKING SYSTEM**

This work is very much similar to mine. The major difference is that the biometrics used in this case is fingerprint. The system grants access to individual whose fingerprints are pre-stored in the memory of the system. The goal was to eliminate the need for keeping track of keys or remembering a combination password, or PIN. The lock only opens when an authorized user is present, since there are no door locks that can be picked, keys or combinations to be stolen or copied, the fingerprint-based lock therefore provides an awesome solution to conventional difficulties experienced. The report of the work concentrated on the utilization of fingerprints to open locks, as opposed to customary technique for of keys

**2.6.3 AUTOMATIC ATTENDANCE SYSTEM USING FACE RECOGNITION**

This work was all about creating a better and faster automated attendance system in classroom using biometric facial recognition. The aim was to automate the whole process of attendance capture with very little or no human involvement. The work proposed that there will be a camera installed in the class. The camera will take a picture of the whole classroom then it will detect the faces of each individual in the image, recognize the students whose faces have been detected and then update their attendance. The process will be carried out two times first at the beginning of the class and at the end of the class.

**CHAPTER THREE**

**METHODOLOGY**

**3.1 INTRODUCTION**

This chapter covers the details about the system requirement of this project, it covers the design and the specifications of the system developed in this project. It also unfolds the different aspect of this project, the mode of operation of each aspect and the mode of operation of the system as a whole.

The system design of the project consists of two major aspect, the hardware aspect and the software aspect. The software aspect, consists of the facial recognition software itself and the program for the microcontroller. The block diagram of the system is as shown below



Figure 3.1: BLOCK DIAGRAM OF THE SYSTEM

**3.2 PRINCIPAL HARDWARE AND COMPONENTS**

* Atmel Atmega168 microcontroller
* FT232RL FTDI cable
* 180 Degree Rotation Servo Motor
* Vero board
* Jumper wires
* LED
* Resistors
* capacitors
* Crystal oscillator
* Push buttons

## 3.2.1 MICROCONTROLLER

The microcontroller used is the Atmel Atmega168 microcontroller. This microcontroller is an 8-bit microcontroller (i.e. it can process 8-bit of information at a single time) with 28 pins. It operates with a voltage ranging from 1.8v to 5.5v. It was built based on the reduced instruction set computer architecture (RISC). Some of it features include: 16 Kbytes of In-System Programmable Flash with Read-While-Write capabilities, 1K bytes SRAM, 512 bytes electrically erasable programmable read only memory (EEPROM), 23 general purpose I/O lines, three flexible Timer/Counters with compare modes, internal and external interrupts, 32 general purpose working registers, a serial programmable universal synchronous asynchronous receiver transmitter (USART), a serial peripheral interface (SPI)port, a 6-channel 10-bit analogue to digital converter (ADC) i.e. it has 6 pins which can be used to receive analogue signal and it can detect (1024) discrete signal level, a byte-oriented 2-wire Serial Interface, etc The Atmega168 is majorly used in automation and in embedded system. It is also used in systems where numerous functions are to be performed with a single chip.



Figure 3.2: ATMEL ATMEGA168 MICROCONTROLLER

## 3.2.2 FT232RL FTDI CABLE

The FTDI cable provides a medium through which data can be transmitted and received to and from a microcontroller to a PC through the universal serial bus port (USB). the FTDI cable contains a chip in it called FT32RL chip in it. This chip provides a TTL protocol that enables it to send data at 9600 bit per seconds baud rate the chip consist of 6 pinsouts: the ground cable GND which is the black cable the transmitter pin TX which is the orange wire sends data to the microcontroller the receiver pin RX which is the yellow wire receives data from the microcontroller, the VCC pin which is the red pin wire the clear to send CTS pin which is the brown pin, and the data terminal ready which is the green wire and it automatically reset the microcontroller whenever a new code is uploaded to the microcontroller.



Figure 3.3: FT232RL FTDI CABLE

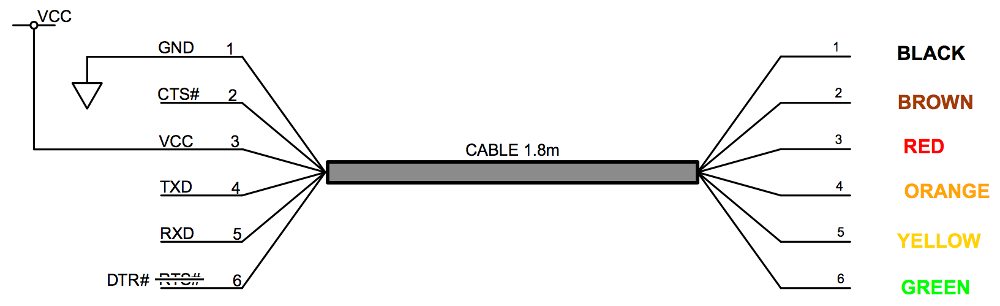


Figure 3.4: PINS OF FTDI AND THEIR COLOR CODE

## 3.2.3 SERVO MOTOR

A servo motor is either a rotary or a linear actuator which the angular or linear position can be precisely controlled. It possesses a dc motor, a potentiometer, a control unit and also a sensor gives feedback about the position. The motor is joined to the control wheel by gears. When the dc motor rotates, the potentiometers resistance changes thereby regulating precisely the movement of the control circuit. the servo motor contains three terminals one is the ground, one is the VCC that powers the servo and the last is the data wire which transport the desired position. The speed of a servo motor reduces as it gets close the desired position. This term is called proportional control. Servos motors are controlled by sending electrical pulses of variable width. This pulse is sent to the motor through the data wire. The 180 degrees servo motor can turn 90 degrees in both clockwise or anti-clockwise direction and can turn a total of 180 degrees. The servo motor receives a pulse every 20 milliseconds and the length of the pulse is what determine the angle at which it turns for example a 1.5ms pulse will rotate the servo motor at 90 degrees. A pulse lesser than 1.5ms rotate the motor in the anti-clockwise direction while a pulse greater than 1.5ms will move the servo in clockwise direction as it tends towards 180 degrees. The servo does not hold it position forever so the pulse must be sent repeatedly to keep the servo motor at the desired position. The servo motors are of two major types: the AC servo and the DC servo the ac motor. The AC servo motor requires large current to operate and are mostly used for industrial purposes. The DC servo motors does not require large current it its case hence are mostly used for smaller and domestic purposes. Servo motors are used mostly in robotics, automation, airplanes etc.



Figure 3.5: 180 DEGREE ROTATION SERVO MOTOR

**3.3 SOFTWARE DESIGN**

The microcontroller is programmed in C++ this program controls the microcontroller to perform the desired function. The program will interpret what signal it receives from the facial recognition software on the PC. If it is a high signal, the program tells the Microcontroller to open the door through the servo motor and then closes it after 7 seconds. If it is a low signal, the door remains closed. The facial recognition software was programmed in python using OpenCV framework. The OpenCV framework is an open source computer vison software library built based on the principles of principal component analysis (PCA). We also used an image classifier called haar classifier. Many other python libraries were also used. The hardware requirement is a computer with a very good processing power and speed.

**3.4 SYSTEM OPERATION**

The software operation is can be grouped into two major stages. The enrolment stage and the authentication stage.

## 3.4.1 THE ENROLMENT STAGE

This is the stage where the face of an individual is taken by the camera and the image of this face is stored in a database these images are known as face print. This would serve as a reference point during authentication. This process is known as face training in PCA. The flowchart of the enrolment is shown below

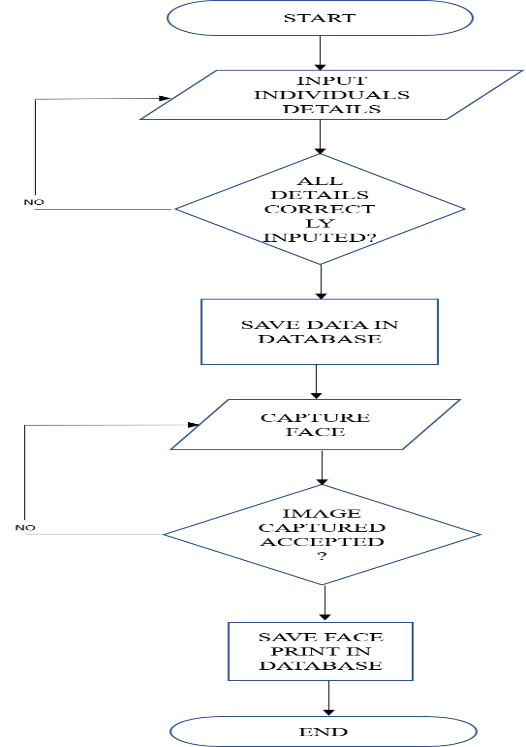


Figure3.6: ENROLLMENT STAGE FLOWCHART

## 3.4.2 THE IDENTIFICATION AND AUTHENTICATION STAGE

When an individual has been enrolled into the system, to gain access though to door, the system has to identify and authenticate him. The authentication stage is the stage where the face of an already enrolled user is identified by the system and access is granted to the identified user. If an individual who has not been enrolled approaches the system for authentication, the individual is tagged an unauthorised user hence would be denied access by the system. The flowchart of this stage is as shown below

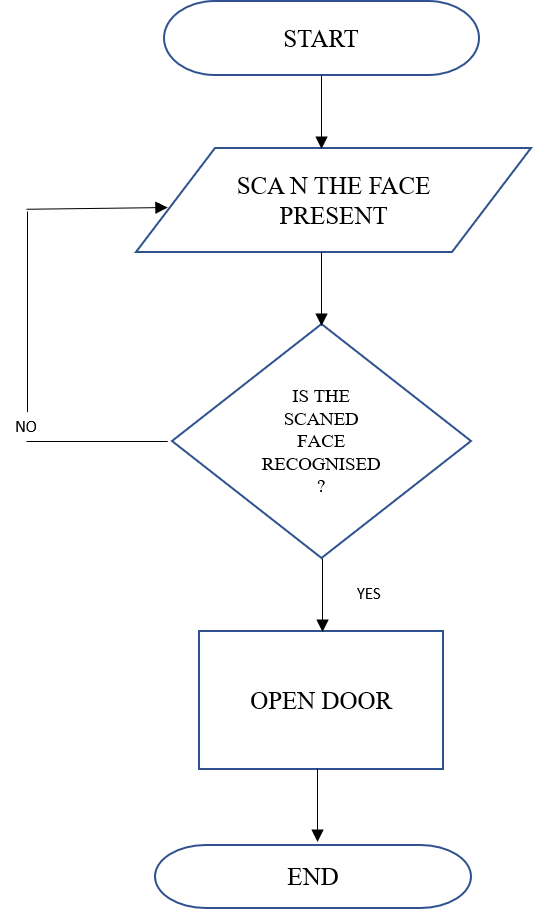


Figure3.7: IDENTIFICATION AND AUTHENTICATION STAGE FLOWCHART

**CHAPTER FOUR**

**CONSTRUCTION, IMPLEMENTATION, TESTING AND RESULT ANALYSIS**

**4.1 CONSTRUCTION OF THE AUTOMATED DOOR ACCESS SYSTEM WITH FACIAL RECOGNITION**

The construction of this project was grouped into the various stages listed below

* Circuit Diagram
* Initial Connection of the components on a breadboard
* Final connection of the component on a Vero board and soldering of the components
* Packaging

## 4.1.1 CIRCUIT DIAGRAM

The circuit diagram of the project was designed and simulated on proteus software. Proteus is a software developed by Labcenter Electronics Ltd used for electrical and electronic design and automation. The circuit simulation was done to ensure the all the component worked well and the system worked perfectly well as a whole before the implementation.

The FTDI programmer was used to link communication between the Microcontroller and the facial recognition application on the PC. It contains the FT32RL chip inside that provides USB to TTL protocol. It would send data at 9600 bits per second. The FTDI programmer was connected to the microcontroller in the following order: The TX of the FTDI goes to the RX of the microcontroller, The RX of the FT232RL goes to the TX of the microcontroller, The CTS is connected to the RESET pin of the microcontroller, and both grounds are connected together (GND to GND). The pin 9 and 10 of the microcontroller is connected to the pins of a crystal oscillator of16MHz frequency. The crystal oscillator provides synchronous speed 16mHz (that is it provides an accurate reasonable time reference) the microcontroller needs to run and process the instruction burnt into it. The 22µf capacitor C1 is connected from pin 9 to the ground and capacitor C2 is connected from pin 10 to the ground. The capacitors are used to eradicate the noise and also ensure this stability of the microcontroller. Without these components arranged in this configuration, the source codes can’t be uploaded into the microcontroller successfully. And the and the microcontroller can’t execute the codes uploaded into it. The reset pin is connected via a 10kΩ resistors from the VCC to a push button and the other pin of the push button is connected to the ground because the reset pin is active low so when the push. Another 10kΩ resistor is connected from the VCC to the LED and the other pin of the LED is connected to the ground. The LED serves as a power indicator. The servo motor has three terminals the ground which is the grey wire the data pin which is the yellow wire and the red pin which is the power wire. The power wire is connected to the VCC of the microcontroller and the ground is connected to the GND of the microcontroller. The data pin is connected to digital pin 7 of the microcontroller. This would send angle of rotation to the Servo motor i.e. 0 for closing and 70 for opening as defined in the code

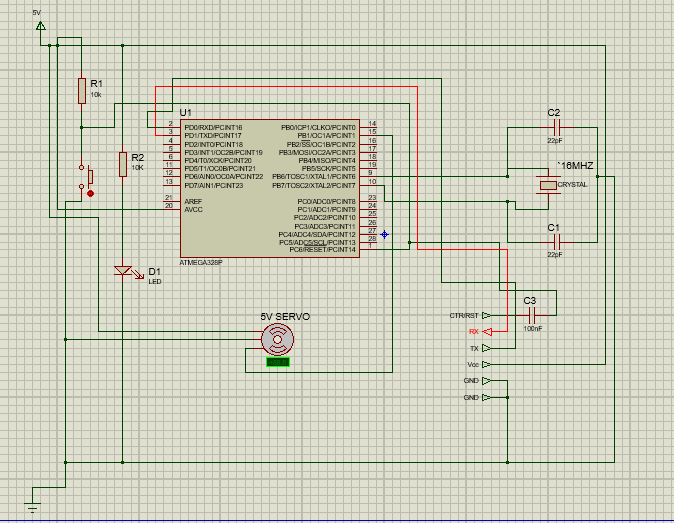


Figure 4.1: THE CIRCUIT DIAGRAM

**4.1.2 CONNECTION OF THE COMPONENTS ON A BREADBOARD**

This is the next stage after simulating the circuit diagram on Proteus. This is essential because while the Proteus provides a virtual simulation, connecting the circuit diagram on a breadboard provides a real-life simulation of the circuit diagram. The circuit diagram was implemented in a breadboard to ensure that all the components function well and are in good conditions. Breadboarding also helps to ensure that the circuit works perfectly before soldering it permanently of the Vero board.



Figure 4.2: BREAD BOARDING OF THE COMPONENTS

## 4.1.3 FINAL CONNECTION OF THE COMPONENT ON A VERO BOARD AND SOLDERING OF THE COMPONENTS

The components were mounted on the Vero board and soldered permanently to ensure firm connection of the components on the Vero Board. The soldering was done properly to avoid short circuit, open circuit and bridging

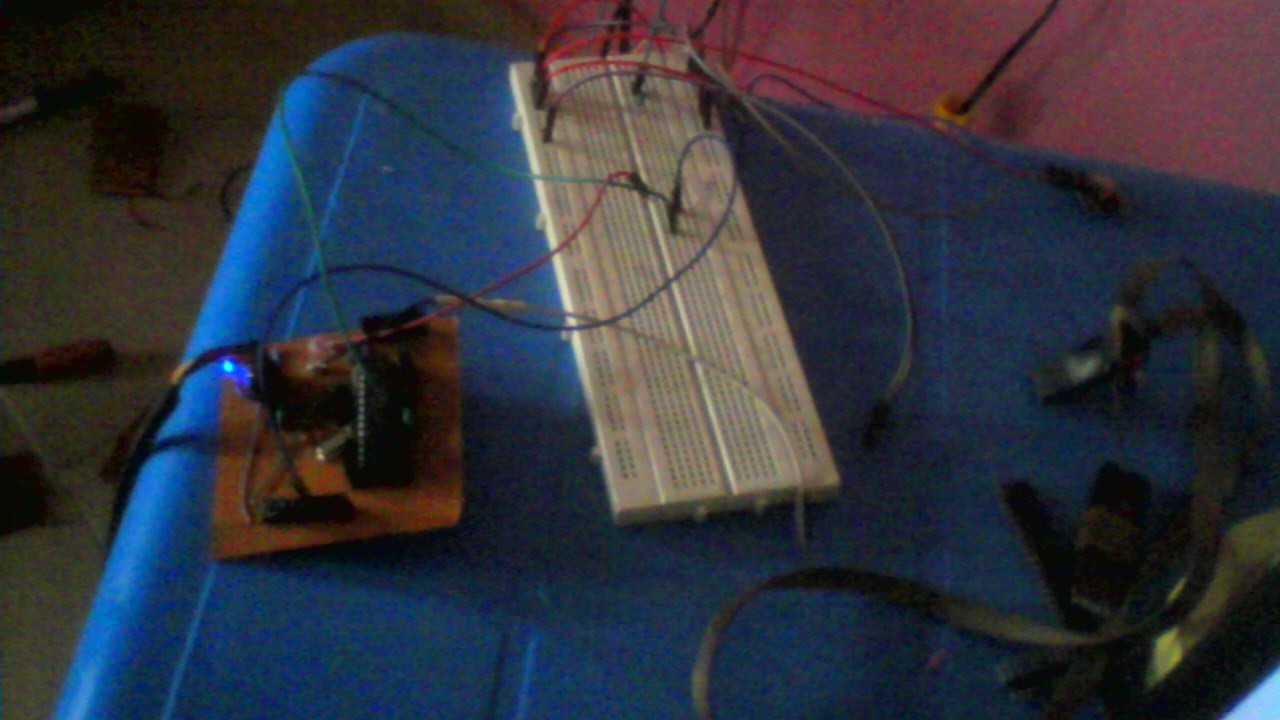


Figure 4.3: SOLDERING OF THE COMPONENTS TO VERO BOARD

## 4.1.4 PACKAGING

The project was packaged well in a wooding case.

## 4.1.5 SOFTWARE IMPLEMENTATION

The facial recognition software was developed using python programming language. the codes were written using the python IDE. And the computer vision framework used was the OpenCV. Other framework used in implementation of the facial recognition software include

* PySerial: - A python library that enables the python software communicate to the microcontroller through a serial port
* Python imaging library (PIL): - A python library that allows for open manipulating and saving of image
* Haar cascade classifier: - is an object detection algorithm used for identifying and recognizing object which it was trained to identify.

In implementing the software, I initially tried using EmguCV with C# and haar classifier to program the facial recognition but the result I got was not impressive. I later tried using OpenCV with C# but the OpenCV refused to work with the C# language then I finally resolved to using python with OpenCV, although the performance was below expectation, the was preferable to the C# software so I finally settled for the python software.

The microcontroller was programed in C++ using the Arduino IDE this was possible by downloading and including a special library to the Arduino IDE called minicore library this library enables us to use the Arduino IDE to program the Atmega168 chip. The library for the servo motor also had to be include to the IDE this enables us to control the servo motor.



Figure 4.4: SCREEN SHOT OF THE ARDUINO CODE

**4.2 TESTING OF THE AUTOMATED DOOR ACCESS SYSTEM WITH FACIAL RECOGNITION**

Various test was carried out to ensure that the system worked perfectly. Component testing was carried out to ensure that all the components where in good condition before using them. Then Integration testing was also carried out on each modules of the project. This was done to ensure that the separate modules interact well with each other. Then the system testing was done to ensure that the system as a whole functioned as expected.

**4.3 OBSERVATIONS AND RESULT OF THE TEST**

The software was tested with five faces of five different individual. Each with 10 face images trained in the database the result of the testing shows that the accuracy of the software was lower than the desired result. I also observed that the accuracy of the result was affected majorly by two factors. The first factor is the quality of the image its sees and the quality of the image mostly depends on the quality of the camera taking the image. The second factor that affected the accuracy of the result was the amount of light present in the environment. The software had a higher accuracy sometimes up to 85% when there is high amount of light in the environment compared to dark areas which sometime have an accuracy of between 45% to 55%. The software also performed well during the day than during the night. Also, the angle at which the face was taken also determines the level of accuracy of the software. And finally, the processing speed of the computer was also a factor that affects the accuracy of the software too. During the test, there was instances of false acceptance i.e. recognizing a face which has not been trained to the database and false rejection i.e. not recognizing individuals whose faces has been trained. It was also observed that the OpenCV framework has a higher accuracy when it has lesser faces trained i.e. the lower the number of faces trained the higher the level of accuracy of the software.



Figure 4.5: THE DATASET

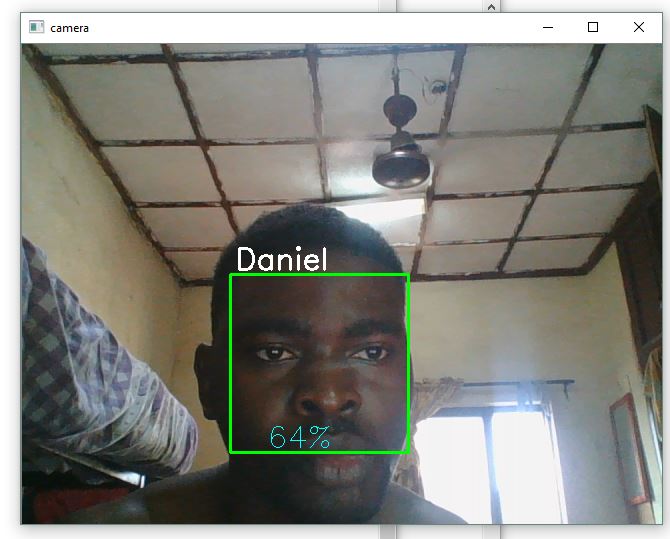


Figure 4.6: RECOGNIZING A FACE

**4.4 BILL OF ENGINEERING MEASUREMENT AND EVALUATION (BEME)**

The cost of all components used in implementing the system is shown in the Bill of Engineering Measurement and Evaluation (BEME). The BEME also shows the cost of each components, the unit price of the components, the quantity of each of the components used and total amount of the components and the overall cost of producing the system.

**Table 4.1: Bill of Engineering Measurement and Evaluation (BEME) for Automated door access system with facial recognition**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S/N** | **Components and Materials** | **Quantity** | **Unit Price (#)** | **Amount (#)** |
| 1 | ATMEGA168 SOCKET | 2 | 1500 | 3000 |
| 2 | ATMEGA168 IC | 2 | 3000 | 6000 |
| 3 | 22pF CAPACITORS | 4 | 150 | 600 |
| 4 | LED | 10 | 20 | 200 |
| 5 | 10kΩ RESISTORS | 5 | 10 | 50 |
| 6 | 16MHz CRYSTAL OSCILLATOR | 1 | 1000 | 1000 |
| 7 | VERO BOARD | 2 | 600 | 1200 |
| 8 | SOLDERING LEAD | 1 | 1500 | 1500 |
| 9 | PUSH BUTTON | 2 | 300 | 600 |
| 10 | JUMPER WIRES | 30 | - | 600 |
| 11 | MALE HEADER PINS | 1 | 500 | 500 |
| 12 | FEMALE HEADER PIN | 2 | 500 | 1000 |
| 13 | FTDI CABLE | 1 | 7500 | 7500 |
| 14 | SERVO MOTOR | 1 | 3500 | 3500 |
| 15 | WOODEN CASE | 1 | 500 | 500 |
| 16 | \*5V DC MOTOR | 1 | 500 | 500 |
| 17 | \*L293D MOTOR DRIVER | 1 | 800 | 800 |
| 18 | \* 5V DC ELECTRONIC LOCK | 1 | 3500 | 3500 |
| 19 | MISCELLANEOUS |  |  | 3000 |
|  | TOTAL |  |  | 35,550 |

All the above listed components with the asterisks (\*) were used at the other stages of development of the project but were not in the final design stage. This is because at the implementation stage I initially used and electronic lock but I had difficulty in in programming the lock to remain at a state. Then I tried using a DC motor to slide the door open and close but I had the same problem so I finally resolve in using the servo motor and that solved the problem.

**CHAPTER FIVE**

**SUMMARY, RECOMMENDATION AND CONCLUSION**

**5.1 SUMMARY OF THE WORK DONE**

The automated door lock system with facial recognition guides against unauthorized access to any building whatsoever hence promoting security of lives and properties in our society. This is possible by ensuring that only the right and authorized people can gain access to a place at the right time hence preventing unauthorized access and to a building to perpetrate evil and also stopping abuse of access privilege.

**5.2 ACHIEVEMENT**

While working on this project, I learnt python programming language and improve my programming skills and competence. I learnt the basic principles of microcontroller, how they work and the potential they have in advancing our technological and computing power. I also dug deep on how to use the open CV for things like age detection and gesture detection. I also learnt how to interface software with hardware. I was able to apply my basic knowledge of automation in selecting the right door opening and closing mechanism. Finally, I was able to create a system that will solve the problems of security in our society thereby contributing to the well-being of humanity at large.

**5.3 CHALLENGES ENCOUNTERED**

* Deciding the door opening and closing mechanism was a difficult task as all the available mechanism had their pros and cons
* Programming the facial recognition software to attain a high level of accuracy was almost an impossible task
* Deciding the right computer vision framework (CV) was a very difficult task as the two major CV available had their pros and cons
* Configuring the framework with the Graphics user interface software (GUI) was challenging because python was not really built for programming GUI software’s
* The accuracy of the haar classifier is very low and this affected the accuracy of the software.
* Classifiers with better accuracy are not readily available to the general public and are very expensive.
* Many factors affected the accuracy of the classifier such as the light of the area, the quality of the image it is seeing which is determined by the quality of the camera.
* The web camera of the system I used in testing the facial recognition software produced a low-quality image with so much noise. This affected the accuracy of the result
* Selecting the best and right electrical component is was a challenging task
* Understanding the basic principles of facial recognition and computer vision was difficult for me due to the broadness of this field and the limited time I have to spend on the project

**5.4 RECOMMENDATION**

The Project is opened for review, upgrade and improvement. The system can be made into an embedded system that can be mounted on the door just like keypads. The OpenCV and the EmguCV can also be made more flexible to work with when trying to use it with other platforms it was not originally designed for. Biometric data can be stolen and replicated hence the CV frameworks should be able to detect between a natural human face and an artificially designed face to make the system more secure and reliable. The haar classifier accuracy is very low and needs to be improved. Also, classifier with higher accuracy should be made available to the general public at affordable prices in order to encourage researchers in this field.

**5.5 CONCLUSION**

The automated door access system with facial recognition displays a more security advanced type of door access system that counters the problem posed by keylocks, the keypad lock and the RFID locks. This system can be modified to match the exact needs of an organization employing this system for security e.g. The time at which individual can gain access to the building can also be programmed into the system. I am confident and rest assured that using this system would lead to a total elimination of security threats and make our society 100% secured

**REFERENCES**

|  |  |
| --- | --- |
| [1] | I. Q. a. F. A. Muhammad Naeem, "FACE RECOGNITION TECHNIQUES AND APPROACHES: A SURVEY," 2015. |
| [2] | A. T. ,. B. ,. R. a. B. N. Ashish Choudhary, "Automatic Attendance System Using Face Recognition," 2016. |
| [3] | V. R. Chawngsangpuii, "DIFFERENT APPROACHES TO FACIAL RECOGNITION," 2015. |
| [4] | X. Lu, "Image Analysis for Face Recognition". |
| [5] | "www.scholarpedia.org/," [Online]. Available: http://www.scholarpedia.org/article/Elastic\_Bunch\_Graph\_Matching. |
| [6] | "https://en.wikipedia.org/wiki/Electronic\_lock," [Online]. Available: https://en.wikipedia.org/wiki/Electronic\_lock. |
| [7] | "http://mathworld.wolfram.com/OrthogonalTransformation.html," [Online]. Available: http://mathworld.wolfram.com/OrthogonalTransformation.html. |
| [8] | A. Kawale, "Fingerprint based locking system," 2013. |
| [9] | H. H. K. TIN, "GENDER AND AGE ESTIMATION BASED ON FACIAL IMAGES," 2011. |
| [10] | T. D. S. A. P. M. A. S. SYED NAVAZ, "FACE RECOGNITION USING PRINCIPAL COMPONENT ANALYSIS," 2013. |
| [11] | "https://www.microchip.com/wwwproducts/en/ATmega168," [Online]. |
| [12] | P. S. Kar, "PRINCIPAL COMPONENT ANALYSIS," 2017. |
| [13] | N. K. Sharma, "Face recognition using LDA," 2017. |
| [14] | N. K. Sharma, "Principal component analysis," 2017. |
| [15] | A. R. K. N. Jain, "Introduction to Biometrics," *Springer science &business media,* 2011. |
| [16] | V. G. a. P. T. K, "A Digital System With Door Lock system using RFID Technology," *International journal of computer Applications,* vol. 5, 2010. |
| [17] | v. p. s. Shervin Emami, "Facial Recognition Using OpenCV," *Journal of Mobile, Embedded and Distributed System,* vol. 4, 2012. |

# **Appendix A**

Code for recognizing a face

import cv2

import numpy as np

import os

import serial

serl = serial.Serial('COM8',9600)

recognizer = cv2.face.LBPHFaceRecognizer\_create()

recognizer.read('trainer/trainer.yml')

cascadePath = "haarcascade\_frontalface\_default.xml"

faceCascade = cv2.CascadeClassifier(cascadePath);

font = cv2.FONT\_HERSHEY\_SIMPLEX

#iniciate id counter

id = 0

# names related to ids: example ==> name1 matches id 1 etc

names = ['None', 'Daniel', 'koyin', 'Ilza', 'Z', 'W']

# Initialize and start realtime video capture

cam = cv2.VideoCapture(0)

cam.set(3, 640) # set video widht

cam.set(4, 480) # set video height

# Define min window size to be recognized as a face

minW = 0.1\*cam.get(3)

minH = 0.1\*cam.get(4)

while True:

ret, img =cam.read()

gray = cv2.cvtColor(img,cv2.COLOR\_BGR2GRAY)

faces = faceCascade.detectMultiScale(

gray,

scaleFactor = 1.2,

minNeighbors = 5,

minSize = (int(minW), int(minH)),

)

for(x,y,w,h) in faces:

cv2.rectangle(img, (x,y), (x+w,y+h), (0,255,0), 2)

id, confidence = recognizer.predict(gray[y:y+h,x:x+w])

# Check if confidence is less them 100 ==> "0" is perfect match

if (confidence >= 50):

id = names[id]

confidence = " {0}%".format(round(confidence))

serl.write('x'.encode())

print("Access Granted")

else:

id = "unknown"

confidence = " {0}%".format(round(100 - confidence))

serl.write('y'.encode())

print("Access Denied")

cv2.putText(img, str(id), (x+5,y-5), font, 1, (255,255,255), 2)

cv2.putText(img, str(confidence), (x+5,y+h-5), font, 1, (255,255,0), 1)

cv2.imshow('camera',img)

k = cv2.waitKey(10) & 0xff # Press 'ESC' for exiting video

if k == 27:

break

# Do a bit of cleanup

print("\n [INFO] Exiting Program and cleanup stuff")

cam.release()

cv2.destroyAllWindows()