

December, 2017.

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR
THE AWARD OF
BACHELOR OF ENGINEERING (B.Eng.) IN COMPUTER
ENGINEERING

SUBMITTED TO THE
DEPARTMENT OF COMPUTER ENGINEERING,
FACULTY OF ENGINEERING,
FEDERAL UNIVERSITY OYE-EKITI, NIGERIA.

CPE/12/0883

ADEWALE, AYODELE ADEOKIJI

DEVELOPMENT OF A PRINCIPAL
COMPONENT ANALYSIS BASED FACE
RECOGNITION SYSTEM USING K-NEAREST
NEIGHBOUR ALGORITHM

CERTIFICATION

This project with the title

**DEVELOPMENT OF A PRINCIPAL COMPONENT ANALYSIS FACE
RECOGNITION SYSTEM USING K-NEAREST NEIGHBOUR ALGORITHM**

Submitted by

ADEWALE, AYODELE ADEOKIJI

(CPE/12/0883)

Has satisfied the regulations governing the award of degree of

BACHELOR OF ENGINEERING (B.Eng) in Computer Engineering

Federal University Oye-Ekiti, Ekiti State Nigeria.

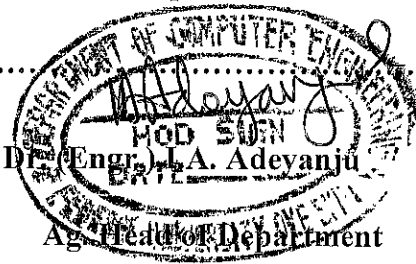
I.A. Adeyanju

20-12-2017

Dr. (Engr.) I.A. Adeyanju

Date

Supervisor



20-12-2017

Date

External Examiner

Date

DECLARATION

This project is a result of my own work and has not been copied in part or in whole from any other source except where duly acknowledged. As such, all use of previously published work (from books, journals, magazines, internet and so on) has been acknowledged within the main report to an entry in the References list.

I agree that an electronic copy or hardcopy of this report may be stored and used for the purposes of plagiarism prevention and detection. I understand that cheating and plagiarism constitute a breach of University Regulations and will be dealt with accordingly.

Copyright

The copyright of this project and report belongs to Federal University, Oye-Ekiti.

Student's full name: ADEWALE AYODELE ADEKUNJI

Sign. & Date:  13/12/2017

DEDICATION

This research work is dedicated to God Almighty, the Alpha and Omega of my life.

ACKNOWLEDGEMENT

I humbly wish to appreciate the management of Federal University Oye-Ekiti, the non-academic staff of the Computer Engineering department, my supervisor and the head of department (HOD) Dr. (Engr.) Ibrahim Adeyanju, my level advisor Engineer Nnamdi Okomba and all other lecturers in the department for their guidance and support throughout my stay in the university. I also acknowledge my parents for their support both financially and emotionally.

I also want to acknowledge my siblings Ayomide, Ayooluwa and Ayofaith. I also acknowledge my class mates Fanijo Samuel, Olisaemeka Isife, Gbenga Olufeyimi, Falokun Oladeji, Waliyullah Raheem, Joshua Ngene, Ibraheem Mutolib, Yemi Omotayo, Oladimeji Oladepo, Olaleye Timileyin and Ubani Bright. I also want to acknowledge my friends Oluwafunmibi Abe, Tolu Orisabinone, Olorundero Pelumi, Prince Marins, Agbramu Watson, Adoghome Miracle, Blessing Omotoriogun, Raheem Hussien and many others I cannot mention by name. God bless you all.

ABSTRACT

Recognition is an important task in many organisations ranging from law enforcement to education. Therefore, organisations are constantly in search of more efficient and error free ways to carry out the recognition process. Existing methods of recognition can be categorized as traditional or technology assisted. The aim of this project is to develop a recognition system that is based on authentication using one physiological trait of an individual.

The proposed recognition system was designed based on unimodal biometrics. The biometric recognition system uses the face as the only physiological trait. The processes involved in the unimodal biometric system include data acquisition, biometric image preprocessing, feature extraction, matching and evaluation using accuracy, false accept rate (FAR) and false reject rate (FRR) as metrics.

The developed system was evaluated using accuracy, false accept rate (FAR), false reject rate (FRR), with each metric giving a positive result. It has an accuracy of 86 %, false accept rate (FAR) of 0.11, false reject rate (FRR) of 0.15 and an average execution time of 3.60 seconds. The results gotten show that the developed system is efficient and can be implemented in other types of biometric systems.

This project work designed and implemented a face biometric based recognition system. This was achieved by extracting the features from the face using PCA and classifying the facial features using K-Nearest Neighbour with Euclidean distance ($K=1$). The developed system can be used in applications such as attendance taking and access control.

Table of Contents

CERTIFICATION	ii
DECLARATION	iii
DEDICATION	iv
ACKNOWLEDGEMENT	v
LIST OF FIGURES	xi
LIST OF TABLES	xiii
CHAPTER ONE	1
INTRODUCTION	1
1.1 Preamble	1
1.2 Statement of Problem.....	2
1.3 Aim and Objectives.....	3
1.4 Scope of Study	4
1.5 Significance of Study	4
1.6 Methods of Study	5
CHAPTER TWO	7
LITERATURE REVIEW	7
2.1 Recognition Systems.....	7

2.1.1	Traditional Recognition System	7
2.1.2	Technology Assisted Recognition	8
2.2	Biometrics Systems.....	9
2.2.1	Face Recognition	12
2.2.2	Fingerprint Recognition.....	15
2.2.3	Iris Recognition	17
2.2.4	Palm Vein Recognition.....	18
2.2.5	Speech Recognition	19
2.2.6	Multi-Modal Biometric Systems	21
2.3	Biometric Image Preprocessing	25
2.3.1	Image Enhancement.....	25
2.3.2	Normalization	26
2.3.3	Binarization.....	27
2.4	Biometric Feature Extraction.....	27
2.4.1	Principal Components Analysis (PCA)	28
2.4.2	Linear Discriminant Analysis (LDA)	31
2.4.3	Elastic Bunch Graph Matching (EBGM)	33
2.5.	Algorithms for Biometric Classification.....	35

2.5.1	Support Vector Machine (SVM)	35
2.5.2	Artificial Neural Network (ANN)	37
2.5.3	Self Organized Map (SOFM)	39
2.5.4	K-Nearest Neighbour (K-NN)	40
2.7	Related Works.....	43
CHAPTER THREE		51
DESIGN METHODOLOGY		51
3.1	Overview of The Face Recognition System	51
3.2	Data Acquisition	51
3.3	Biometric Image Preprocessing	53
3.4	Feature Extraction Using Principal Component Analysis (PCA).....	53
3.5	Classification Using K-Nearest Neighbour	55
3.6	Experimental Set-Up.....	55
3.6	Proposed Evaluation Metrics	56
CHAPTER FOUR		59
SYSTEM IMPLEMENTATION AND RESULTS.....		59
4.1	System Implementation	59
4.2	Individual Results From Test Images	60

4.3	Confusion Matrix Results	62
4.4	Evaluation With Accuracy, FRR and FAR.....	63
CHAPTER FIVE		65
CONCLUSION AND RECOMMENDATIONS		65
5.1	Conclusion	65
5.2	Recommendations.....	65
References.....		66
APPENDIX A.....		74
APPENDIX B.....		75

LIST OF FIGURES

Figure

2.1 Fingerprint sensor.	12
2.2 Palm vein sensor.	12
2.3 A face recognition system processing the image of a human face.	14
2.4 The Human Fingerprint and its different parts	16
2.5 The Five Basic Fingerprint Patterns, (a) Tended Arch (b) Arch (c) Right Loop (d) Left Loop (e) Whorl.	16
2.6 The Human Iris.	18
2.7 (a) An image of the human palm, (b) the infrared image of the palm and (c) the extracted palm vein pattern.	19
2.8 A Typical Speech Recognition System.	21
2.9 Fusion at different levels in a Biometric System.	24
2.10 Standard Eigenfaces: Feature vectors derived using eigenfaces.	30
2.11 Example of Six Classes Using LDA.	33
2.12 Elastic Bunch Map Graphing.	34
2.13 An Overview of the SVM Process.	37

2.15 Brief architecture of a SOM Network.	40
2.14 K-Nearest Neighbour.....	42
3.1 Block Diagram of the Overview of the Biometric Recognition System	52
4.1 The Implementation of the Developed Face Recognition System.	60
4.2 Column Chart Showing the Confusion Matrix.....	63

LIST OF TABLES

Table

2.1 Comparison of Various Biometric Traits.	10
2.2 Summary of Distance Measures in Image Processing.....	43
4.1 Showing The Test Image ID, The Recognised Image ID, The Type of Prediction, the Execution Time and True Positive (TP)/True Negative (TN) /False Positive (FP)/False Negative (FN).	61
4.2 The Confusion Matrix.....	63
4.3 The Accuracy, The False Accept Rate (FAR) and The False Reject Rate (FRR).....	64

CHAPTER ONE

INTRODUCTION

1.1 Preamble

Recognition is the identification of a thing or individual from previous encounters or knowledge. Recognition could also be defined as “the action or process of recognising or being recognised” (Garje & Agrawa, 2012). The process of recognition is carried out by businesses or industries to help them know the background of their employees, those present or absent from work, create records for their employees and assign security clearance to them. Recognition is very helpful when organisations want to determine those who have had access to areas in the building or records, restrict access to certain area or records and to get information or update their records on their employees (Lin, 2000). In education, it is used as measure to determine the identity of a prospective student, create records for students, if the student attending class is registered for the course and to determine if the student writing the exam of a course is who he or she claims to be (FUOYE, 2015).

The methods used presently for recognition can be divided into two major groups which are: Traditional and Technology assisted methods. The traditional method of recognition includes manual recognition (USA Committee on Homeland Security and National Security, 2006) and the use of identification (ID) cards. The technology assisted method of recognition include all the methods that carry out the recognition process with the aid of electronic

equipment or computers such as the use of passwords (Lin, 2000), radio frequency identification (RFID) tags (Olanipekun & Boyinbode, 2015), smart card (Wambugu, 2011), magnetic stripe cards (Deugo, 2015) and biometrics (Shoewu, Makanjuola, & Olatinwo, 2014).

“Biometrics is defined as the unique (personal) physiological characteristics or traits of human body” (Falohun, Fenwa & Oke, 2016). Unique identification of humans mainly for verification and identification can be done efficiently and effectively using Biometric Identification Systems. There are many types of biometric features such as fingerprint, face, voice/speech, iris, palm vein etc. (Mishra & Trivedi, 2011). This project aims to develop a biometric based recognition system using one of the physiological traits (face) of the human body.

1.2 Statement of Problem

Recognition is an important task in many organisations ranging from law enforcement to education. Therefore, organisations are constantly in search of more efficient and error free ways to carry out the recognition process. Existing methods of recognition can be categorized as traditional or technology assisted.

The traditional based methods of recognition are not effective because of challenges ranging from the misidentification by the human identifier to the misplacing of identification cards. The technology assisted method of recognition are generally more effective than the traditional methods because they reduce the risk of errors that are common in the traditional

methods. Technology assisted methods of recognition include all the methods that carry out the recognition process with the aid of electronic equipment or computers. Although the technology assisted methods are generally more effective than the manual systems, most of them still cannot solve the problem of impersonation or loss of identification means.

A biometric based recognition system will help eliminate the problem of impersonation and also help eliminate the problem of losing identification means because no two human beings share the same biometric identifiers and biometric identifiers cannot be misplaced (Falohun, Fenwa & Oke, 2016). This project aims to develop a biometric based recognition system using one of the physiological traits of the human body; the face. The use of one trait instead of multi traits is because uni-modal biometric systems are easier to implement and less expensive compared to multimodal systems (Zuva, Esan & Ngwira, 2014).

The physiological trait (face) was selected because of its universality, high performance, ease of collection and wide usage in forensic and civilian applications. It is also considered among the least intrusive of all biometric verification techniques and is relatively easy to implement.

1.3 Aim and Objectives

The aim of this project is to develop a recognition system that is based on authentication using one physiological trait of an individual. The specific objectives are:

1. To design a face recognition system using principal component analysis (PCA) and K-Nearest Neighbour (KNN).

2. To implement the designed biometric system using a software prototype.
3. To evaluate the effectiveness of the developed biometric system.

1.4 **Scope of Study**

The project will develop a biometric based recognition system. The recognition system will make use of only one biometric trait; the face. It will not include the use of other biometric traits such as speech, palm vein and iris. The project emphasizes the use biometrics for recognition although it might also be applicable to access control.

1.5 **Significance of Study**

This project is situated in the area of biometric systems. There are several application areas of biometrics including:

- **Access Control:** Biometrics can be used to limit access to a secure area of system that is only those that have their biometric details in the system are allowed to gain access. The access control process is usually in two steps which are identification and authentication. Biometrics can be used in this two steps, identification (requiring a one-to-many search in the templates database) and comparison authentication (this involves a one to one comparison of the measured biometric with the template that is associated with the claimed identity) (Falohun, Fenwa, & Oke, 2016). Situations in which biometrics can be used for access control include: when a access to a room is to be limited to only authorized users

for example the vault of a bank or a laboratory and when access to a computer system is to be limited to only authorized users for example a computer system containing business plans.

- **Time and Attendance Management:** The problems of time and attendance systems mostly used today cannot be over emphasized. Biometrics helps solve the problem of manipulation of time and attendance management systems. It also saves people from having to bother about knowing passwords or misplacing tokens that come with other forms of time and attendance management systems (Shoewu, Makanjuola, & Olatinwo, 2014).
- **Surveillance:** Biometrics can help automate screening large crowds for fugitives, missing children, or for border control (in airports or at land borders). The cost of such implementations of biometrics is very high and the rates for existing biometric systems vary (Jain, Ross, & Prabhakar, 2004).

1.6 Methods of Study

The methods to be used in achieving this project will include the following:

- i. Continual review of relevant literatures in the library and online resources related to recognition, feature extraction, biometrics and image processing.
- ii. Interaction with recognition system experts and biometric systems experts.
- iii. Design of the face biometric recognition system.

- iv. Biometric data capturing of users will be carried out; data will be collected from at least thirty (30) users.
- v. The biometric data captured will be preprocessed appropriately.
- vi. Feature extraction would be done on the preprocessed biometric images.
- vii. Implementation of the system using extracted features.
- viii. Evaluation of the implemented biometric system using false acceptance rate (FAR), false rejection rate (FRR) and accuracy.

CHAPTER TWO

LITERATURE REVIEW

2.1 Recognition Systems

Recognition systems are systems that help in the recognition process. Recognition is very important in many organisations, industries and the education sector which has led to different recognition systems to be developed. Existing methods of recognition taking can be categorized as traditional or technology assisted.

2.1.1 Traditional Recognition System

The traditional recognition system include recognition systems that the done is manually and processed manually. Examples of this system include the manual recognition and the use of identification cards (ID cards). The manual recognition process which is commonly used in the education sector involves a human identifier tries to recognise an individual either by information provided by the individual or with previous knowledge gained by meeting the individual on at a previous time (Nakajimaa, Pontilb, Heiselec, & Poggioc, 2003). This method is easy to cheat as anybody can claim an identity which is not theirs and it is difficult to process as the processing is done manually.

The identification card (ID card) replaces manual recognition process with a plastic card that carries the details of the individual. With this recognition method the individual just has to present the plastic card with his or her details on it to whoever needs to carry out the

recognition process. This system does not solve impersonation and misplacing of the identification means (Lin, 2000).

2.1.2 Technology Assisted Recognition

Technology assisted recognition systems are ones that the recognition process is done with the aid of electronic equipment such as computers. Technology assisted attendance systems include as the use of radio frequency identification (RFID), smart card, electronic tags, barcode badges, magnetic stripe cards and biometrics (Josphineleela & Ramakrishan, 2012) among others. Technology assisted recognition systems are more effective and efficient than the traditional systems (Deugo, 2015).

A radio frequency identification (RFID) based recognition system consists of a RFID reader, RFID tags, computer system or a microcontroller (Moharil & Dandare, 2016), and host system application. RFID based recognition system uses radio waves to transfer data on the RFID tag to the recognition system (Chiagozie & Nwaji, 2012). Each student is given a RFID tag which is typically embedded into their ID cards, the RFID reader is incorporated into the computer system or microcontroller and as the student arrive for lecture their ID cards are scanned and compared to those in the database by the host system application. If there is a match, the relevant information necessary for recognition are recorded and the information is used to compute the individuals details (Olanipekun & Boyinbode, 2015).

A smart card based recognition system consists majorly of a smart card reader and smart cards (Ling, 2012). The students are issued smart cards which have their details programmed

on them. For the recognition to be carried out, each student's smart card is scanned by the smart card reader and the student details necessary for the recognition to be recorded are read from the smart card and the details are recorded in the database through a computer system which the smart card reader is integrated on. All the computations that are to be carried out on the individual details are carried out by the program on the computer system (Wambugu, 2011).

For a barcode based recognition system, the main hardware device that is needed is the barcode scanner (Mahmod, 2005). The student ID cards will have barcodes at their backs which will contain the necessary student details. The barcode scanner is integrated on a computer system. To carry out recognition, the barcode at the back of the student ID card is scanned and the student's details necessary to compute the details are read by the barcode scanner and stored in the database through the computer system. The individual's details are computed on the system eliminating the need to compute manually (Sudha, Shinde, Thomas, & Abdugani, 2015).

2.2 Biometrics Systems

“Biometrics is defined as the unique (personal) physiological characteristics or traits of human body” (Falohun, Fenwa & Oke, 2016). It is mostly used in the area of identifying a person through their physiological traits (Chaurasia, 2012). Biometric systems use an automated technique of recognizing a person based on physiological and behavioral traits (Zuva, Esan, & Ngwira, 2014). Biometric identifiers are the distinctive measurable characters

used to label and describe individuals (Adeyanju, Omidiora, & Oyedokun, 2015). The biometric traits include: face, fingerprint, palm vein, finger vein, iris and speech. A comparison of different biometric traits based on the following criteria universality (how common is it), distinctiveness (is it easily distinguishable between individuals), permanence (does it change over time), collectability (is it easy to collect), performance (how accurate is it as a biometric identifier), acceptability (do the user find it intrusive) and circumvention (ease of deceiving systems based on the biometric trait) is shown in table 2.1 (Jain, Ross, & Prabhakar, 2004).

Table 2.1 Comparison of Various Biometric Traits. (Jain, Ross, & Prabhakar, 2004)

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Key: H-high, M-medium and L-low

Biometric systems can either be used as identification system or an authentication (verification) system. When a biometric system is used as an identification system its purpose is to discover the identity of an unknown person. It does this by comparing the image of a biometric data gotten from the individual to those in the database in order to find a match. The identification system is used by law enforcement agencies to search for criminals when they are trying to solve a crime (Shoewu, Makanjuola, & Olatinwo, 2014). When a biometric system is used as an authentication system, then its purpose is to verify if the individual is actually who he or she claims to be. It does this by searching the database for a match to the biometric data gotten from the individual (Shoewu, Makanjuola, & Olatinwo, 2014). A recognition system is an implementation of the identification system.

There are two modes of operation for biometric systems which are Unimodal in which just one physiological trait is used and multimodal in which more than one physiological trait is used. Most of the biometric systems in use are unimodal (Raghavendra, Ashok, & Hemantha, 2010). The mode of operation used by a biometric system depends on the available funds and the purpose for developing the system. Multimodal biometric systems are more efficient but costlier to implement than unimodal biometric systems.

A very important process when developing a biometric system is data acquisition. Data acquisition is the process of sensing and imaging of the read biometric trait. The data acquisition sensor must be able to detect, locate, recognize and take an image of the biometric trait (Jain, Ross, & Prabhakar, 2004). Examples of data acquisition sensors include camera,

fingerprint sensor, hand vein sensor and microphone. Figures 2.1 and 2.2 show a fingerprint and palm vein scanner respectively. The image of the biometric trait is the required data for the biometric system which all the necessary image preprocessing steps and processing steps to get the necessary information required for matching to be carried out.



Figure 2.1 Fingerprint sensor. (Shoewu, Makanjuola, & Olatinwo, 2014)



Figure 2.2 Palm vein sensor. (Watanabe, Endoh, Shiohara, & Sasaki, 2005)

2.2.1 Face Recognition

A face is a unique anatomical feature which contains the eyes, nose and mouth. Human beings have been using the face as a means of recognition for ages. The human brain has

developed highly specialized areas dedicated to the analysis of the facial images (Anila & Devarajan, 2012). Over the years advancement in computing capability has enabled face recognition to become automated. It can now be used for both verification and identification (open-set and closed-set) (USA Committee on Homeland Security and National Security, 2006).

Face recognition was started around the 1960s and the first semi-automated system for face recognition required the administrator to locate features (such as eyes, ears, nose, and mouth) on the photographs before it calculated distances and ratios to a common reference point, which were then compared to reference data (USA Committee on Homeland Security and National Security, 2006). “Face recognition systems recognize human face using facial features” (Adeyanju, Omidiora, & Oyedokun, 2015). Although face recognition has increased in reliability significantly over time, it is still not accurate all the time. The ability to correctly classify the image of the face depends the following variables which include lighting, pose, facial expressions and image quality (Anila & Devarajan, 2012). There are two major approaches to solving the face recognition problem: geometric (feature based) and photometric (view based) (USA Committee on Homeland Security and National Security, 2006).

A face recognition system must be able to detect the face (face detection), locate the face and recognize the face. Face detection involves the process of determining that image fed into the face recognition system actually contains a face. After detecting the face it has to be able

to locate the face in the image and determine where the features of the face are located, recognize it and extract the necessary facial features. Figure 2.3 shows a face recognition system processing the image of a human face (Jain, Ross, & Prabhakar, 2004). In face recognition, the following features are important for system recognition: nose, eyes, eyebrows, mouth and nostril. Face recognition is widely accepted by users because it is not intrusive.

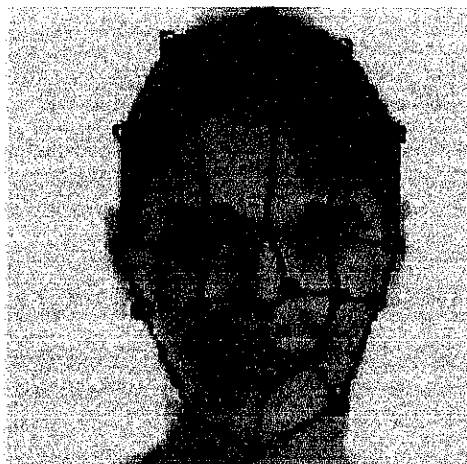


Figure 2.3 A face recognition system processing the image of a human face. (Jain, Ross, & Prabhakar, 2004)

2.2.2 Fingerprint Recognition

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. The endpoints and crossing points of ridges are called minutiae. The upper skin layer segments of the finger are the ridges while the lower segments are the valleys (Shoewu, Makanjuola, & Olatinwo, 2014). It is a widely accepted assumption that the minutiae pattern of each finger is unique and does not change during one's life. Ridge endings are the points where the ridge curve terminates, and bifurcations are where a ridge splits from a single path to two paths at a Y-junction (Mishra & Trivedi, 2011). Figure 2.4 shows the human fingerprint and its different parts. When human fingerprint experts determine if two fingerprints are from the same finger, the matching degree between two minutiae pattern is one of the most important factors. The five basic fingerprint patterns are arch, tended arch, left loop, right loop and whorl as shown in figure 2.5.

Fingerprint recognition systems are the most widely used biometric systems in different application areas because it is the most mature and accepted. It is the most accurate biometric traits and the probability of two fingerprints being the same is 1 in 1.9×10^{15} (Chaurasia, 2012). Fingerprint recognition proceeds by identifying all the minutiae points and then extracting their features and last is to match the two points. Fingerprint Recognition involves three main steps. These steps need to be followed so that accurate matching of fingerprints can be performed. These steps include Image Pre-processing, Minutiae detection and feature extraction and finally Minutiae Matching (Chaurasia, 2012). Minutiae detection is a key part

of fingerprint recognition because it is the minutiae that shows the distinctiveness between fingerprint patterns.

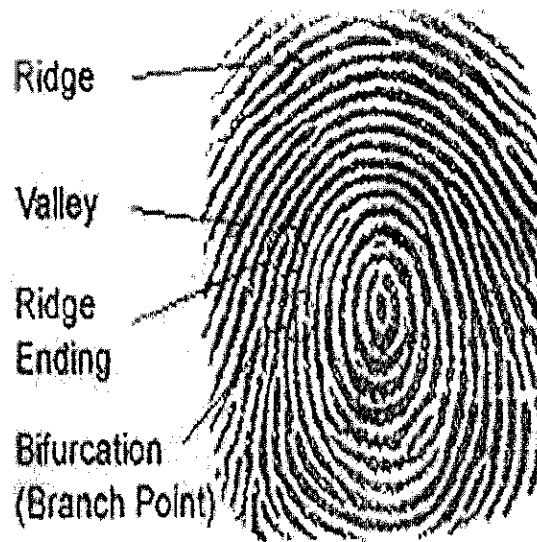


Figure 2.4 The Human Fingerprint and its different parts. (Chaurasia, 2012)

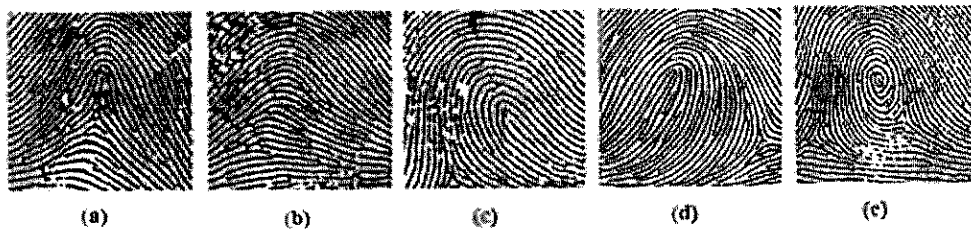


Figure 2.5 The Five Basic Fingerprint Patterns, (a) Tended Arch (b) Arch (c) Right Loop (d) Left Loop (e) Whorl. (Shoewu, Makanjuola, & Olatinwo, 2014)

2.2.3 Iris Recognition

The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye. The iris is perforated close to its center by a circular aperture known as the pupil. The function of the iris is to control the amount of light entering through the pupil, and this is done by the sphincter and the dilator muscles, which adjust the size of the pupil. The iris' unique epigenetic pattern remains stable throughout adult life making a very good biometric traits for biometric systems (Masek, 2003). Figure 2.6 shows the image of an iris.

The stages of iris recognition can be divided into three stages and these stages are segmentation (locating the iris region in an eye image), normalization (creating a dimensionally consistent representation of the iris region), and feature encoding (creating a template containing only the most discriminating features of the iris). The segmentation stage can be carried out using Hough Transform, Daugman's Integro-differential Operator or Active Contour Models. Normalization can be carried out using Daugman's Rubber Sheet Model, Image Registration or Virtual Circles. Feature encoding can be carried out using Laplacian of Gaussian Filters, Haar Wavelet, Zero-crossings of the 1D wavelet, Log-Gabor Filters, Gabor Filters or Wavelet Encoding (Masek, 2003). Although iris recognition is very reliable, it is considered intrusive by most end users (Raghavendra, Ashok, & Hemantha, 2010).

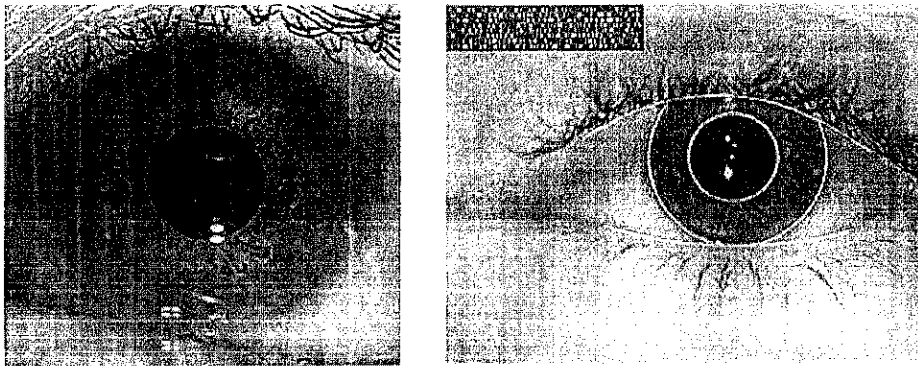


Figure 2.6 The Human Iris. (Jain, Ross, & Prabhakar, 2004).

2.2.4 Palm Vein Recognition

Palm vein is the vascular patterns of an individual's palm and a palm vein biometric system uses the vascular patterns of an individual's palm as personal identification data (Watanabe, Endoh, Shiohara, & Sasaki, 2005). It offers a high degree of privacy and security for biometric recognition because intrinsic physiological patterns are naturally hard to observe. The palm vein imaging requires near-infra-red (NIR) illumination for extracting the complex vascular structures residing inside the palm (Mirmohamadsadeghi & Drygajlo, 2011).

A palm unlike the finger or the back of a hand has a broader and more complicated vascular pattern and thus contains a wealth of differentiating features for personal identification. It has no hair which can be an obstacle for photographing the blood vessel pattern, and it is less susceptible to a change in skin color (Watanabe, Endoh, Shiohara, & Sasaki, 2005). Figure 2.7 below shows the image of a palm, the infrared image of the palm and the extracted palm vein pattern.

In palm vein recognition feature extraction from NIR images (finding efficient descriptors for palm vein appearance) is a key issue. There are different feature extraction methods that have been studied and developed for palm vein, dorsal hand vein and finger vein recognitions such as Hessian phase, localized Radon transform, ordinal code, Laplacianpalm based on Principal Component Analysis, complex matched filtering, repeated line tracking (Mirmohamadsadeghi & Drygajlo, 2011).

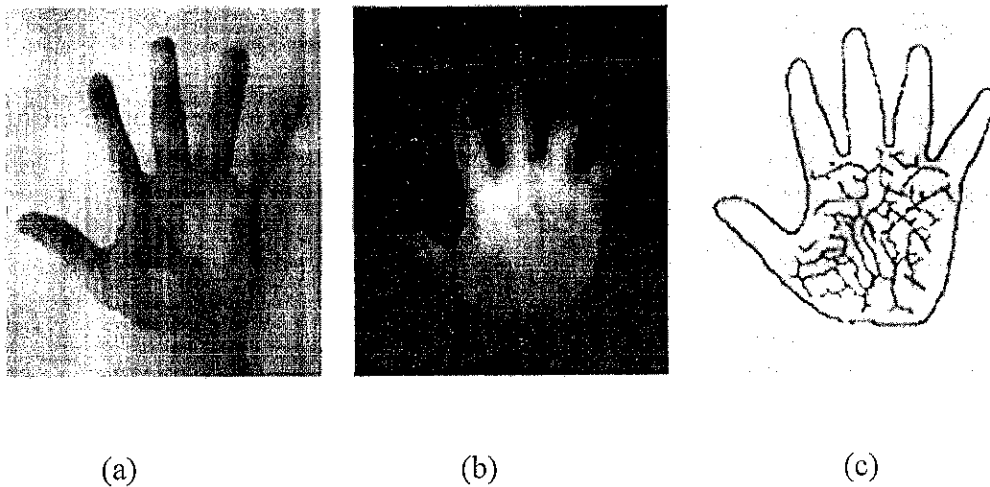


Figure 2.7 (a) An image of the human palm, (b) the infrared image of the palm and (c) the extracted palm vein pattern. (Watanabe, Endoh, Shiohara, & Sasaki, 2005)

2.2.5 Speech Recognition

The primary means of communication between people is speech (Juang & Rabiner, 2004). Speech recognition is natural and easily accepted by the end-user. Speech recognition is divided into two related speech tasks which are: speech understanding and speech

recognition. Speech understanding is getting the meaning of a statement such that one can respond properly whether or not one has correctly recognized all of the words while Speech recognition is simply transcribing the speech without necessarily knowing the meaning of the statement (Paul, 1990). Speech recognition systems can be divided into the independent speaker verification where Linear Prediction Cepstral Coefficients (LPCC) can be used, feature extraction where Mel Frequency Cepstral Coefficients (MFCC) can be used and the opinion generator where Gaussian Mixture Model (GMM) can be used (Raghavendra, Ashok, & Hemantha, 2010).

The input of a speech recognition system is a stream of sampled and digitized speech data which is matched against stored patterns which represent various sounds in the language which the speech recognition system was developed in. The stored patterns represent sound units (words, phonemes) and linguistic constraints (Raj & Singh, 2011). Speech recognition systems face the following difficulties: acoustic patterns which could either be systematic variations or natural variations, linguistic patterns are hard to characterize and pattern matching algorithms are by nature inexact. Figure 2.8 shows a typical speech recognition system which shows the speech input, the speech recognizer, the acoustic model, the pronunciation model and the language model (Raj & Singh, 2011).

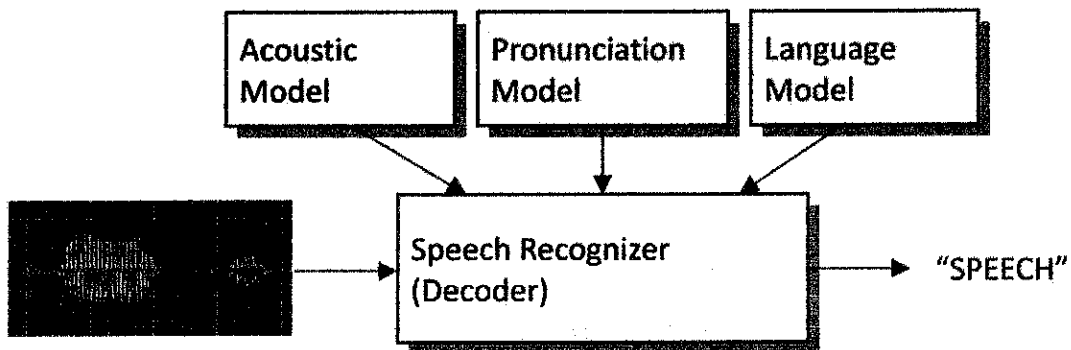


Figure 2.8 A Typical Speech Recognition System. (Raj & Singh, 2011)

2.2.6 Multi-Modal Biometric Systems

Majority of the biometric systems in use today are unimodal biometric systems. Unimodal biometric systems (systems which use only one biometric trait) are susceptible to noise intra-class variation, spoof attacks and so on. Multimodal biometric systems are designed to use more than one biometric data which makes them more reliable because of the presence of multiple, independent pieces of evidence thus handling the limitations of the unimodal biometric systems (Raghavendra, Ashok, & Hemantha, 2010).

An advantage of multimodal biometric systems is that offer substantial improvement in the matching accuracy of a biometric system depending upon the information being combined and the fusion methodology adopted. They also addresses the issue of non-universality or insufficient population coverage, It is increasingly difficult (if not impossible) for an impostor to spoof multiple biometric traits of a legitimately enrolled individual. Another

advantage is that they also effectively address the problem of noisy data, they also help in the continuous monitoring or tracking of an individual in situations when a single trait is not sufficient and a multimodal biometric system may also be viewed as a fault tolerant system which continues to operate even when certain biometric sources become unreliable due to sensor or software malfunction, or deliberate user manipulation (Ross, Nandakumar, & Jain, 2006).

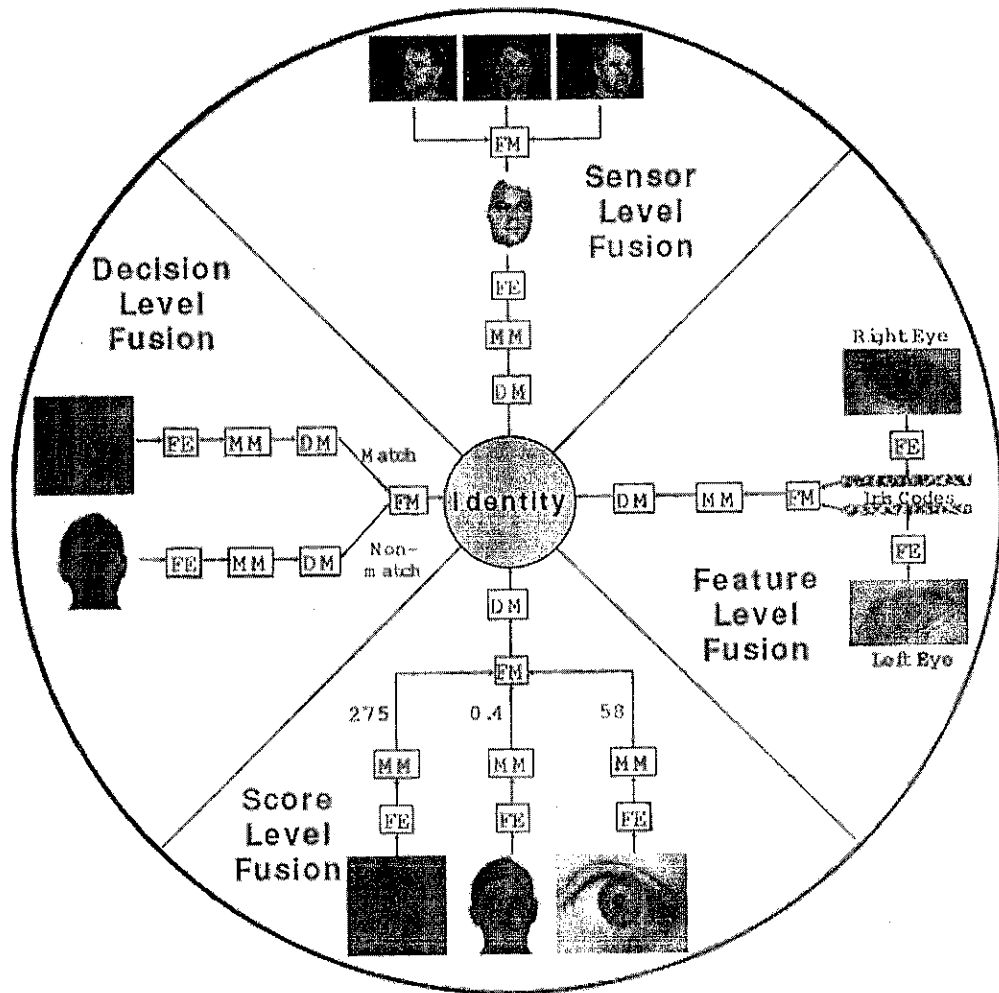
The process of combining the information provided by multiple biometric systems is called fusion. Fusion can be accomplished at various levels in a biometric system. The levels of fusion are broadly classified as (i) fusion prior to matching (ii) fusion after matching (Raghavendra, Ashok, & Hemantha, 2010). Fusion prior to matching involves integration of information from multiple biometric sources at the sensor level or at the feature level (Ross, Nandakumar, & Jain, 2006). Feature level fusion refers to combining different feature sets extracted from multiple biometric sources. To fuse the data at sensor level, the multiple cues must be compatible and correspondence between points in raw data must be known in advance (Raghavendra, Ashok, & Hemantha, 2010). However fusion at this level is difficult in practice because feature sets of various modalities may not be compatible and concatenation is not possible when feature sets are incompatible.

Fusion after matching can be divided into four categories dynamic classifier selection, fusion at the decision level, fusion at the rank level and fusion at the match score level (Ross, Nandakumar, & Jain, 2006). The dynamic classifier selection chooses the results of that

biometric source which is most likely to give the correct decision for the specific input pattern. Fusion at the match score level involves when each biometric system outputs a match score indicating the proximity of the input data to a template and is known as fusion at the measurement level or confidence level.

Fusion at the decision level can take place when each biometric system independently makes a decision about the identity of the user (in an identification system) or determines if the claimed identity is true or not (in a verification system). Fusion at the rank level involves carrying out the fusion when the output of each biometric system is a subset of possible matches (i.e., identities) sorted in decreasing order of confidence (Ross, Nandakumar, & Jain, 2006). Most of the multimodal biometric systems fuse information at the match score level or decision level. Fusion at the decision level is considered to be rigid due to the availability of limited data set therefore fusion at the match score level is preferred, as it is relatively easy to access and combine the scores presented by the different unimodal biometric system (Raghavendra, Ashok, & Hemantha, 2010).

A pie chart illustrating fusion at the different levels, is shown in figure 2.9. It shows when the features are extracted, when they are matched, when fusion occurs and when the system makes a decision. Each of the quadrants represent one of the four types of fusion which are fall under one of the two categories of fusion which are decision level fusion (fusion after matching), sensor level fusion(fusion prior to matching), feature level fusion (fusion prior to matching) and score level fusion (fusion after matching).



FE: feature extraction module; MM: matching module; DM: decision-making module; FM: fusion module.

Figure 2.9 Fusion at different levels in a Biometric System. (Nandakumar, 2008)

2.3 Biometric Image Preprocessing

Image processing is the process of getting the required data from an image. Image processing can be divided into the following stages: Image acquisition (getting the required image), Image enhancement (highlighting certain features of interest in an image), Image restoration (an area that also deals with improving the appearance of an image), Color image processing, Wavelets and Multiresolution processing and Object recognition to mention a few (Gonzalez & Woods, 2002). Biometric image preprocessing can be divided into three parts namely: image enhancement, normalization and binarization.

2.3.1 Image Enhancement

In biometrics after the image has been acquired, the preprocessing process begins starting from conversion of the images to greyscale, if they colored. After converting them to greyscale then image enhancement is carried out. "Image enhancement is the process of manipulating an image so that the result is more suitable than the original for a specific application". Image enhancement is problem based therefore the image enhancement technique selected is determined by what type of enhancement is necessary. Image enhancement is subjective (Gonzalez & Woods, 2002). Image enhancement can be done either in the spatial domain or the frequency domain.

In the spatial domain the enhancement operates directly on pixels. The value of a pixel with coordinates (x, y) in the enhanced image F^{\wedge} is the result of performing some operation on the pixels in the neighbourhood of (x, y) in the input image, F . Neighbourhoods can be any shape,

but usually they are rectangular. Examples of spatial domain image enhancement include; contrast image enhancement, negative image enhancement and histogram image enhancement etc (Chaurasia, 2012).

For image enhancement in the frequency domain the enhancement operates on Fourier transfer of an image. We simply compute the Fourier transform of the image to be enhanced, multiply the result by a filter (rather than convolve in the spatial domain), and take the inverse transform to produce the enhanced image (Chaurasia, 2012).

2.3.2 Normalization

Normalization is the process of standardizing the intensity values in a biometric image so that the intensity values lie within a desired range. It can be done by adjusting the range of grey-level values in the image or by using histogram equalization (Josphineleela & Ramakrishan, 2012).

The histogram of a digital image with gray levels in the range $[0, L-1]$ is a discrete function $h(r_k) = n_k$, where r_k is the k th gray level and n_k is the number of pixels in the image having gray level r_k . It is common to normalize a histogram by dividing each of its values by the total number of pixels in the image, denoted by n . Thus, a normalized histogram is given by $p(r_k) = \frac{n_k}{n}$ for $k=0, 1, \dots, L-1$. Note that the sum of all components of a normalized histogram is equal to 1 (Gonzalez & Woods, 2002).

2.3.3 Binarization

Binarization is the process of converting the greyscale image into binary image. A binary image is an image represent with one (1) and zero (0) values. Digital systems work with binary therefore the need for the conversion of the images to binary images.

To carry out binarization, a threshold value is determined and the pixel which have a higher value than the threshold value are converted to white pixels and the pixel with values less than or equal to the threshold value are the black pixels (Chaurasia, 2012).

2.4 Biometric Feature Extraction

Biometric feature extraction is the process of getting features that will be useful in classifying and recognition of biometric images. Feature extraction can also be defined as transforming input data into a set of features. This is done after the image sensing and preprocessing stages. It describes the relevant shape information contained in a pattern so that the task of classifying the pattern is made easy by a formal procedure (Kumar & Bhatia, 2014). In pattern recognition and image processing, feature extraction is a special form of dimensionality reduction. The goal of feature extraction is to represent the most relevant information from the input data with little storage space (reduced dimensionality).

Feature extraction can be divided into two general stages: feature selection and classification. Feature selection is the process of selecting the most meaningful features that best describe the input data. A good feature set contains discriminating information, which can distinguish

one object from other objects (Kumar & Bhatia, 2014). Feature selection is critical to the feature extraction process because the classifier will not be able to recognize from poorly selected features. Classification is the process of grouping the selected featured that are related based on a predefined criteria.

Feature extraction techniques include Template matching, Deformable templates, Unitary Image transforms, Graph description, Projection Histograms, Contour profiles, Zoning, Geometric moment invariants, Zernike Moments, Spline curve approximation, Fourier descriptors, Gradient feature and Gabor features (Jain, Ross, & Prabhakar, 2004). Feature extraction approaches include Fourier descriptor, Principal component analysis (PCA), Gabor filter, Independent Component Analysis (ICA) and Fractal theory technique (Kumar & Bhatia, 2014).

2.4.1 Principal Components Analysis (PCA)

Principal Components Analysis (PCA) commonly referred to as the use of eigenfaces is seen as one of the most important results from applied linear algebra. PCA is a simple, non-parametric method of extracting of extracting relevant data from confusing data set (Shlens, 2003). The PCA approach is used to reduce the dimension of the data by means of data compression basics and reveals the most effective low dimensional structure of image patterns. This reduction in dimensions removes information that is not useful and precisely decomposes the image structure into orthogonal (uncorrelated) components known as



eigenfaces (USA Committee on Homeland Security and National Security, 2006). The PCA algorithm is stated thus (Omidiora, Fakolujo, Ayeni, & Adeyanju, 2008):

1. Center the data: the images that will be used to train the system must be centered. This is done by subtracting the mean image from each of the training images. A column vector such that each entry is the mean of all corresponding pixels of the training images (original data) is known as the mean image.
2. Create data matrix: after the training images (original data) have been centered they are combined to create the data matrix A of size $N \times M$ with M being the number of training images and each image is represented by a column.
3. Create covariance matrix: to create the covariance matrix the data matrix is multiplied by its transpose.

$$\Omega = AA^T \quad (2.1)$$

4. Compute the eigenvalues and eigenvectors: after computing the covariance matrix, the corresponding eigenvalues and eigenvectors of the covariance matrix are calculated using the formula below.

$$\Omega V = \Lambda V \quad (2.2)$$

Where, V is the set of eigenvectors associated with the eigenvalues Λ .

5. Order eigenvectors: the eigenvectors are then arranged in order from the highest to the lowest making sure that only the eigenvectors associated with non-zero eigenvalues are selected. The matrix of eigenvectors formed is the eigenspace also known as the projection matrix.

6. Project training images (original data): this is the process of projecting each of the centered image into the eigenspace. This is done by calculating the dot product of centered image with each of the ordered eigenvectors (projected matrix). The new vector of the projected image should have as many values as the eigenvector matrix.

PCA is sensitive to the relative scaling of the original variables. Depending on the field of application, it is also named the discrete Karhunen– Loeve transform (KLT), the Hotelling transform or proper orthogonal decomposition (POD) (Kumar & Bhatia, 2014). Figure 2.10 shows an example of feature vectors gotten using eigenfaces derived from PCA.

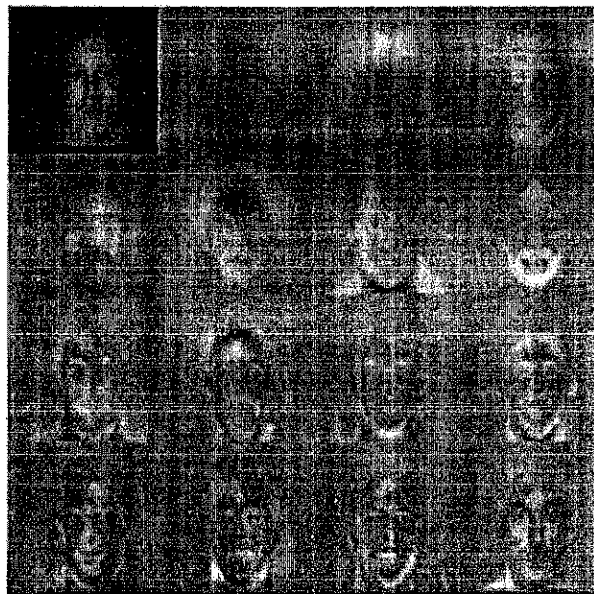


Figure 2.10 Standard Eigenfaces: Feature vectors derived using eigenfaces. (USA Committee on Homeland Security and National Security, 2006).

2.4.2 Linear Discriminant Analysis (LDA)

Linear Discriminant Analysis (LDA) is a statistical approach for classifying samples of unknown classes based on training samples with known classes. This technique aims to maximize between-class (i.e., across users) variance and minimize within-class (i.e., within user) variance. When dealing with high dimensional data, this technique faces the small sample size problem that arises where there are a small number of available training samples compared to the dimensionality of the sample space (USA Committee on Homeland Security and National Security, 2006). Figure 2.11 shows an example of six classes of face images created using LDA. The algorithm for LDA is stated thus (Omidiora, Fakolujo, Ayeni, & Adeyanju, 2008):

1. Calculate the within class scatter matrix: this is a measure of the amount of scatter between items in the same class. A scatter matrix (S_i) for the i th class is calculated as the sum of the covariance matrices of the centred images in that class.

$$S_i = \sum_{x \in x_i} (x - m_i)(x - m_i)^T \quad (2.3)$$

where, m_i is the mean of the images in the class.

The within class scatter matrix (S_w) is the sum of all the scatter matrices and is calculated using the equation below.

$$S_w = \sum_{i=1}^C S_i \quad (2.4)$$

where, C is the number of classes.

2. Calculate the between class scatter matrix: this is a measure of the amount of scatter between classes. It is calculated as the sum of the covariance matrices of the difference between the total mean and the mean of each class. It is denoted as S_B and the equation for computing it is shown below.

$$S_B = \sum_{i=0}^C n_i (m_i - m)(m_i - m)^T \quad (2.5)$$

where, n_i is the number of images in the class, m_i is the mean of the images in the class and m is the mean of all the images.

3. Solve the generalized eigenvalue problem: the next step is to compute the generalized eigenvectors (V) and eigenvalues (Λ) of the within class and between class scatter matrices using the equation below.

$$S_B V = \Lambda S_W V \quad (2.6)$$

4. Keep first $C-1$ eigenvectors: the eigenvectors are then sorted using their associated eigenvalues from the highest to the lowest. The first $C-1$ eigenvectors are kept forming the Fisher basis vectors.
5. Project images onto Fisher basis vectors: this is the process of projecting each of the original images onto the fisher basis vectors. This is done by calculating the dot product of the original image with each of the fisher basis vectors. This is done because these are the points that the line has been created to discriminate, not the centered images.



Figure 2.11 Example of Six Classes Using LDA. (USA Committee on Homeland Security and National Security, 2006)

2.4.3 Elastic Bunch Graph Matching (EBGM)

Elastic Bunch Graph Matching (EBGM) relies on the concept that real face images have many nonlinear characteristics that are not addressed by the linear analysis methods, such as variations in illumination (outdoor lighting vs. indoor fluorescents), pose (standing straight vs. leaning over) and expression (smile vs. frown). EBGM is a feature extraction algorithm used mostly in face recognition systems (Bolme, 2003). A Gabor wavelet transform creates a dynamic link architecture that projects the face onto an elastic grid. The Gabor jet is a node on the elastic grid, notated by circles on the shown in figure 2.12, which describes the image behavior around a given pixel. It is the result of a convolution of the image with a Gabor filter, which is used to detect shapes and to extract features using image processing. The difficulty with this method is the requirement of accurate landmark localization, which can sometimes be achieved by combining PCA and LDA methods (USA Committee on

Homeland Security and National Security, 2006). EGBM can be carried out using the following steps (Bolme, 2003):

Step 1: jets are selected by hand to serve as examples of facial features

Step 2: create a bunch graph in which each node of the bunch graph corresponding to a facial landmark and containing a bunch of model jets extracted from the model imagery.

Step 3: for every image, landmark point are located. A novel jet is first extracted from a novel image. This jet's displacement from the actual location is estimated by comparing it to the most similar model jet from the corresponding bunch.

Step 4: for each image a face graph is created by extracting a jet for each landmark. The locations of the landmarks and the value of the jets are contained in the graph.

Step 5: landmark locations and jet values are used as functions to compute face similarity.

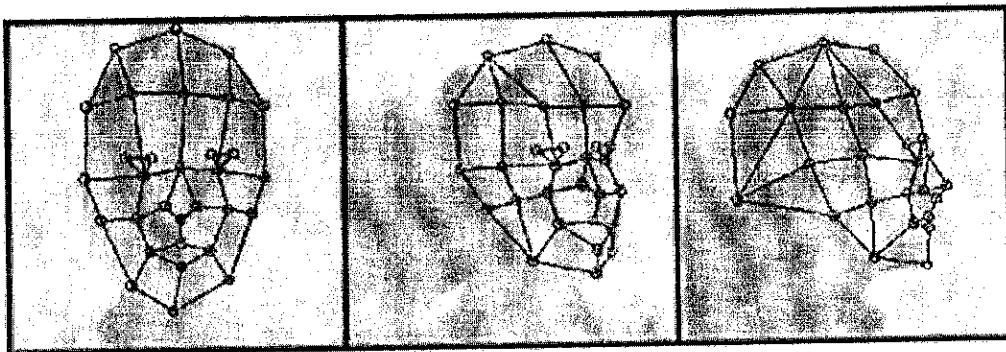


Figure 2.12 Elastic Bunch Map Graphing. (USA Committee on Homeland Security and National Security, 2006)

2.5. Algorithms for Biometric Classification

Machine learning has provided algorithms that have been used for biometric classification because it is about designing algorithms that allow a computer to learn. Learning here means finding statistical regularities or other patterns in the data (Ayodele, 2010). Algorithms that have been used for biometric classifications include: support vector machine (SVM), K-nearest neighbor (KNN), artificial neural network (ANN), fuzzy logic, self-organized map (SOM) and counter propagation network (CPN).

2.5.1 Support Vector Machine (SVM)

Support vector machine (SVM) is one of the most useful techniques in classification problem. An obvious example is facial recognition. SVM is a supervised learning model with associated learning algorithm that analyses data and recognize patterns, used for classification. It takes a set of input data and predicts, for each given input which of two possible classes forms output, making it a non-probabilistic binary linear classifier (Jayaram, Prashanth, & Taj, 2015).

Normally SVMs are limited to solving binary classification problems for linear separable classes but this limitation can be overcome by using sophisticated kernel functions enabling it to solve more complex binary classification problems (Scheidat, Leich, Alexander, & Vielhauer, 2009). Since the feature vectors in biometrics is not linear separable because they come from several people, the well-known radial basis function kernel is normally used. SVM is implemented by : For each person p of the N persons that are to be

enrolled the SVM is trained using the enrolment samples of p as positive samples and all other enrolment samples of the remaining $N - 1$ persons as negative samples. After the enrolment process the entire system consists of N SVMs, one for each enrolled person (Scheidat, Leich, Alexander, & Vielhauer, 2009).

Based on this system structure it is easily possible to devise an identification and verification procedure for new samples from users that try to authenticate on the system. In the verification a user tries to be verified as an enrolled person. The sample from this user is presented to the matching SVM. The user is then accepted or rejected based on the SVM output. The identification process works similarly. Here the sample of the user is presented to all SVMs. If no SVM accepts the sample, the user is rejected. If only one SVM accepts the sample, the user is identified as the corresponding person. If more than one SVM accepts the sample, the result is ambiguous which again leads to the rejection of the user (Scheidat, Leich, Alexander, & Vielhauer, 2009). The SVM algorithm is shown in figure 2.13.

However, the SVM cannot be defined when the feature vector of the sample is missing an item application. In this framework, the support vector machine (SVM) has been successfully used in the classification algorithm, which can be applied to the spatial original appearance or the applied extraction method after the subspace feature. The advantage of traditional neural network SVM classifier is that SVM can realize the better performance of generalization (Kamalakumari & Vanitha, 2017).

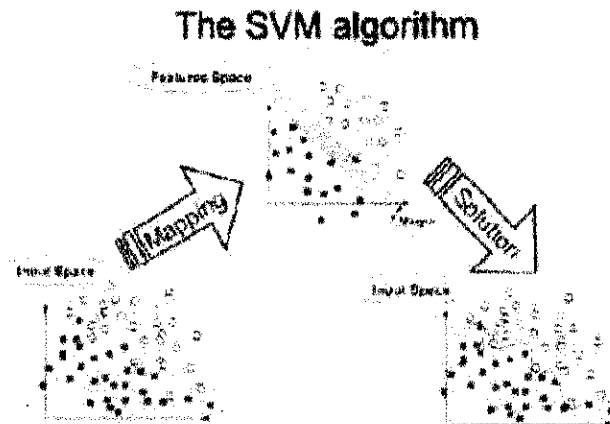


Figure 2.13 An Overview of the SVM Process. (Ayodele, 2010)

2.5.2 Artificial Neural Network (ANN)

The ANN is chosen for the simplicity of the proposed system and the ability to monitor pattern matching is directly due to the previous learning algorithm. It has been successfully applied to many classification schemes (Kamalakumari & Vanitha, 2017). In the vast majority of cases, the network will have a single output variable, although in the case of many-state classification problems, this may correspond to a number of output units (the post-processing stage takes care of the mapping from output units to output variables). If you do define a single network with multiple output variables, it may suffer from cross-talk (the hidden neurons experience difficulty learning, as they are attempting to model at least two functions at once). The best solution is usually to train separate networks for each output, then to combine them into an ensemble so that they can be run as a unit (Ayodele, 2010).

Figure 2.14 shows a brief architecture of an artificial neural network.

An example of a training algorithm in ANN is the back propagation, it is the easiest algorithm to understand. In back propagation, the gradient vector of the error surface is calculated. This vector points along the line of steepest descent from the current point, so we know that if we move along it a "short" distance, we will decrease the error. A sequence of such moves (slowing as we near the bottom) will eventually find a minimum of some sort. The difficult part is to decide how large the steps should be. Large steps may converge more quickly, but may also overstep the solution or (if the error surface is very eccentric) go off in the wrong direction (Ayodele, 2010).

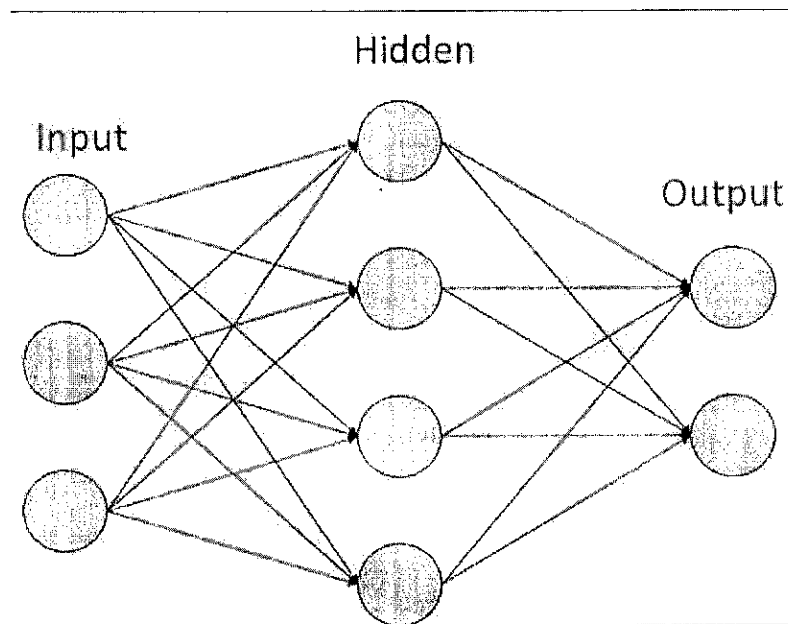


Figure 2.14 Brief architecture of Artificial Neural Network (tutorialspoint, 2017)

2.5.3 Self Organized Map (SOFM)

Self-Organizing Feature Map (SOFM, or Kohonen) networks are used quite differently to the other networks. Most networks are designed for supervised learning tasks, SOFM networks are designed primarily for unsupervised learning. SOFM is a non-linear classifier and it can also be used for feature extraction when a non-linear approach is to be taken throughout the pattern recognition process (Adeyanju, Awodoye, & Omidiora, 2016). The architecture of a SOFM network is shown in figure 2.15.

It can learn to recognize clusters of data, and can also relate similar classes to each other. The user can build up an understanding of the data, which is used to refine the network. As classes of data are recognized, they can be labelled, so that the network becomes capable of classification tasks. SOFM networks can also be used for classification when output classes are immediately available. The attribute of SOFM that makes this possible is their ability to highlight similarities between classes (Ayodele, 2010).

A second possible use is in novelty detection. SOFM networks can learn to recognize clusters in the training data, and respond to it. If new data, unlike previous cases, is encountered, the network fails to recognize it and this indicates novelty. A SOFM network has only two layers: the input layer, and an output layer of radial units (also known as the topological map layer). SOFM are trained using an iterative algorithm. Starting with an initially-random set of radial centers, the algorithm gradually adjusts them to reflect the clustering of the training data. At one level, this compares with the sub-sampling and K-Means algorithms used to assign

centers in SOM network and SOFM algorithm can be used to assign centers for these types of networks (Ayodele, 2010).

The basic SOFM algorithm runs a through a number of epochs, it executes a training case by applying the following algorithm:

- Select the winning neuron (the one whose center is nearest to the input case);
- Adjust the winning neuron to be more like the input case (a weighted sum of the old neuron center and the training case).

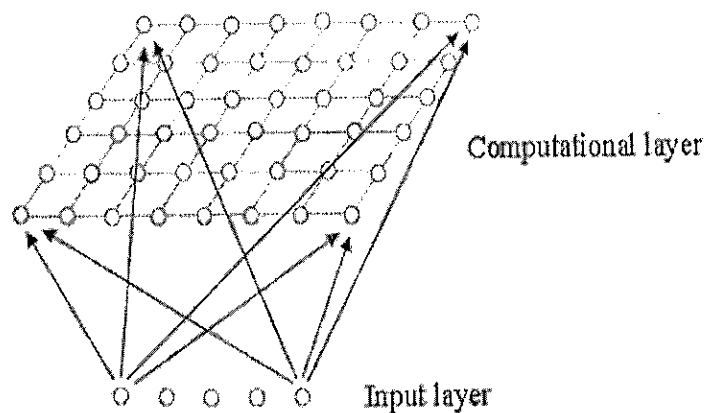


Figure 2.15 Brief architecture of a SOM Network. (Mishra, Mishra, Nayak, & Panda, 2016)

2.5.4 K-Nearest Neighbour (K-NN)

The simple classification of the program is the classification of the spatial image of the neighborhood. According to this scheme, the group of images in the test group is identified by a label in the learning set, where the distance is measured in the image space in the nearest

point of the assignment. If all the images have been normalized to zero mean and unit variance, then this process is equivalent to selecting the image that is most relevant to the test image in the training set (Kamalakumari & Vanitha, 2017). Figure 2.16 illustrates an implementation of the KNN algorithm.

As a result of the standardization process, the result is independent of the intensity of the light source and the effect of the automatic gain control of the camera. The feature selection implementation uses this learning algorithm by restricting each classification to depend on only a single function. The Euclidean distance metric is usually chosen to determine the proximity of the KNN data points (Kamalakumari & Vanitha, 2017). The distance between all the pixels in a data set is assigned. It defined as the Euclidean distance between two pixels. The Euclidean metric is the point R_n in R_n of the function $d: R_n$ and is used to assign $N \times = (X_1, \dots, X_N)$ and $Y =$ any two vectors (γ_1, \dots, n) This gives the "standard" between the two vectors R_n , from which the distances are made up of the matrices of x, y, x, \dots . The distance between all possible pairs of points (X, Y) (Kamalakumari & Vanitha, 2017). Examples of other distance measures that can be with K-NN are the Chessboard distance and the City Block distance. Table 2.1 below shows a summary of various distance measures used with K-NN.

The KNN algorithm can be summarized as follows:

1. A positive integer k is specified, along with a new sample.
2. Select the k entries in our database which are closest to the new sample.

3. Find the most common classification of these entries.

4. This is the classification that will be given to the new sample.

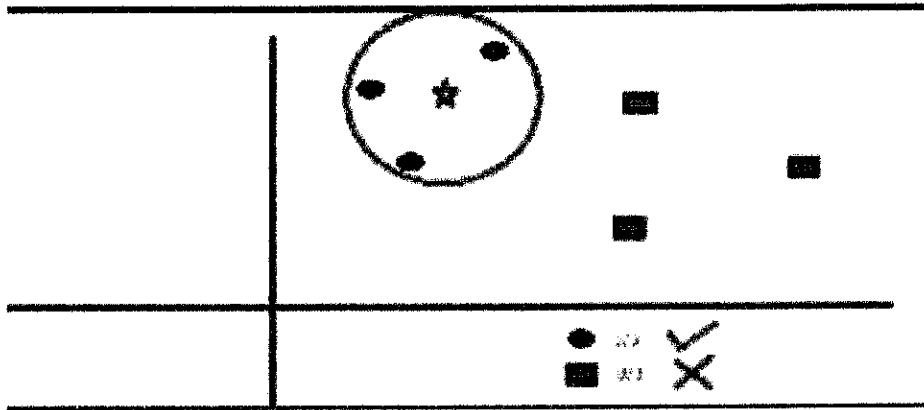
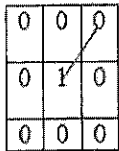
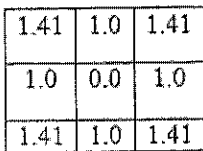
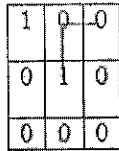
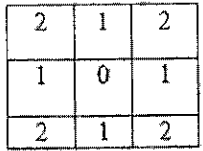
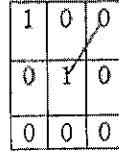
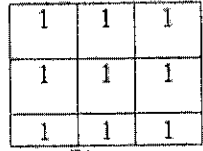


Figure 2.16 K-Nearest Neighbour. (Srivastava, 2014)

Table 2.2 Summary of Distance Measures in Image Processing (Shondaganga F, 2015)

Distance Metric	Description	Illustration	
Euclidean	The Euclidean distance is the straight-line distance between two pixels.	 <p>Image</p>	 <p>Distance Transform</p>
City Block	The city block distance metric measures the path between the pixels based on a 4-connected neighborhood. Pixels whose edges touch are 1 unit apart and pixels diagonally touching are 2 units apart.	 <p>Image</p>	 <p>Distance Transform</p>
Chessboard	The chessboard distance metric measures the path between the pixels based on an 8-connected neighborhood. Pixels whose edges or corners touch are 1 unit apart.	 <p>Image</p>	 <p>Distance Transform</p>

2.7 Related Works

A bimodal biometric based recognition system will help improve the efficiency and effectiveness of the recognition process. It overcomes the limitations and improves greatly on the available systems used for recognition. Several research work has been done in this field of biometric based recognition.

An experiment was carried out on facial recognition system based on black African faces (with and without tribal marks) using the optimized Fisher Discriminant Analysis due to the lack of research on black African faces. The system was able to perform reliable recognition in a constrained environment using Black African faces and a recognition performance accuracy of between 88 and 99% were obtained at different cropping levels (Omidiora, Fakolujo, Ayeni, & Adeyanju, 2008).

In this paper they described the concepts of face recognition methods & its applications. This paper provides a better understanding about face recognition methods and applications. The paper discusses face recognition is a biometric system used to identify or verify a person from a digital image. This paper describes the common methods used in facial recognition system like holistic matching method, feature extraction method and hybrid methods. It discusses that face recognition systems should be able to automatically detect a face in an image. This involves extracts its features and then recognize it, regardless of lighting, expression, illumination, ageing, transformations (translate, rotate and scale image) and pose, which is a difficult task. (Parmar & Mehta, 2013).

A research was carried out worked with four support vector machines (SVM) kernels to see if its good performance in characterization can be extended into emotion recognition. The four SVM kernels used were Radial Basis Function, Linear Function, Quadratic Function and Polynomial Function. The Quadratic function kernel outperformed the other three kernels in terms of percentage accuracy and the average accuracy increased with increasing

image dimension of the extracted features although computational time was non-uniform and therefore inconclusive. The Quadratic function kernel had an average accuracy of 99.33%. (Adeyanju, Omidiora, & Oyedokun, 2015).

A research was conducted to evaluate the performance of an improved SOFM and modified CPN techniques to recognize face images with black African face database and establish the more efficient between the two techniques. Their work showed that SOFM learned with the ability to organize information without providing an error signal and learned the distribution of set of patterns without any class information while CPN learned by adjusting its interconnection weight combinations with the help of error signals then learned the distribution of set of patterns with class information. CPN outperformed SOFM techniques in face recognition based on recognition accuracy with an average of 89.25% and computational time with an average of 194.25 seconds at the different resolutions considered (Adeyanju, Awodoye, & Omidiora, 2016).

Due to the difficulties in human face recognition from unconstrained and motion characterized scenes are usually accounted for due to varying illumination and pose of subjects in the scenes, a number of technical approaches have been developed to manage these nuisance factors to make recognition possible and optimal. A review of these techniques were carried out and it was discovered that technical limitations of those approaches indicate that face recognition in unconstrained video sequences remains an open problem domain (Fagbola, Olabiyisi, Egbetola, & Oloyede, 2017).

A biometric attendance system was developed based on fingerprint reconstruction technique (Josphineleela & Ramakrishan, 2012). They developed an algorithm that is proposed to reconstruct the phase image, which is then converted into the grayscale image. The fingerprint reconstruction algorithm is used to automate the whole process of taking attendance, manually which is a laborious and troublesome work and waste a lot of time, with its managing and maintaining the records for a period of time is also a burdensome task. The algorithm was evaluated and used to test the susceptibility of fingerprint systems to attack (Josphineleela & Ramakrishan, 2012). The image obtained from fingerprint reconstruction algorithm used showed that type-I attack (matching the reconstructed fingerprint against the original fingerprint) and type-II attack (match the reconstructed fingerprint against different impressions of the original fingerprint) can be effectively launched against a fingerprint recognition system (Josphineleela & Ramakrishan, 2012).

A fingerprint image preprocessing process was studied leaving out image enhancement thus the fingerprint image has to be of good quality for the technique to be successfully implemented. The steps proposed are converting the given grey scale image to binary image (binarization), central line thinning of the image, dilation of the thinned image, thinning of the dilated image, removing unwanted portions from the image (Refining) and producing dual image. It was discovered that this proposed steps produced a better result than the traditional fingerprint image preprocessing process (Chaurasia, 2012).

A unimodal biometric attendance system was developed using fingerprint as the biometric trait. They compared its results with the traditional (manual) attendance taking methods. They found that the system recorded a 94% success rate for eight students who participated in the study. The biometrics based attendance system produced approximately 3.8 seconds execution time on the average while the traditional (manual) method of attendance produced approximately 17.8 seconds execution time on the average. Results of the biometric based attendance system confirm improved performance as compared to the manual method of attendance (Shoewu, Makanjuola, & Olatinwo, 2014).

A fingerprint classification system was developed using Self Organizing Map (SOM) algorithm in order to reduce the run time complexity and increase the performance of the system. The SOM based classification system successfully reduced the run time of identification and verification operation of images. It was concluded that the SOM algorithm based system can be used for large scale of verification and identification operation efficiently and with less time complexity (Mishra, Mishra, Nayak, & Panda, 2016).

A biometric based examination clearance system was developed using fingerprint as the biometric trait. The system was developed to help overcome the shortcomings of the manual paper based clearance process. In identification, the system recognized an individual by comparing his/her biometrics with every record in the database. It was discovered that the system was more secured, credible and error free to checkmate student malpractices, impersonation and other unlawful acts as compared to existing manual-paper based. A user

evaluation was carried out and it was discovered that most of the false rejections were due to user errors caused by unfamiliarity with the system (Saheed, Hambali, Adeniji, & Kadri, 2017).

A research was carried out where they combined multiple biometrics to check if they will enhance the performance of personal authentication system in accuracy and reliability. In their paper they compared thirteen (13) combination methods in the context of combining the voiceprint and fingerprint recognition system in two different modes: verification and identification. The experimental results showed that Support Vector Machine and the Dempster-Shafer method are superior to other schemes (Wang, Wang, & Tan, 2004).

A research was carried out to evaluate the performance of sum rule-based score level fusion and support vector machine (SVM)-based score level fusion. The three biometric characteristics used were fingerprint, face and finger vein. A normalization scheme based on min-max normalization was proposed. The results show that the proposed scheme gives high accuracy when combined with the fusion methods studied. The results of the research show that (SVM)-based score level fusion attains better performance levels compared to that of sum rule-based score level fusion as far as the kernels and its parameters are carefully selected (He, et al., 2009).

A multimodal biometrics recognition based on score level fusion of fingerprint and finger vein was developed. The matching results of fingerprint recognition were scores, while matching results of finger vein recognition were distances. Therefore the matching results of

the finger vein were normalized using Min-max normalization. The experimental results based on homologous biometrics database show that the fusion of fingerprint and finger vein leads to improvement in performance. The recognition rate of the proposed system was 98.74% compared to 95.3% and 93.72% of the fingerprint and finger vein respectively when they were used separately (Cui & Yang, 2011).

A multibiometric identification system was developed fusing iris and fingerprint traits. The matching was done with help of hamming-distance. The iris and fingerprint templates are matched separately and scores are combined by using sum rule-based score level fusion which increase the recognition rate. Therefore improving the system accuracy and dependability. The developed system biometric system proved to better than unimodal biometric systems because of its lower error rate and large population coverage (Garje & Agrawa, 2012).

A biometric system for access control and the two biometric traits used were the fingerprint and face and they discussed the benefits of a bimodal biometric system over a unimodal biometric system. The two biometric traits integrated were fingerprint and face biometric to improve the performance in access control system. Concerning fingerprint biometric in their work restoration of distorted and misaligned fingerprints caused by environmental noise such as oil, wrinkles, dry skin, dirt, displacement etc was considered. The noisy, distorted and/or misaligned fingerprint produced as a 2-D on x-y image, was enhanced and optimized using a hybrid Modified Gabor Filter-Hierarchal Structure Check (MGF-HSC) system model. In

face biometric the Fast Principal Component Analysis (FPCA) algorithm was used in which different face conditions (face distortions) such as lighting, blurriness, pose, head orientation and other conditions are addressed. The algorithms used improved the quality of distorted and misaligned fingerprint image. It also improved the recognition accuracy of distorted face during authentication (Zuva, Esan, & Ngwira, 2014).

A multimodal biometric system using sum rule based matching score level fusion of fingerprint and iris images was developed. The scores obtained from the biometric systems were normalized to convert these scores into the same nature. After we getting a set of normalized scores sum rule-based fusion is used. The developed system enhanced the performance of system and security level of biometric systems compared to unimodal biometric systems (Rishishwar, Subhash, & Raghuwanshi, 2016).

CHAPTER THREE

DESIGN METHODOLOGY

3.1 Overview of The Face Recognition System

The proposed recognition system was designed based on unimodal biometrics. The biometric recognition system uses the face as the only physiological trait. The processes involved in the unimodal biometric bimodal system include data acquisition, biometric image preprocessing, feature extraction, matching and evaluation. Figure 3.1 shows the block diagram of the proposed biometric recognition system.

The first task in developing the recognition system is the acquiring of face images which is done at the data acquisition stage. After data acquisition the next step is biometric image preprocessing, the preprocessing steps to be employed are image resizing and greyscale conversion. Once the preprocessing is done then feature extraction using principal component analysis (PCA) is carried out. The features extracted using PCA are then classified using K-Nearest Neighbour (KNN) and used to carry out matching.

3.2 Data Acquisition

Face images were acquired from (30) participants. The participants were both male and female students of Federal University Oye-Ekiti Nigeria. The data set is made up of face images from twenty-three (23) male students and seven (7) female students. The participants filled the questionnaire attached in the Appendix A before their biometric data was acquired.

The images of the face were taken with an eight (8) megapixel camera. The dimensions of the face images taken were 1872 x 3328.

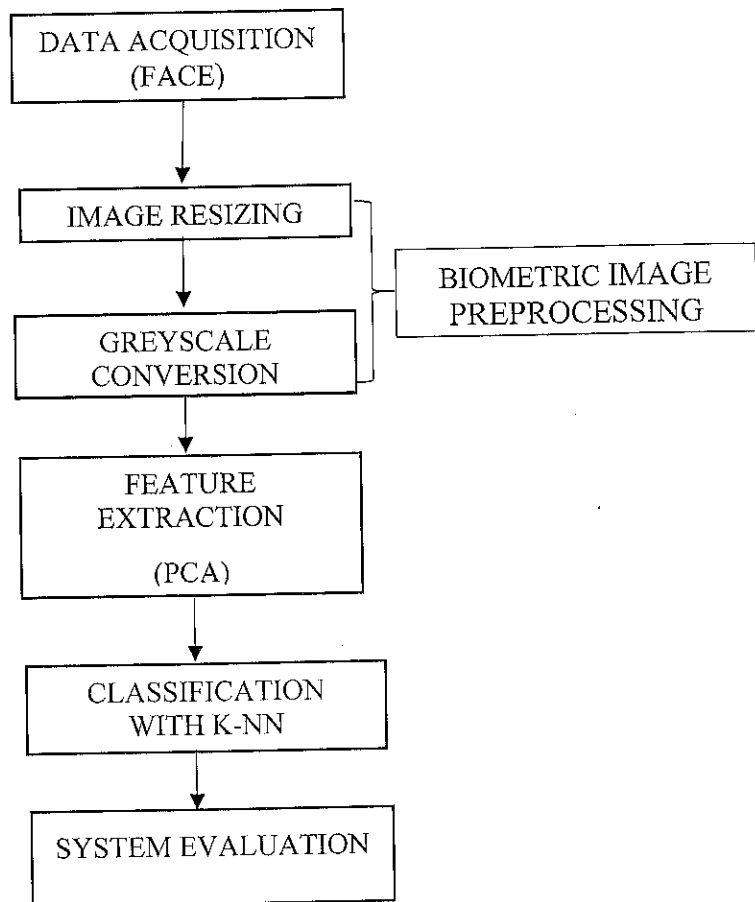


Figure 3.1 Block Diagram of the Overview of the Biometric Recognition System

3.3 Biometric Image Preprocessing

The images of the face were preprocessed to enable easy feature extraction and to improve the efficiency of the recognition system. The preprocessing steps taken on the facial images included image resizing and greyscale conversion.

The images were resized manually from their original size of 1872 x 3328 to a smaller size 252 x 448 using the resize function in the Microsoft application Paint. The images were resized to improve the speed and efficiency of the Matlab program.

The next preprocessing step after the images have been resized is to convert them to greyscale. They are converted to greyscale images (with pixel values between 0 and 255) using the 'rgb2gray' command in Matlab. They were converted to grayscale to enable easy computation in Matlab. After which they are passed to the feature extraction stage.

3.4 Feature Extraction Using Principal Component Analysis (PCA)

Feature extraction is the process of identifying and picking out the most relevant features (information) for the biometric image (data) that would be the most useful in the biometric process of identification and authentication (Kumar & Bhatia, 2014). The feature to be extracted from the facial images is the location and shape of the facial attributes. The facial attributes include the eyes, the nose and the mouth. The feature extraction technique that will be used for face recognition is the linear technique known as principal component analysis (PCA).

Principal Component Analysis (PCA) also known as the use of eigenfaces converts the set of correlated face images to a set of uncorrelated eigenfaces which will be the principal components (Kumar & Bhatia, 2014). The normalized facial images were the input for the PCA and it was also used for dimension reduction. The following steps were followed to use the PCA feature extraction technique:

1. Center the data X.
2. Compute the covariance matrix C.
3. Obtain the eigenvectors and eigenvalues of the covariance matrix.

The covariance matrix C is calculated with the equation below

$$C = A^T * A \quad (3.1)$$

Where, $A = \begin{pmatrix} a_{1.1} & \dots & a_{1k} \\ \cdot & \cdot & \cdot \\ a_{j1} & \dots & a_{jk} \end{pmatrix}$. The eigenvector is calculated from the covariance matrix

after the dimension reduction has been carried out in order to stop the attendance system from slowing down or running out of memory because of computations. The eigenvectors are then arranged from the highest to the lowest by their corresponding eigenvalues. The eigenfaces are formed by discarding the eigenvectors with eigenvalues of zero while the eigenvectors with non-zero eigenvalues are kept.

3.5 Classification Using K-Nearest Neighbour

K-Nearest Neighbour is a simple classification method which makes use of the distance between the image pixels to classify the images after feature extraction has been carried out. K-Nearest Neighbour can be used with different distance measures. Euclidean distance was chosen as the distance metric because it is the easiest distance metric to understand and implement.

In this project K-NN was used with the Euclidean distance with $K=1$. The Euclidean distance is the distance between two points in Euclidean space. The input data for the Euclidean distance matching are the features extracted from the images during the feature extraction stage; the features extracted will first be converted internally to a raster before the Euclidean analysis is performed. Euclidean distance is defined mathematically as (Gonzalez & Wood, 2012):

$$D_e(p, q) = [(x - s)^2 + (y - t)^2]^{\frac{1}{2}} \quad (3.2)$$

Where p and q are pixels with coordinates (x, y) and (s, t) respectively.

3.6 Experimental Set-Up

The biometric system was developed using Matlab. The face images were acquired from thirty participants (students) in Federal University Oye-Ekiti, Ikole campus, Ekiti state. Three face images were acquired from each individual using an eight (8) megapixel camera.

A 2-fold evaluation methodology was employed with a ratio 60:40 in the training and test datasets. The images were taken in a controlled environment therefore the pose in each image is similar across all participants and each participant kept a straight face while the images were being taken. All the images from three (3) individuals were selected for negative testing and did not form part of the training set. In total fifty-four (54) images, consisting of two (2) images from twenty-seven (27) participants were selected for the training set. The test set consists of thirty-six (36) images, including twenty-seven (27) images from 27 participants and nine (9) images from the three (3) participants used as negative testing.

Both train and test images were preprocessed by first resizing them manually from their original size 1872 x 3328 to a smaller size 252 x 448. They were then converted to greyscale images using the 'rgb2gray' Matlab function. Feature extraction was done using PCA as discussed in section 3.4. Then K-NN with Euclidean distance and K=1 was used as classifier to choose the recognized image from the train set. A threshold was used to stop the recognition system from recognising faces that formed those selected for negative testing.

3.6 Proposed Evaluation Metrics

The performance of the system will be evaluated to determine the effectiveness of the developed system. The following metrics are going to be used to evaluate the system:

1. True Positive (TP): this is the number of times the system makes a correct decision and chooses the right face as the answer.

2. True Negative (TN): this is the number of times the system gives a correct answer by indicating an unknown face when it is tested with faces that were not part of the faces used to train the system.
3. False Positive (FP): this is the number of times the system fails to recognise a face it was trained with.
4. False Negative (FN): this is the number of times the system recognises a face it was not trained with.
5. Accuracy: this is computed as the ratio of total of the true positive (TP), true negative (TN) to the total number of test images multiplied by hundred (100).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (3.3)$$

6. False Accept Rate (FAR): this is the probability that the biometric system will recognise a user that was not used to train it. It can be computed as the ratio of the number of false recognitions to the number of identification attempts.

$$FAR = \frac{FN}{\text{number of identification attempts}} \quad (3.4)$$

7. False Recognition Rate (FRR): this is the probability that the biometric system will not recognise a user that was used to train the system. It can be computed as the ratio of the number of false recognition to the number of identification attempts.

$$FRR = \frac{FP}{\text{number of identification attempts}} \quad (3.5)$$

8. The Execution Time: this is the amount of time it takes the program to finish running the recognition process.

CHAPTER FOUR

SYSTEM IMPLEMENTATION AND RESULTS

4.1 System Implementation

The system was implemented by developing a standalone software application using Matlab. Therefore the developed application does not require Matlab to work and can be used on computers that do not have Matlab installed on them. The developed application as shown in figure 4.1 has four buttons namely: Browse a Face for Testing, Preprocess-Greyscale, Feature Extraction-PCA and Classify-KNN. The application has two display boxes, the first is the input test face which shows the selected test face and the second is the predicted output face which as the name implies shows the predicted recognised face.

The “browse a face for testing” button allows the user to select a test image from any folder in the computer system. The “preprocess-greyscale” button carries out the second preprocessing task on the image which is conversion from a coloured image (RGB image) to a greyscale image (black and white image). The feature “extraction-PCA” button carries out the feature extraction process using PCA. The “classify-KNN” button does the classification and selects the output face.

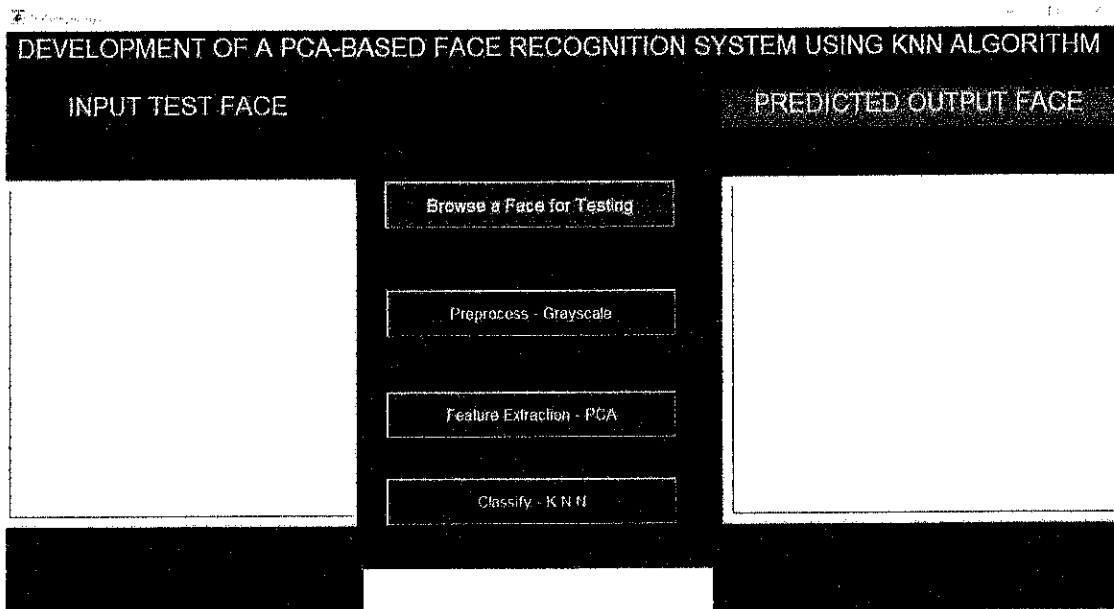


Figure 4.1 The Implementation of the Developed Face Recognition System.

4.2 Individual Results From Test Images

All the images in the test set were used to test the face recognition system, and the following was recorded: the recognised image, the execution time, whether the prediction was right or wrong and whether they were True Positive (TP)/True Negative (TN) /False Positive (FP)/False Negative (FN). Table 4.1 below shows each image and their recorded results.

The test image ID is the name the test image was stored with in the test data set, the recognised image ID is the name of the recognised image from the train set, the type of prediction shows whether the system was right or wrong and the execution time shows how

long it took the system to finish carrying out its processes on each image. The table shows that the average execution time for all the images is 3.60 seconds.

Table 4.1 Showing The Test Image ID, The Recognised Image ID, The Type of Prediction, the Execution Time and True Positive (TP)/True Negative (TN) /False Positive (FP)/False Negative (FN).

TEST IMAGE ID	RECOGNISED IMAGE ID	PREDICTION	EXECUTION TIME(s)	TP/TN/FP/FN
1	1 1	Right	3.686	TP
2	2 1	Right	3.646	TP
3	3 2	Right	3.644	TP
4	4 1	Right	3.653	TP
5	5 2	Right	3.651	TP
6	23 2	Wrong	3.637	FP
7	7 2	Right	3.597	TP
8	8 1	Right	3.650	TP
9	10 1	Wrong	3.645	FP
10	10 1	Right	3.659	TP
12	12 2	Right	3.652	TP
14	14 2	Right	3.601	TP
15	15 2	Right	3.654	TP
16	16 2	Right	3.615	TP
17	17 2	Right	3.629	TP
18	18 1	Right	3.636	TP
19	19 2	Right	3.631	TP
21	21 2	Right	3.673	TP
22	22 2	Right	3.625	TP
23	23 2	Right	3.619	TP
24	24 2	Right	3.627	TP
25	25 2	Right	3.635	TP
26	26 1	Right	3.618	TP
27	21 2	Wrong	3.634	FP
28	26 1	Wrong	3.634	FP
29	29 2	Right	3.632	TP
30	30 1	Right	3.639	TP
11	Not recognised	Right	1.395	TN
11 1	Not recognised	Right	1.403	TN
11 2	Not recognised	Right	1.398	TN
13	27 2	Wrong	1.936	FN
13 1	Not recognised	Right	1.520	TN
13 2	Not recognised	Right	1.492	TN
20	Not recognised	Right	1.401	TN
20 1	Not recognised	Right	1.496	TN
20 2	Not recognised	Right	1.493	TN

4.3 Confusion Matrix Results

The confusion matrix of the results is formed from the following evaluation metrics: True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). Table 4.2 below shows the confusion matrix of the results while figure 4.2 shows a bar chart distribution of the confusion matrix.

True positive (TP) is the number of times the system makes a correct decision and chooses the right face as the answer. The system was tested with twenty-seven (27) images of user which had their images in the train set and it made the correct decision twenty-three times (23).

True negative (TN) is the number of times the system gives a correct answer when it is tested with faces that were not part of the faces used to train the system. The test folder contains thirty-six (36) images of which nine (9) were not used to train the system and it made the correct decision eight times.

False positive (FP) is the number of times the system fails to recognise a face it was trained with. The test folder contained twenty-seven (27) images of individuals the system was trained with and it got four wrong.

False negative (FN) is the number of times the system recognises a face it was not trained with. The test folder contained nine (9) images which were not used to train the system and it recognised only one (1) of them.

Table 4.2 The Confusion Matrix

23(TP)	8(TN)
4(FP)	1(FN)

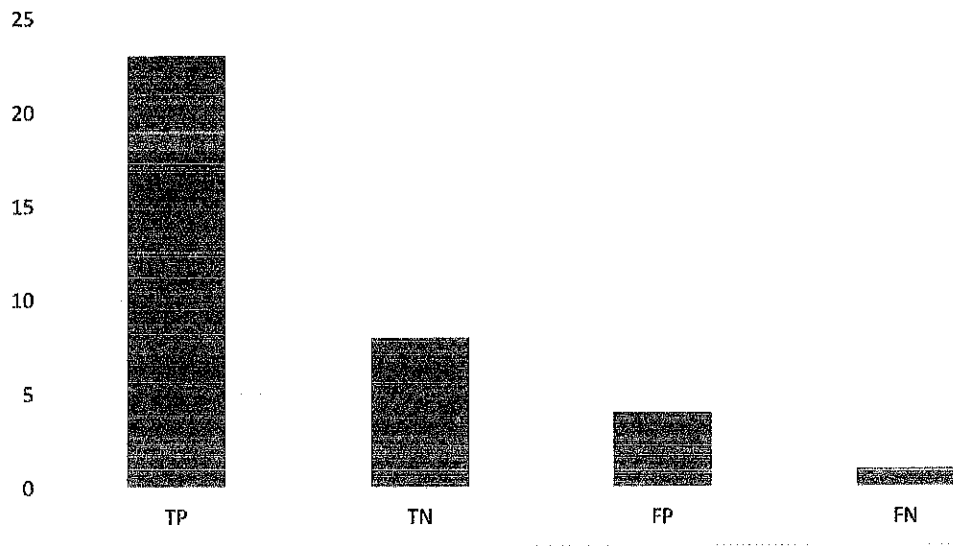


Figure 4.2 Column Chart Showing the Confusion Matrix

4.4 Evaluation With Accuracy, FRR and FAR

The other metric used to evaluate the recognition system are the accuracy, the false accept rate and the false reject rate. The results gotten from these evaluation metric are shown in table 4.3 below.

The accuracy is computed as the ratio of total of the true positive (TP) and true negative (TN) to the total number of test images multiplied by hundred (100). TP=23, TN=8, FP=4, FN=1 and the folder has a total of thirty-six (36) pictures giving the system an accuracy of 86%.

$$Accuracy = \frac{23 + 8}{36} \times 100 = 86\%$$

False accept rate (FAR) is the probability that the biometric system will recognise a user that was not used to train it. It can be computed as the ratio of the number of false recognitions to the number of identification attempts. The system was tested with nine (9) pictures that were not in the train set and it only recognised one of the images giving it a false accept rate of 0.11.

$$FAR = \frac{1}{9} = 0.11$$

False reject rate (FRR) is the probability that the biometric system will not recognise a user that was used to train the system. It can be computed as the ratio of the number of false recognition to the number of identification attempts. The system was tested with twenty-seven images of user which had their images in the train set and it did not recognise four giving it a false reject rate of 0.15.

$$FRR = \frac{4}{27} = 0.15$$

Table 4.3 The Accuracy, The False Accept Rate (FAR) and The False Reject Rate (FRR)

ACCURACY	86%
FALSE ACCEPT RATE (FAR)	0.11
FALSE REJECT RATE (FRR)	0.15

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This project work designed and implemented a face recognition system. This was achieved by extracting the features from the face using PCA, and classifying them using K-Nearest Neighbour with Euclidean distance. The system had a high accuracy of 86%, FAR of 0.11 and FRR of 0.148 with an average execution time of 3.60 seconds. The results indicate that the system can be used in applications such as attendance taking and access control.

5.2 Recommendations

The project has shown the accuracy and efficiency of a biometric recognition system but more work can be done in the following areas:

1. Attempt the use of other values of K such as $K = 3, 5, 7$ etc. to implement the system.
2. Attempt the use of other biometric classifiers such as Support Vector Machine (SVM) and Self Organising Feature Map (SOFM) to classify the features extracted by the feature extraction technique employed.
3. Implementing the system as a multimodal biometric recognition system that incorporates other biometric traits such as fingerprint.

References

- Adeyanju, I. A., Awodoye, O. O., & Omidiora, E. O. (2016). Performance Evaluation of an Improved Self-organizing Feature Map and Modified Counter Propagation Network in Face Recognition. *British Journal of Mathematics & Computer Science*. Article no.BJMCS.22588, 1-12.
- Adeyanju, I. A., Omidiora, E. O., & Oyedokun, O. F. (2015). Performance Evaluation of Different Support Vector Machine Kernels for Face Emotion Recognition. *SAI Intelligent Systems Conference* (pp. 804-806). London: SAI Intelligent Systems.
- Anila, S., & Devarajan, N. (2012). Preprocessing Technique for Face Recognition Applications under Varying Illumination Conditions. *Global Journal of Computer Science and Technology Graphics & Vision*, Vol. 12, No.11, 13-18.
- Ayodele, T. O. (2010). *New Advances in Machine Learning*. Shanghai: InTech .
- Bolme, D. S. (2003). *Elastic Bunch Graph Matching (M.Sc Thesis)*. Colorado: Colorado State University.
- Chaurasia, O. P. (2012). An Approach to Fingerprint Image PreProcessing . *I.J. Image, Graphics and Signal Processing*, No.5, Vol.6, 29-35.
- Chiagozie, O. G., & Nwaji, O. G. (2012). Radio Frequency Identification (RFID) Based Attendance System With Automatic Door Unit. *Academic Research International*, Vol 2, No.2, 168-183.

- Cui, F., & Yang, G. (2011). Score Level Fusion of Fingerprint and Finger Vein Recognition . *Journal of Computational Information Systems*, 7:16 , 5723-5731 .
- Deugo, D. (2015). *Attendance Tracking* . Ottawa: The School of Computer Science, Carleton University, Ottawa, Ontario.
- Fagbola, T. M., Olabiyisi, S. O., Egbetola, F. I., & Oloyede, A. (2017). Review of Technical Approaches to Face Recognition in Unconstrained Scenes with Varying Pose and Illumination. *FUOYE Journal of Engineering and Technology*, Vol. 2, Issue 1 , 1-8.
- Falohun, A., Fenwa, O., & Oke, A. (2016). An Access Control System using Bimodal Biometrics. *International Journal of Applied Information Systems (IJ AIS)* , Vol. 10, No.5 , 41-47.
- FUOYE. (2015). *Federal University Oye-Ekiti Student's Handbook of Information*. Ado-Ekiti: PETOA Educational Publishers.
- Garje, P. D., & Agrawa, S. S. (2012). Multibiometric Identification System Based On Score Level Fusion . *IOSR Journal of Electronics and Communication Engineering*, Vol. 2, Issue 6 , 07-11 .
- Gonzalez, R. C., & Wood, R. E. (2012). *Digital Image Processing Third Edition*. New Jersey: Pearson Education International.
- Gonzalez, R. C., & Woods, R. E. (2002). *Digital Image Processing Second Edition*. New Jersey : Prentice-Hall,Inc.

- He, M., Horng, S.-J., Fan, P., Ray-ShineRun, Chen, R.-J., Lai, J.-L., . . . Sentosa, K. O. (2009). Performance Evaluation of Score Level Fusion in Multimodal Biometric Systems. *Elsevier*, , doi:10.1016/j.patcog.2009.11.018, 1-12.
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technologies*, , vol. 14, no. 1, 1-66.
- Jayaram, M. A., Prashanth, G. K., & Taj, S. (2015). Classification of Ear Biometric Data using Support Vector Machine. *British Journal of Applied Science & Technology*, 11(1), Article no.BJAST.19509, 1-10.
- Josphineleela, R., & Ramakrishan, M. (2012). An Efficient Automatic Attendance System Using Fingerprint Reconstruction Technique. *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 10, No. 3, March.
- Juang, B., & Rabiner, L. R. (2004). *Development, Automatic Speech Recognition – A Brief History of the Technology*. Atlanta: Georgia Institute of Technology, Rutgers University and the University of California.
- Kamalakumari, J., & Vanitha, M. (2017). A Review on Automatic Heterogeneous Face Recognition. *International Journal of Advance Research in Computer Science and Management Studies*, Vol. 5, No. 1, 68-75.

- Kumar, G., & Bhatia, P. K. (2014). A Detailed Review of Feature Extraction in Image Processing Systems. *Fourth International Conference on Advanced Computing & Communication Technologies* (pp. 5-12). ResearchGate.
- Lin, S.-H. (2000). An Introduction to Face Recognition Technology . *Informing Science Special Issue on Multimedia Informing Technologies-Part 2, Vol.3, No.1*, 1-7.
- Ling, W. P. (2012). *Integrated Staff Attendance System (ISAS) (Technical Report)*. Pahang: Faculty of Computer Systems & Software Engineering University Malaysia Pahang.
- Mahmod, N. L. (2005). *Student Attendance Online System Using Barcode Reader (B.Sc Report)*. Malaysia: Faculty of Computer System & Software Engineering, University College of Engineering & Technology.
- Masek, L. (2003). *Recognition of Human Iris Patterns for Biometric Identification*. The University of Western Australia.
- Mirmohamadsadeghi, L., & Drygajlo, A. (2011). Palm Vein Recognition with Local Binary Patterns and Local Derivative Patterns. *International Joint Conference on Biometrics (IJCB)* (pp. 1-6). Washington: IEEE.
- Mishra, A., Mishra, A., Nayak, N. B., & Panda, M. (2016). Fingerprint Classification and Matching Using Self Organizing Feature Map. *International Journal Of Modern Engineering Research, Vol. 6, Iss. 4* , 72-79.

- Mishra, R., & Trivedi, P. (2011). *Student Attendance Management System Based On Fingerprint Recognition and One-To-Many Matching (B.Tech. Thesis)*. Orissa: National Institute of Technology Rourkela.
- Moharil, R. S., & Dandare, S. N. (2016). Microcontroller based Attendance Management System . *International Journal of Engineering and Innovative Technology (IJEIT)*, Vol.5, No. 10 , 47-52.
- Nakajimaa, C., Pontilb, M., Heiselec, B., & Poggioc, T. (2003). Full-Body Person Recognition System . *Pattern Recognition 36* , 1997–2006.
- Nandakumar, K. (2008). *Multibiometric Systems: Fusion Strategies and Template Security (A Phd. Dissertation)*. Michigan: Department of Computer Science and Engineering, Michigan State University.
- Olanipekun, A., & Boyinbode, O. (2015). A RFID Based Automatic Attendance System in Educational Institutions of Nigeria . *International Journal of Smart Home*, Vol. 9, No. 12, , 65-74 .
- Omidiora, E., Fakolujo, A., Ayeni, R., & Adeyanju, I. (2008). Optimised Fisher Discriminant Analysis for Recognition of Faces Having Black Features . *Journal of Engineering and Applied Sciences*, Vol. 3, No.7 , 524-531.
- Parmar, D. N., & Mehta, B. B. (2013). Face Recognition Methods & Applications . *International Journal of Computer Technology & Applications*, Vol 4 No. 1., 84-86.

- Paul, D. (1990). Speech Recognition Using Hidden Markov Models. *The Liru:oln Laboratory Journal, Vol 3, No. 1* , 41-62.
- Raghavendra, R., Ashok, R., & Hemantha, K. G. (2010). Multimodal Person Verification System Using Face and Speech. *Procedia Computer Science 2* , 181–187.
- Raghavendra, R., Ashok, R., & Hemantha, K. G. (2010). Multimodal Person Verification System Using Face and Speech. *Science Direct Procedia Computer Science 2*, 181–187.
- Raj, B., & Singh, R. (2011). Design and Implementation of Speech Recognition Systems. *Class 1: Introduction*. Pittsburgh, Pennsylvania, United States of America: Carnegie Mellon. School of Computer Science.
- Rishishwar, A., Subhash, V., & Raghuwanshi, N. (2016). Sum Rule Based Matching Score Level Fusion of Fingerprint and Iris Images for Multimodal Biometrics Identification. *International Research Journal of Engineering and Technology (IRJET), Vol. 03, Issue: 02*, 1370-1376.
- Ross, A., Nandakumar, k., & Jain, A. (2006). *Handbook of Multibiometrics*. Springer.
- Saheed, Y. K., Hambali, M. A., Adeniji, I. A., & Kadri, A. F. (2017). Fingerprint Based Approach for Examination Clearance in Higher Institutions . *FUOYE Journal of Engineering and Technology, Vol. 2, Issue 1*, 47-50.

Scheidat, T., Leich, M., Alexander, M., & Vielhauer, C. (2009). *Support Vector Machines for Dynamic*. Magdeburg: AIAI-2009 Workshops Proceedings .

Shlens, J. (2003). *A Tutorial on Principal Component Analysis Derivation, Discussion and Singular Value Decomposition* . Princeton: Princeton University.

Shoewu, O., Makanjuola, N., & Olatinwo, S. (2014). Biometric-based Attendance System: LASU Epe Campus as Case Study. *American Journal of Computing Research Repository, Vol. 2, No. 1*, 8-14.

Shondaganga F. (2015). *Methods For Measuring Distance In Images*. India.

Srivastava, T. (2014). *Introduction to K-Nearest Neighbors : Simplified* (Date Accessed: 04/05/2017). Retrieved from Analytic Vidhya: www.analyticsvidhya.com

Sudha, K., Shinde, S., Thomas, T., & Abdugani, A. (2015). Barcode based Student Attendance System . *International Journal of Computer Applications (0975 – 8887), Vol. 119, No.2*, 1-4.

tutorialspoint. (2017). *Artificial Intelligence-Neural Network* (Date Accessed: 12/12/2017). Retrieved from tutorialspoint: https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_neural_networks.htm

USA Committee on Homeland Security and National Security. (2006). *Face Recognition*. Washington: Committee on Technology. National Science and Technology Council.

- Wambugu, M. R. (2011). *Smart Card Attendance Register (Project Report)*. Nairobi: Department of Electrical and Electronics Engineering, University of Nairobi.
- Wang, Y., Wang, Y., & Tan, T. (2004). *Combining Fingerprint and Voiceprint Biometrics for Identity Verification: an experimental comparison*. Beijing: Center for Biometrics Authentication and Testing National Laboratory of Pattern Recognition, Institute of automation, Chinese Academy of Sciences.
- Watanabe, M., Endoh, T., Shiohara, M., & Sasaki, S. (2005). Palm vein authentication technology and its applications. *The Biometric Consortium Conference*. Arlington: The Biometric Consortium, Hyatt Regency Crystal City, Arlington, VA, USA.
- Zuva, T., Esan, O., & Ngwira, S. (2014). Hybridization of Bimodal Biometrics for Access Control Authentication. *International Journal of Future Computer and Communication*, Vol. 3, No. 6, 444-451.

APPENDIX A



FEDERAL UNIVERSITY OYE-EKITI,
EKITI STATE, NIGERIA.

DEPARTMENT OF COMPUTER ENGINEERING

Information Sheet/ Consent Form

Project: DEVELOPMENT OF A PRINCIPAL COMPONENT ANALYSIS FACE RECOGNITION SYSTEM USING K-NEAREST NEIGHBOUR ALGORITHM

Researcher: Ayodele Adeokiji Adewale

Recognition is the identification of a thing or individual from previous encounters or knowledge. Recognition is an important task in many organisations ranging from law enforcement to education. Therefore, organisations are constantly in search of more efficient and error free ways to carry out the recognition process. This user study aims to acquire the facial images of participants as part of a research project. You will be required to have the picture of your face taken with a camera. The exercise should take 2 minutes.

Please tick box

1. I confirm I have read and understand the above information for this study and have had the opportunity to ask question.
2. I understand that my permission is voluntary and that I am free to withdraw at any time, without giving any reason, without my legal rights being affected.
3. I agree to take part in the above study.

ID of Participant/ Surname

Date

Signature

APPENDIX B

FEDERAL UNIVERSITY OYE-EKITI,
EKITI STATE, NIGERIA.

DEPARTMENT OF COMPUTER ENGINEERING ENTRY QUESTIONNAIRE

This questionnaire will provide us with background information that will help us analyse the answers you give in later stages of this experiment. You are not obliged to answer a question, if you feel it is too personal.

User ID:	<input type="text"/>
----------	----------------------

Please place an "X" in the box that best matches your opinion. Please answer the questions as fully as you feel able to.

Part 1: PERSONAL DETAILS

This information is kept completely confidential and no information is stored on computer media that could identify you as an individual.

1. Please select your AGE group (Years):
15-20 years <input type="checkbox"/> 20-30 years <input type="checkbox"/> 30-40years <input type="checkbox"/> 40-50years <input type="checkbox"/>

2. Please indicate your GENDER:
Male..... <input type="checkbox"/> Female..... <input type="checkbox"/>

3. What is your FIELD of work or study?	<input type="text"/>
---	----------------------

4. Please indicate whether you are a member of staff or a student:
STAFF <input type="checkbox"/> STUDENT <input type="checkbox"/>

TASK: BIOMETRIC DATA ACQUISITION

Your face images will acquired using a camera.

1. Please take the required position for your facial image to be taken.
2. You have now completed TASK.

THANK YOU AND GOD BLESS!!!