CERTIFICATION

This project titled, **BIOMETRIC IDENTIFICATION SYSTEM FOR STAKEHOLDERS (A CASE STUDY OF MOUNTAIN TOP UNIVERSITY),** prepared and submitted by **OLUSEGUN TIMILEHIN TAMILORE** of matriculation number 16010301039 in fulfilment of the requirements for the degree of **BACHELOR OF SCIENCE (Computer Science)** is hereby accepted.

_____ (Signature and Date)

Dr. M.O. Oyetunji

(Supervisor)

_____ (Signature and Date)

Dr. I.O. Akinyemi

(Head of Department)

Accepted as partial fulfilment of the requirements for the degree of BACHELOR OF SCIENCE (Computer Science)

_____ (Signature and Date)

Prof. A. I. Akinwande

Dean, College of Basic and Applied Sciences

DEDICATION

This project work is dedicated to God Almighty.

ACKNOWLEDGEMENT

I owe much gratitude to God Almighty who gave me the wisdom, knowledge, understanding, strength, divine help and provision from the commencement of this project work to its completion.

I specially appreciate my supervisor Dr. M.O. Oyetunji who took keen interest in my project work and guided me all along, and taking the pains to ensure the successful completion of this project work.

I will like to acknowledge the Head of Department Computer Science and Mathematics Dr. I.O. Akinyemi, and offer deep gratitude for the efforts, constant encouragement, guidance and support. I also appreciate all the members of staff of the department of Computer Science: Dr. Alaba O. B., Dr. Oyetunji M.O., Dr. (Mrs.) Kasali F.A., Mr. Falana O.J., Dr. Idowu P.A., Dr. Ojesanmi O.A., Dr. Adamu O.B., Dr. Okunoye O.B., Dr. (Mrs.) Oladeji F.A., and the Departmental non-teaching members of staff, Mr. Ebo I.O., Oladokun T.R. and Amadi A.I.. I say God bless you richly.

I will not fail to appreciate Mr. Moju T., Mr. Osaghae O., and Mr. Gbemiga A., for their assistance, encouragement and selfless efforts in ensuring the achievement of this project. God bless you deeply.

I heartily thank my parents Mr and Mrs Olusegun A.A., and my wonderful siblings, thank you all for your moral and financial support. I am grateful for all the investments into my education and future.

I sincerely appreciate my friends and all Mountain Top University colleagues for their help and support during the period of working on this project. I say God bless you all.

ABSTRACT

This project was based on Biometric Identification System for Stakeholders for use at Mountain Top University. It evolved from the manual paper system used to store visitor's records at the gates. With the help of the biometric system, visitors' records was managed more effectively and efficiently. This project aimed to create a web-based biometric identification system to properly manage visitor's records.

In order to achieve its aim and objectives, a database was created and design steps were taken using the waterfall model. The developed web-based biometric identification system was then implemented. This project work was built on Django python framework, HTML, CSS, Javascript and OpenCV using Visual Studio Code as the Integrated Development Environment (IDE).

The Biometric Identification System created helped to manage visitors' records in a safer and more secure way. The system provided a faster and more efficient way of keeping records for future references.

The Biometric Identification System was a very useful and efficient way of keeping records compared to the manual method currently used. It was recommended that the system was improved upon to increase the scope and productivity of the system.

Keywords: Stakeholders, Biometrics, Database, Enrolment, Identification, Minutiae, Verification.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE
INTRODUCTION

1.1. Background of the Study

The identification of other human beings has been important to the underlying structure of human culture and society since the beginning of human civilisation. Questions regarding the identity of individuals such as “Is this the person who he or she claims to be?”, “Has this applicant been here before?”, “Should this individual be given access to our system?” are asked millions of times every day by organizations in financial institutions, health care, e-commerce, telecommunication, and government. As our society becomes electronically connected to form one big global community, it has become necessary to carry out reliable person recognition often remotely and through automatic means (Jain, Pankanti, Prabhakar, & Wayman, 2004).

Identifying individuals is thus a critical aspect for the functioning of various sectors, such as finance, health, security, government, access control, enforcement, communication and entertainment. More organizations are looking to automated identity authentication systems to enhance customer experience and operating efficiency and to save essential resources. In addition, the ability to achieve a highly precise automatic personal identification system is much more critical as people become even more electronically connected. There are many ways of identifying individuals with the current advances in computer technology, and one of them is biometrics.

A biometric system is basically a pattern recognition system that recognize individuals based on physiological and behavioural characteristics. The objective is to establish an identity based on ‘who you are or what you produce’, rather than by ‘what you possess’ or ‘what you know’ as proposed by traditional identification systems (Asha & Chellappan, 2012). Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioural traits associated with the person (Asha & Chellappan, 2012). Physiological traits are traits or characteristics that can be measured on a part of a body at some point in time and they include fingerprint, hand geometry, facial recognition and retina and iris. Behavioural traits on the other hand are learned over a period of time. Behavioural traits include signature, gait, keystroke dynamics and voice patterns.

The concept of using human features for identification purposes is not a new one. History details that potters from East Asia signed their pottery by placing their fingerprint in the clay as it cured.

In addition, traders from Egypt were identified by physical traits, such as height, weight, eye colour, hair colour and other physical features. Criminologists used fingerprints during the 19th century to help identify habitual criminals. However, human characteristics were measured manually before the advent of biometric systems. Biometric systems therefore differ in that they allow the automated comparison and verification of human characteristics. The systems do not identify individuals on their own as additional information is required (e.g. stored template(s) in a database), rather they compare the information already submitted. Biometric systems and applications hereby use for such automated process mathematical and statistical methods for the qualitative and quantitative measurement of relevant features which are extractable from human characteristics (Kindt, 2013).

Traditionally, knowledge-based identification systems such as passwords and ID cards have been used to limit access to safe systems, but these techniques can be infringed readily and are unreliable. Biometric cannot be borrowed, robbed or forgotten, and forging one is nearly impossible. Because biometric identifiers are unique to people, it is more reliable in identity verification than token and knowledge-based techniques.

The need for large-scale identity management systems has reinforced the importance of using biometrics. Biometric techniques are becoming the basis for a wide range of extremely safe alternatives for identification and private verification (Chaudhari, Pawar, & Deore, 2013). The very aim of identity management is to accurately determine an individual's identity in the context of multiple distinct applications.

This project is centred on developing a biometrics identification system that will allow individuals to be identified at entry points. An individual is prompted to present fingerprint sample to the scanner, if it matches to the one on file, the system will automatically open the database for assessment of information and the individual will be able to sign in and sign out at entry points.

1.2. Statement of the Problem

It is difficult to ascertain and validate the identity of an individual through manual means (i.e. paper and pen). Records are not properly kept and as a result, it is difficult to retrieve information.

The following are the problems stated with the current manual system used in the healthcare environment:

i. Poor security protocol at entry points: At entry points, stakeholders are identified by ID cards and manually writing their bio-details. These can be tampered with.
ii. There is no central database containing the biometric details of stakeholders.
iii. There is no proper record of stakeholders' entry being kept.

1.3. Aim and Objectives

The aim of this project is to design a fingerprint biometric identification system that will accept for Mountain Top University stakeholders which includes staff, students and visitors.

The objectives of this project are:

i. To develop a web-based fingerprint recognition system for the identification of Mountain Top University stakeholders.
ii. To create a central database for stakeholders' biometric information
iii. To design a proper interface for querying stakeholders information.

1.4. Methodology

The biometrics identification system (Fingerprint recognition system) will be a web application to capture the biometrics data of Mountain Top University stakeholders. Identification of enrolled individuals will also be done by the system.

A central database will be developed using the MySQL database to store information of enrolled stakeholders. The system will manage the enrolment of stakeholders' information into the database.

This system will be developed using a Windows Operating System, Apache server will be used to access the database, MySQL for the database and Python for the backend, JavaScript and Cascading Style Sheet (CSS) for design purposes. Working with a database schema and interface for querying records and data. Also a Python library called Open Computer Vision (OpenCV) will be used for processing the biometric trait (Fingerprint).

1.5. Scope of the Study

The scope of this project work is Mountain Top University (MTU).

1.6. Significance of the Study

This study is significant as it helps address the issues of security and incident tracking. It helps to keep consistent and reliable record of entries and exits.

1.7. Definition of Terms

Stakeholders: Staff, Students, Parents and visitors of Mountain Top University.

Biometrics: This is the identification of an individual based on unique physiological or behavioural characteristics.

Database: This an organised collection of data stored on a computer system.

Enrolment: This is the process of newly capturing biometric data to be stored in a database.

Identification: This is the act of establishing or indicating who or what an individual or something is.

Minutiae: These are characteristics by which fingerprints can be identified.

Verification: This is the process of establishing the truth, accuracy, or validity of something.

CHAPTER TWO

LITERATURE REVIEW

2.0. Introduction

The term “biometric” is derived from two Greek words; “bios” which means life, and “metrikos” which means to measure. Strictly speaking, it refers to the science involving the statistical analysis of biological characteristics. However, by language misuse, the term biometrics usually refers to automatic technologies for measuring and analysing biological and anthropological characteristics for identification. We should therefore refer to people's biometric recognition as those security applications that assess human features for validation or identification of identity. We will use the short term "biometrics," however, to refer to "biometric people recognition." (Marcos Faundez-Zanuy, 2006)

According to Down and Sands (2004), “Biometrics is an authentication process relying on the automatic detection or validation of an person based on distinctive physiological or cognitive features”. According to Maguire (2009), “Biometrics denotes the recognition of humans on the basis of inherent physical or behavioral characteristics”. Also according to (Chaudhari, Pawar, & Deore, 2013), “Biometrics are automated methods of identifying a individual based on a trait of physiology or behavior.”.

Physiological traits measured include fingerprints, retina, iris, ear, hand geometry, palm print, odour, palm veins, face, and DNA. Behavioural traits measured include voice patterns, handwriting, signature, keystroke dynamics, lip motion, and gait. The selection of a particular trait for use in a specific application should be based on certain properties or factors. According to (Chaudhari, Pawar, & Deore, 2013) and Marcos Faundez-Zanuy (2006), they are,

i. **Universality**: Each person should possess the characteristic which can be used for identification.
ii. **Distinctiveness**: Every person should be sufficiently different in terms of the characteristics with another person for each person to be distinguishable.
iii. **Permanence**: The characteristic should be sufficiently stable over time (with respect to the corresponding criterion), different environmental conditions, etc. That is, they should not alter for the most part throughout human existence.
iv. **Collectability**: The characteristic should be acquirable and quantitatively measurable.

v. **Acceptability:** People should be willing to accept the biometric system, and do not feel that it is annoying, invasive, etc.

vi. **Performance:** Before the system can be functional, the degree of precision and speed of detection must be quite high.

vii. **Circumvention:** The ability fraudulent people and techniques to deceive the biometric system should be negligible. A system requires to be more difficult to circumvent identity management system and provide added safety.

2.1. Conceptual Review

Biometrics can operate in two modes based on the application context. They are identification and verification.

i. **Identification**

Identification is also known as recognition. In this mode, the system determines who the individual is by searching all the templates already stored in the database. The system performs a one-to-many comparison of the individual's biometrics and the biometrics templates stored in the database until a match is found. It asks the question, "Who is this person?" If the individual is not enrolled in the system, then he or she cannot be identified and the search fails.

Two modes are possible, positive and negative identification. The positive identification tends to determine if a given person is really in a specific database. Such a method is applied when the goal is to prevent multiple users of a single identity. A negative identification determines if a given person is not in a ―watch list database. Such a method is applied for example when the goal is to identify persons registered under several identities.

ii. **Verification**

It is also known as authentication. In this mode, the system verifies if an individual is who he or she claims to be or not. The system performs a one-to-one comparison of the individual's biometric template and only one chosen template stored in a centralized or a distributed database, e.g. directly on a chip for an identity document. It asks the question, "Is this person who he or she claims to be?" This method is used for securing and restricting access to specific persons.

The process of a biometric system can be divided into two phases. The enrolment phase and the identification phase.

2.1.1. Enrolment Phase

Also referred to as the registration process, the enrolment phase is the first stage in biometric identification. During enrolment, the data subject (i.e. the individual) submits physiological or behavioural traits (e.g. fingerprint) and then captures them via the appropriate device (e.g. fingerprint sensor). The traits are stored as samples. These samples can go through measures to optimize and improve quality. A feature extractor then utilizes algorithms to process the optimized samples in order to identify and retrieve the distinct characteristics. For a fingerprint sample, the features will be minutiae points and local orientations, while the size and comparative locations of the eyes, nose, and mouth will probably be included for a facial picture. The obtained features that might consist of one or more pairs will then be used to create the template.

Templates, however, being extracted reference biometric features, take different forms and formats (or representations). For instance, a table or a (fixed-length) numerical (binary) string (e.g. 101010 depicting a feature vector or not) may be templates that differ in detail and length. The templates for each of the features will also differ. For example, the minutiae features can be represented as an unordered set of tuples consisting of coordinates of the minutiae and local orientation for fingerprinting. For hand geometry, the hand's geometric properties are represented by a fixed-length ordered vector of the finger and/or palm lengths and widths. Iris is depicted as binary strings of fixed length. (Kindt, 2013)

Then the template will be stored in a database. The database can be a central or distributed database, such as the one in which the template of each user is stored on a smart card and distributed to users (Chaudhari, Pawar, & Deore, 2013). The size of a template in bits and bytes is typically much smaller than the size of the image. The decreased quantity of kilobytes enables templates to be stored in microprocessors (e.g. Chips), for example, that have a restricted capacity for storage (and processing), and can be integrated in smart cards or documents. The number of bits on a template may vary and limit the possibility for particular biometric features to save data on a card or token, depending on the biological or behavioural properties and algorithms used. Therefore, the enrolment stage typically offers a template of the biometric trait that will be used for subsequent comparisons. (Kindt, 2013)

2.1.2. Identification Phase

Identifying or verifying an individual is the fundamental responsibility of the identifying phase. The biometric data obtained from the collected sample shall be compared during this phase with the template(s) recorded when enrolled. The templates are compared to find a match and then a decision is made.

There is a decision for biometric verification, that is, ' the comparison decision determining the legitimacy in a verification operation of a biometric claim ' and a decision on a biometric identification, which is a 'comparison choice as to whether a particular biometric database reference(s) is in a biometric database or not.' (Kindt, 2013)

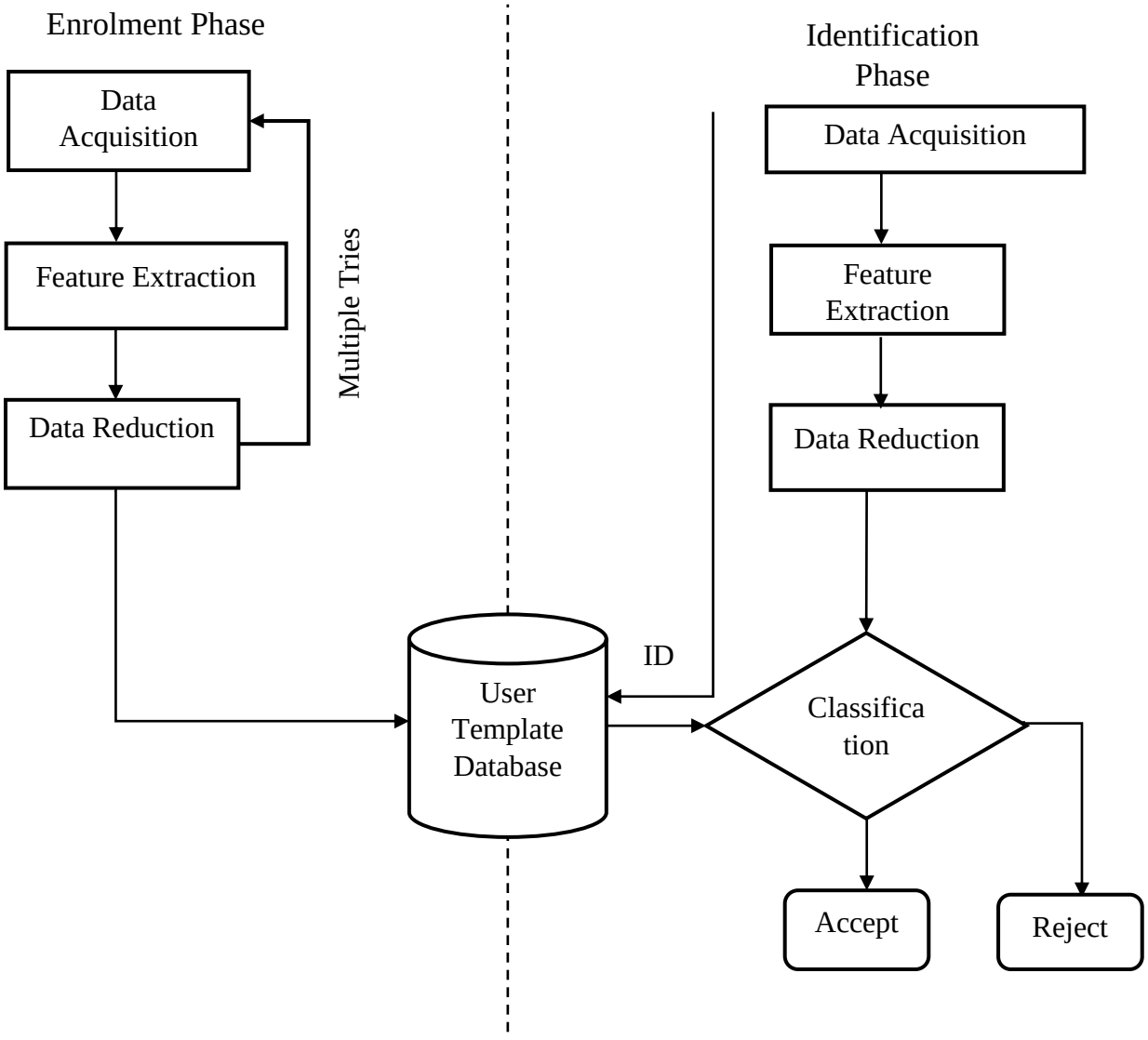

Figure 2.1 The architecture of a biometric system (Chaudhari, Pawar, & Deore, 2013).

2.2. Theoretical Review

The idea of identifying humans using body parts goes way back in history. Prints of hands, feet, and fingers have already been used in ancient times because of their unique characteristics (Kindt, 2013). In 1994, a group of cave explorers discovered the Chauvet Cave in the Ardeche valley in southern France. Paintings believed to have been created by prehistoric men and estimated to be around 30,000 to 32,000 years were also discovered in the cave. The paintings contained handprints. Some of these handprints are believed to have fixed by the originators of the images to identify themselves (Jean, 2002).

Ancient Assyrians, Babylonians, Japanese and Chinese signature records were the first documented use of fingerprints. King Hammurabi (1792–1750 BC) of Babylon is known to have introduced one of the first written codes of law in clay tablets worldwide. The kings of Babylon allegedly authenticated the tables with an impression from their right hands in the tablets. Fingerprints were also used in commercial operations registered on tablets of clay in Babylon (Kindt, 2013). For at least 2000 years, Chinese have used fingerprints and handprints for authenticity. Joao de Barros, a Spanish explorer and writer, writes that Chinese dealers stamped children palm prints and footprints on ink paper to differentiate between the children (Chaudhari, Pawar, & Deore, 2013). Documents from the Tang dynasty (618–907) in China referred to the use of fingerprints and hand-prints on contracting arrangements. (Kindt, 2013).

Johannes Evangelista Purkinje, a Czech physiologist and anatomy lecturer at Breslau University, completed the first contemporary fingerprint research. He suggested a classification scheme for fingerprints in 1823. In July of 1858, when Sir William Herschel pressed handprints on the back of the contracts, the English started using palm and fingerprints in India. From palm prints, Herschel shifted to prints with the correct index and middle fingers. In the 1850s, Sir William Herschel began to place signatures of hand and fingerprints on agreements in British Indian colonies, serving as a British civil service agent. The prints were used to prevent employees from being charged twice or someone else from being personified upon pay. He is often acknowledged as the first European to recognize the importance of fingerprint as a means of identifying people. (Kindt, 2013)

In the 1890s, Alphonse Bertillon was a French anthropologist and police officer in Paris and developed a method for identifying repeat offenders who gave many aliases each time they were

detained. This technique named after him engaged various readings of the body (Bertillonage). Measurements included diameter of the skull, arm and foot length. The French police mostly made use of its system, but it faded fast when certain subjects were falsely identified.

Sir Francis Galton published in the late 19th century a comprehensive fingerprint survey in which he submitted a fresh classification scheme with 10 fingerprints. He calculated that there is an identical probability of 1 in 64 billion of two individual fingerprints. Galton identified the features that can be used to identify fingerprints (minutia), which are still the same as those used today. (Chaudhari, Pawar, & Deore, 2013)

In the 1890s also, the police in Bengal, India, started using fingerprints to identify criminals under the leadership of British police officer Sir Edward Richard Henry. Henry set up the first British fingerprint archives in London in 1901, as assistant commissioner of the metropolitan police. The Galton classification system was further developed, which resulted in the Galton-Henry system. The first systematic use of the use of fingerprints in the United States of America for criminals was initiated in 1903 by the New York State Prison System. Fingerprints were used in Kansas Federal Penitentiary in Leavenworth in 1904 and in the Police Department in the St. Louis [Missouri]. The United States Army in 1905 started to use fingerprints. In 1907, the US Navy started to use fingerprints and the Marine Corps joined in the use the next year. During the coming twenty-five years, more and more federal law enforcement agencies also joined in the use of fingerprints to identify individuals. In 1936, ophthalmologist Frank Burch suggested the idea of using the iris pattern to identify an individual. (National Biometric Security Project, 2008).

Some of the oldest works on machine face recognition can be found in Palo Alto, California in the 1960s at an organization known as Panoramic Research. This research was carried out under contract with the US Government by Woody Bledsoe, a pioneer in the field of automated reasoning. The method he created was called "man-machine face recognition" and employed a process known as feature extraction. This method was based exclusively on the ability to obtain usable feature points. The distances and proportions were calculated to a common point of reference compared to the reference data. The first signature identification system was created in 1965 by North American aviation. (Chaudhari, Pawar, & Deore, 2013)

The International Biometrics Association (IBA) was established in 1986–1987 as the first organisation in the biometric sector. In the 1980s, Dr. John Daugman at the University of

Cambridge developed Iris recognition technology. In 1998, as a non-profit sector trade organization, the International Biometric Industry Association (IBIA) was established in Washington, DC, to further the common global interest of biometrics. Focusing on the events 11 September 2001 and the need for rapid growth and use in biometric technology, the National Biometric Security Projection (NBSP) was established in 2001 (National Biometric Security Project, 2008).

After the start of the 20th century, the lot of biometric techniques are used by human beings in their daily life.

2.2.1. Overview of Biometric Technologies

Facial Recognition

This is probably the most common and natural way of performing biometric recognition, as humans are able to distinguish themselves based on their appearance. The objective of facial identification is to determine an individual based on facial characteristics like the eye socket location, space between cheekbones and eyebrows, etc. (Down and Sands, 2004). Facial (face) recognition is a computer application that recognizes or verifies an individual automatically from a video source using a digital image or video frame. This can be done by comparing the example provided with the data contained in the database. Techniques of facial identification include the identification of skin pattern, 2-D and 3-D methods. (Babich, 2012)

DNA

DNA or Deoxyribonucleic acid is the part of a cell that contains genetic data distinctive to each individual. DNA (Deoxyribonucleic Acid) is the distinctive one-dimensional code for one's individuality. Exceptions are identical twins as they possess similar DNA patterns. DNA typing is a biometric technique that measures and analyses DNA samples to differentiate individuals with a certain probability. DNA samples can be obtained from varying sources: paper or plastic container, sweat, T-shirt, glass, ear wax, socks, chews, hair, nails, blood, urine etc.

This technology has some major drawbacks (Kresimir & Mislav, 2004). They include:

i. Contamination and sensitivity, since it is easy to steal a piece of DNA from an individual and use it for an ulterior purpose

ii. No real-time application is possible because DNA matching requires complex chemical methods involving expert's skills

iii. Privacy issues since DNA sample taken from an individual is likely to show susceptibility of a person to some diseases.

All this limits the use of DNA matching to forensic applications.

Iris

Iris recognition is the method by which an individual can be recognized by analysing the iris pattern. The iris is a muscle in the eye that controls the pupil's size and the amount of light entering the eye. It is the coloured part of the eye with colouring depending on the quantity of melatonin pigment in the muscle. Each iris structure is featuring a complex pattern. This may be a mixture of particular features known as corona, crypts, filaments, freckles, pits, furrows, striations and rings. (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009).

The user looks at the sensor, in this case a camera, and the detailed structure of his / her iris is illuminated using near-infrared light. The algorithm in question then generates a mathematical representation of the complex iris structure. The image is also altered to decrease noise and other insignificant data created by eyelashes and eyelids occluding (masking) the iris and to account for the resolution problems due to the amount of illumination. During the recognition process a live iris image is converted to a template and is compared with the enrolled template via a bit-to-bit comparison, which measures the correlation between the irises. (Chaudhari, Pawar, & Deore, 2013)

Iris recognition is regarded to be one of the precise methods of biometrics. The iris is shielded by eyelid, cornea and aqueous humor that minimizes the probability of harm, unlike fingerprinting. (Babich, 2012).

Retina

It is based on the structure of the blood vessels in the retina of the brain as the blood vessels at the rear of the eye have a distinctive pattern, from eye to eye and from individual to individual. Retina is not immediately noticeable and therefore a consistent infrared light source is needed to illuminate the retina. Infrared energy is absorbed more quickly by the blood vessels in the retina than by the adjacent tissue. The image of the retinal blood vessel model is then analysed.

Retina scans require that the person removes their glasses, place their eye close to the scanner, stare at a specific point, and remain still, and focus on a specified location for approximately 10 to 15 seconds while the scan is completed. A retinal scan includes the use of a consistent, low intensity light source, which is then pictured and analysed on the retina for the illumination of blood vessels. The blood vessel models are handled by a coupler. Furthermore, the retina of a deceased person decays too rapidly to be used to deceive a retinal scan. A retinal scan has an error rate of 1 in 10,000,000, compared to fingerprint identification error being sometimes as high as 1 in 500. (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009)

Speech Recognition

Speaker or voice recognition is a biometric mode that uses an individual's voice for recognition purposes. There are two primary factors that make a person's voice distinctive. First of all, it is the physiological component recognized as the voice tract. Secondly, it is a behavioural component known as the voice accent. By combining these two factors, it is almost impossible to accurately mimic the voice of another person. Taking advantage of these features, the biometrics technology developed voice recognition systems to confirm the identity of each person using only their voice.

Hand Geometry

Hand geometry is the use of geometric shape of the hand for recognition purposes. It is based on the reality that almost every person's palm is shaped differently, and that the shape of a person's hand does not change after a certain age. These methods include estimating the length, width, thickness and surface area of the hand.

Hand geometry recognition devices evaluate the physical size of a hand (or finger) from a 3D image. The measurements gathered shall include the form, width and length of the fingers, and knuckles and the thickness of the hand (or finger). The user positions his / her hand on the sensor, which contains guidance poles, to guarantee the right placement of the user's hands and fingers. The sensor uses a camera to draw pictures of both the top and the sides of the hand. The sensor does not record any surface details, such as finger prints or palm prints, wounds or skin colour, and the resulting image is black and white.

Facial Thermogram

The facial thermogram needs a (costly) infrared camera to identify patterns of facial heat that are peculiar to every human being. The pattern of heat radiated by the human body is characteristic of

a person and can be caught by an infrared camera in an unobtrusive manner much like a regular (visible range) photograph (Asha & Chellappan, 2012).

The thermogram-based system does not necessitate contact and is non-invasive, but the acquisition of images is difficult in uncontrolled environments where heat radiating surfaces (e.g., room heaters and vehicle exhaust pipes) are present in the vicinity of the body. (Asha & Chellappan, 2012)

Keystroke Dynamics

Keystroke dynamics is a technique of verifying the identity of a person by their typing rhythm, which can be used by skilled typists as well as amateur two-finger typists.

Keystroke dynamics technology measures dwell time (the length of time a person holds each key) as well as flight time (the time it takes to move between the keys). Taken during several login sessions, these two metrics generate rhythm measurements that are specific to each customer. (Down & Sands, 2004)

Gait

Gait is essentially the unique way one walks, and it is a complicated biometric spatio-temporal. Gait is a behavioural biometric and may not stay stable, particularly over a lengthy span of time, owing to body weight changes, significant accidents affecting the joints or brain. Since gait-based devices use video footage of a walking individual to evaluate several distinct movements of each articulate joint, input is extensive and computationally costly. Approaches for gait identification include a machine-based vision, a floor sensor and a wearable sensor.

2.2.2. Errors and Failures of Biometric Systems

To determine unique information, biometric technologies strive to create a realistic and unalterable depiction of biometric characteristics. Intrinsically, this method is susceptible to error as mistake happens at each stage of the process. For subsequent contrast, it will not be feasible to obtain appropriate characteristics in case of a poor performance sample. If the characteristics show inadequate distinguishing data, the development of the template may fail. (Kindt, 2013)

Errors and errors happen in the stage of enrolment, the stage of removal and the phase of comparison. Ultimately, these mistakes and failures at various phases contribute to a decision making mistake.

False Accept errors

False accept errors also regarded as False Match mistakes happen when acceptance of a non-matching biometric information combination (Chinedum, 2017). In the case of identification/screening, the biometric system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database or pattern associated with an incorrectly claimed identity (in the case of verification) (Jain, Pankanti, Prabhakar, & Wayman, 2004). False accept mistakes are evaluated as the acceptance frequency of False or False Match.

False Reject errors

False reject errors occur when a matching pair of biometric data is rejected. The biometric system incorrectly claims input pattern failure to match a matching pattern in the database (identification/screening) or pattern associated with the correctly claimed identity (verification) (Jain, Pankanti, Prabhakar, & Wayman, 2004). Also known as False Non-Match errors, they are evaluated as either False Reject rate or False Non-Match rate.

Practical biometric systems also have significant failures both in terms of failure to acquire (FTA) and failure to enrol (FTE) (Jain, Pankanti, Prabhakar, & Wayman, 2004).

Failure to Acquire (FTA)

There is a likelihood that the system will fail to create a reference sample or template in some cases during the enrolment process. This error may be due to the fact that the data subject loses a necessary trait, such as losing specific fingers due to an incident or damaging the trait (Kindt, 2013). This is called a failure to enrol (FTE).

Failure to Enrol (FTE)

There is also a likelihood that a system will not acquire a specified biometric trait (FTA) for the comparison beforehand. This is the case if it is not possible to accept the output of the automated data capture method. This error may happen during the enrolment or later comparison capture or extraction steps (Kindt, 2013).

2.2.3. Performance Measurement of Biometric Systems

A biometric system's efficiency is based on criteria like false rejection rate, false acceptance rate, equal error rate, receiver operating characteristic curve, threshold, and failure to enrol rate.

False Acceptance Rate

False acceptance rate (FAR), measure the percentage of occasions a rejected person is favorably matched by the biometric system, i.e. how many times the "bad guys" beat the system (Down & Sands, 2004). It is the likelihood of a sample being wrongly stated to correspond with one "non-self" random template (Marcos Faundez-Zanuy, 2006).

False Rejection Rate

The false rejection rate (FRR) estimates the proportion of times a person who should be recognized favourably is rejected — that is, how many times the "good guys" are unable to gain entry. If people who should be given access are constantly denied access, they will not have access to a safe database or place to execute their allocated responsibilities (Down & Sands, 2004). The biometric system wrongly states the inability to match the entry pattern with the corresponding pattern in the database (identification / screening) or the pattern incident with the properly asserted identity (validation) (Jain, Pankanti, Prabhakar, & Wayman, 2004). False rejection rate estimates the percentage of valid inputs being rejected.

The FAR and FRR are interrelated: reducing a biometric system's FAR will increase the FRR and vice versa. In reality, they will apply to and therefore be determined by the system limit which the data controller may choose and which the system must therefore satisfy. The FAR shall be put to a minimum for high-security apps deploying favourable demands (because it is extremely undesirable to have unlawful individuals approved), but this will mean a rise in the FRR (suggesting that approved individuals are wrongly rejected). In reality, FAR and FRR of systems have non-zero structures. (Kindt, 2013)

Overall, false acceptance rates (FAR) and false rejection rates (FRR) will be used to show a system's efficiency or practical execution. Their use is popular, particularly in the commercial sector. They refer to the performance of the complete comparative process including all steps (e.g., including whether the decision policy accepts different capture efforts) until the system's final decision. The rates also rely on the biometric feature the system uses. Hand geometry, for instance, has a high FAR with identification functionality relative to other biometric features. The quality of the data stored and used for comparison is also very crucial. Other system specifications will also determine the rates (Kindt, 2013). Although a system with a FRR of 0.01 per cent and a FAR of 0.0001 per cent may seem reasonable, this may be intolerable or very hard to manage if, for

example, the database contains of 50 million records, which would give 50 incorrectly verified identity claims (or non-identity claims, in the case of a watch list) and 5,000 false rejections. (Child, 2013)

Biometric trait	**Test**	**Test conditions**	**False reject rate**	**False accept rate**
Fingerprint	FVC 2006	Heterogeneous population including manual workers and elderly people	2.2%	2.2%
Face	FRVT 2006	Controlled illumination, high resolution	0.8% - 1.6%	0.1%
Voice	NIST 2004	Text independent, multi-lingual	5% - 10%	2% - 5%
Iris	ICE 2006	Controlled illumination, broad-quality range	1.1% - 1.4%	0.1%

Table 2.2 False reject and false accept rates (Jain, Nandakumar, & Nagar, Biometric Template Security, 2008)

Threshold

The decision threshold is the minimum value to be achieved by the biometric comparison process. It is chosen in order to optimize the error rate of the system according to the application requirements. The system's acceptance or refusal decision on the comparison is computed by comparing the system's response to the threshold. Tightening the decision threshold would usually imply raising the FRR and lowering the FAR. The reduction of the threshold would reduce the FRR and boost the FAR. This threshold is set by the system administrator, the system developer or the system vendor. The data subjects usually have no effect and no idea of the error rate and threshold set in the event that they are not explicitly informed. (Kindt, 2013)

Equal Error Rate & the Receiver Operating Characteristic (ROC) Curve

Since the manufacturer of the biometric system does not know for which implementation the system will be used, the efficiency of the system could be reflected by stating where the FMR (FAR) is equivalent to the FNMR (FRR), i.e. that the amount or percentage of false matches is (approximately) equivalent to the amount or percentage of true non-matches. In that case, this error rate is referred to as the Equal Error Rate or EER. The EER (i.e. the error rate when FMR ≈ FNMR) is a measure used for the quality of a biometric system that operates in a common commercial or civilian environment. (Kindt, 2013)

Equal error rate (EER), also known as the crossover rate, is the point on a graph where the FAR and FRR lines intersect. A reduced crossover rate shows a system with a good sensitivity level and generally implies that the system performs well (Down & Sands, 2004).

The matching algorithm uses certain parameters (e.g. a threshold) to make a decision. Usually, the FAR and FRR can be traded against each other in biometric systems by altering those other parameters (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). The receiver operating characteristics (ROC) curve is the trade-off at different operating points between the FMR and FNR of a system. In a given test environment, it is a comprehensive measure of system accuracy (Jain, Pankanti, Prabhakar, & Wayman, 2004). The ROC curve is used to get a graphical view of error rates and to test and report on the error rates of multiple biometric algorithms or systems tested (Kindt, 2013). A typical ROC curve is shown in Figure 2.2 in relation to biometric applications, including the EER.

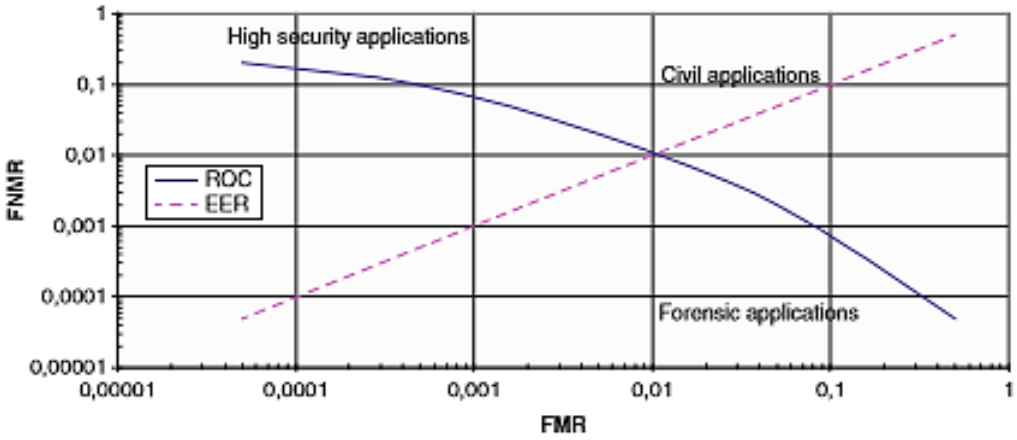

Figure 2.2 Typical ROC curve (Kindt, 2013)

Failure to Enrol Rate (FTE or FER)

This is the percentage of data input that is regarded invalid and cannot be entered into the system. Failure to enrol occurs when data collected by the sensor is deemed invalid or of bad quality.

It should be noted that suppliers typically market products with measures depending on laboratory trials in optimal situations. Practical applications of these products, however, demonstrate different statistical results and alter the real basis of performance. These variations are caused by factors such as familiarity of users, speeds of networks, environmental impacts and design of products. Published efficiency measures will become more credible as more effective standards become accessible, but organizations should still consider independent testing. In order to provide the best knowledge of real results in the installed system, these independent experiments should be carried out within the organization's own environment and customer population guidelines. (Down & Sands, 2004)

The table below summarizes the results of some studies, such as FVRT (Face Recognition Vendor Test), CESG (Communications Electronics Security Group), FVC (Fingerprint Verification Competition) and NIST (National Institute of standard technologies), and SVC (Signature Verification Competition).

Biometric	Test	Test parameter	Attempts	FRR	FAR	FTE	FTA
Face	FRVT	11-13 months spaced	1	4%	10%	-	-
	CESG	200 users, 1-3 months spaced	3	6%	6%	0.0%	0.0%
Fingerprint	FVC	100 users, Mainly age 20-30	1	2%	0.02%	-	-
	CESG	200 users, Mainly age > 25	3	2%	0.01%	1%–2%	0.4% – 2.8%
Hand	CESG	200 users, Mainly age > 25	1	3%	0.3%	0.0%	0.0%
	CESG	200 users, Mainly age > 25	3	1%	0.15%	0.0%	0.0%
Iris	CESG	200 users, Mainly age > 25	1	2%	0.0001%	0.5%	0.0%
	CESG	200 users, Mainly age > 25	3	0.25%	0.0001%	0.5%	0.0%
Voice	NIST	Text independent	1	7%	7%	-	-
	CESG	Text dependent	3	2%	0.03%	0.0%	2.5%
Signature	SVC	60 users, skilled forgeries	1	2.89%	2.89%	-	-

Table 2.2 Error rates of various biometrics pairs. FRR= False Rejection Rate, FAR= False Acceptance Rate, FTE= Failure to Enrol rate, FTA= Failure to Acquire rate. *(Marcos Faundez-Zanuy, 2006)*

2.3. Fingerprint Recognition System

During the 19th century, the concept that no two individuals have the same fingerprints and that patterns of fingerprints did not significantly change throughout life was accepted. This resulted in the use of fingerprints for individual recognition (Chaudhari, Pawar, & Deore, 2013). A fingerprint is a pattern of ridges and furrows on the tip of each finger, according to (Kresimir & Mislav, 2004).

A fingerprint is defined by (Thakkar, 2014) as a distinct pattern of ridges and valleys on an individual's finger surface. A ridge is described as a single curved segment, while the region between two adjacent ridges is a valley. So the dark fingerprint areas are called ridges, and the white area between them is called valleys.

Because of their increased acceptability, immutability and individuality, fingerprints have long been used for biometric identification. The likelihood of two fingerprints being equal is 1 in 1.9 x 10^{15} (Afsar, Arif, & Hussain, 2004). These characteristics make highly efficient and effective use of fingerprint technology in industries where a significant degree of security is important.

According to (Nath, Ray, & Ghosh, 2011), there are three levels of features possessed by a fingerprint namely, Level 1 (pattern), Level 2 (minutiae points) and Level 3 (pores and ridge shape).

Level 1 features refer to the unknown fingerprint's general pattern shape— a whorl, loop, or some other pattern. It cannot be used to individualize this level of detail, but it can assist to narrow down the search. Level 2 features refers to particular friction ridge paths— general friction ridge flow and significant ridge route deviations (ridge characteristics called minutiae) such as ridge ends, lakes, islands, bifurcations, scars, incipient ridges, and crossings. Minutiae can be defined as the ending point or fork of the ridge lines (Thakkar, 2014). They can be of many different types. These types are:

i. **Ridge ending** is the point where the ridge ends suddenly.
ii. **Ridge bifurcation** is the point where a single ridge branches out into two or more ridges.
iii. **Ridge dots** are very small ridges.
iv. **Ridge islands** are slightly longer than dots and occupy a middle space between two diverging ridges.

v. **Ponds or Lakes** are the empty space between two diverging ridges.

vi. **Spurs** is a notch protruding from a ridge.

vii. **Bridges** are the small ridges that join two longer adjacent ridges.

viii. **Crossovers** are formed when two ridges cross each other

The most frequently used types of minutiae are ridge endings and ridge bifurcations as all other types of minutiae are based on a mixture of these two types. Level 3 characteristics refers to the intrinsic detail in a developed fingerprint — pores, ridge units, border detail, scars, etc.

Figure 2.3 Level 1 Features (Fingerprint Patterns) (Prasad, Al-Ani, & Nejres, 2015)

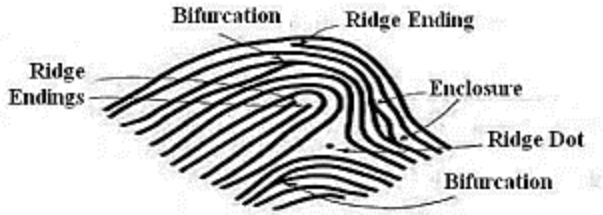

Figure 2.4 Level 2 Features (Minutiae) (Chaudhari, Pawar, & Deore, 2013)

There are five steps in fingerprint recognition.

1. **Image Acquisition**

   This is the process of retrieving a fingerprint image from a capture device like scanners, optical sensors, capacitive sensors or thermal sensors.

2. **Image Enhancement**

   The efficiency of minutiae extraction algorithms and other recognition techniques for fingerprints depends strongly on the image quality of the input fingerprint. The ridges and valleys alternate in an ideal fingerprint image and flow in a locally constant path. The objective of enhancing the image is to improve the clarity of the ridge structures in recoverable regions and to mark the unrecoverable regions as too noisy for further processing. (Bhowmik, Bhowmik, Azam, & Rony, 2012). Image enhancement includes binarization and thinning.

   i. **Image binarization** is a process that transforms the 8-bit gray image into a 1-bit image with a ridge value of 0 and a furrow value of 1 (Singh, Shah, & Gupta). Following the operation, the fingerprint ridges are displayed in black color while the furrows are white. Good algorithms for binarization should reduce information loss and provide effective computing complexities. (Nath, Ray, & Ghosh, 2011).

   ii. **Thinning** is the method applied to the binary image, from the earlier phase, by thinning certain pattern forms until it is represented by1-pixel wide lines. Fingerprint thinning is generally done through morphological operations such as erosion and dilation to decrease the size of the ridges to a single pixel while maintaining the extent and functionality of the initial form (Bhowmik, Bhowmik, Azam, & Rony, 2012). After finishing the thinning phase, no further removal of pixels should be feasible. (Kaur & Garg, 2015).

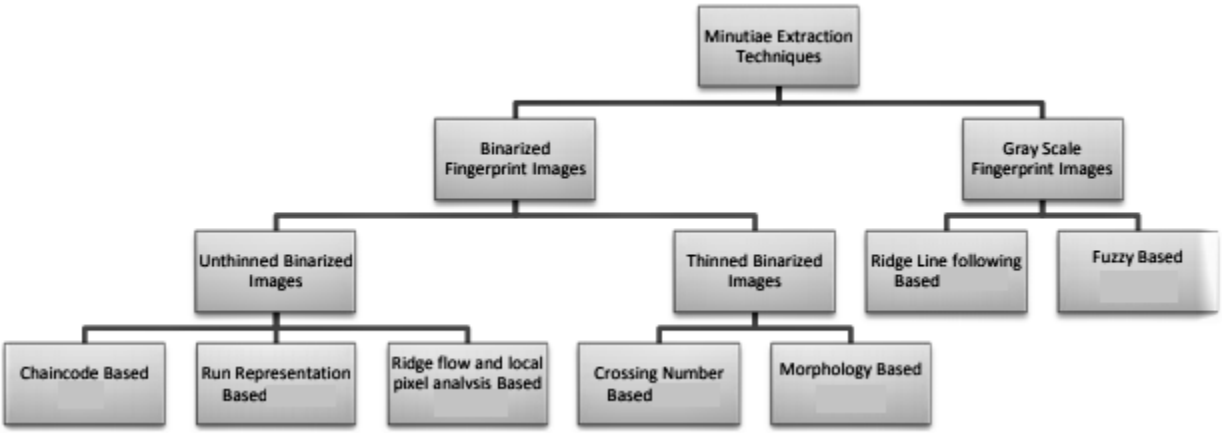

Figure 2.5 Classification of Minutiae Extraction Techniques (Bansal, Sehgal, & Bedi, 2011)

3. Minutiae Extraction

This is the process of extracting minutiae points from a thinned fingerprint image. Minutiae extraction is just a simple job of extracting singular points from a thin ridge map. The efficiency of presently available minutiae extraction algorithms relies strongly on the quality of the fingerprint images input. The position of minutiae and the angles of minutiae are obtained after minutiae extraction. (Kaur & Garg, 2015)

There are many minutiae extraction methods and they can be classified into two categories as shown above in figure 2.5:

i. Those that work on binarized fingerprint images
ii. Those that work directly on gray-scale fingerprint images

The most frequently used technique of minutiae extraction is the Crossing Number technique. This is due to its computational efficiency and inherent simplicity. This technique includes the use of a skeleton image where the ridge flow pattern is 8-connected. The minutiae are obtained by checking the local area of each edge pixel in the image using a 3X3 matrix as shown in the table below.

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Table 2.3 3X3 neighbourhood

Crossing Number Value	**Property**
0	Isolation point
1	Ridge ending point
2	Ridge continuing point
3	Bifurcation point
4	Crossing point

Table 2.4 Properties of Crossing Number

The Crossing Number value is then computed as follows:

$$CN = \frac{1}{2}\sum_{i+1}^{8} |P_i - P_{i+1}|$$

It is defined as half the sum of the differences in the eight neighbourhood between pairs of adjacent pixels (Bansal, Sehgal, & Bedi, 2011). If the crossing number is 0, 1, 2, 3 and above 3 then minutiae points are categorized as, Isolation Point, Termination / Ridge End Point, Normal ridge / Ridge Continuation Point, Bifurcation Point and Crossing Point respectively. The properties of CN are summarized in Table 2.4 above.

There may be many false ridges that may affect the accuracy of matching if not removed. These can be removed by taking into account the distance between the minutiae points. If two endings or two bifurcations or termination and bifurcation are too close to each other, they will be removed. (Sojan & Kulkarni, 2016)

4. Fingerprint Matching

This is the process of comparing the characteristics of a fingerprint obtained with the features of a fingerprint template that was enrolled and earlier stored. Matching fingerprint images is an incredibly challenging issue, primarily owing to the big variation of the same finger in different prints (i.e. large intra-class variations) (Nath, Ray, & Ghosh, 2011). Fingerprint matching techniques can be classified into 3 major categories:

i. **Correlation-based Matching:** Two fingerprint images are overlaid and for distinct alignments (e.g. different displacements and rotations) the correlation between the respective pixels is calculated. Fourier transform can be used to speed up the correlation computation as well as Fourier-Mellin Transform. (Nath, Ray, & Ghosh, 2011)

ii. **Feature-based (or Minutiae- based) Matching:** Typical techniques for fingerprint recognition use feature-based matching, where minutiae (i.e. ridge ending and ridge bifurcation) are obtained from the enrolled fingerprint image and the fingerprint image input, and the number of associated minutiae pairings between the two images is used to identify a legitimate fingerprint image. This is the most common and universally used technique as it is based on the contrasting

of fingerprints produced by fingerprint examiners. Minutiae-based pairing mainly involves finding the balance between the template and the minutiae input sets resulting in the highest number of minutiae pairings (Singh, Shah, & Gupta).

The minutiae matching issue has primarily been addressed as a point pattern matching issue that has been researched widely producing families of approaches such as relaxation techniques, algebraic and operational research strategies, tree-pruning approaches, techniques of minimizing energy, Hough turn, etc. (Nath, Ray, & Ghosh, 2011)

iii. **Pattern-based (or Image-based):** Matching Pattern-based algorithms compare fundamental fingerprint patterns (e.g., local orientation and frequency, ridge shape, texture data) between a earlier recorded template and a candidate fingerprint. The images must be placed around a key point on each image in the same place. In a pattern-based algorithm, the template includes the type, size and position of patterns within the matched fingerprint image. To determine the degree of match, the candidate fingerprint image is then contrasted graphically with the template.

2.4. Review of Related Works

Fingerprint techniques of enhancement

Hastings (2007) has created a technique to enhance the ridge pattern by using the oriented diffusion process by adapting the anisotropic diffusion to smooth the image in the direction parallel to the ridge flow. The intensity of the image differs perfectly as one crosses the ridges or valleys, removing most of the small errors and breaks, but preserving the character of the individual ridges and valleys. Fronthaler, kollreider, & Bigun (2008) proposed fingerprint enhancement to enhance matching performance and computing effectiveness by using an image scale pyramid and directional temporal domain filtering.

Hong, Wan, & Jain (1998) presented a fast fingerprint enhancement algorithm that can dynamically enhance the clarity of the ridge and furrow structures of the fingerprint image sample depending on the predicted local ridge position and frequency. They assessed the performance of the image enhancement algorithm using the obtained minutiae goodness index and the precision of an online fingerprint verification system.

Bhupesh Gour, Bandopadhyaya, & Sharma (2008) also created a technique for extracting minutiae from fingerprint images using midpoint ridge contour representation.

Tabassum (2013) suggested an efficient and effective minute removal algorithm to enhance the general performance of an automatic fingerprint identification system since it is essential to maintain real minutae while removing false minutae in post processing (Kaur & Garg, 2015).

Fingerprint techniques of feature extraction

Maio & Maltoni (1990) used minutiae derived directly from gray-level fingerprint images. Their algorithm is focused on a gray-level ridge tracing, which extracts ridges by sequentially pursuing each gray-level ridge until it finishes or forks. Their algorithm does not directly binarize the gray-level fingerprint during thorough processing, but still implicitly binarizes the gray-level ridge tracer.

Helpful and efficient fingerprint segmentation was provided by Sen, Weiwei, & Yangsheng (2002). They obtain two new features with which their algorithm can differentiate the noisy region from the foreground and thus reduce the number of false minutiae. They use a monitored neural RBF network to identify patterns and pick typical patterns to train the classifier. Their experimental findings indicate a substantial enhancement in the performance of fingerprint segmentation.

Fingerprint verification techniques

Rao, NagaRaju, Reddy, & Prasad (2008) proposed a technique for the identification of fingerprints using a gray-level watershed method to discover the ridges on the fingerprint image directly scanned or inked. Gu, Zhou, & Yang (2006) proposed a method of fingerprint verification that involves both minutiae and model-based orientation fields. It provides solid discriminatory data other than minutiae points. Fingerprint matching is performed by pairing matcher decisions depending on the field of orientation and minutiae. Lumini & Nann (2008) created a technique for minutiae-based fingerprinting and its two-class pattern identification approach to the problem. By matching minutiae into genuine or imposter through Support Vector Machine, they categorized the acquired feature vector resulting in notable performance improvement.

A fingerprint identification method centered on fuzzy logic methods was provided by Sagar, Ngo, & Foo (1995). Since the entire procedure of the fingerprint verification systems is very computationally expensive and therefore requires more expensive hardware to meet the response-

time requirements, they developed a matching algorithm that initially encodes the discovered minutiae points in a compressed format and a fuzzy approximation theorem is used to match these encoded data with the fingerprint being tested. The benefit of this algorithm is that it is easy and less costly.

Jain, Hong, Pankanti, & Bolle (1997) defined a prototype automatic identification verification system that use fingerprints to authenticate an individual's identity. They developed an enhanced minutiae extraction algorithm that claims to be faster and more precise than previous algorithms. A corresponding algorithm based on alignment is suggested. This algorithm is capable of discovering the correspondence between input minutiae and the recorded template without exhaustive search and has the capacity to adapt to nonlinear deformations and inaccurate transformations between input and template. (Hasan & Abdul-Kareem, 2013)

CHAPTER THREE
METHODOLOGY

3.1 Overview

The design of a biometrics identification system is to improve the security system of the school. With the improved changes in information and technology, security procedures are becoming advanced.

This chapter explains the necessary step-by-step description of how solutions to actualize stated objectives of the research work will be carried out. It outlines the various steps that were thoroughly adopted in achieving the objectives of the research along with the logic behind the adopted methods.

3.2 Software Development Life Cycle (SDLC)

Software Development Life Cycle (SDLC) is a process used to plan, create, test and deploy an information system. It involves a comprehensive system describing how particular a software can be developed, maintained, replaced, modified or improved. The life cycle depicts a strategy to improve software performance and the overall method of development. The model used for this project is the waterfall model.

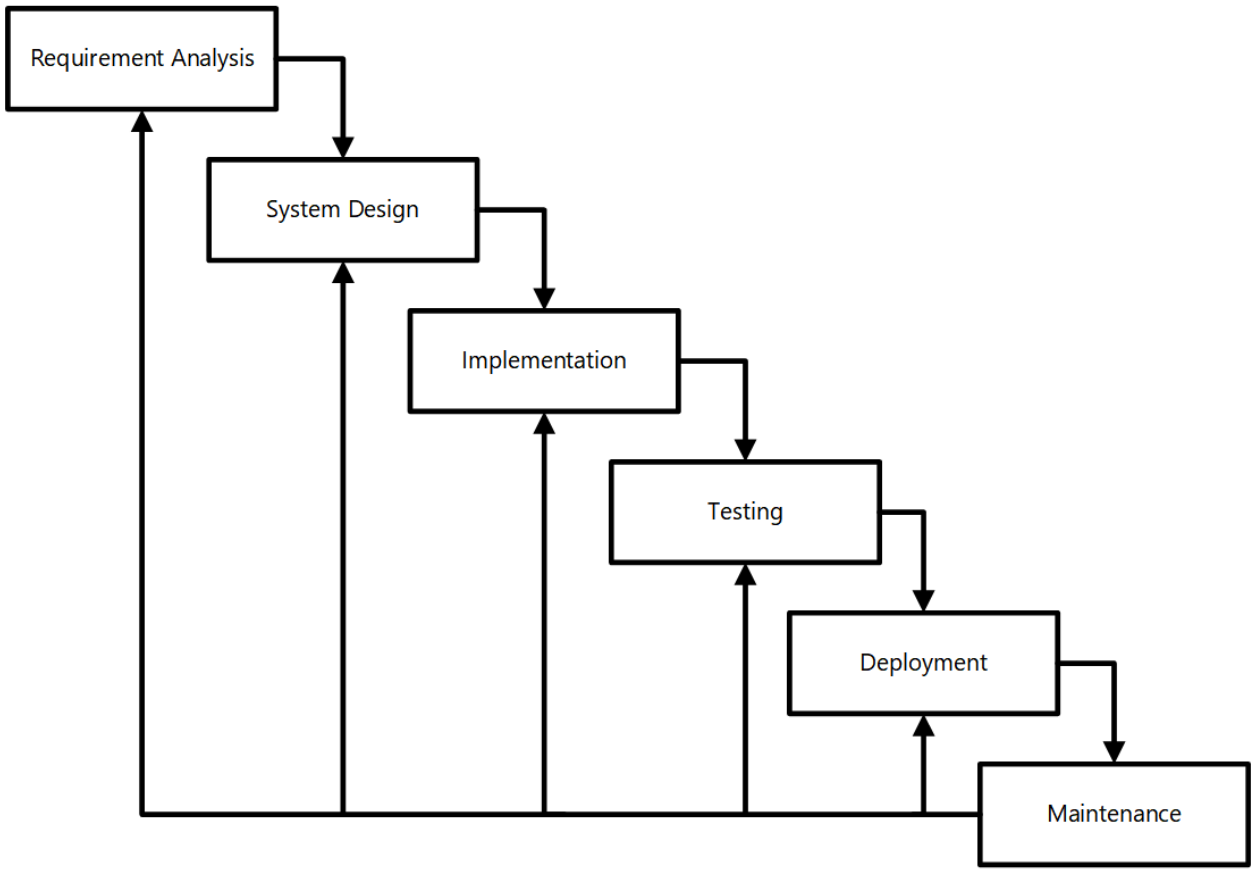

Figure 3.1 Sequential phases in waterfall model

3.2.1 Requirement Analysis

At this stage, all possible requirements of the system to be developed are captured in this phase and documented in a requirement specification document.

3.2.2 System Design

At this stage, the requirements specification are examined from the first stage and the design of the system is prepared. This incorporates the two essential elements which are the functional and non-functional requirements needed to make the framework functionalities particularly convincing and efficient in order to ensure that the customer's demands are fulfilled. The design of the system helps to define the requirements of the system as well as the overall system architecture.

3.2.3 Implementation

This stage involves the planning and writing code for the program. In this stage, the system is divided into smaller parts called units. Each unit is then designed and tested for its functionality. This is called unit testing.

3.2.4 Integration and Testing

After each unit is tested, all the units are then coupled together to produce a system. The whole system is then tested for flaws and failures.

3.2.5 Deployment

After the system has being tested as a whole, it is then released into the market as a product for use by customers.

3.2.6 Maintenance

As customers make use of the software product, issues will start to arise and they need to be addressed. In this stage, upkeep is done to make changes and offer courses of actions to various customer issues. In addition, upgrade of the system to better versions are done to improve the product.

3.3 Analysis of Existing System

In the current system, person identification is done using identity cards, pen and paper. The current system involves using pen and paper technique to keep records of stakeholders.

3.3.1 Problems of Existing System

After studying the existing system, the following problems where identified.

1. Data Loss: Paperwork is required to keep record of the entry and exit of stakeholders. This can cause data loss as the papers can be misplaced or damaged.
2. Time Wasting: The pen and paper method currently used is time consuming.
3. Error Prone: The current system is liable to have errors.

3.3.2. Proposed System

The Biometric Identification System is a web-based application where stakeholders will be able to enrol their fingerprint and also check in and check out of the gate. The characteristics of the proposed system are as follows.

i. The stakeholder enrols his/her fingerprint and biodata.
ii. The stakeholder is prompted to check in when coming in and sign out when leaving.
iii. To view the stakeholder's information, the administrator is responsible for that.

3.3.3. Advantages of the Proposed System

The suggested system has been associated with certain merits that enhance the system design. Some are described below:

i. It is bias-free (every user is served equally).
ii. It is faster.
iii. It is more efficient.
iv. It is more secure.

3.4. Application Requirements Analysis

This phase involved getting to know and understand what users need the system to do for them and also stipulate what the system needs so as to function properly and efficiently. It involved getting to know the functional and non-functional requirements of the system.

3.4.1 Functional Requirements

This is used to describe the precise functions or actions of the proposed system. The functional requirements for the system are as follows:

i. The system must have a page to capture biometric data of stakeholders.

ii. The system must have a page that displays the stakeholder's biodata. The stakeholder should then be able to sign in.

iii. The system should allow the administrator to have unlimited access to the database, generate reports and view stakeholder biodata.

3.4.2. Non-Functional Requirements

This described the app's behaviour as it relates to its functionality. It elaborates the performance characteristics of the app. Most of the non-functional requirements of the system was integrated at each level of the software developmental process. The major non-functional requirement that this work will address is performance and security.

3.4.3. Hardware Requirements

The section of hardware configuration is an important task related to any software development project because it states the physical devices needed to operate the biometric identification system. The hardware requirements are:

i. Processor: Intel Pentium and higher

ii. Processor Speed: 1.6GHz or higher

iii. RAM: 2GB or higher

iv. Hard Disk: 80GB or higher

v. Network Card: Any network card

vi. Network Connection: Must be present either in LAN or Wireless connection

3.4.4. Software Requirements

The required software specifications needed for the proposed system are:

i. An Operating System: Windows/Linux/MacOS

ii. A web browser such as Google Chrome, Mozilla Firefox, Opera Mini, UC Browser, etc.

3.5. Application architecture design and tools

Python: This project is developed on a Python framework called Django. Django is a Python Web high-level framework that promotes rapid development and smooth, pragmatic design. Built by experienced designers, it takes care of a lot of the web development issues, so you can concentrate on writing your app without having to reinvent the wheel. It is a free and open source framework.

Django's main objective is to ease the development of complicated, database-driven websites. The structure emphasizes reusability of components, less code, low coupling, rapid development and the idea that you do not repeat yourself. Python is used throughout, even for setting files and data models.

OpenCV: OpenCV (Open Source Computer Vision Library) is an open source computer vision and machine learning software library. OpenCV was built to provide a common infrastructure for computer vision applications and to accelerate the use of machine perception in the commercial products. It has C++, Python, Java and MATLAB interfaces and supports Windows, Linux, Android and Mac OS. It also runs on mobile operating systems like Android, iOS, Maemo, BlackBerry 10.

3.6. Module

The module's design phase may also be called a low-level design. The built system is broken up into smaller units or modules and clarified to each of them so that the programmer can start coding directly. The modules included in this project are as follows.

3.6.1 Administrator Module

In this module, the administrator manages both the user and admin modules. The admin view user information and can generate reports.

3.6.2 User Module

In this module, the stakeholder is able to register/enrol with the required details and also sign in and sign out using biometric means.

3.7. Flowchart of Biometrics Identification System

The flowchart depicts flow of control in program modules. The flowchart does not mention anything about how data flows through the system.

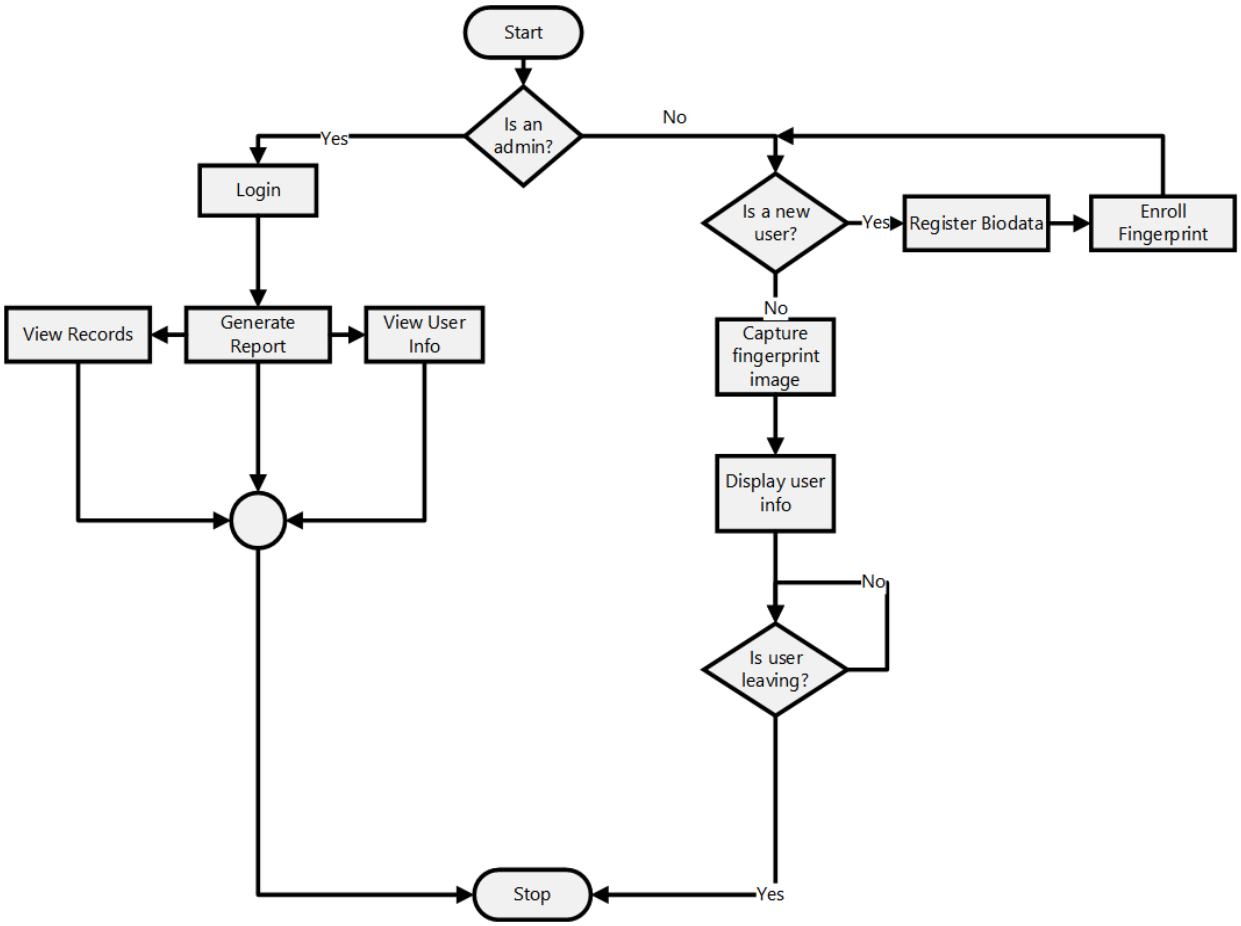

Figure 3.2 Flowchart diagram

3.8. Use Case Diagram for the Proposed System

The use case diagram explains the structual process regarding the different modules under the biometric identification system and also entails information of the roles of users in the system.

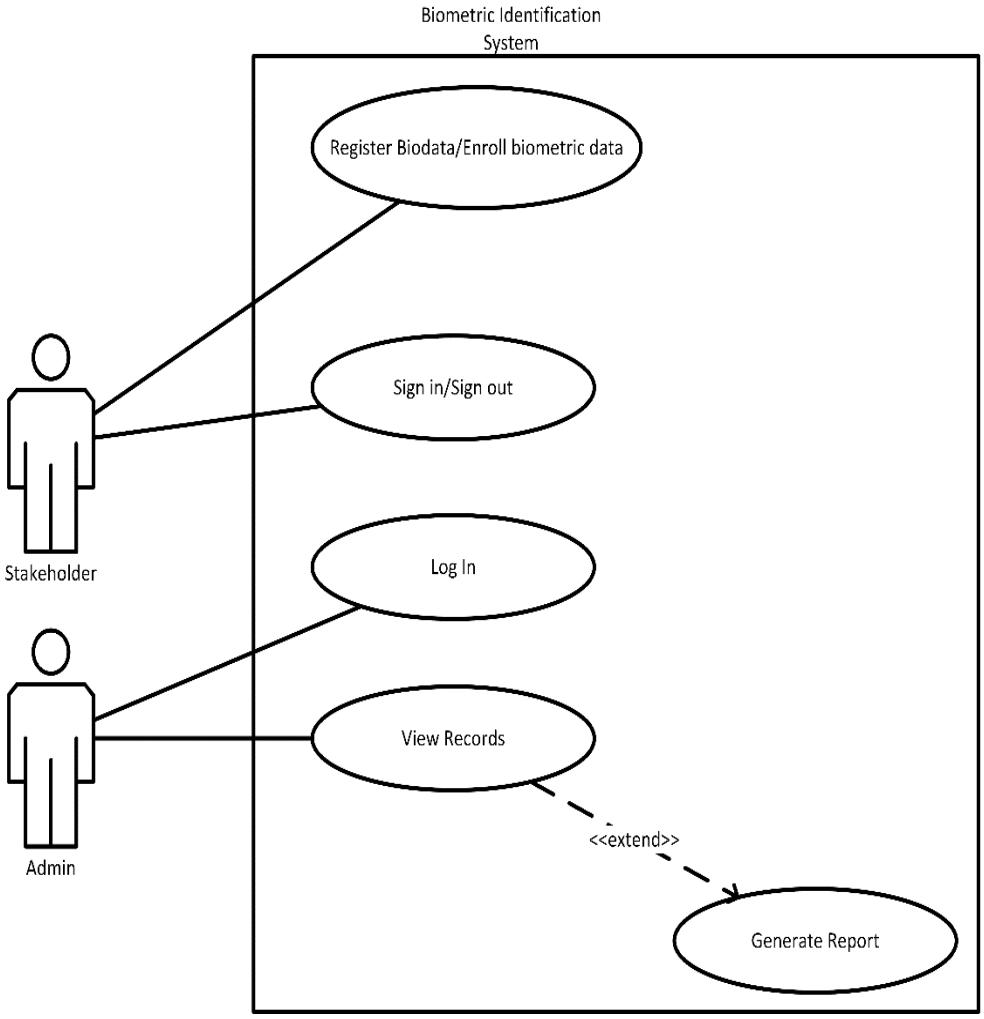

Figure 3.3 Use case diagram

3.9. Data Flow Diagram for the Proposed System

Data flow diagrams are used to graphically represent the flow of data in a business information system. The data flow diagram describes the processes that are involved in the Biometric Identification System to transfer data from the input to the file storage.

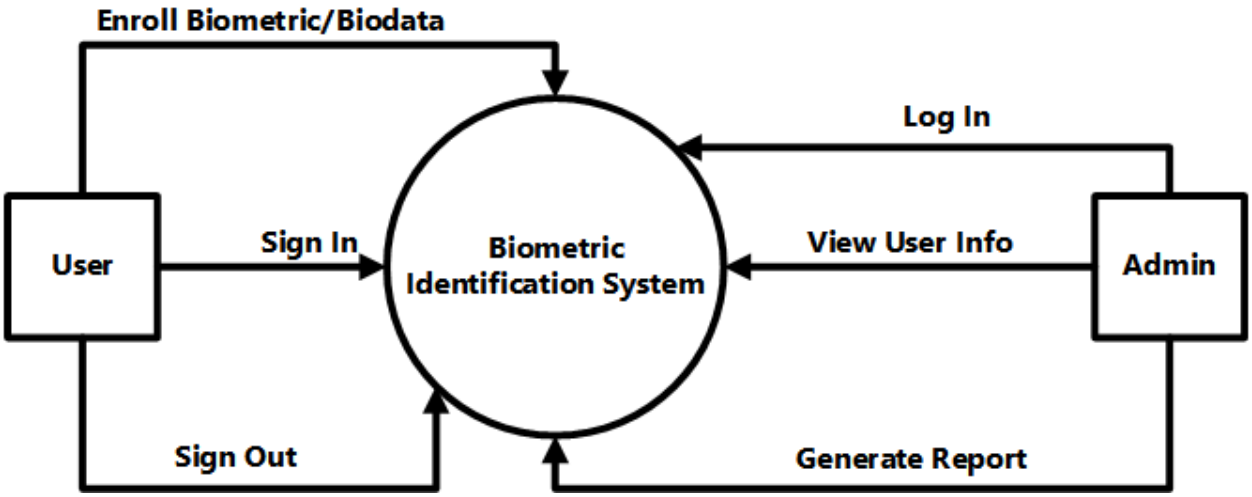

Figure 3.4 Data flow diagram

3.10. Entity Relationship Diagram

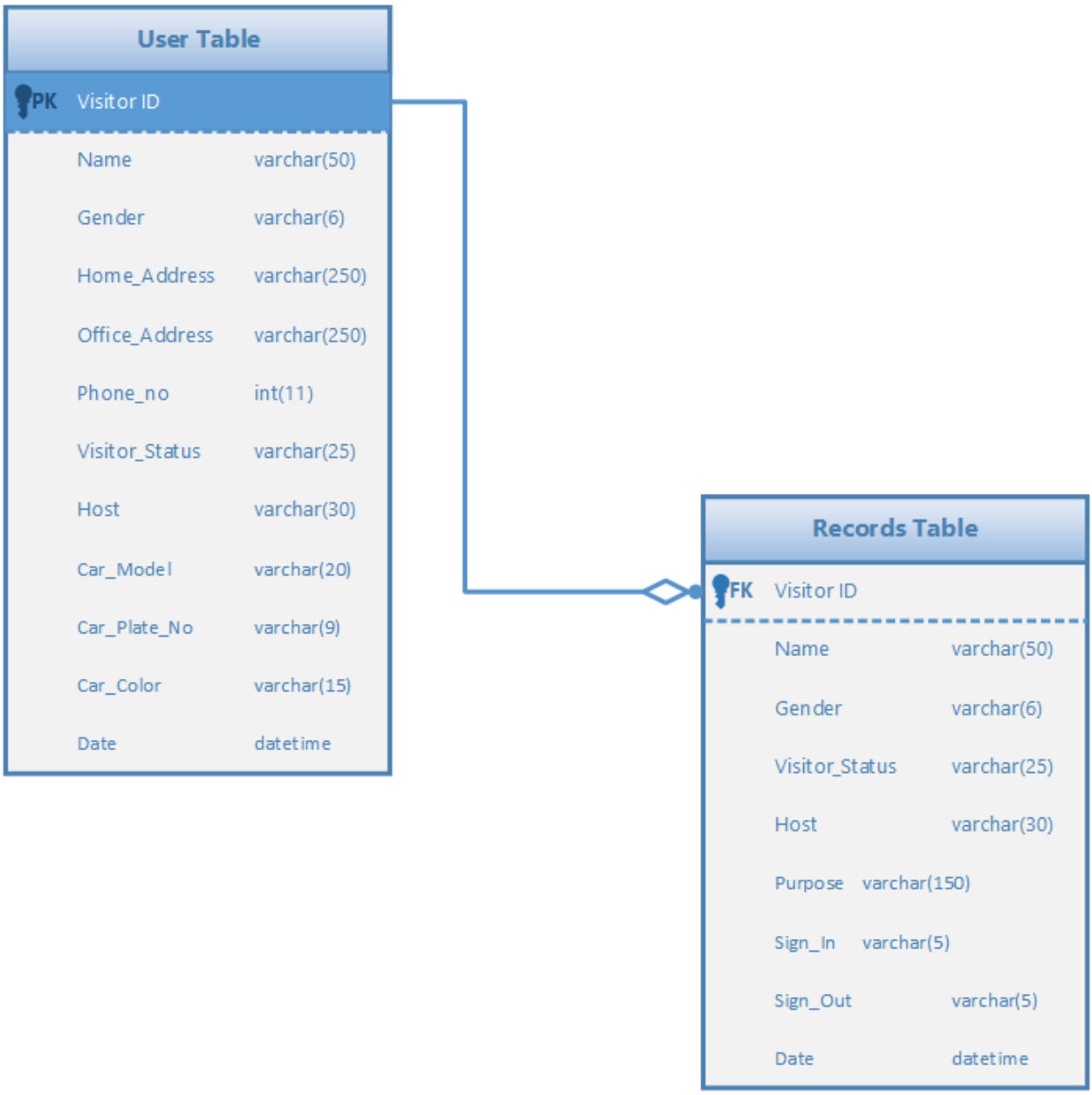

Figure 3.5 Entity relationship diagram

CHAPTER FOUR

RESULT AND RESULT DISCUSSION

4.1. Introduction

This chapter shows the result of the objectives mentioned. It demonstrates the information of implementing a biometric identification system. It also offers explicit description of how the proposed framework was designed and the underlying functionalities that define its makeup. The main aim of system design is to identify the modules in the system, and how the modules interact with each other.

4.2. System Testing

Testing is the process of executing a system to find errors. Without testing, hidden errors will surface after sometime of use and perhaps irreversible damage has been done to valuable data. Testing does not only discover errors made during coding, but also errors in the previous phase. The goal therefore of testing is to discover the requirements, design and coding errors. System testing follows the logical conclusion that all parts of the system are tested and found to be working properly under all kinds of situations and then the system is achieving the goal of processing the data perfectly according to user rules and requirements.

4.3. Database Design

In the database design, the entities have different attributes, data types and relationships which are defined based on the user requirements. The entities in the database design are:

i. User
ii. Admin
iii. Records

Column	Datatype
Visitor_ID	int(10)
Name	Varchar(60)
Gender	Varchar(6)
Home_address	Varchar(250)
Office_address	Varchar(250)
Phone_no	int(11)
Visitor_status	Varchar(25)
Host	Varchar(30)
Car_model	Varchar(15)
Car_color	Varchar(15)
Date	Datetime
Fingerprint	Varchar(100)

Table 4.1 User database design

Column	Datatype
Id	int PRIMARY KEY
Visitor_Id	int FOREIGN KEY
Name	Varchar(50)
Gender	Varchar(6)
Visitor_Status	Varchar(25)
Host	Varchar(30)
Purpose	Varchar(150)
Sign_In	Varchar(5)
Sign_Out	Varchar(5)
Date	Datetime

Table 4.2 Reports Database design

Column	**Datatype**
Username	Varchar(30)
Password	Varchar(50)

Table 4.3 Admin Database design

4.4.System Design

The system is only open to the admin as he/she operates the system for the user. The first page is the homepage which has options for registering new visitors, signing in and signing out.

4.4.1. Home Page

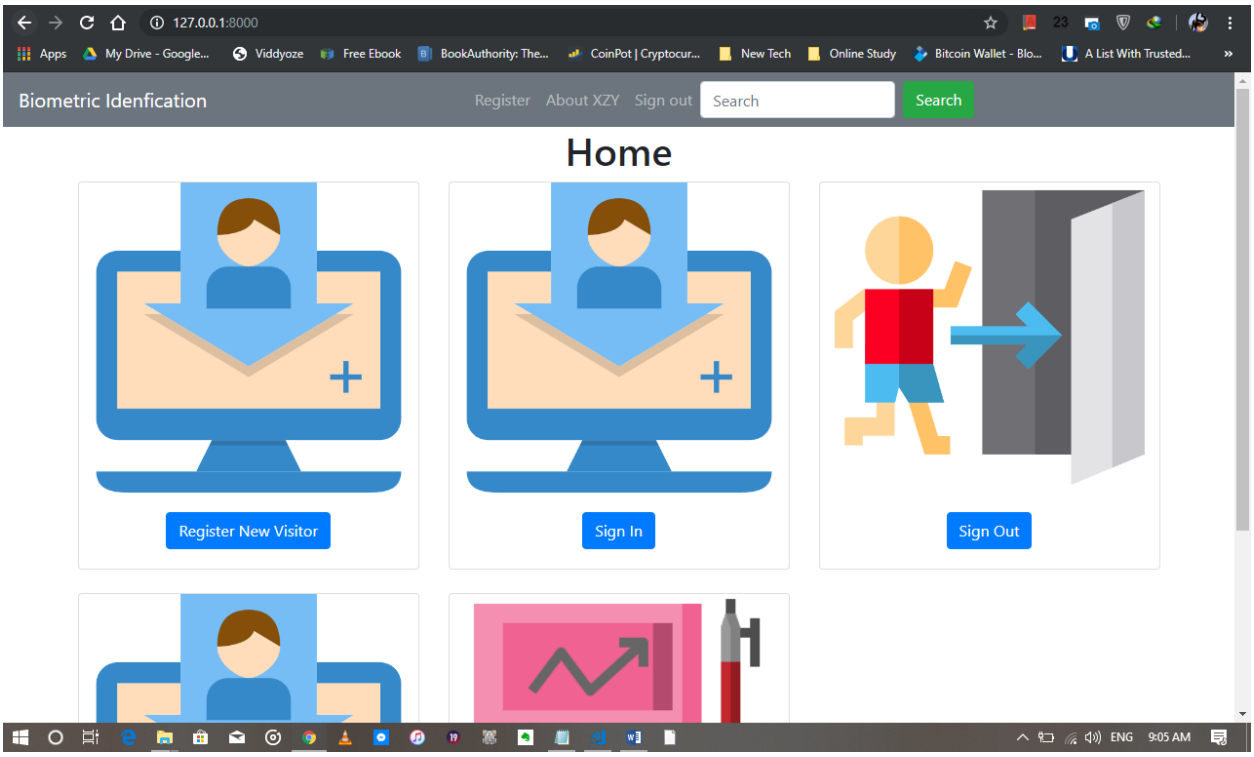

Figure 4.4 Home page design

Figure 4.4 above describes the home page which is the first page the system user sees when he/she accesses the system. It has access to different functionalities like registration of new visitors, signing in and signing out.

4.4.2. Registration

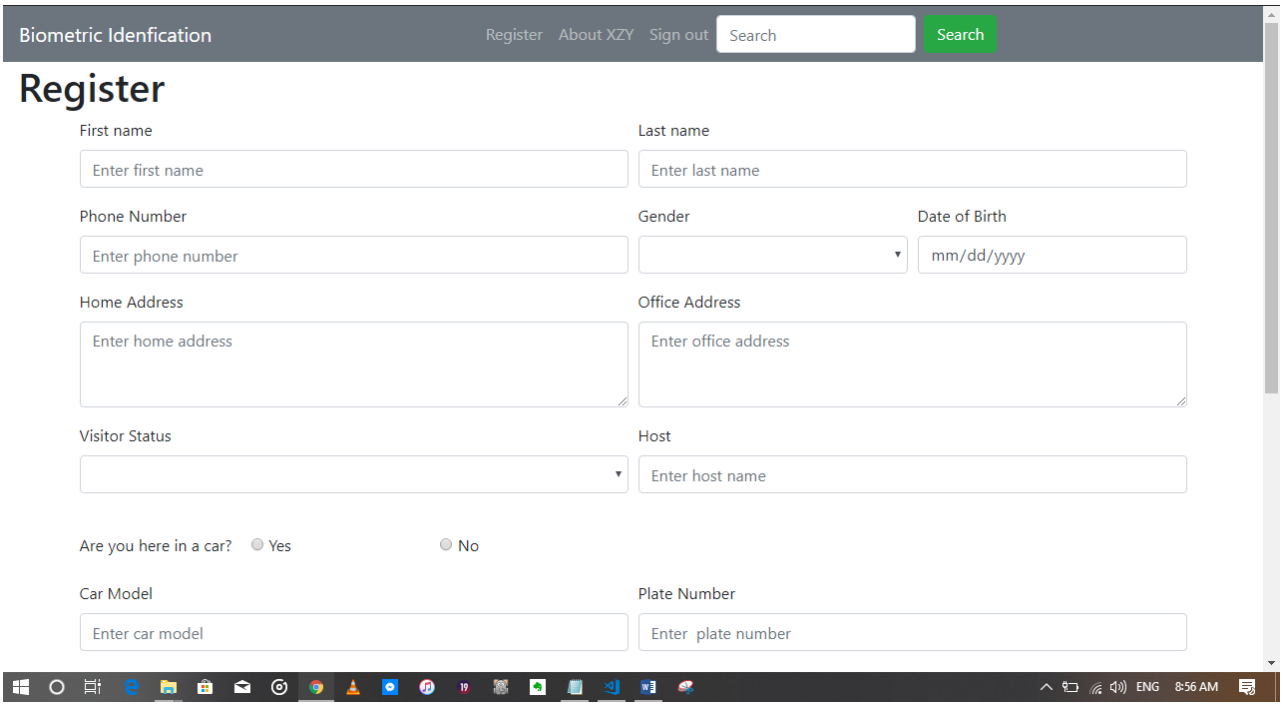

Figure 4.5 Register page

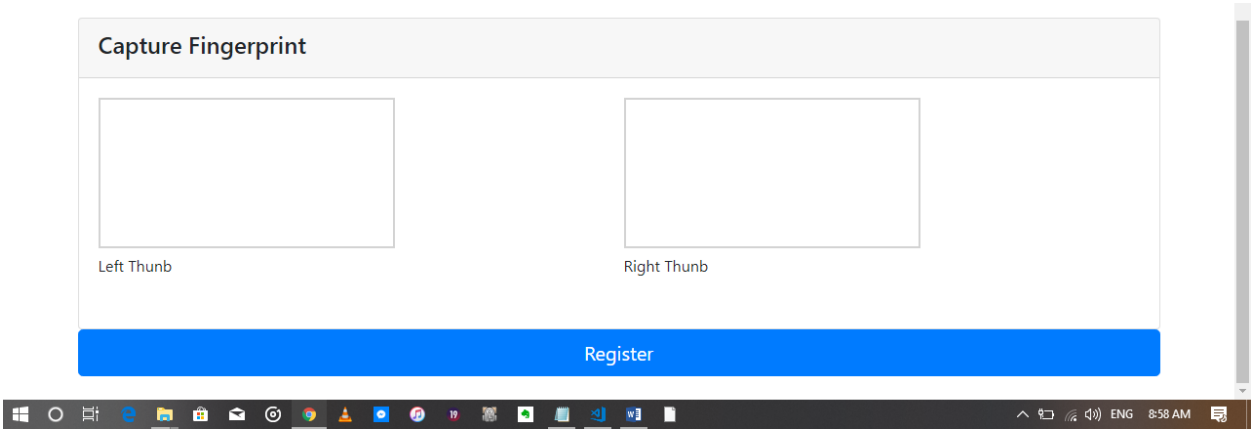

Figure 4.6 Biometric field on registration page

Figure 4.5 above describes the registration page where a new visitor/stakeholder registers his/her biodata and fingerprint image. The registration page also has a biometric field for capturing biometric data which in this case is the fingerprint image.

4.4.3. Sign In

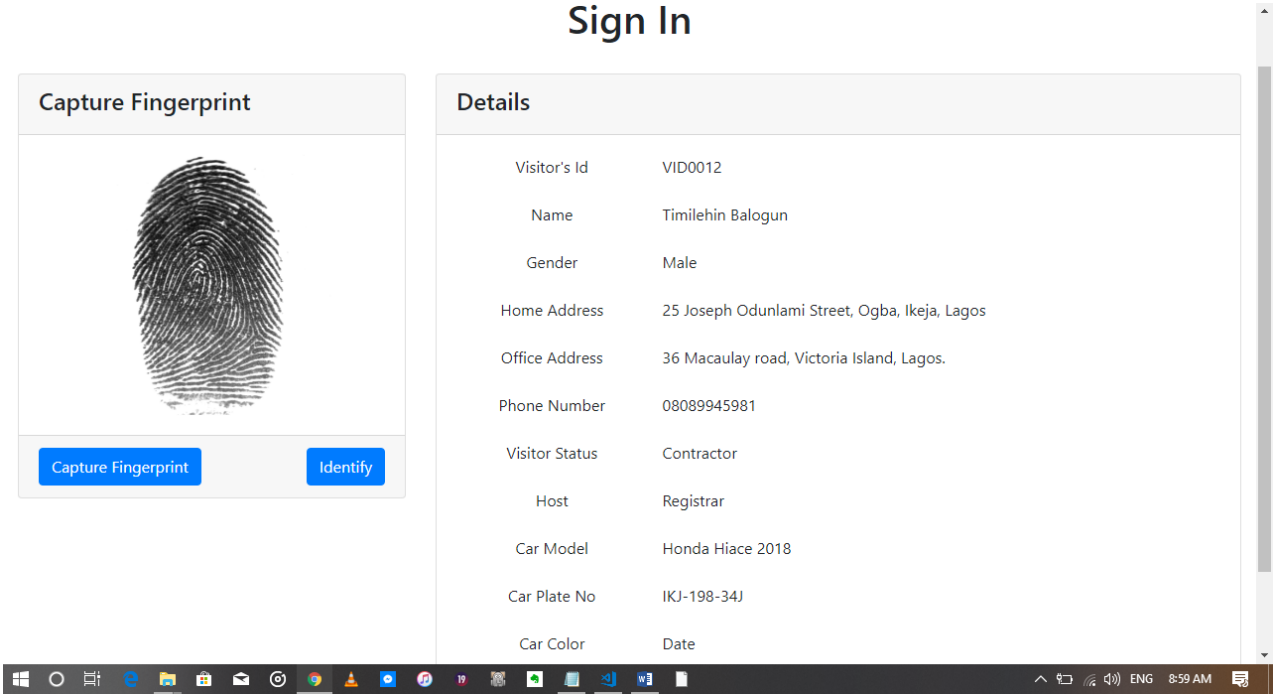

Figure 4.7 Sign in page design

This is where the stakeholder signs in at the entry point of the premises. The sign in is done by capturing the biometric trait (fingerprint image).

4.4.4. Sign out

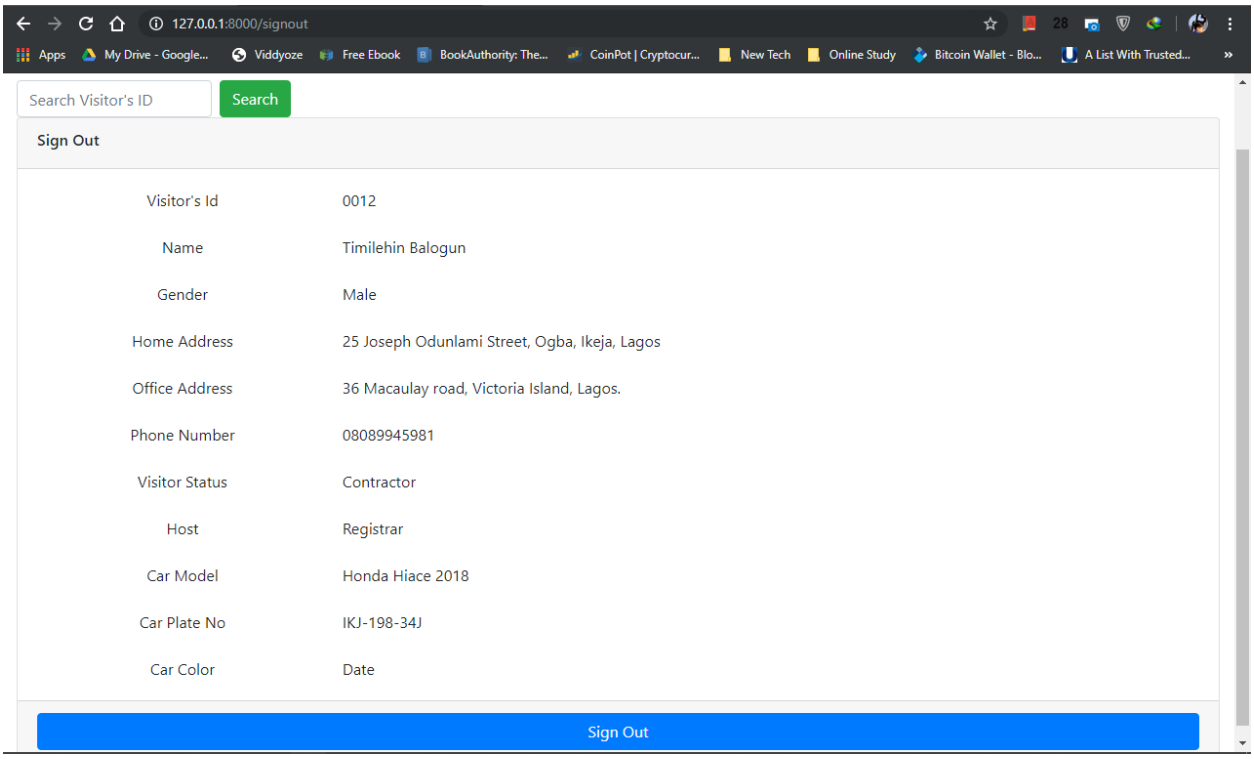

Figure 4.8 Sign out page design

Figure 4.8 above describes the sign out page where the visitor/stakeholder signs out when he/she is leaving the premises.

CHAPTER FIVE
SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary

Recent advancements in information technology has made identification of individual easier and enhanced security in both private and public sectors. Presently, there are several biometric security systems that use different human biometric characteristics for identification. Examples include fingerprint, signature, face, hand, voice, iris, etc. Out of these, fingerprint is more frequently used because of its high uniqueness and ease of capturing.

Having analysed the current traditional method of identifying individuals and keeping records at entry points in Mountain Top University, a web based biometric identification system has been designed to improve the effectiveness and efficiency. The proposed system eliminates paperwork involved in the existing system.

5.2 Conclusion

Biometrics is an automatic method of identifying an individual based on one or more physiological or behavioural characteristics. Biometric identification provides an opportunity for a more secure and responsible environment. It also provide a better solution for the increased security requirement of the society than the traditional means of identification.

In conclusion, this study has proposed a biometric system to aid identification of persons at entry points through the use of fingerprint. The biometric identification system eliminates the need for identity cards and other documents for identification. The biometric system improves the manual means of identification thereby bolstering security at entry points.

5.3 Recommendation

It is recommended that the Mountain Top University make use of this biometric identification system. The system will reduce the errors encountered, and the manual process involved in the activities and also, to increase operation speed. I encounter the university to try and encourage the students and staff to carry out further research in the development of biometrics identification systems. Upgrade approach of technology should be recognized, acknowledged and accepted since the society resides in a University of Technology.

REFERENCES

Afsar, F., Arif, M., & Hussain, M. (2004). Fingerprint Identification and Verification System using Minutiae Matching. *National Conference on Emerging Technologies,* (pp. 141-146).

Asha, S., & Chellappan, C. (2012). Biometrics: An Overview of the Technology, Issues and Applications. *International Journal of Computer Applications, 39*(10), 35.

Babich, A. (2012). *Biometric Authentication. Types of biometric identifiers.* Bachelor's Thesis, HAAGA-HELIA University of Applied Sciences.

Bansal, R., Sehgal, P., & Bedi, P. (2011). Minutiae Extraction from Fingerprint Images - a Review. *International Journal of Computer Science Issues,* 74 - 85.

Bansal, R., Sehgal, P., & Bedi, P. (2011, September). Minutiae Extraction from Fingerprint Images - A Review. *International Journal of Computer Science Issues (IJCSI), 8*(5), 74-85.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009, September). Biometric Authentication: A Review. *International Journal of Science and Technology, 2*(3).

Bhowmik, P., Bhowmik, K., Azam, M. N., & Rony, M. W. (2012, June). Fingerprint Image Enhancement and its Feature Extraction for Recognition. *International Journal of Scientific & TTechnology Research, 1*(5), 117-121.

Chaudhari, R. D., Pawar, A. A., & Deore, R. S. (2013). The Historical Development Of Biometric Authentication Techniques: A Recent Overview. *International Journal of Engineering Research & Technology (IJERT), 2*(10).

Chinedum, D. A. (2017). Design and Implementation of a Biometric Informatiion System. *International Journal of Scientific Research and Innovative Technology, 4*(2).

Down, M. P., & Sands, R. J. (2004). Biometrics: An Overview of the Technology, Challenges and Control Considerations. *Information Systems Control Journal, 4.*

Fronthaler, H., kollreider, K., & Bigun, J. (2008). Local Features for Enhancement and Minutiae Extraction in Fingerprints. *IEEE Transactions on Image Processing, 17*(3), 354-363.

Gour, B., Bandopadhyaya, T. K., & Sharma, S. (2008). Fingerprint Feature Extraction using Midpoint Ridge Contour Method and Neural Network. *International Journal of Computer Science and Network Security, 8*, 99-109.

Gu, J., Zhou, J., & Yang, C. (2006). Fingerprint Recognition by Combining Global Structure and Local Cues. *IEEE Transactions on Image Processing, 15*, 1952 – 1964.

Hasan, H., & Abdul-Kareem, S. (2013). Fingerprint image enhancement and recognition algorithms: A Survey. *Neural Comput & Applic*. doi:10.1007/s00521-012-1113-0

Hastings, R. (2007). Ridge Enhancement in Fingerprint Images Using Oriented Diffusion. *IEEE Computer Society on Digital Image Computing Techniques and Applications*, 245-252.

Hong, L., Wan, Y., & Jain, A. (1998). Fingerprint image enhancement: algorithm and performance evaluation. *IEEE Trans Pattern Anal Mach Intell, 20*(8), 777–789.

Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric Template Security. *EURASIP Journal on Advances in Signal Processing*. doi:doi:10.1155/2008/579416

Jain, A. K., Pankanti, S., Prabhakar, S., Hong, L., Ross, A., & Wayman, J. L. (2004). Biometrics: A Grand Challenge. *Proceedings of International Conference on Pattern Recognition.* Cambridge, UK.

Jain, A., Hong, L., Pankanti, S., & Bolle, R. (1997). An Identity authentication system using fingerprints. *Proc IEEE, 85*(9), 1365–1388.

Jean, C. (2002, October). *In Heilbrum Timeline of Art History*. Retrieved from The Metropolitan: http://www.metmuseum.org/toah/hd/chav/hd_chav.html

Kaur, J., & Garg, U. (2015). New Approach to Fake Minutia Removal based Fingerprint Identification Technique. *International Journal for Scientific Research & Development, 3*(9), 751-769.

Kindt, E. (2013). *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, Law, Governance and Technology.* Springer. doi:DOI 10.1007/978-94-007-7522-0_2

Kresimir, D., & Mislav, G. (2004). A Survey of Biometric Recognition Methods. *46th International Symposium Electronics in Marine, ELMAR-2004*, (pp. 184-193). Zadar, Croatia.

Lumini, A., & Nann, L. (2008). Advanced Methods for Two-Class Pattern Recognition Problem Formulation for Minutiae-Based Fingerprint Verification. *Journal of the Pattern Recognition Letters, 29*, 142-148.

Maguire, M. (2009, April). The Birth of Biometric Security. *ANTHROPOLOGY TODAY, 25*(2), 9-15.

Maio, D., & Maltoni, D. (1990). *Quantitative-qualitative firiction ridge analysis: an introduction to basic and advanced Ridgeology.* Boca Raton: CRC Press.

Marcos Faundez-Zanuy. (2006, June). Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine, 22*(6), 15-26.

Nath, D., Ray, S., & Ghosh, S. K. (2011, January). Fingerprint Recognition System : Design & Analysis.

National Biometric Security Project. (2008). *Biometric Technology Application Manual Volume One: Biometric Basics*.

Prasad, R. S., Al-Ani, M. S., & Nejres, M. S. (2015, April). An Efficient Approach for Fingerprint Recognition. *International Journal of Engineering Innovation & Research, 4*(2), 307-313.

Rao, G., NagaRaju, C., Reddy, L. S., & Prasad, E. V. (2008). A Novel Fingerprints Identification System Based on the Edge Detection. *International Journal of Computer Science and Network Security*, 394-397.

Sagar, V., Ngo, D., & Foo, K. (1995). Feature selection for fingerprint identification. 1995.

Sen, W., Weiwei, Z., & Yangsheng, W. (2002). *Features extraction and application in fingerprint segmentation.* Beijing, China: National Laboratory of Pattern Recognition, Chinese Academy of Sciences.

Singh, R., Shah, U., & Gupta, V. (n.d.). *Fingerprint Recognition.* Indian Institute of technology, Kanpur, Department of Computer Science & engineering.

Sojan, S., & Kulkarni, R. K. (2016, July). Fingerprint Image Enhancement and Extraction of Minutiae and Orientation. *International Journal of Computer Applications, 145,* 13 - 19.

Tabassum, M. (2013). A New Method for Biometric Based Recognition. *International Journal of Scientific and Research Publications, 3*(9).

Thakkar, D. (n.d.). *Minutiae Based Extraction in Fingerprint Recognition*. Retrieved 8 4, 2019, from Bayometric: https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition/

APPENDICES

```
from django.http import HttpResponse

from django.shortcuts import render

import datetime


# Create your views here.



def index(request):

    # return HttpResponse("Hello, world!")

    return render(request, "home/index.html")


def register(request):

    date = datetime.datetime.now()

    return render(request, "home/register.html")


def signin(request):

    date = datetime.datetime.now()

    return render(request, "home/signin.html")


def signout(request):

    date = datetime.datetime.now()
```

```
    return render(request, "home/signout.html")



from django.urls import path


from .import views


urlpatterns = [
    path('', views.index, name = 'home'),
    path('register', views.register, name = 'register'),
    path('signin', views.signin, name = 'signin'),
    path('signout', views.signout, name = 'signout')
]



from django.db import models


# Create your models here.
class Register(models.Model):
    vid = models.AutoField(db_column = 'VID', primary_key = True)
    name = models.CharField(db_column = 'Full Name', max_length = 50)
    sex = models.CharField(db_column = 'Gender', max_length = 6)
    home_address = models.CharField(db_column = 'Home Address', max_length = 250)
```

```
    office_address = models.CharField(db_column = 'Office Address', max_length = 250)
    phone_number = models.IntegerField(db_column = 'Phone No')
    visitor_status = models.CharField(db_column = 'Visitor Status', max_length = 25)
    car_model = models.CharField(db_column = 'Car Model', max_length = 15)
    car_plate_no = models.CharField(db_column = 'Car Plate No', max_length = 9)
    car_color = models.CharField(db_column = 'Car Color', max_length = 15)
    date = models.DateTimeField(db_column = 'Date')

    def __str__(self):
        return f"{self.vid} registered"

class Records(models.Model):
    vid = models.IntegerField(db_column = 'VID')
    name = models.CharField(db_column = 'Full Name', max_length = 50)
    sex = models.CharField(db_column = 'Gender', max_length = 6)
    visitor_status = models.CharField(db_column = 'Visitor Status', max_length = 25)
    host = models.CharField(db_column = 'Host', max_length = 30)
    purpose = models.CharField(db_column = 'Purpose', max_length = 150)
    signin = models.TimeField(db_column = 'Sign In')
    signout = models.TimeField(db_column = 'Sign Out')
    date = models.DateField(db_column = 'Date')

    def __str__(self):
```

```
        return f"{self.vid} came {self.signin} and left {self.signout}"
```

```
{% load static %}

<!DOCTYPE html>
<html>

<head>
  <title>
    {% block title %}{% endblock %}
  </title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <!--Bootstrap CSS-->
  <link rel="stylesheet" href="{% static 'home/bootstrap-4.3.1/css/bootstrap.min.css' %}">
  <link rel="stylesheet" href="{% static 'home/css/sb-admin.css' %}">
  <link rel="stylesheet" href="{% static 'home/css/sb-admin.min.css' %}">

  <!--JQuery-->
  <script href="{% static 'home/js/jquery.min.js' %}"></script>
  <!--Bootstrap JS-->
  <script href="{% static 'home/bootstrap/js/bootstrap.min.js' %}"></script>
```

```
  <script href="{% static 'home/bootstrap-4.3.1/js/bootstrap.js' %}"></script>
  <script href="{% static 'home/bootstrap-4.3.1/js/bootstrap.min.js' %}"></script>
  <script href="{% static 'home/js/popper.min.js' %}"></script>
</head>

<body>
  <nav class="navbar navbar-expand-sm bg-secondary navbar-dark">
    <a class="navbar-brand" href="#">Biometric Idenfication</a>
    <button class="navbar-toggler" type="button" data-toggle="collapse" data-
target="#collapsibleNavbar">
      <span class="navbar-toggler-icon"></span>
    </button>
    <div class="collapse navbar-collapse justify-content-center" id="collapsibleNavbar">
      <ul class="navbar-nav">
        <li class="nav-item">
          <a class="nav-link" href="#">Register</a>
        </li>
        <li class="nav-item">
          <a class="nav-link" href="#">About XZY</a>
        </li>
        <li class="nav-item">
          <a class="nav-link" href="#">Sign out</a>
        </li>
```

```
      </ul>
      <form class="form-inline my-2 my-lg-0">
        <input class="form-control mr-sm-2" type="text" placeholder="Search">
        <button class="btn btn-success my-2 my-sm-0" type="button">Search</button>
      </form>

    </div>
  </nav>
  <div class="container-fluid">
    {% block body %}{% endblock %}
  </div>
</body>

</html>
```

```
{% extends "home/base.html" %}
{% block title %}
  Home
{% endblock %}
{% block body %}
  <h1><center><span class="label label-primary label-lg">Home</span></center></h1>
  <div class="container">
```

```
<div class="card-deck">
  <div class="card col-md-4">
    <img class="card-img-top" src="../../static/home/icons/png/registration.png" alt="Card image" style="width:100%">
    <div class="card-body text-center">
      <a href="{% url 'register' %}" class="btn btn-primary ">Register New Visitor</a>
    </div>
  </div>
  <div class="card col-md-4">
    <img class="card-img-top" src="../../static/home/icons/png/registration.png" alt="Card image" style="width:100%">
    <div class="card-body text-center">
      <a href="{% url 'signin' %}" class="btn btn-primary ">Sign In</a>
    </div>
  </div>
  <div class="card col-md-4">
    <img class="card-img-top" src="../../static/home/icons/png/001-exit.png" alt="Card image" style="width:100%">
    <div class="card-body text-center">
      <a href="# " class="btn btn-primary ">Sign Out</a>
    </div>
  </div>
</div>
```

```
    <br>
    <div class="card-deck">
      <div class="card col-md-4">
        <img class="card-img-top" src="../../static/home/icons/png/registration.png" alt="Card image" style="width:100%">
        <div class="card-body text-center">
          <a href="# " class="btn btn-primary ">View Visitor Info</a>
        </div>
      </div>
      <div class="card col-md-4">
        <img class="card-img-top" src="../../static/home/icons/png/report.png" alt="Card image" style="width:100%">
        <div class="card-body text-center">
          <a href="# " class="btn btn-primary ">Generate Report</a>
        </div>
      </div>
      <div class="col-md-4 col-offset-4"></div>
    </div>
  </div>
{% endblock %}
```