A FRAMEWORK FOR NATION-WIDE INTEGRATION OF BIOMETRIC INFORMATION

A Thesis Presented to the Department of

Computer Science

African University of Science and Technology

In Partial Fulfilment of the Requirements for the Degree of

MASTER of Computer Science

By

BELLO, Habibah Onyioyibo

Abuja, Nigeria

December 2017.

CERTIFICATION

This is to certify that the thesis titled “A Framework for Nation-wide Integration of Biometric Information” submitted to the school of postgraduate studies, African University of Science and Technology (AUST) Abuja, Nigeria for the award of the Master's degree is a record of original research carried out by Bello Habibah Onyioyibo in the Department of Computer Science.

FRAMEWORK FOR NATION-WIDE INTEGRATION OF BIOMETRIC INFORMATION

By

BELLO, Habibah Onyioyibo

A THESIS APPROVED BY THE COMPUTER SCIENCE DEPARTMENT

RECOMMENDED: _____

Supervisor, Dr. Onifade F.W. Olufade

_____

Co-supervisor

_____

Head, Department of Computer Science

APPROVED: _____

Chief Academic Officer

December 9th, 2017

ABSTRACT

Having a central database for Nigeria which organizations can rely on for identification/verification purposes has been a plan in the pipeline for many years now. This has become urgent because of the nation's current security challenges and the problem of multiple enrolments across various organizations. All of these organizations collect data, but the data collected is not useful outside the collecting organizations.

According to various reports, the Nigerian government has been trying to create a central database to contain Nigerian nationals' basic information and biometric information as well, to be managed by the Nigerian Identity Management Commission (NIMC), but to no avail. The project 'National Identity Database' creation was started in 2007 and to date has not yet been successful.

This thesis aims to create a central platform for integration of all of these biometric data in order to curb these problems while considering security of access control. In this work, we have created four different web applications and databases, to represent information of four different organizations; Nigerian Immigration System, Independent National Electoral Commission, Bank, NIMC, with NIMC serving as the central point. The data represented includes basic information and biometric information (fingerprints) of their enrolees. The web applications where designed using C#.net on visual studio IDE alongside other supporting software like MySQL connector, Adobe Fireworks and database access with PhpMyAdmin. Each application includes four modules, enrolment, admin, query and verification module. The verification module serves as the platform where different organizations' applications can interface to the central database, giving the opportunity to identify individuals from any point.

The overall system developed provides a platform for this, in order to curb multiple and indiscriminate collection of biometric (fingerprint) data which is a major challenge in the country at present.

Keywords: Biometric, Central database, Fingerprint, Verification and Identification

ACKNOWLEDGEMENTS

All praises are due to almighty Allaah, the Lord of the universe, the Omniscient, for giving me the knowledge and understanding to carry out this work.

My thanks and prayers will never cease for my parents, Alh. & Haj. M. I. Bello, for their support in every possible way and for encouraging me all through the MSc program. My appreciation goes to the management of AUST and the African Capacity Building Foundation for granting me a scholarship to pursue my MSc program in this prestigious school. My appreciation also goes to the HOD Computer Science department, Prof. Amos David for his profound leadership. I am specifically indebted to my supervisor, Dr. Onifade F.W. Olufade who guided and supported me every step of the way and from whom I learnt the art of research. To my dearest siblings, my cute nephews and my lovely aunty, mummy Agasa, you all are the best. Thank you for the support and encouragement.

Lastly but not exhaustively, my appreciation also goes to all my friends, classmates and the staff of RFID. Thank you for your contributions and encouragement.

DEDICATION

To my parents Alh & Haj. M. I. Bello, my greatest support system.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

BVN	Bank Verification Number
CBN	Central Bank of Nigeria
DBMS	Database Management System
DNA	Deoxyribonucleic Acid
EURODAC	European Dactyloscopy
IAFIS	Integrated automatic fingerprint identification system
INEC	Independent Electoral Commission
NDNAD	National Deoxyribonucleic Acid Database
NID	National Identity Database
NIMC	National Identity Management Commission
NIS	Nigerian Immigration Service

CHAPTER 1
INTRODUCTION

1.a Background to Biometrics

The adoption of biometrics can still be considered as not being a popular technology in developing nations. However, various practices have shown the use of physical characteristics for identification purposes have been in use since ancient times. For example, in ancient Babylon, Assyria, China and Japan, fingerprints were used to sign contracts (Taha & Norrozila, 2015). In the 1890s Alphonse Bertillon a Paris police clerk, who was also an anthropologist, developed a method of multiple body measurements called Bertillonage. He based this method on a claim that bones do not grow after age 20, so measurements of anyone after that age should remain the same. As a result, a 20-60 minute-long measuring procedure was done to identify criminals. The records of length, height, breath of heads, fingers, arms and leg were done by hand and filed. It was relatively fast and effective method for that time His system was used by police authorities until it failed because some people shared the same measures ("The German Biometric Strategy Platform Biometrics State of the Art, Industry Strategy Development, and Platform Conception Study," 2009.). It was a relatively fast and effective method for that time, until two different people had the same measurements. Paris police switched to fingerprinting, which soon became widespread and Bertillonage was forgotten. Today different biometric technologies are widely employed in criminal prosecution, identity management and police records. In the 1960s, research on computer-based, automated recognition started, and the first commercial use, a fingerprint application, took place in 1968 (Dessimoz & Champod, 2008).

Biometrics is a developing area of technology, which seeks to uniquely identify, verify or authenticate persons based on certain features in the human body, which are distinct across individuals. These features refer to physiological and behavioural traits possessed which are unique in nature (Sapkal & Deshmukh, 2016). Due to the inaccuracies of conventional methods of identification such as pins or passwords (Mahfouz, Mahmoud, & Eldin, 2017), biometric technologies are now being widely adopted as a better replacement for identification in organizations, government agencies etc. (Sapkal & Deshmukh, 2016).

Biometrics are more appealing because they are closely bound to an individual and are supposedly more reliable, difficult to forge, lose or falsify.

Government and authorities seek enhanced security solutions to protect borders, issue secure identification documents and monitor public places (Breedt & Martin, 2004), thus in recent times there have been massive efforts by nations to adopt biometrics in identifying their citizens. Many countries have national identification systems based on databases containing some biometric information of its nationals. Examples are India (AADHAR), United States (FBI IAFIS), UK (NDNAD), the EU (EURODAC).

Biometrics generally refers to a wide range of traits: iris, hand, gaits, fingerprint, face DNA, keystroke, voice etc. However, in the literatures, fingerprints are seen as one of the best traits to be used because of the high level of structural differences from person to person (De Luis-García, Alberola-López, Aghzout, & Ruiz-Alzola, 2003). Thus, it is most widely adopted because it is a mature and affordable technology.

Following from the above, we have decided to adopt the fingerprint as our main biometric trait for use as the biometric trait in our platform for the central database.

1.b State of National Security in Nigeria

Recent years have been characterized by a more stringent requirement for people to be identifiable in response to security threats and to combat the escalating problems of identity theft. This increasing need to determine who an individual is has resulted in substantial growth in the implementation and use of biometric applications (The Irish Council for Bioethics, 2009).

Many countries, both developed and developing nations, have been victims of security issues. Nigeria is no exception. In recent years, the nation has been in the midst of many security problems stemming from the infamous group Boko Haram; not only that, the country is also dealing with the problem of high crime rates in other aspects, including armed robbery, kidnapping, ritual killings, corruption etc. Many of these crimes

remain unsolved due to lack of concrete evidence to pin the actual perpetuator to the crime. This is despite the fact that various Nigerian organizations have biometric information on Nigerian nationals which can be useful in solving some criminal problems as needed; however, the data is scattered across different organizations, lying idle and not being used to their full potential.

According to a publication from the INEC, through the 2015 general elections registration exercise alone, it collected the biometric details of about 68 million Nigerians (The Scoop, 2015), which includes 10 fingerprints images, facial image and bio-data. In addition, various commercial banks at the instance of the CBN, through the BVN exercise have also gathered millions of items of biometric information from Nigerians. According to statistics from the Nigeria Inter-Bank Settlement System Plc, NIBSS, show that about 20,833,635 bank customers registered for the BVN (Udo, 2015).

The Nigeria Communications Commission (NCC) requires that every single active mobile telephone number have an individual's biometric data registered to it. According to NCC statistics, there were more than 145 million active mobile phone lines in Nigeria as at June 2015 (Bolade, 2015).

If all these biometrics are integrated into a whole as a centralized database while excluding redundancy, then they can be put to use in solving some of the security concerns and criminal problems of Nigeria.

1.c Aim and Objectives

The aim of this research work is to develop a framework for nation-wide integration of biometric information.

The following objectives combine to achieve the aim:

1. To develop a platform that can serve as a wrapper for biometric data captured;
2. To develop a centralized database system of biometric information of Nigerian nationals; and
3. To integrate security control of access to system.

1.d Scope and Limitation

The framework developed from this study is meant for unimodal biometric system, as it will only cover fingerprints because of their uniqueness, availability and ease of collection. According to (Edgar, 2006), of

all the methods of identification, fingerprinting alone has proved to be both infallible and feasible. Its superiority over the older methods, such as branding, tattooing, distinctive clothing, photography and body measurements (Bertillon system), has been demonstrated time after time. While many cases of mistaken identification have occurred with these older systems, to date the fingerprints of no two individuals have been found to be identical. This model does not provide a framework for policies to regulate its use. I assume that such a system will be regulated and deployed by corresponding government agencies in charge. Theft and social engineering methods of unauthorized access are not considered.

The framework shall also consider some of the soft biometric traits, it will include:

- Age;
- Gender; and
- Ethnicity.

This study does not, however, cater for other numerous biometric such as hand geometry, iris scan, due to its unavailability in other organizations' databases and unused nature in this part of the world.

1.e Significance of the Study

The significance of this study should be felt in various sectors of the country, including the judicial sectors, military, health care sector and others, but most importantly, it would be significant in the area of national security. The framework could serve as a platform for government and authorities to seek for enhanced security solutions to protect borders, issue secure ID documents, monitor public places and combat terrorism.

Some specific applications include adoption in:

- Identification documents and border control;
- Criminal prevention and prosecution;
- Identifying known or suspected criminals; and
- Control of illegal immigration.

1.f Justification of Study

According to (Rotimi, Francis, Adebayo, & Owolabi, 2013) “a national database is an organized data or numerical environment where every citizen of a nation and the immigrants are uniquely identified and possesses a strong national virtual identity. National database may be population, identity, security, electorate, group or association’s classified information or data of national interest”. The national identity will help to deter people using multiple identities and be a good mechanism in the fight against crime and terrorism.

1.g Definition of Terms

1. Biometrics: a technology that identifies individual uniquely based on their physiology or behavioural traits
2. Biometric template: the individual mathematical data set calculated from a biometric sample
3. Biometric system: an automated system capable of taking a biometric sample, extracting biometric data, comparing it with other biometric data and deciding whether or not the recognition process has been successful
4. Framework: a layered structure indicating what kind of programs can or should be built and how they would interrelate
5. Central database: a database that is located, stored and maintained in a single location. This location is most often a central computer or database system, for example a desktop or server CPU, or a mainframe computer.

1.h Organization of the Study

The study is structured into five chapters. The first chapter gives an introduction to the thesis, comprising the background, the aim and objectives and the significance. The second chapter, which is the literature review, gives an in-depth overview of the concepts that relate to this work, it also presents a review of previous work done by other researchers in this field. The third chapter, research methodology, gives an insight into how the work was implemented, the methods and software adopted. Discussion of results, the

fourth chapter, presents the implemented work, giving explanations on how the applications and databases function. Lastly, chapter five gives a brief summary of the entire thesis work and presents a conclusion.

CHAPTER 2
LITERATURE REVIEW

2.a Introduction

This chapter gives an overview of the basic concepts that relate to the research, starting with explanation of some basic concepts in database systems, to biometric technology, with emphasis on fingerprinting, as it is the biometric feature adopted in this study. It also presents a review of some previous works that have been done by other researchers.

2.b Overview of Database Systems

A database management system (DBMS) is software that allows creation, definition and manipulation of database (Ramez & Navathe, 2011). A DBMS is actually a tool used to perform any kind of operation on data in a database. A database is a collection of related data organized in a way that data can be easily accessed, managed and updated (Malik & Patel, 2016). A DBMS also provides protection and security to a database (Deepika & Soni, 2013).

Any piece of information can be a data, for example, an image, a number, an address, even a biometric template. A database is a place where related pieces of information are stored and various operations can be performed on it (Kulkarni & Urolagin, 2012). Some examples of popular DBMSs are MySQL, Oracle, Sybase, Microsoft Access and IBM DB2.

2.b.i Evolution of Database Technology

The earliest forms of database systems were the hierarchical and network systems, introduced from the mid-1960s through to the 1980s (Ramez & Navathe, 2011). Although they provided large organizations with large record support, they had challenges of flexibility in accessibility and changes in requirements.

Next, the era of relational systems began in the early 1980s, providing answers to data abstraction and program-data independence. However, the need to transit from simple to complex structured objects led to the object-oriented database systems.

The object-oriented database systems were introduced in the 1980s; they included object-oriented paradigms like abstraction, inheritance, and encapsulation. They provided a more general data structure but unfortunately, did not gain much attention as expected. They are now mainly adopted for use in specialized applications, with less than 5% penetration (Ramez & Navathe, 2011).

Presently, with the success in traditional databases, developers are expanding the capabilities of database systems to support more diverse applications ranging from scientific, image storage and retrieval, time series, to data mining etc. (Ramez & Navathe, 2011).

2.c Database Architecture

As per the architecture of a database, logically, it can be divided into two:

- 2-tier client architecture
- 3-tier client architecture

2.c.i Two-Tier Architecture

Two-tier Client/Server architecture is used for user interface programs and application programs that run on the client side. An interface called ODBC (Open Database Connectivity) provides an API that allows client-side programs to call the DBMS. Most DBMS vendors provide ODBC drivers. A client program may connect to several DBMSs. In the architecture, some variation in client functionality is also possible. For example in some DBMSs, more functionality is transferred to the client including data dictionary and optimization. Such clients are called data server. If the architecture of DBMS is two-tier, then it must have an application through which the DBMS can be accessed. Programmers use two-tier architecture where they access the DBMS by means of an application. Here the application tier is entirely independent of the database in terms of operation, design, and programming (Ramez & Navathe, 2011).

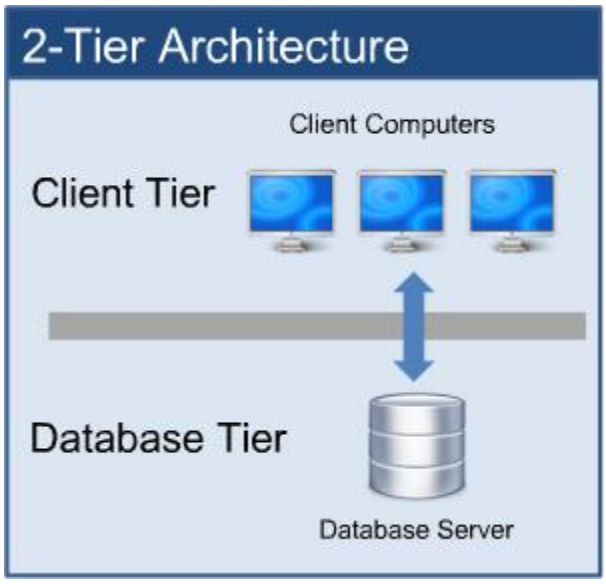

Figure 2.1: Two-tier architecture

Source: http://sapabap-basics.blogspot.com.ng/p/1introduction.html

2.c.ii Three-Tier Architecture

Three-tier client/server database architecture is a commonly used architecture for web applications. An intermediate layer called application server or web server stores the web connectivity software and the business logic (constraints) part of application used to access the right amount of data from the database server. This layer acts like a medium for sending partially processed data between the database server and the client (Ramez & Navathe, 2011).

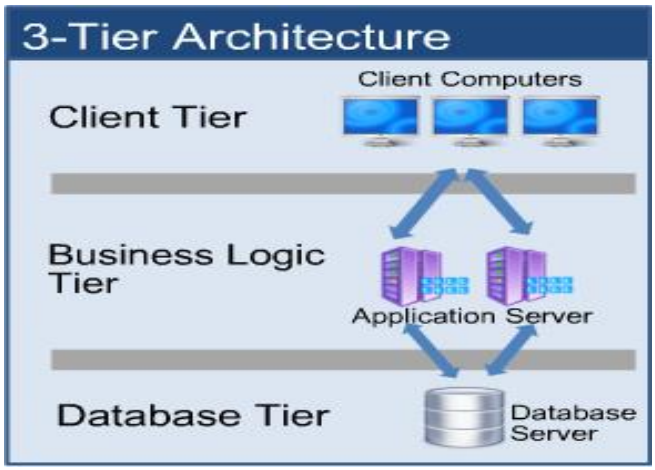

Figure 2.2: Three-Tier Architecture

Source: https://vcomsat.files.wordpress.com/2013/10/3tier.jpg

2.d Database Access Control

There is a rising need for the use of information and communication technology, leading to much e-format data being generated (Sukhai, 2004). All of this data must be stored. Thence, security efforts are constantly being made to safeguard the data from unauthorized individuals, organizations or states, who want to unethically use classified information without permission.

Access control (usually defined by the database administrator or security policy of the owning organizations) can be seen as a data-protection technique which ensures that a user accessing a database is authorized to access some or all parts of the database, and if not, does not get access to the database (Kulkarni & Urolagin, 2012). A database to be used in storing biometric templates needs have an access control mechanism due to privacy concerns. For example, stealing a biometric trait, using it to create a fake trait and penetrating a system with it, is not uncommon practice (Ahuja & Chabbra, 2011). Therefore, access control mechanisms should be defined based on pre-defined rights/privileges (Kulkarni & Urolagin, 2012) to avoid adding, modification, removal or theft, all of which are attacks that can be carried out on databases containing biometrics templates (Ahuja & Chabbra, 2011).

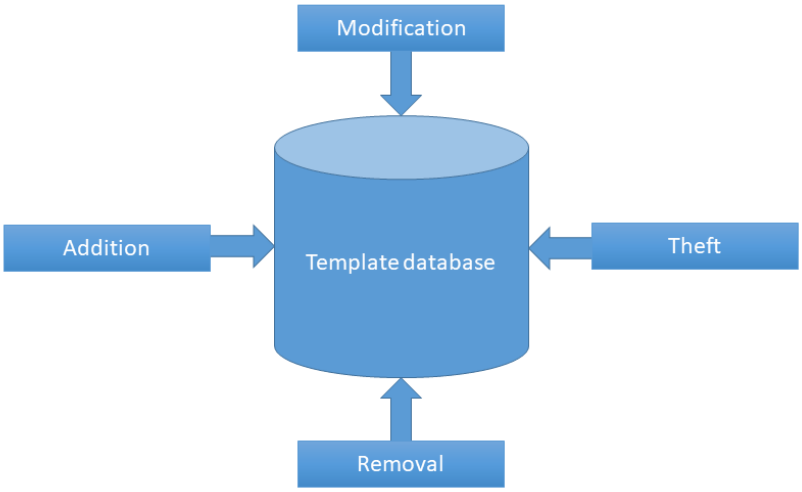

Figure 2.3: Attacks on Template Database

It is impossible to discuss a database without including access control; including access control to a database is like placing a lock on your door to control entry. Keeping the data stored in a database secured is a fundamental service provided by almost all DBMSs (Deepika & Soni, 2013). These two are practically intertwined for a safe system.

2.d.i Components of Access Control

Proper identification, authentication, authorization and accountability are the important components of an access control, a process that relies on its components to enforce security (Sukhai, 2004). Identification involves identifying users who will be allowed to access the database; this is followed by authentication, which verifies that anyone accessing the database is one of those 'identified'. Next is the authorization, which gives specifications as to what exactly each user is allowed to view from the database, and lastly is accountability, which keeps track of who accesses and what was accessed in the database, so users can be held accountable for whatever actions they performed. The main underlying idea of an access control process is to protect the confidentiality, integrity and availability of data (Sukhai, 2004). However, finding a balance between security and accessibility is also key.

2.e Biometrics: Its Current State

As opposed to traditional methods of identification which are either based on what you know (knowledge-based), for example passwords, pins etc., or what you own (token-based), for example ID cards, chips etc., biometrics identification systems (BISs) are identification systems based on physiological or behavioural characteristics of an individual (Pal & Khethavath, 2016). Because of its reliability, biometrics technology is increasingly being adopted for use in various domains ranging from border control (visa and immigration documentation), identity documents (passports with readable biometrics) to national security (terrorism, criminal prosecution) (Bala, 2008).

2.e.i Application of Biometrics

Depending on the application context, a biometric system may be called either a verification system or an identification system (De Luis-García, Alberola-López, Aghzout, & Ruiz-Alzola, 2003):

- Identification: An identification system recognizes an individual by searching the entire template database for a match. It conducts one-to-many comparisons to establish the identity of the individual. In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (El-Sisi, 2011). Biometric comparison and information fusion algorithms are applied against all recordings in the database, generating a set of probabilities that the current recording matches any given identity in the biometric database. The identity of the closest match is returned to the end-user (Holland & Komogortsev, 2014).
- Verification: Biometric verification is used to validate a user as a supplied identity. A verification system verifies a person by comparing the captured biometric characteristic with his own biometric template pre-stored in the system. It conducts one-to-one comparison to determine whether the identity claimed by the individual is true. A verification system either rejects or accepts the submitted claim of identity (El-Sisi, 2011). An acceptance threshold determines whether the user

is genuine or an imposter. The acceptance or rejection of the authentication attempt is returned to the end-user (Holland & Komogortsev, 2014).

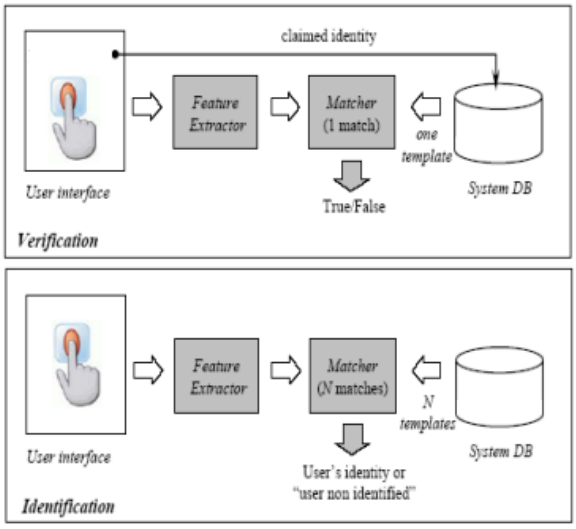

Figure 2.4: Block Diagram of a BIS

Source: (Sharma & Agarwal, 2016)

2.e.ii Types of Biometrics

There are various biometric traits that can be used to identify people. According to Namburu, (2007). The various biometric modalities can be broadly categorized as:

- Physical biometrics: This involves some form of physical measurement and includes modalities such as face, fingerprints, iris-scans, hand geometry etc.
- Behavioural biometrics: These are usually temporal in nature and involve measuring the way in which a user performs certain tasks. This includes modalities such as speech, signature, gait, keystroke dynamics etc.
- Chemical biometrics: This is still a nascent field and involves measuring chemical clues such as odour and the chemical composition of human perspiration**.**

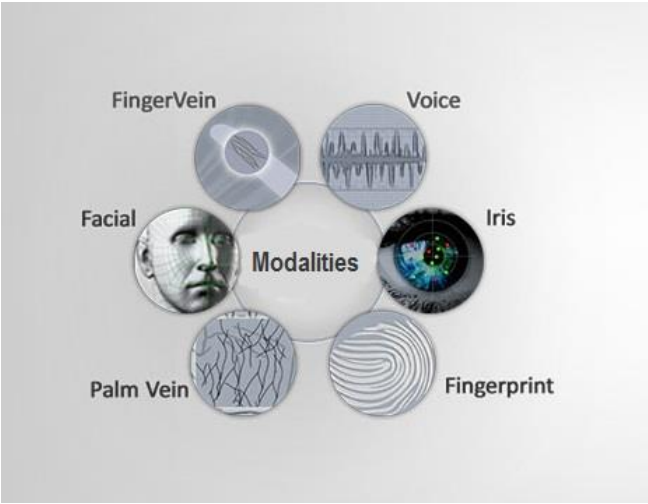

Figure 2.5: Various Biometric Traits

Source: http://www.m2sys.com/blog/wp-content/uploads/2014/11/Modalities.jpg

Of all these different biometric modalities, the fingerprint is still the most common in use for identification, mainly because of its reliability, ease of collection and consistent use. According to the Federal Bureau of Investigation (Edgar, 2006), of all the methods of identification, fingerprinting alone has proved to be both infallible and feasible. While many cases of mistaken identification have occurred through the use of these older systems, fingerprint has been established to be the most precise means of identification (Rajharia & Sharma, 2013; Taha & Norrozila, 2015). To date the fingerprints of no two individuals have been found to be identical.

2.f Fingerprints

A fingerprint is an impression left from a fingerprint epidermis when a finger is pressed against a smooth surface (El-Sisi, 2011). The fingerprint consists of ridges and valleys which run roughly in parallel. Ridges (also called ridge lines) are dark whereas valleys are bright (Chaurasia, 2012). Injuries such as superficial burns, abrasions, or cuts do not affect the underlying ridge structure and the original pattern is duplicated in any new skin that grows (El-Sisi, 2011). Each individual has a unique fingerprint. This uniqueness stems

from the local ridge characteristics and their relationships (Maltoni, Maio, Jain, & Prabhakar, 2009). It is also referred to as minutiae patterns.

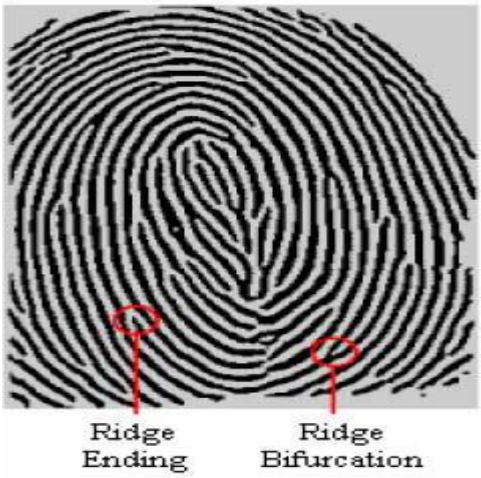

Figure 2.6: Diagram of a Typical Fingerprint Showing Ridge Endings and Bifurcations

Source: **http://www.circuitstoday.com/working-of-fingerprint-scanner-2**

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 (Rajharia & Sharma, 2013). We should note however, that there are different types of minutiae, in addition to these two main types mentioned above. Some of the others include core, delta, island, pore and crossover (see figure 2.7). A set of minutiae are usually used to represent a fingerprint. The number, locations, and sparsity of the minutiae vary from finger to finger in any particular person, and from person to person for any particular finger. When a set of finger images is obtained from an individual, the number of minutiae is recorded for each finger, according to the Henry Classification System. Only 13 are needed to identify a unique fingerprint.

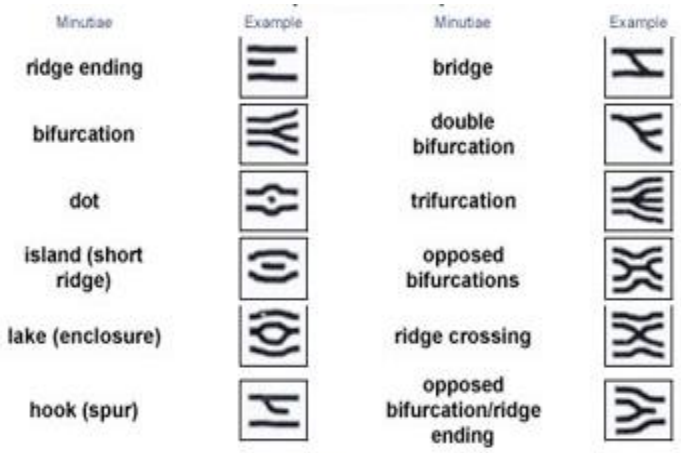

Figure 2.7: Basic and Composite Ridge Characteristics

Source: https://www.pinterest.com/pin/327848047849054725/

The precise locations of the minutiae are also recorded in the form of numerical coordinates for each finger. The result is a function that can be entered and stored in a computer database. A computer can rapidly compare this function with that of anyone else in the world whose finger image has been scanned. Most existing fingerprint identification systems match two fingerprints using the minutiae-based method (En, Jianping, & Guomin, 2005).

2.f.i Fingerprint Topologies

Fingerprints have three different feature categories, levels 1, 2 and 3 (Ahuja & Chabbra, 2011; A. K. Jain & Feng, 2016). Level 1 features refer to very visible details like singularities, ridge flow, pattern type, while level 2 features refer to minutiae points such as bifurcations, ridge endings and ridge skeletons. Level 3 features, on the other hand, are micro details of fingerprints that can only be obtained from very high resolution images (≥1000 ppi). They include sweat pores, dots and emerging ridges.

However, only singular point and minutiae features are considered in the current fingerprint standard (Charles, Patrick, & Ramaswamy, 2007), other features outside these two are referred to as extended features (Jain, 2010). Singular points can further be categorized broadly into:

Arch: Here, all ridges enter on one side and exit the other. This is the simplest and least common pattern; only about 5% of population have this pattern (Edgar, 2006). This pattern has no core or delta. Its sub group are:

- Plain arch
- Tented arch.

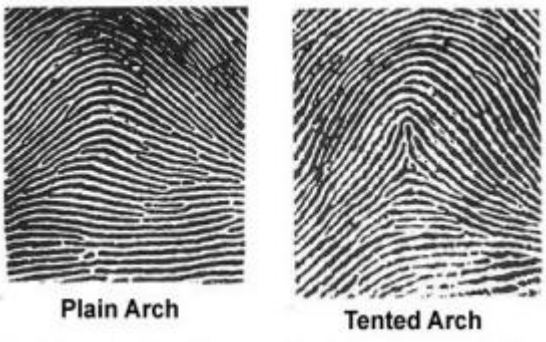

Figure 2.8: Diagram of Arch Patterns
Source: (Edgar, 2006)

Whorl: key features are at least two deltas and one core, about 30-35% of population have this pattern (Edgar, 2006). There are four types of whorl patterns:

- Plain whorl
- Central pocket whorl
- Double loop
- Accidental whorl.

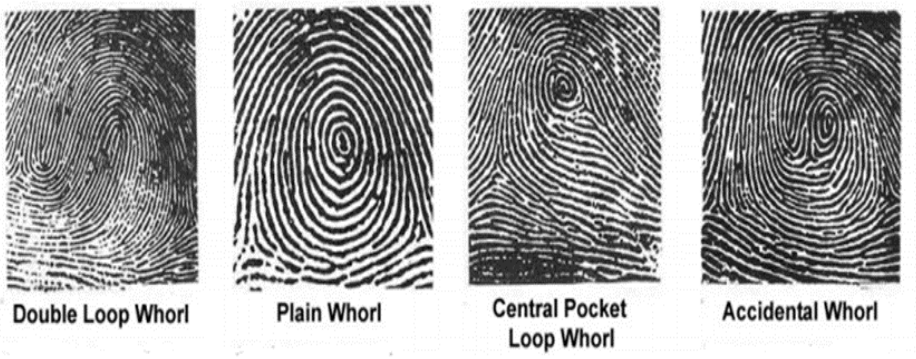

Figure 2.9: Diagram of Whorl Patterns

Source: Edgar (2006)

Loop: This type of pattern is the most numerous of all and constitutes about 65 percent of all prints (Edgar, 2006). The key features of loop are: core, which is the centre area of a finger print pattern and the delta, which is the triangular shape made by ridges. There are two types of loops:

- Radial loop
- Ulnar loop.

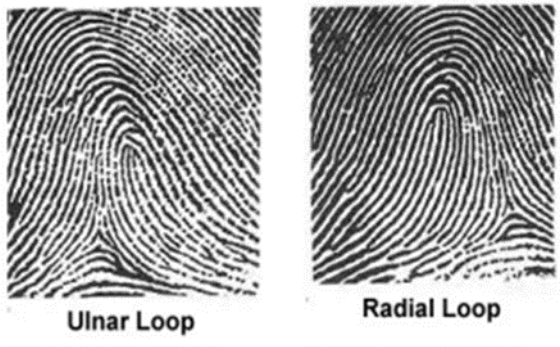

Figure 2.10: Diagram of Loop Patterns

Source: Edgar (2006)

2.f.ii Fingerprint Processing

2.f.ii.1 Pre-processing

Because the output quality of the minutiae extraction algorithm depends a lot on the quality of the input fingerprint image, it is necessary for the fingerprint to be enhanced to get the finest quality before minutiae extraction is performed. Enhancement algorithms can be done on two kinds of images:

- Binary images
- Gray-level images.

A binary ridge image is an image where all the ridge pixels are assigned a value one and valley pixels are assigned a value zero. However, after applying a ridge extraction algorithm on the original gray-level images, information about the true ridge structures is often lost, depending on the performance of the ridge extraction algorithm. Therefore, enhancement of binary ridge images has its inherent limitations. In a gray-level fingerprint image, ridges and valleys in a local neighbourhood form a sinusoidal-shaped plane wave, which has a well-defined frequency and orientation.

2.f.ii.2 Minutiae Extraction

After the fingerprint has been processed, the minutiae extraction algorithm is one of the most commonly used algorithms for extracting features that characterize a fingerprint. The minutiae are specific points in a fingerprint image; they are the local discontinuities in the ridge flow pattern, and provide the features that are used for identification (Mohammed & Rajesh, 2015). The set of minutiae types are usually restricted to two types, they are ridge endings and bifurcations.

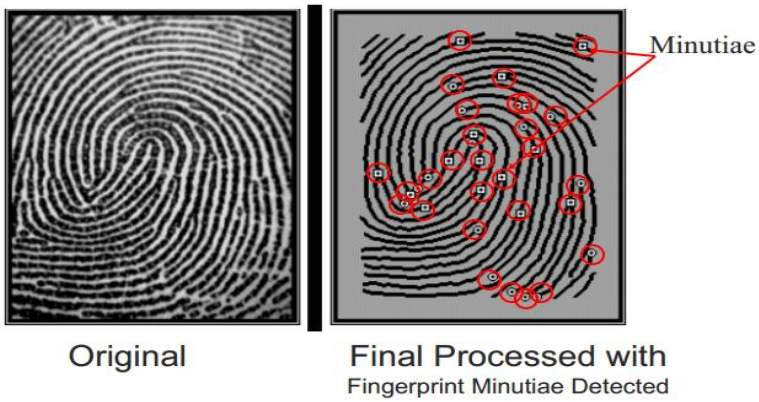

Figure 2.11: Minutiae points of a processed fingerprint image

Source: Savvides (n.d.)

The different minutiae feature locations and types can identify different individuals. These are what are stored in the biometric template.

2.g Review of Related Work

Chaurasia, (2012) in an approach to fingerprint image pre-processing, employed the use of different fingerprint processing algorithms, arranged in a particular order to produce the best processing. The research work concentrated upon how to process the given fingerprint sample so that correct minutiae can be detected, to produce better images which are clearer and identifying minutiae points from them are easy. The study detects true minutiae points so the fingerprint recognition system will produce accurate results. She employed the steps in the following order:

1. Normalization
2. Orientation Image Estimation
3. Frequency Image Estimation
4. Region Mask Generation
5. Filtering (Gabor Filter).

In 2015, Naja & Rajesh evaluated the impact of enhancement algorithms on a fingerprint image using what they called the goodness index (GI) on performance evaluation of a verification system. The enhancement algorithm was done on gray-level images in the following stages: normalization, segmentation, orientation

estimation and ridge frequency estimation, Gabor filtering, binarization and thinning. Enhancement was done on 50 fingerprint images. First, the GI was evaluated when the minutiae were extracted without applying the enhancement algorithm and then was computed when the enhancement algorithm applied to the input fingerprint images before the minutiae were extracted. The GI values were always higher with enhancement algorithm applied. In addition, performance of the fingerprint verification system is significantly improved when our fingerprint enhancement algorithm is applied to the input fingerprint images.

Breedt & Martin (2004), proposed a model to be used in developing a passport system that employs a set of national repository data to store biometric templates. The model consists mainly of a client side and a server side. Five main areas were identified based on the function they performed: the document read, biometric scan, client, server, template database. The server side consisted of a biometric template database and a server side module responsible for a number of the operations described in Wayman's generic biometric model. Its operation included: signal processing/feature extraction process and decision making (by performing verification). The client side consisted of client module and client application. Its operations included data collection, either from biometric scan or the data in the document certificate and transmission of acquired data to the server for processing. Their model also allowed for multiple biometrics in one client terminal. The biometric templates were stored and transmitted in encrypted format (asymmetric or symmetric) and digital certificates issued to the client and server.

(Kozievitch et al., 2010) in their study focused on the contextual integration of fingerprint images which came from various sources: different very large digital libraries and the compound object perspective (CO). The compound object referred to as the CO1 structure, has its components from the initial subsystems of the four digital libraries (DLs) used. The sources of the four DLs include recorded prints (DL1), training (DL2), crime scene (DL3) and distorted images (DL4). The interface of CO1 comprised the union information of its four components, along with the union of their respective vocabularies (individual,

fingers, thumb, quality, distortion, parameters). The proposed integrated digital library is a 4-tuple consisting of a union repository, a union catalogue, union services and a union society. The 5S (streams, structure, spaces, scenarios and societies) framework along with the 5S approach were adopted to integrate the digital libraries. Mapping and harvesting services here used to represent the minimal union services which are necessities for integration of these digital libraries. The Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH) was proposed, either the OAI-ORE or DCC for content packaging while the CO1 structure could be represented by RDF. Their study came up with an E-R diagram design, implementation of skin distortion model and testing of the blurring distortion.

Bamigbade & Onifade, (2014), also proposed the gender, ethnicity, hair colour, eye (GEHE) model to improve retrieval time of a biometric template from a multimodal database and consequently improve identification time. For their study, they employed the use of two primary biometric traits, fingerprint and face and four soft biometric traits, GEHE. The minutiae were extracted from the gray-level fingerprint image and the facial templates were extracted using the simple invariant feature transform. The two templates were then fused together and partial least square techniques was employed to eliminate redundancy by linearly extracting few latent features. The fused templates were then clustered using four datasets, the GEHE, into 128 clusters. Only the latent features of the templates were stored to avoid arbitrarily large databases. From their clustering algorithm, retrieval time is improved and the error rate, which is mostly attributed to multimodal systems, was reduced.

Uz et al. (2007) used hierarchical Delaunay triangulations to achieve improved minutiae-based fingerprint by combining multiple fingerprint impressions into one super template. Their key idea was exploiting the invariant features computed from the minutiae triangles such as the side length, and angle under rigid transformations. Using the following steps; hierarchical Delaunay triangulations, affine refinement, super-template updating to achieve a 'super template' from the various templates, an initial super template is chosen, the best quality template and continuously updated and improved by merging with other template impression. They experimented with three different schemes; score level fusion, template selection (T-SEL) and template synthesis (T-SEL).

Schellberg (2015) in his study 'Global Expansion of Offender DNA Databases' presented an overview of countries currently having national programs for implementation, and legislation for their national databases for criminal offenders. The profile and samples of offenders are collected, and if they are convicted, they are stored in this national database, but otherwise destroyed. As at 2015, 50 countries have already implemented a national database. These countries have also adopted a national standard with the CODIS software being used in over 35 out of the 50 countries that have implemented systems so far.

Finally, Rotimi et al. (2013) did a study on the prospects and challenges of creating a central national database for Nigeria. In their study, they considered using an entity-relationship (ER) model to design a database. Their aim was to identify individuals uniquely. They proposed the primary key of the model to be a national security (NS) code. They proposed two types of NS code: NS Code–citizen and NS Code–immigrant. NS code–citizen (NSCC) means national security number for the Nigerians by birth or parent(s) by birth or nationalized citizen. NS code–immigrant (NSCI) means national security number for the legal immigrant. However, the proposed NS code is not yet available for Nigerians and according to them, "would require data capturing which may be cumbersome therefore, special attention, funds, work free days and public registration days must be declared by the Federal government for the registration exercise" as stated in their study.

2.h National Database Examples

2.h.i The Social Security Master File

The Death Master File is a database compiled from the Social Security Administration (SSA) that currently contains over 89 million records, as of April 2014. The file is created from internal SSA records on deceased individuals that previously held a social security number and whose deaths were reported to the SSA. A family member, an attorney, a mortuary, etc. gather most of this information in connection with filings for death benefits. The Death Master File is continuously updated and includes corrections to old data as well as the addition of new deceased entries. The file includes the following information on decedents, when made available to the SSA:

- First Name / Last Name
- Social Security Number
- State Issued
- Birth Date / Death Date
- Last Residence
- Lump Sum Payment.

2.h.ii The EURODAC System

EURODAC is an abbreviation of European Dactyloscopy or fingerprint identification. It is the EU-wide database of asylum-seekers' and irregular migrants' fingerprints. It holds the personal data of nearly 2.3 million individuals and has been transformed into a policing as well as migration database. The EURODAC system comprises the central unit, a national unit in each member state, and the infrastructure for transmitting data between national units and the central unit. All participating states are obliged to "promptly take the fingerprints of all fingers of every applicant for asylum of at least 14 years of age". This is subsequently transmitted to the central unit database and stored for 10 years, together with the following information:

- Fingerprint data;
- Member State of origin, place and date of the apprehension;
- Sex;
- Reference number used by the Member State of origin;
- Date on which the fingerprints were taken; and
- Date on which the data was transmitted to the Central System.

2.h.iii The UK Police National DNA Database

The UK National DNA Database (NDNAD) is a police intelligence database that uses DNA to identify criminal suspects and to find links between different crimes. It was set up in April 1995 by the Forensic Science Service which has since become a world expert in the use of forensic DNA technology. This

database is used to store tissue samples, genetic information and personal data indefinitely. It also contains more routine information about people, for example their name and sex. It contains profiles of over 2.1 million individuals and it is the most extensive DNA database in the world. No other police force has greater freedom to obtain, use and store genetic information from its citizens.

2.h.iv The FBI's Integrated Automated Fingerprint Identification System

The Integrated Automated Fingerprint Identification System (IAFIS) is a national automated fingerprint identification and criminal history system maintained by the FBI. IAFIS houses the fingerprints and criminal histories of 70 million subjects in the criminal master file, 31 million civil prints and fingerprints from 73,000 known and suspected terrorists processed by the U.S. or by international law enforcement agencies.

2.h.v NIMC's National Identity Database

The Nigerian National Identity Database (NID) is a proposed integrated national database to maintain information of Nigerian nationals obtained from various organizations' databases. The idea of an NID was first conceived in 2005 when the government tasked to NIMC to create a national identity management system (NIMC Harmonization Policy, 2007). The goal of the NIMC was to harmonize the different data (including hard and soft biometric data) that are contained in various organizations' databases. Although, various attempts have been made thus far in this line, it has not yet been achieved fully as this was stated recently by the acting secretary to the government of the federation, Mrs. Habibah Lawal (Clement, 2017). Therefore, this research work aims to create a model that can be adopted by NIMC for easy and effective integration of the biometrics data.

CHAPTER 3

RESEARCH METHODOLOGY

This chapter discusses the way in which the implementation of the research work was carried out, explaining the methods, languages and software used in implementing the thesis work.

3.a Data Collection

The data set used for this research includes both hard biometrics, soft biometric traits and other relevant data of individuals.

As hard biometrics, the following were used:

1. Fingerprint templates: the fingerprints captured were for both thumbs. The fingerprints were captured using the digital persona U4500 fingerprint scanner. This fingerprint scanner uses fingerprint minutiae data format to store fingerprints.
2. Facial images: full 24-bit colour frontal images were taken with facial expression neutral, teeth closed and both eyes open. In addition, three samples of facial images were taken, with one left and one right and one frontal (for the central database). They were captured using an Android phone device and were stored in JPEG format.

The soft biometric traits used were:

1. Gender
3. Height
4. Ethnicity
5. Age.

Other data sets included in the data set were:

1. Address
2. Language
3. Place of birth
4. Profession.

3.b Model Description and Architecture

The system focused on reducing multiple enrolment of individuals' fingerprint data. The approach taken for designing the platform for this is that any of the organizations (NIS, Banks, INEC) that want to register/enrol an individual, will have to verify from the central database first to ensure that this individual has not been previously enrolled in any other organization. If the individual has been enrolled previously, then he or she would be registered without collecting fingerprints again (since he or she has been verified). Otherwise, if not been registered, then he or she would be registered and his or her fingerprints collected. This is in order to have only one capturing point for fingerprints. Only one organization would enrol an individuals' fingerprints. Every other organizations may only verify an individual from the central database but may not collect and store the fingerprint data.

The flow chart of the system is shown below:

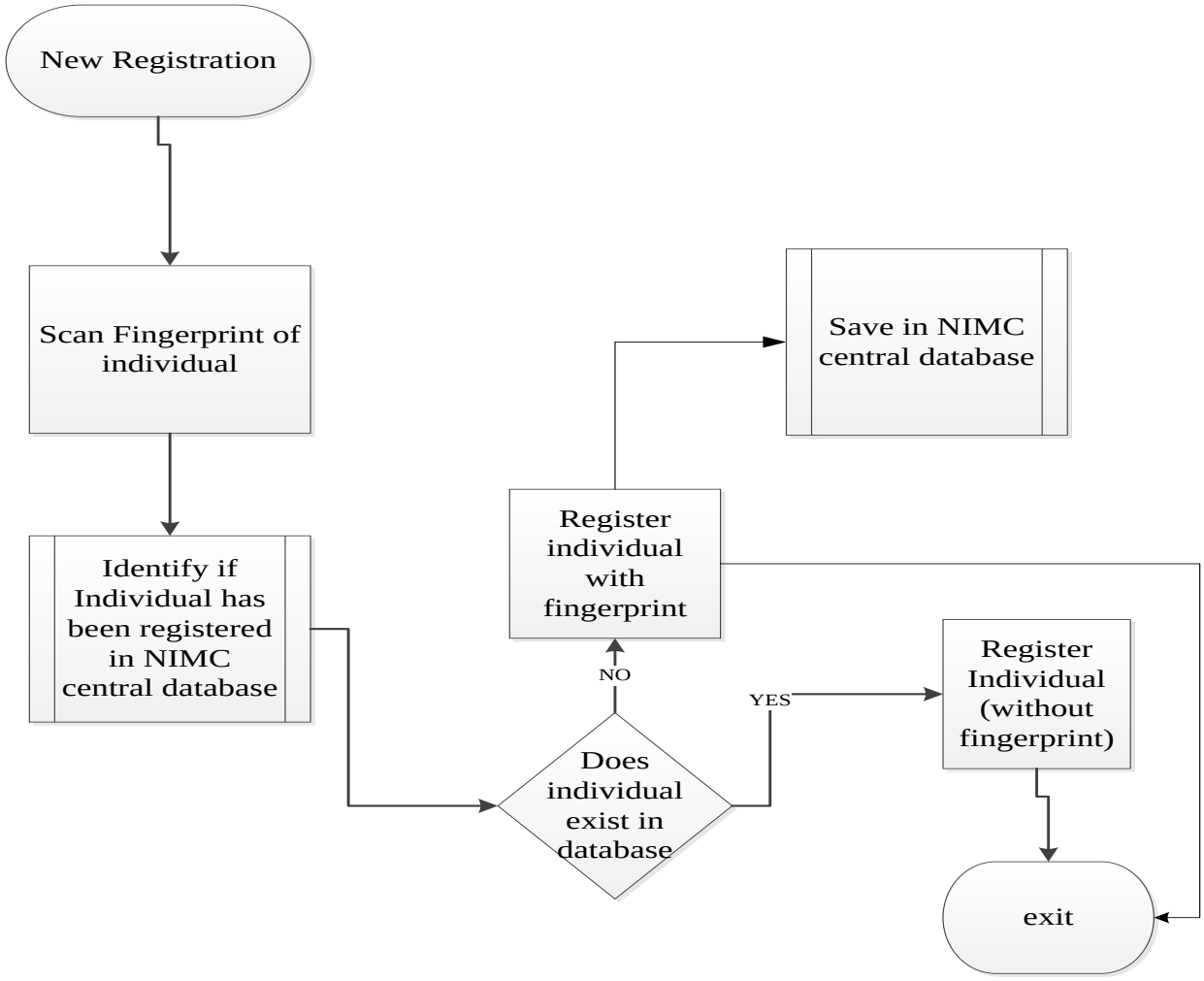

Figure 3.1: Flow Chart of Proposed Methodology

This was done in order to eliminate redundancy of storing multiple fingerprint templates across various organizations for a single individual. The central database for the four organizations that was used in the research work contained all information and the information earlier described in section 3.1 was stored in them.

3.b.i Nigerian Identity Management Commission

The current database of the NIMC was mimicked, storing important details of individuals that were obtained through the national ID card registration exercise that has been ongoing since 2011. The datasets listed in 3.1 above were all included in this database. The database was modelled using an ER diagram.

3.b.ii Independent National Electoral Commission

The same procedure was carried out for the INEC database, representing all the aforementioned datasets, but most importantly, including the voter's identification number (VIN) which is used as the unique identifier in this database.

3.b.iii Central Bank of Nigeria

The bank verification number (BVN) (alongside other information) was used as the unique identifier for individuals' information in this database. However, it also contains the fingerprint biometric, which was used as the core identifier for the centralized database.

3.b.iv Nigerian Immigration Service

The unique entity in this database for identifying individuals is the passport number. But just as in other databases too, it also contains biometric information (i.e. fingerprints) which was adopted as the core identifier in the centralized database. Thus, this database was mimicked in order to have many impressions of the same fingerprint of every individual therein.

3.c Centralized National Identity Database

The NIMC's database serves as the central database. This database was created to serve as the central identity database. It consists of the information contained from the other four organizations' databases. It serves as the go-to database for all of the organizations to verify individuals based on their biometric (fingerprint) details. All organizations were connected to the central database. The diagram below presents a general structural overview of the current system across the country:

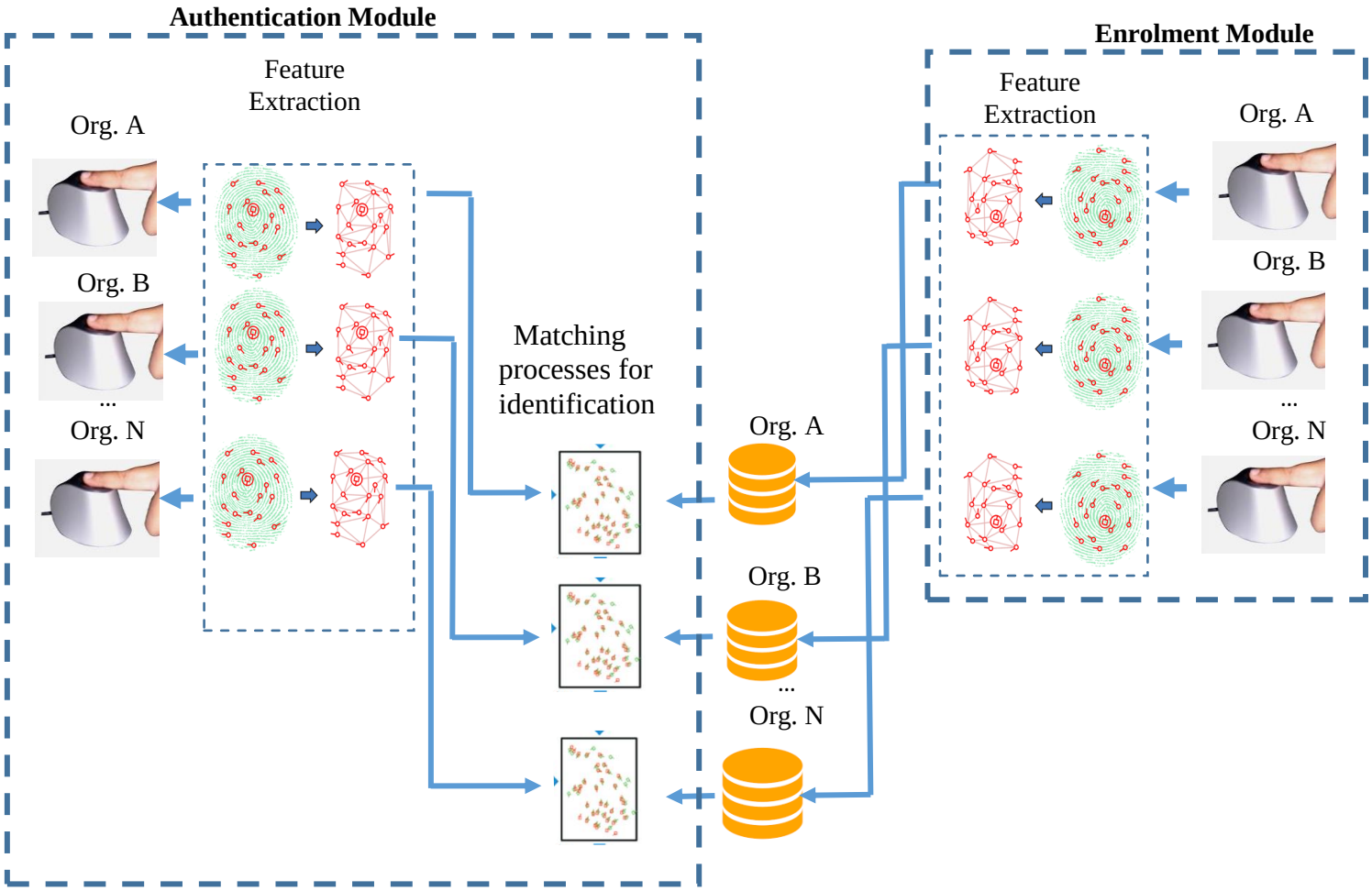

Figure 3.2: Architecture of the Current System in Nigeria

The above diagram shows the different organizations in Nigeria, each having its own database and identification system independent of the other, such that the data in each organization cannot be made use of by other organizations for identification nor verification purposes of individuals, leading to multiple and indiscriminate collection of individuals' fingerprint data during enrolments and registrations.

The next diagram presents the structural framework for the proposed system to be adopted for this research, containing the central database to which all organizations are connected, providing a platform for previous fingerprint registration to be identified and avoid duplication.

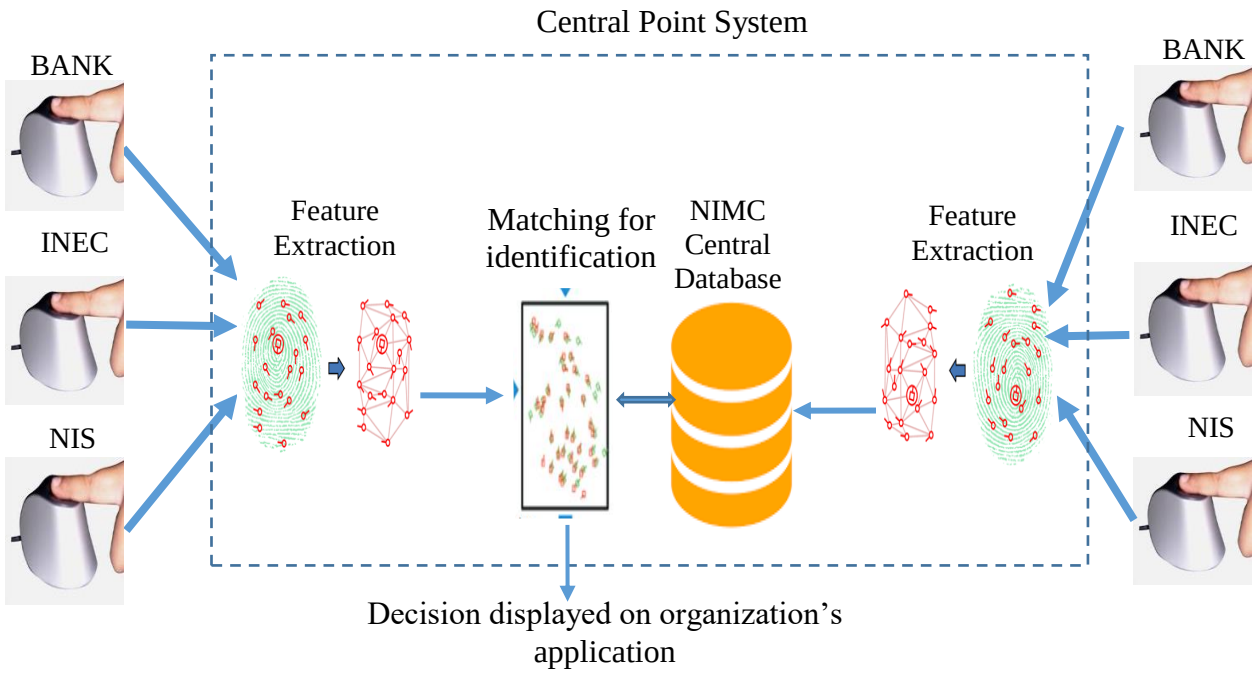

Figure 3.3: Architecture of Proposed Fingerprint-Based Enrolment and Authentication System

3.c.i Identification of Enrolees

In order to identify from the NIMC database if an enrolee has been previously registered in any of the other organizations or in NIMC previously, the fingerprint of an individual is scanned and compared with those stored in the NIMC database. It also gives room for verification using the NIN number if the individual has been registered with the NIMC before. As per the identification via fingerprints, we have used both the left thumb and the right thumb where the decision fusion acceptance criteria is based on the AND (conjunctive) rule, adopting the decisions from using combined biometrics (Daugman, 2000), The probabilities of the false reject or false accept rate will be reduced. As in our case, the left thumb will be represented as L while the right as R. The following error rates are considered:

- P_L (FA) = probability of a false accept using L alone.
- P_L (FR) = probability of a false reject using L alone.
- P_R (FA) = probability of a false accept using L alone.

- P_R (FR) = probability of a false reject using L alone.

Following from the above probabilities, in identification for our system, a false accept can occur only when both L and R give a false accept. Thus, the combined probability of false accept using both L and R will be:

P_{AND} (FA) = P_L (FA) P_R (FA), which clearly gives a lower probability than either used alone.

3.d Database Creation (Back End Design of Application)

For the back end of the applications, the databases where developed using PhpMyAdmin which is a tool for MySQL database management. The tables were designed to hold information of the individuals for enrolment as described in section 3.1. PhpMyAdmin was used because, with it, one can create, alter, drop, import and export MySQL database tables. It also gives support for running MySQL queries, optimization, repair and carry out other database management commands.

3.e Windows Form Development (Front End Design)

In order to create an interface for the databases access layer, we adopted the Netframework, which is a web-based application framework, using C#.net as the programming language. This was done in order to avoid issues with authorizations, authentications etc. The applications were developed targeting the Microsoft 3.5.Net framework, which is compatible with Microsoft legacy operating systems. These were particularly chosen for the following reasons:

1. It is object-oriented language, which better represents real life situations than procedural programming, helping us to map our programs to the problem domain.
2. It is maintained by Microsoft; about 90% of the operating system platforms in Nigeria for both client and server use Microsoft, thereby eliminating compatibility issues during deployment and maintenance/upgrade.
3. The .net framework is a consistent object-oriented environment, which supports other languages like VB.net, C++, F#, asp.net, JavaScript, Iron Python etc.

4. The C# language has a very large base class library, which are large classes built by Microsoft and open source developers that can be imported and referenced in our application along with other dynamic link libraries and services, which we can hook to our program.
5. It has a development environment, Visual Studio, which is very robust, making it easier to design, debug, compile, test, deploy and maintain our project in the same environment without adding plugins. It also uses the common language runtime environment, which is a sandbox that prevents the OS from crashing if the software crashes.

3.f Performance Evaluation of Model

In order to evaluate the accuracy of the verification process via fingerprints stored in the database, we tested by randomly querying some of the stored templates with query templates, using the fingerprint matching algorithm. However, for the fusion of our fingerprint template, we have chosen decision level fusion, fusing both the left and right thumbs. This is because, when two biometric tests of equal power are combined, for example encoding both eyes' iris patterns, or two of a person's fingerprints **(**as in our case), then the appropriate shift in operating threshold (whether for the "AND" rule or the "OR" rule) will enhance performance and reduce the net equal-error rate (Daugman, 2000).

3.g Tools Used for Research

3.g.i Standard Query Language

IBM developed the standard query language (SQL) in the 1970s. It is an ANSI (American National Standard Institute) standard, which allows for database manipulation. This research work employed the SQL language for the following:

- Creating of new databases;
- Creating new tables in databases;
- Executing queries; and
- Setting permissions on tables, procedures and views.

3.g.ii Visual Studio

We adopted Visual Studio as our integrated development environment (IDE) for creating our application. Microsoft Visual Studio is an IDE from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web apps, web services and mobile apps. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can produce both native code and managed code.

3.g.iii MySQL Connector

The MySQL connector serves as an application, which provides connectivity between Visual Studio and the MySQL database on the Windows operating system. To be specific, version 6.3.5 was used ensure connectivity with the version of visual studio and Wamp server used. This provided the framework upon which the connection string between the two applications would work seamlessly.

3.g.iv Adobe Fireworks

This is a graphic design and editing software. It was incorporated for the purpose of designing elegant graphic images and text. This made the application appear more user friendly in terms of appearance, considering the fact that emphasis is placed on user experience and interaction.

CHAPTER 4
RESULTS AND DISCUSSION

4.a Introduction

This chapter presents the results obtained from the various steps of the development of the framework for this project. Ranging from the development of the various organizations' web application, the forms designed, the various tabs, modules contained therein. It also presents an insight into the database created.

4.b Organizations' Web Applications

The applications are for the four different organizations involved, NIS, NIMC, INEC and Commercial Bank. Each of them has the query module, the enrolment module, the verification and finally the admin module. The enrolment module gives the interface for new individuals to be registered using the applicants' enrolment form, which was designed on visual studio.

The verification module is used to verify (using both left and right fingerprints as discussed in section 3.6)

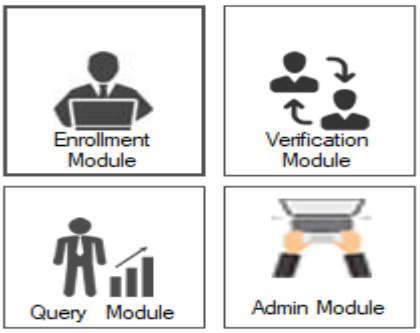

Figure 4.1: Diagram of an Application's Main Dashboard

From the central database if the applicant has been registered previously under any of the organizations. The verification is common to all organizations. It is the platform which is used to ensure that an individual's fingerprint is not being collected indiscriminately by disabling or enabling the fingerprint capture tab. The admin module as the name implies is for the system administrator to manage users of the application, the database and different settings.

Lastly, the query module is used to get needed information from the database as desired.

4.b.i NIS's Application Design

Its enrolment form collects all the basic information discussed in 3.1, however, upon registration; the 'passport number', which is the unique identifier for this organization, is generated automatically.

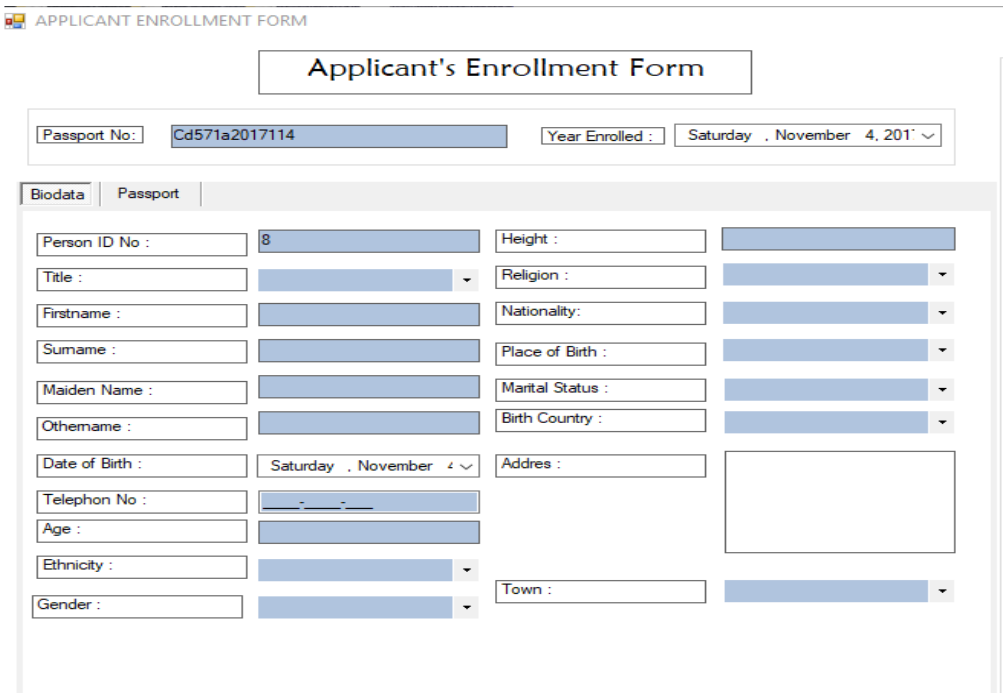

Figure 4.2: NIS enrolment form

4.b.ii INEC's Application Design

Just as in NIS, INRC's enrolment form collects all the basic information discussed in section 3.1. However, upon registration, the VIN, which is the unique identifier for this organization, is automatically generated.

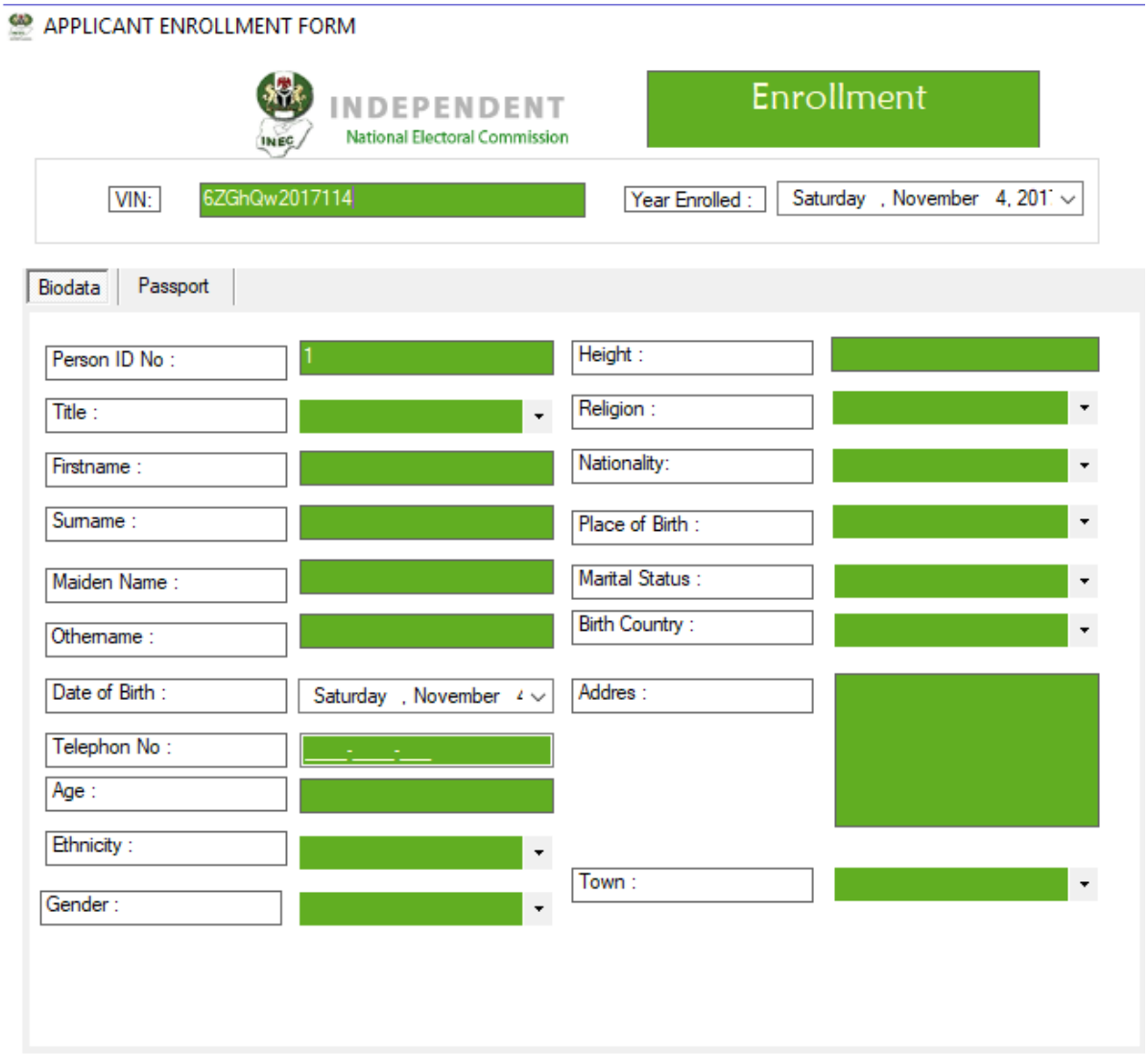

Figure 4.3 : INEC Enrolment Form

4.b.iii Commercial Banks Application Design

Just as in other organizations, its enrolment form collects all the basic information discussed in section 3.1. However, upon registration, the BVN which is the unique identifier for bank customers is automatically generated.

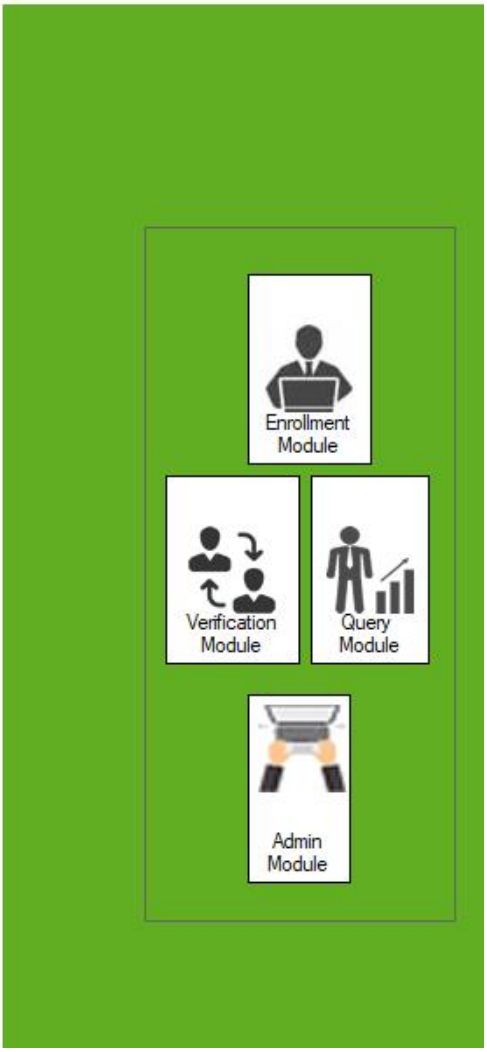

Figure 4.4: Commercial Bank Enrolment Form

4.b.iv NIMC Application Design

For NIMC, its enrolment form collects all of the information discussed in section 3.1, it was designed in accordance to the NIMC enrolment form which NIMC is currently using to register Nigerians for the National ID card.

Figure 4.5: NIMC Application Main Dashboard

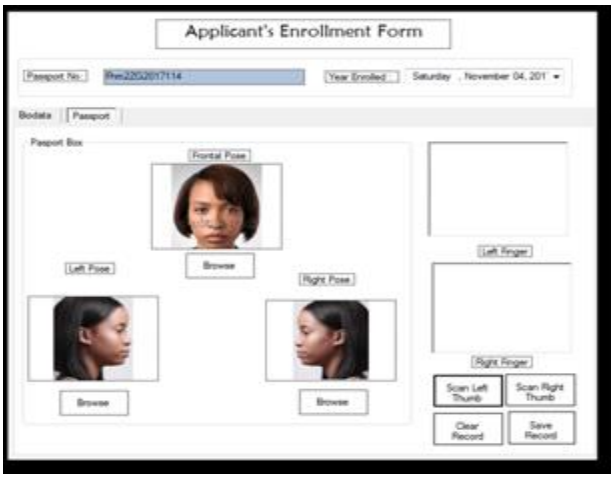

Figure 4.6: NIMC Enrolment Form

The use case diagram below illustrates how the applications of the organizations function:

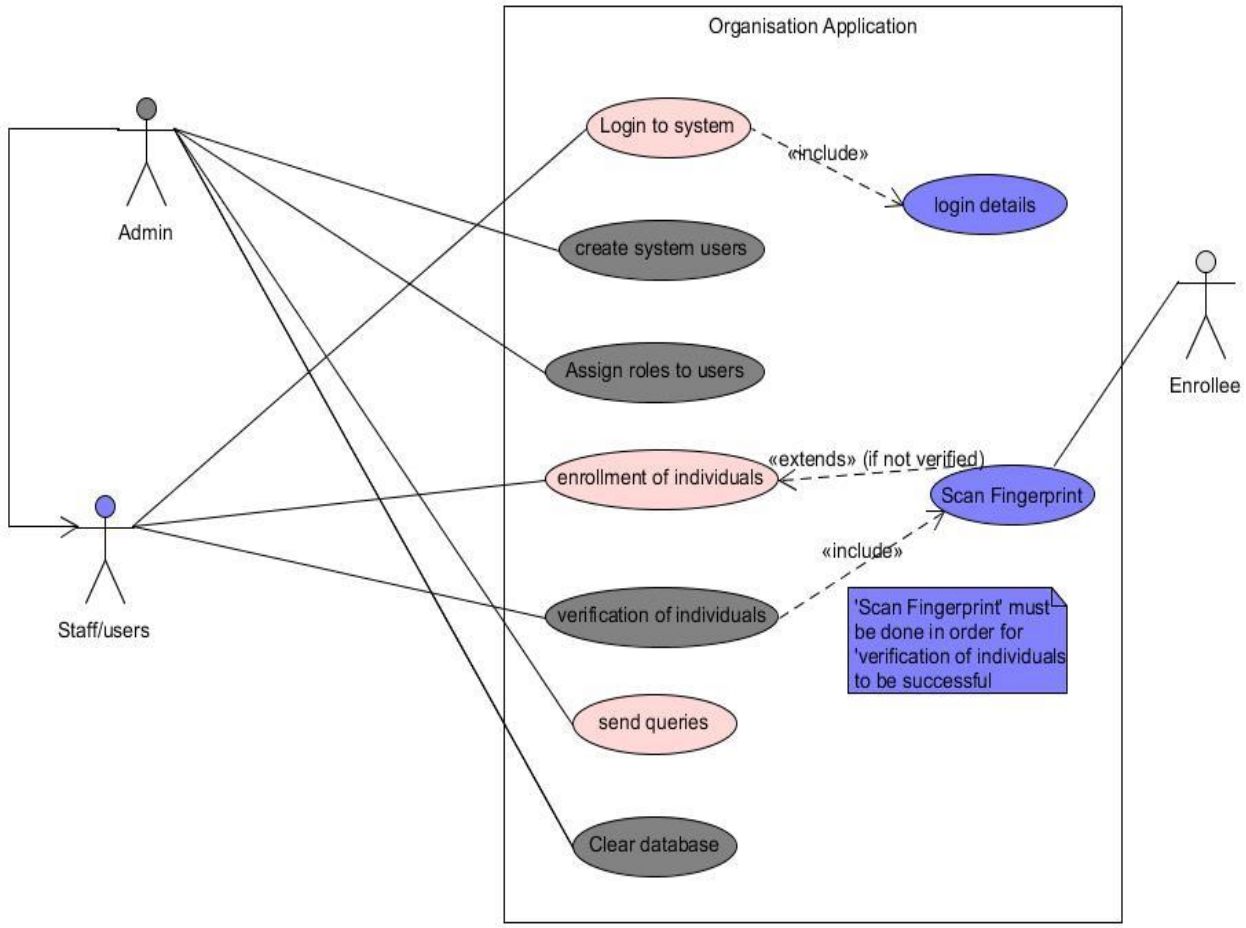

Figure 4.7: Use Case Diagram of Application

4.c Databases of the Organizations

As described in section 3.4, different databases were created, one for each organization. The applications are connected to their backend database. However, for each application, two connections are established, one to its own database and the other to the central database.

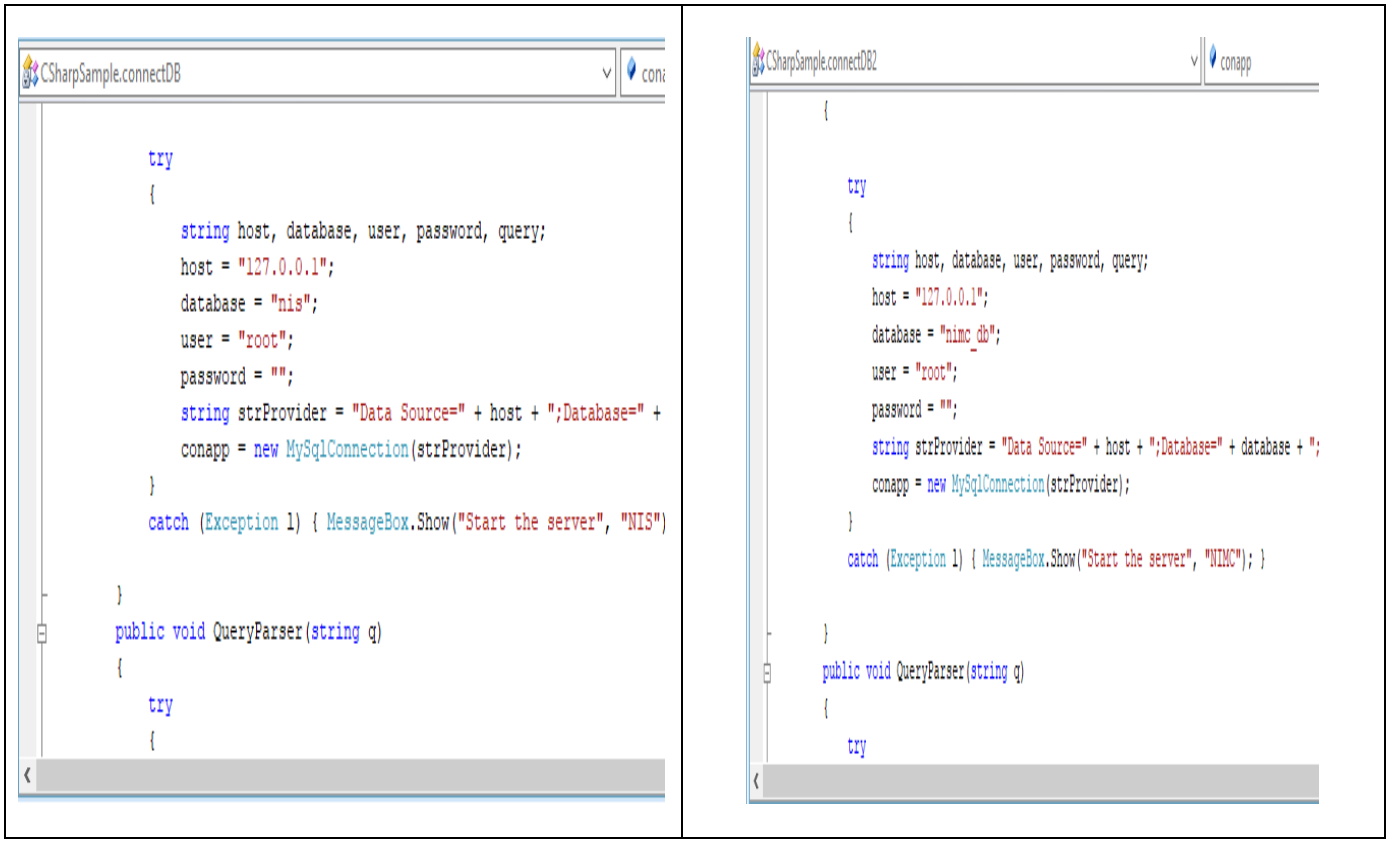

Figure 4.8: Sample of Multiple Connection for Applications

4.d Authentication of Enrollees

The verification module in each of the application was used to achieve this. It is the platform that queries the central database using fingerprints (right and left thumbs) to check if the enrolee has been registered previously in another organization. Based on our decision criteria as chosen in section 3.6, the user is then verified as either registered in the other organization or not. In the case that an individual has been previously registered, then an enrolment is done while disabling the fingerprint collection section. However, if otherwise, the enrolee can be registered including the fingerprint collection.

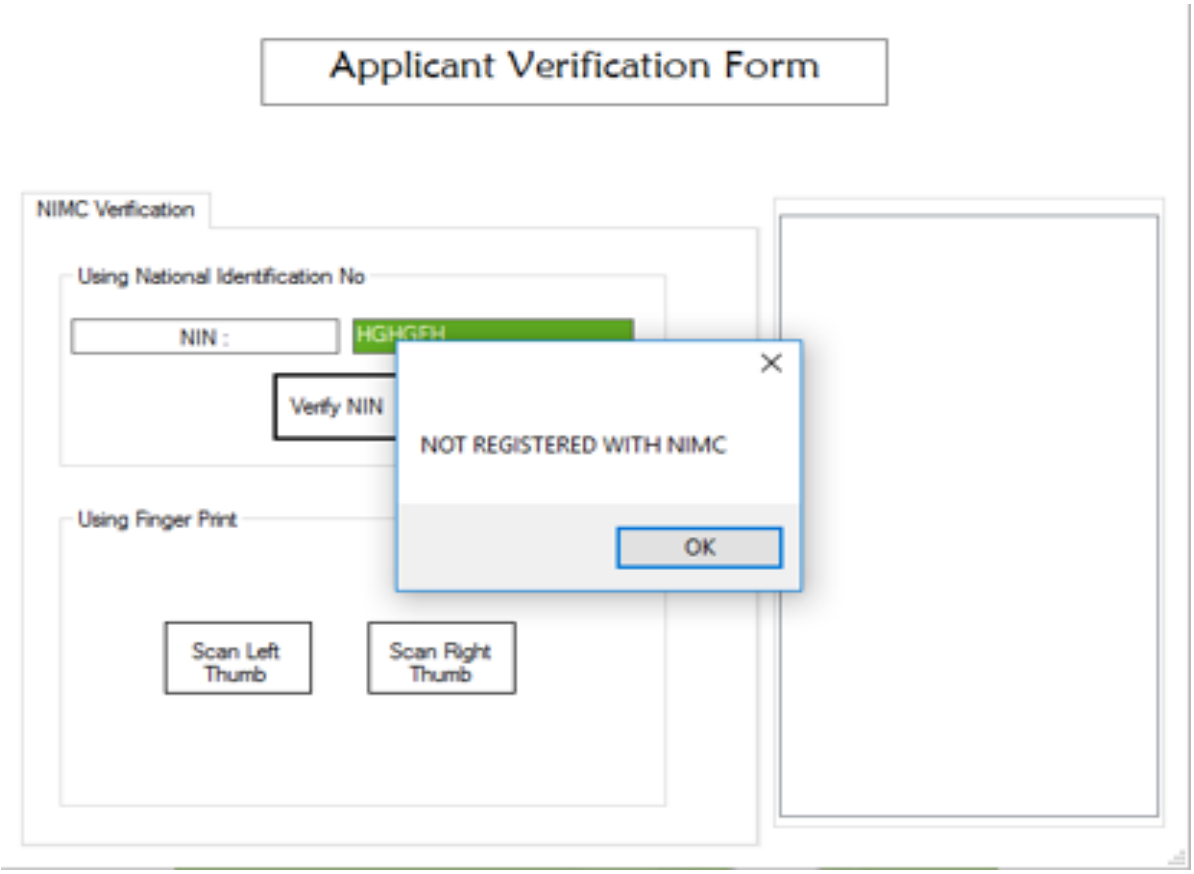

Figure 4.9: Verification Platform for Applications

4.e Security Control of System

In order to keep the system safe, security control measures have been incorporated via the administration module of the system. Two categories of users of the system have been defined; the admin (level 1) and the ordinary users (level 2) who are staff in the organization who can capture people's data through the enrolment module. The ordinary users can also verify enrolees, however, they cannot perform tasks such as adding users, modifying the database etc., this are tasks specific to the admin. Among other things the admin can also do, is to lock the account of staff (in case of breach of policies, for example) to prevent access to the system.

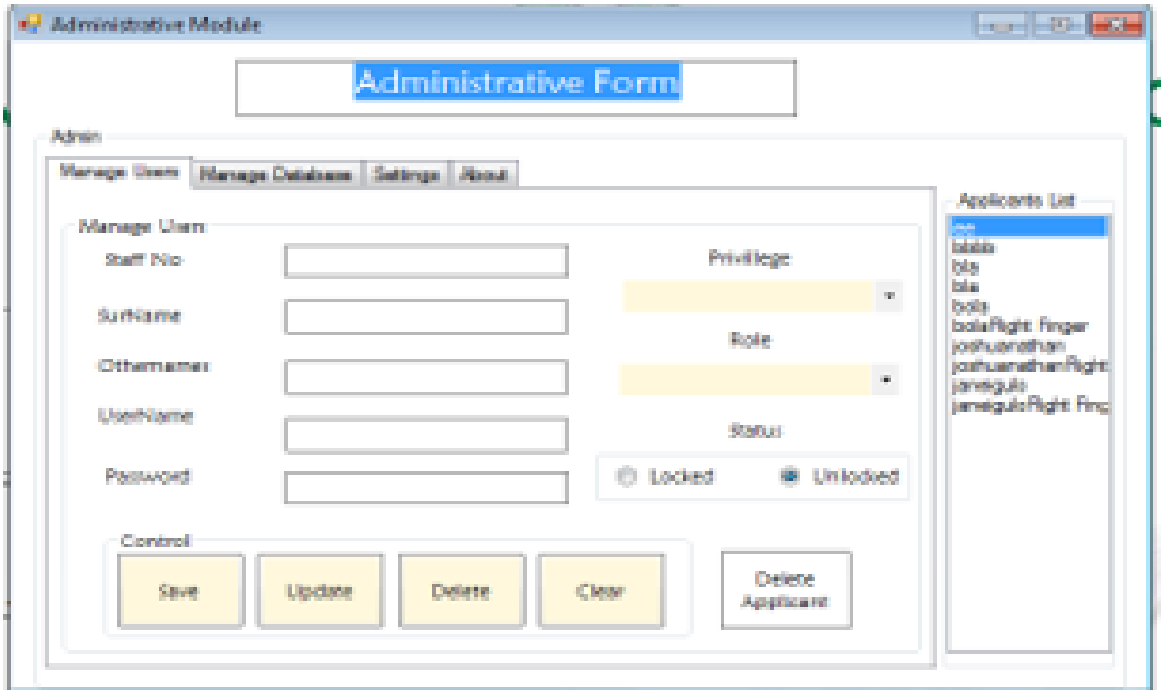

Figure 4.10: Admin's control panel

CHAPTER 5

SUMMARY, CONCLUSION AND RECOMMENDATION

5.a Summary

This thesis presented a framework for different organizations, providing a common platform among them to carry out authentication of individuals they want to enrol into their organization. The data collected for use included biometric information like fingerprint and facial image, while other basic information for identifying the individuals was collected too. This includes name, address LGA, state, gender etc. The above-mentioned data were used to create databases for the different organizations that were represented (NIS, INEC, Banks, NIMC). After this, the interface applications were designed using C#.net.

5.b Conclusion

This research work developed a platform that can easily be adopted by the other organization and NIMC in achieving their long time plan of integrating the biometric information from different organizations. The platform further gives ease for authentication of Nigerians from any organization location that has access to the central database. This, it will stop the long time culture of continuously collecting and storing biometric information of individuals by various organizations while still having no use in authenticating an individual from any point outside the collecting organization. Just as in the case of the BVN which the central bank has used to create harmony across commercial banks, this platform will also create harmony across various government organizations and agencies by giving them a central point for authenticating an individual independent of the organization where this individual's biometrics was previously captured.

5.c Recommendation

After successfully developing this framework to serve as a wrapper for biometric information captured by various organizations, the following recommendations are made:

1. The framework should be implemented and deployed for use by the NIMC as a platform upon which a nation-wide identity system can be built.

2. Government should strictly urge and enforce other organizations against indiscriminate collection of biometric information of its citizens. Henceforth, any new capturing of biometrics should be verified first from NIMC, the central point from which other organizations can make use of for authentication/verification.

5.d Suggestions for Further Work

In further research, the following points are raised as suggestions:

- Other biometric traits such as iris and facial recognition should be included as options for authentication and not only fingerprint.
- To achieve a better platform, better SDKs should be used in building the applications. The one used for this thesis work was a free trial version with various limitations.
- In addition, various fingerprint readers with different formats can be used in order to have different formats for saving the fingerprints to add a more realistic flavour to the work.

REFERENCES

Ahuja, M. S., & Chabbra, S. (2011). Biometric encryption: Combining fingerprints and cryptography. *Communications in Computer and Information Science*, *169 CCIS*, 505–514. https://doi.org/10.1007/978-3-642-22577-2_69

Bala, D. (2008). Biometrics and information security. *Proceedings of the 5th Annual Conference on Information Security Curriculum Development - InfoSecCD '08*, 64–66. https://doi.org/10.1145/1456625.1456644

Bamigbade, K., & Onifade, O. (2014). Gehe : a Mul Tif Actored Model of Soft and Hard Biometric Trait for Ease of. *IEEE*.

Bolade, P. (2015). Active Telephone Lines In Nigeria Hit 145.4 Million – NCC. Retrieved January 1, 2001, from http://techcabal.com/2015/06/05/active-telephone-lines-in-nigeria-hit-145-4-million-ncc/

Breedt, M., & Martin, O. (2004). Using A Central Data Repository For Biometric Authentication In Passport Systems. *Issa*, (2054024), 1–12. Retrieved from http://dblp.uni-trier.de/db/conf/issa/issa2004.html#Breedt04

Charles, W., Patrick, G., & Ramaswamy, C. (2007). *SP 800-76-1. Biometric Data Specification for Personal Identity Verification*.

Chaurasia, O. P. (2012). An Approach to Fingerprint Image Pre-Processing. *International Journal of Image, Graphics and Signal Processing*, *4*(6), 29–35. https://doi.org/10.5815/ijigsp.2012.06.05

Clement, I. (2017). FG to merge BVN, driver's licence, National Identity card. Retrieved October 20, 2017, from http://www.tribuneonlineng.com/fg-merge-bvn-drivers-licence-national-identity-card/

Daugman, J. (2000). Biometric decision landscapes. *Technical Report-University of Cambridge Computer Laboratory*, (482), 13. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.14.3071&rep=rep1&type=pdf

De Luis-García, R., Alberola-López, C., Aghzout, O., & Ruiz-Alzola, J. (2003). Biometric identification systems. *Signal Processing*, *83*(12), 2539–2557. https://doi.org/10.1016/j.sigpro.2003.08.001

Deepika, & Soni, N. (2013). Database Security: Threats and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5), 810–813.

Retrieved from http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0309.pdf

Dessimoz, D., & Champod, C. (2008). Linkages between Biometrics and Forensic Science. *Handbook of Biometrics*, 425–459. https://doi.org/10.1007/978-0-387-71041-9_21

Edgar, H. (2006). *THE SCIENCE OF FINGERPRINTS Classification and Uses*. Federal Bureau of Investigation.

El-Sisi, A. (2011). Design and implementation biometric access control system using fingerprint for restricted area based on Gabor filter. *International Arab Journal of Information Technology*, *8*(4), 355–363.

En, Z., Jianping, Y., & Guomin, Z. (2005). Fingerprint matching based on global alignment of multiple reference minutiae. *Journal Pattern Recognition*, *38*(10), 1685–1694. https://doi.org/10.1016/j.patcog.2005.02.016

Holland, C. D., & Komogortsev, O. V. (2014). Software framework for an ocular biometric system. *Etra*, 365–366. https://doi.org/10.1145/2578153.2582174

Jain, A. (2010). *Automatic Fingerprint Matching Using Extended Feature Set*.

Jain, A. K., & Feng, J. (2016). Latent Fingerprint Matching, (January 2011), 1–27. https://doi.org/10.1109/TPAMI.2010.59

Kozievitch, N. P., da S. Torres, R., Park, S. H., Fox, E. A., Short, N., Abbott, A. L., … Hsiao, M. (2010). Rethinking Fingerprint Evidence Through Integration of Very Large Digital Libraries. *VLDL Workshop at 14th European Conference on Research and Advanced Technology for Digital Libraries (ECDL2010)*, 23–30.

Kulkarni, S., & Urolagin, S. (2012). Review of Attacks on Databases and Database Security Techniques. *International Journal of Emerging Technology and Advanced Engineering*, *2*(11), 253–263. Retrieved from https://pdfs.semanticscholar.org/d9b9/cf28733684fbc679c3517f69a12241942b93.pdf

Mahfouz, A., Mahmoud, T. M., & Eldin, A. S. (2017). POSTER: A Behavioral Biometric Authentication Framework on Smartphones. *ASIA CCS '17 (12th ACM SIGSAC Symposium on Information, Computer and Communications Security)*, 923–925. https://doi.org/10.1145/3052973.3055160

Malik, M., & Patel, T. (2016). Database Security - Attacks and Control Methods. *International Journal of Information Sciences and Techniques*, *6*(1/2), 175–183. https://doi.org/10.5121/ijist.2016.6218

Maltoni, D., Maio, D., Jain, A., & Prabhakar, S. (2009). *Handbook of Fingerprint Recognition* (2nd ed.). London: Springer-Verlag.

Mohammed, N., & Rajesh, R. (2015). Fingerprint image enhancement: algorithm and performance evaluation. *International Journal of Innovative Research in Computer and Communication Engineering*, *3*(1).

Namburu, P. (2007). *A Study and Review on Fingerprint Image Enhancement and Minutiae Extraction*. Rourkela.

Pal, D., & Khethavath, P. (2016). Security in Computing and Communications, *625*, 146–156. https://doi.org/10.1007/978-981-10-2738-3

Rajharia, J., & Sharma, A. (2013). Fingerprint-Based Identification System : – A Survey, *1*(3), 98–101.

Ramez, E., & Navathe, S. (2011). Chapter 2 : outline. In *Fundamentals of Database Systems* (6th Editio, pp. 1–26). Pearson Addison-Wesley.

Rotimi, J., Francis, O., Adebayo, O., & Owolabi, O. O. (2013). Creation of Central National Database in Nigeria : Challenges and Prospects, *3*(12), 6–14.

Sapkal, S., & Deshmukh, R. R. (2016). Biometric Template Protection with Fuzzy Vault and Fuzzy Commitment. *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '16*, 1–6. https://doi.org/10.1145/2905055.2905118

Savvides, M. (n.d.). *Introduction to Biometric Technologies and Applications*. *Carnegie Mellon CyLab*.

Schellberg, T. (2015). Global Expansion of Offender DNA Databases. Retrieved from http://www.wsp.wa.gov/.../dna/.../Global_Expansion_Of_Offender_DNA_Databases_By_Sc...

Schulz, S. (2005). The German Biometric Strategy Platform Biometrics State of the Art , Industry Strategy Development , and Platform Conception Study. *International Organization*.

Sharma, K., & Agarwal, P. (2016). Review Paper on Fingerprint Biometric and Security, *7*(4), 240–247.

Sukhai, N. B. (2004). Access control & biometrics. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development - InfoSecCD '04*, 124. https://doi.org/10.1145/1059524.1059552

Taha, K. E., & Norrozila, S. (2015). A Survey of Multi-Biometrics and Fusion Levels. *Indian Journal of Science and Technology, 8*(32). https://doi.org/10.17485/ijst/2015/v8i32/91488

The Irish Council for Bioethics. (2009). *Biometrics: Enhancing SEcurity or invading Privacy?*

The Scoop. (2015). "How many Nigerians to vote, how many candidates to run…": Jega had the answers yesterday. Retrieved September 11, 2017, from http://www.thescoopng.com/2015/01/14/many-nigerians-vote-many-candidates-run-jega-answers-yesterday/

Udo, B. (2015). BVN: Over 20.8 million customers enrol 40 million bank accounts. Retrieved August 11, 2017, from https://www.premiumtimesng.com/news/top-news/192328-bvn-over-20-8-million-customers-enrol-40-million-bank-accounts.html

Uz, T., Uz, T., Bebis, G., Bebis, G., Erol, A., Erol, A., … Prabhakar, S. (2007). Minutiae-Based Template Synthesis and Matching Using Hierarchical Delaunay Triangulations. *2007 First IEEE International Conference on Biometrics: Theory, Applications, and Systems*, 1–8. https://doi.org/10.1109/BTAS.2007.4401958

APPENDIX

Code snippet from NIMC main form

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Text;
using System.Windows.Forms;
using Neurotec.Biometrics;
using Neurotec.Gui;

namespace CSharpSample
// used to group all the classes used
{
    public partial class MainForm : Form
 {
        Nffv _engine;
// string variable to access the main class in the DLL responsible for capturing fingerprint templates
        string _userDatabaseFile; // variable to hold the name of the database file containing the name of users captured during scanning.
        UserDatabase _userDB;
        public MainForm(Nffv engine,string userDatabaseFile)
//this is a constructor, which has the same name as the form, taking the default argument once the form is instantiated.
 {
 _engine = engine; // assigning the engine classes to a variable so that it can be used in the application

 _userDatabaseFile = userDatabaseFile; // the userdatabase file is assigned to variable.

 try
 {
 _userDB = UserDatabase.ReadFromFile(userDatabaseFile); //read method which enables reading user details from and store in an instantiated database object.
```

```
}
catch
{
_userDB = new UserDatabase(); // if cannot read then instantiate a new database object and store in the
    variable.
}
                InitializeComponent();
        }


        private void MainForm_Load(object sender, EventArgs e)
{
if (connectDB.DisableControl == "userlevel2") //used at the admin form to disable and enable controls
    depending on user privileges
{
this.Show();
}
else if(connectDB.DisableControl == "userlevel1")
{
this.Show();
}
else
{
this.Hide();
}
                foreach (NffvUser engineUser in _engine.Users) //loop through to obtain the records of
    all users in the database file
                {
                        string id = engineUser.Id.ToString(); //obtain their id
                        UserRecord userRec = _userDB.Lookup(engineUser.Id); //use id to obtain and
    pull out record
                        if (userRec!= null)
                        {
                                id = userRec.Name;
                        }
                        lbDatabase.Items.Add(new CData(engineUser, id)); //add the stored list to the
    listbox for all items.
```

```
                }
                if (lbDatabase.Items.Count > 0) // count the items in the list box and set the count to the
    first item index.
                        lbDatabase.SelectedIndex = 0;
if (connectDB.StatusControl == "locked") // lock account based action of the admin at the admin form.
{
button1.Enabled = false;
button2.Enabled = false;
button3.Enabled = false;
button4.Enabled = false;
MessageBox.Show("ACCOUNT LOCKED! SEE THE ADMINISTRATOR");
}
else
{
button1.Enabled = true;
button2.Enabled = true;
button3.Enabled = true;
button4.Enabled = true;
}
        }
        internal class EnrollmentResult // class that is instantiated to store records of the result after
    enrollment has taken place
        {
                public NffvStatus engineStatus;
                public NffvUser engineUser;
        };

        private void btnEnroll_Click(object sender, EventArgs e)
        {
EnrollForm enrollDlg = new EnrollForm(); // dialog that captures the name of user to be associated with
    the scanned template.
if (enrollDlg.ShowDialog() == DialogResult.OK)
{
try
{
```

```
RunWorkerCompletedEventArgs taskResult = BusyForm.RunLongTask("Waiting for fingerprint...", new
    DoWorkEventHandler(doEnroll),
false, null, new EventHandler(CancelScanningHandler));
EnrollmentResult enrollmentResult = (EnrollmentResult)taskResult.Result;
if (enrollmentResult.engineStatus == NffvStatus.TemplateCreated) // create the template after finger has
    been scanned
{
NffvUser engineUser = enrollmentResult.engineUser;
string userName = enrollDlg.UserName;
if (userName.Length <= 0)
{
userName = engineUser.Id.ToString();
}

pbExtractedImage.Image = engineUser.GetBitmap(); scanned fingerprint is displayed in the picture box
lbDatabase.Items.Add(new CData(engineUser, userName));
lbDatabase.SelectedIndex = lbDatabase.Items.Count - 1; // update database and count
}
else
{
NffvStatus engineStatus = enrollmentResult.engineStatus;
MessageBox.Show(string.Format("Enrollment was not finished. Reason: {0}", engineStatus));
}
}
catch (Exception ex)
{
MessageBox.Show(ex.Message);
}
}
}
```

```
        private void doEnroll(object sender, DoWorkEventArgs args) //method responsible for the
    enrollment process used by creating enrollment result object and also capturing the fingerprint
    through the scanner and displaying the result of the scan.
        {
                EnrollmentResult enrollmentResults = new EnrollmentResult();
```

```
            enrollmentResults.engineUser = _engine.Enroll(20000, out
enrollmentResults.engineStatus);
            args.Result = enrollmentResults;
    }
    internal class VerificationResult // class responsible for displaying the result of vverification
done,including the score.
    {
            public NffvStatus engineStatus;
            public int score;
    };


    private void btnVerify_Click(object sender, EventArgs e) // button event that handles the
verification process
    {
            if (lbDatabase.SelectedIndex < 0)
            {
                    MessageBox.Show("Please select a record from the database.");
            }
            else
            {
                    try
                    {
                            RunWorkerCompletedEventArgs taskResult =
BusyForm.RunLongTask("Waiting for fingerprint...", new DoWorkEventHandler(doVerify),
                                    false, ((CData)lbDatabase.SelectedItem).EngineUser, new
EventHandler(CancelScanningHandler)); // scanning finger to create the template as well as pulling
template out of database.
                            VerificationResult verificationResult =
(VerificationResult)taskResult.Result;
                            if (verificationResult.engineStatus ==
NffvStatus.TemplateCreated)//comparring created template with stored stored template in the
database.
                            {
                                    if (verificationResult.score > 0) // comparing verification result
to threshold value to determing if scanned finger and template match.
                                    {
```

```
                                        MessageBox.Show(string.Format("{0}
verified.\r\nFingerprints match. Score: {1}", ((CData)lbDatabase.SelectedItem).Name,
verificationResult.score));
                                }
else
                                {
                                        MessageBox.Show(string.Format("{0} not
verified.\r\nFingerprints do not match. Score: {1}", ((CData)lbDatabase.SelectedItem).Name,
verificationResult.score));
                                }
                        }
                        else
                        {
                                MessageBox.Show(string.Format("Verification was not finished.
Reason: {0}", verificationResult.engineStatus));
                        }
                }
                catch (Exception ex)
                {
                        MessageBox.Show(ex.Message);
                }
        }
    }
    private void doVerify(object sender, DoWorkEventArgs args) // private class that calls on the
internal class by creating object for each verification done
    {
        VerificationResult verificationResult = new VerificationResult();
        verificationResult.score = _engine.Verify((NffvUser)args.Argument, 20000, out
verificationResult.engineStatus);
        args.Result = verificationResult;
    }
    private void CancelScanningHandler(object sender, EventArgs e) // method called if the scanner
was unable to verify or enroll a user object.
    {
        _engine.Cancel();
    }
                _engine.Users.RemoveAt(lbDatabase.SelectedIndex);
```

```
                lbDatabase.Items.RemoveAt(lbDatabase.SelectedIndex);
                if (lbDatabase.Items.Count > 0)
                        lbDatabase.SelectedIndex = 0;
        }
    }

    private void btnClearDatabase_Click(object sender, EventArgs e) // clear the entire database records both the xml file and the.dat file.
    {
        if (MessageBox.Show("All records will be deleted from database. Do you want to continue?", "Confirm delete", MessageBoxButtons.YesNo, MessageBoxIcon.Question)!= DialogResult.Yes)
        {
            return;
        }

        _engine.Users.Clear();
        lbDatabase.Items.Clear();

        _userDB.Clear();
        try
        {
            _userDB.WriteToFile(_userDatabaseFile);
        }
        catch { }
    }
```