**CHAPTER ONE**

**INTRODUCTION**

* 1. **Background of Study.**

The term biometric is characterized from two Greek words 'bio' signifies life and 'metric' signifies estimation. As per International Standard Organization (ISO), biometric signifies "computerized acknowledgment of people based on their physiological and behavioral attributes". Each individual can be uniquely distinguished based on physiological and behavioral attributes (Zhang, 2009). A biometric framework is a mechanized technique for confirming the identity of a living individual based on physiological and behavioral attributes. It is otherwise called human identifier or human authenticator.

The different biometric perspectives used for individual recognizable proof are: fingerprints, face, hand geometry, palm print, finger veins, gait signature, DNA acknowledgment, iris, facial appearance, voice and so forth. Fingerprint recognition includes catching the images of fingerprints and putting them in information base. The properties of ridges, cores and deltas, whorl, and minutiae points can give a unique identification design (Zhang, 2003; Sarasvati, 2011).

Face is legitimately connected with identity, gender, and age group. Face recognition contains two viewpoints, in particular; face appearance and face expression (Jain, 1998). The facial appearances of an individual can be effortlessly emulated by someone else. In this way, it ought to be joined with non-verbal communication and voice for distinguishing an individual.

The hand geometry based systems measure a client's hand in numerous measurements for example hand length, finger length, finger width, palm length, and palm width. The Charge Couple Device (CCD) camera peruses the hand shape by recording the outlines and these outlines are used for recognizing an individual. In palm prints based identification methods the palm print image of an individual is caught by CCD camera and it is contrasted and the real image stored in the database This coordinating technique depends on palm attributes (principle lines, wrinkles, ridges, and minutiae points) (Zhang, 2003; Nicolae, 2009).

Deoxyribonucleic Acid (DNA) has a twofold helix structure and it gives the most reliable outcome for disconnected individual identification excluding indistinguishable twins’ cases. Each human has a unique DNA arrangement excluding indistinguishable twins. The fraternal twins have diverse DNA sequence and indistinguishable twins have precisely same DNA arrangement. DNA grouping comprises of four letter sets specifically: Adenine (A), Guanine (G), Cytosine(C), and Thymine (T). The obscure nucleotide (N) present in a DNA succession can be either Adenine or Guanine or Cytosine or Thymine (Mishra, 2011).

An iris is gotten subsequent to eliminating pupil, eye brow, skin and other unsettling influences from the eye of an individual. The iris picture comprises of Red (R), Green (G), and Blue (B) colors and every individual including indistinguishable twins has a unique iris. In this manner, an iris based framework can be considered as a solid and secure framework for individual identification (Daugman, 2007).

In voice based recognition techniques the input voice is caught by voice handling machine and the machine uniquely distinguishes an individual based on voice attributes (frequency, emphasis, stream, and rhythm and so on.) (Chetty, 2009). Two people may have same palm print, hand geometry, and finger veins yet every individual has unique fingerprints, iris image, and DNA grouping excluding indistinguishable twins. An identical twin pair may contrast in fingerprints and iris pictures yet they may have a similar DNA arrangement. The fingerprints and irises deteriorate not long after the passing of an individual yet the DNA grouping never breaks down. Consequently, it is consistently critical to utilize fingerprints, iris image, and DNA features based multi-biometric framework for distinguishing an individual.

Therefore, the need for adoption of strategies in verifying the identities of individuals in our world today cannot be over-emphasized. It is a standard practice to give a disclaimer on a person(s) that is/are not identified with a particular association to caution the overall population on the peril of ensuing exchange with the individual; yet; this data some of the time gets to the proposed beneficiaries when some fake demonstrations may require been submitted. So we currently board a time when everybody ought to be cautious and mindful to the identity of everybody in his/her environment for this can work a tool to ensuring national security strategy. Recurring security difficulties and danger of false identity claims in our general public concerns a holistic approach from stakeholders to beat this ugly trend.

Human identification could be a fragile idea which needs consideration in all levels of management. Occurrences of artificial identity pullulate with the nation. It becomes convoluted when the task of checkmating individuals' identity is left for the enforcement agencies alone. Accordingly, there is the prerequisite for the occasion of a fundamental enrolment and verification of people be applied all over and whenever.

Considering that, the formation of the National Identity Management Commission (NIMC) was done in 2007, to set up and control a dependable and practical arrangement of national identity management that will empower a resident or lawful inhabitant to declare his identity and subsequently help in following crimes through criminological assessment of natural traits (Akinlabi, 2014). This is accomplished through the registration of a person by the commission, storing his/her biometric information in a data set and thus converting such stored data into a unique National Identification Number (NIN).

The National Identification Number (NIN) is a non-savvy set of numbers appointed to individual upon fruitful enrolment (Levine, 2014). Enrolment comprises of the recording of someone's segment information and capture of the ten (10) fingerprints, head-to-shoulder facial picture, which are completely acclimated cross-check existing information inside the National Identity Database to confirm that there is no past section of the identical  information. When this measure is finished the data is then stored with a unique NIN that was appointed thereto. The NIN once given to an individual cannot be used again (that is, it cannot be given to an alternate individual whether the past individual is dead). It is the NIN that assists to tie all records of several individual inside the information base and is used to test the identity confirmed.

As stated by Levine (2014), since independence, Nigeria has consistently perceived the need to record the identity of Nigerians and non-residents using biographic information. An attempt to fulfill this need was initiated in 1978 under the Department of National Civic Registration (DNCR), which was charged with registering and giving a National positive distinguishing proof to every citizen of Nigeria who was then 18 years or older.

As stated by Akanbi (2014), the government's essential target at that point was to utilize this program as a productive tool for controlling unlawful movement, to approve other civic documents like travel international IDs, and to arrange a dependable individual identification system for protecting business exchanges with financial institutions. The development of the information and communication technology environment is in the middle of new and high technological threats. Cyber-attacks presently have the adaptability to significantly harm the general public in new and demanding ways.

There is currently no centralized national identity information database and no system of National Identity Management which effectively connects public and individual segment identity plans. While the financial service sectors has been generally proactive within the deployment of distinguishing proof plans for conveyance of its administrations, the plans have contrasted from establishment to establishment within the world. The result has been the creation of several different identification schemes and databases resulting in the duplication of an individual’s identity data by the assorted institutions offering services to it person. Government organizations additionally hold assortment of information bases with no practical incorporation of access or interoperability to support the conveyance of administrations inside these government institutions.

The biometric technologies like fingerprint, face and iris recognition have seen an expanding enthusiasm all through the previous years. Such intrigue has been escalated with different huge scope activities from governments that try to corporate biometric technologies for the aim of identification and verification. Far from being simply ad-hoc technological implementations, biometric devices are presently seen as being vital worth and thus of vital significance. With the view of higher proficiency and viability, governments are embarking to grasp biometric advancements particularly within the identification and verification process of National Identity Management Commission (NIMC).

**1.2 Statement of the Problem**

In a quest to meet up with the National Security Strategy, especially with respect to the nation citizen’s identification and verification, biometrics has a great role to play as it narrows down it functions to the identification and verification of Nigerians and legally authorized immigrants in the country. The need for a unique biometric adoption and a centralized database to be implemented by the Government through the National Identity Management Commission (NIMC) cannot be over-emphasized as multiple conflicting information are generated and found by different government and private agencies. In order to achieve this, this dissertation aim to assess the NIMC biometric system and propose the need to adopt a unique iris biometric technology to compliment the pre-existing facial and fingerprint enrollment and verification process which pose to have lots of vulnerabilities associated with them examples are errors with the dryness or dirt of the finger's skin, as well as with the age. This consequently will differ in a way of biometric data collections from different agencies.

**1.3 Aim and Objectives**

The aim of this work is to evaluate the National Identity Management Commission (NIMC) biometric system and propose an Iris recognition technique that will enhance their biometric systems. The objectives of this research work include:

1. To evaluate fingerprint and facial biometric technology as used by NIMC
2. To evaluate Iris biometric technology.
3. To evaluate a multi-biometric system based technique.
4. To suggest recommendations in ensuring National security strategy is achieved by NIMC through the adoption of Multi-biometric system based technique.

**1.4 Significance of the Study**

The need for human identification is as old as man. In an exceedingly form of contexts, each person have to identify other individuals so as to carryout conversation or transact business. Organizations also seek to spot the individuals with whom they are doing business with so as to supply better service to them and to shield their interests (Jain, et al, 2006). Developments in technology has ushered in vast growth in organizational size, and distance between organization and other people to the extent that individuals who demur when asked for evidence of identity are frequently presume to “have something to hide” (Roger, 2013). The growing trend of terrorism, kidnapping, identity fraud, impersonation, etc. has influenced people and their governments to require action and be more proactive in security matters. This has necessitated the decision for a fast and reliable method of verifying the identity of individuals within the country. Virtually all countries of the planet have developed one or more sort of identification for its citizens.

**1.5 Scope of the Study**

The scope of this research is to review biometric system base technique used by the National Identity Management Commission (NIMC). This research tends to evaluate the basic biometric technologies used by the NIMC namely the fingerprint and facial recognition technique. This work will subsequently cover the biometric devices, operations and vulnerability associated.

**1.6 Limitations of Study**

The limitations of this research includes availability of data and time constraints. Due to the current security challenges and the study’s sensitive nature, accessing willing individuals to give privileged information constitutes a limitation. Also, due to the spread of the Corona virus across the globe and Nigeria in particular, getting door to door response from a vast populace became a huge limitation as this would have helped in getting a better feedback from Nigerians especially the aged persons who have registered and are willing to share their experience on the processes and challenges encountered during registration and verification.

**1.7 Research Questions**

This research work seeks to answer these questions;

1. What are the basic biometric data captured during the NIMC enrollment process?
2. What are the limitations of fingerprint and facial biometric data capture?
3. Are there security vulnerabilities associated with the pre-existing biometric data capture?
4. Is our biometric information safe in the NIMC database?

**1.8 Dissertation Organization**

This research work is divided into five chapters. The first chapter is the introduction which discusses the study’s background, statement of the problem, objectives of the study, research questions, and operational definition of terms. Also included in this chapter is the scope of the research and limitations.

The second chapter will be devoted to the literature review and theoretical framework to provide fundamental and historical background to the study of Biometrics, its technological adoption by the National Identity Management Commission (NIMC). This review includes the sources and channels through which NIMC employ Biometrics technology to improve national security strategy.

The third chapter will cover research methodology taking into account the research question validity and reliability, sample and sampling technique(s), data collection technique and finally the data analysis technique(s) employed in the research.

The fourth chapter will discuss analysis, the assessment of data collected, and research findings. Finally, the fifth chapter contains the summary and conclusion of research work and a recommendation.

**1.9 Definition of Terms**

**Cyber security:** Cyber security is the protection of internet- connected systems and resources like hardware, software and data from cyber - attacks.

**Biometrics**: this is often the automated use of physiological or behavioral characteristics to work out or verify identity.

**Biometric System:** This is often essentially a pattern recognition system that recognizes someone by determining the authenticity of a particular physiological and or behavioral characteristics possessed by the person.

**Authentication**: is additionally frequently employed in the biometric field sometimes as a synonym for verification; actually, within the information technology language authenticating a user means to let the system know the users identity no matter the mode (verification or identification).

**Templates**: are samples of Biometric trait extracted and stored within the biometric system for the aim of subsequent comparisons so as to be verified or identified after enrollment.

**Sensor:** The sensor is a device which transfers the important biometric information of the user into the electrical information then into the digital information.

**Biometric Matching:** The comparison of biometric templates to work out the degree of similarity or correlation is named matching.

**False Rejection Rate (FRR):** This occurs when the biometric system cannot perform a proper match and (incorrectly) rejects a legitimate user

**False Acceptance Rate (FAR):** This occurs when the system incorrectly match a biometric to the wrong stored reference sample, resulting in misidentification.

**Act**: An act is a Bill which has passed through various legislative that is required for it to become a law.

**Information Technology**: The study or use of systems which will be used for storing, retrieving, and sending information.

**Know Your Customer** **(KYC):** is the process of a business verifying the identity of its clients and assessing their suitability, together with the potential risks of illegal intentions towards the account.  
**Security**: Security may be defined as a defence put in place to measure and protect systems for intruders and unauthorized users.

**Policy**: Policy may be a course of action that's proposed by an Organization or government in reference to a selected issue.

**CHAPTER TWO**

**LITERATURE REVIEW**

**2.1 Introduction**

The use of biometric technologies by the government through the National Identity Management Commission (NIMC) has drastically diminished the issue of misidentification by people, private divisions, and public segments and in carrying out different transactions. This is frequently done by gathering biometric samples of individual during enrollment and converting it into a unique National Identification Number (NIN), under which the individual data are stored and may be accessed thereof. Although various divisions have formulated the easiest method of distinguishing her clients and staff by giving them a unique card which carries hardly any tangible data, it is also key to get a dependable and less vulnerable biometric data of every person in a country and guarantee it is stored in an incorporated government database which might be shared or accessed by other organization for uniformity and validity. In a journey to accomplish a greatly improved and dependable biometric security the need to survey other related literature will be done in this chapter.

**2.2 The National Security Strategy of the Federal Republic of Nigeria.**

The National security strategy of Nigeria was created and published by the Office of the National Security Adviser in 2014, the Nigeria National Security Strategy manages the formulation of policies and conduct of operations. Nigeria's overall vital vision is to frame a quiet, independent, prosperous, solid nation" (Bala & Ouédraogo, 2018). The hidden goal is to utilize all components of national capacity to ensure physical security, build individual and collective prosperity, cause national development and advance Nigeria impact in local, continental and worldwide undertakings.

The National Security Strategy 2014 addresses two critical threat areas:

**a. National Security Interests:** The core national interests as defined in Nigeria's National Security Strategy are the protection and government assistance of its people; sway and safeguard of its regional trustworthiness; harmony; democracy; monetary and or economic development; and social equity. Sub-regional security and economic cooperation are delegated key interests. Promotion of peace, security, development, democracy and international participation in Africa and along these lines the world are fringe to Nigeria national interests.

**b. Threats to National Security:** The first strong threat to Nigerian national security incorporate global challenges; terrorist oppression; transnational organized crimes; rock oil robbery or unlawful bunkering; Nigeria's borders; environmental change; shared and ethno-religious clashes; pastoralists and ranchers clashes; legislative issues and federalism in Nigeria; governance; destitution; kidnaping, expansions of small arms and lightweight weapons; multiplication of weapons of mass devastation; illicit relocation; monetary difficulties; budgetary violations; data innovation and cyber security; natural, man-made and clinical related dangers.

The threats counted above are in no way, shape or form the sole threats to Nigeria national security. They are in any case the premier intense and are pronounced possible sources of antagonism, discontent and precariousness that may adversely influence the nation search for national stability, solidarity and development.

**2.3 National Cyber Security Strategy.**

Conventional crimes can easily be checked through physical measures including discovery, examination, apprehension and arraignment. Adopting traditional methods requires the employment of physical methods nonetheless, when these violations become digitalized, extreme inconveniences emerge, making the arrangements unwieldy or at times, infeasible to look out. Digitalization of crimes have given enforcement  officers changes in conventional crime, resulting from the technicalities involved, advancements in crime commission methods, increased anonymity, reduced possibility of successful criminal profiling amongst others.. Thus, customary techniques for tackling violations got unhelpful with the computerization of those crimes.

Odumesi (2014) embraced a working meaning of cybercrime in Nigeria from the technological and sociological viewpoints, characterizing it as "a crime including the maltreatment or abuse of digital assets during a digital domain or through the web, computer networks, computer systems and wireless communication systems." Blitz (2009) defined cybercrime as "misuses and abuses of computer systems or computers connected to the web, which end in direct and/or concomitant losses and also criminal activity that has been facilitated via the web." Loader and Thomas (2000) had clarified, "Cybercrime will be believed to be computer mediated exercises which are unlawful or considered illegal by specific gatherings and which might be conducted through worldwide electronic networks".

Consequently, cyber security policy and procedures give a structure of core values and activity plans intended for network safety and its related occurrences. The strategy handles cybercrimes, digital illegal intimidation (cyber terrorism), digital undercover work (cyber espionage), and online ill- usage and exploitation (Osho & Onoja, 2015).

Being an issue of national priority in Nigeria, cyber security is presently raised to the measure of being taken care of by the Presidency through the Office of the National Security Adviser (ONSA). In an action plan drafted by the Office of the National Security Adviser for the implementation of national cyber security strategy, some of the objectives among others include:

1. To ensure people and associations are mindful to their obligations when handling individual data. Define minimum standard and technical requirements to safeguarding personal information from been compromised by NIMC.
2. To find out and keep up a dependable information communication and transaction condition by giving Public Key Infrastructure (PKI) and digital certificate management administrations with global acknowledgment. Improve security of electronic communications and transactions.

**2.4 National Identity Management Commission (NIMC)**

The NIMC Act 2007 provides for the establishment of the NIMC, its functions, powers the establishment of the National Identity Database, assignment and use of general multi-purpose cards and also the National Identification Number (NIN). The Act also provides the Commission with powers to form regulations connected with its functions. NIMC Act 2007 provides for the repeal of the law that created the previous Department of National Civic Registration (DNCR) and also the transfer of its assets and liabilities to the NIMC.

Consequently, the Commission's mandate will be categorized into four major action tracks, namely:

1. Establish the National Identity Management Commission because the primary legal, regulatory and institutional mechanism for implementing Government's reform initiative (in the identity sector) as contained within the National Policy and NIMC Act.
2. Wind up and take over the assets and liabilities of the previous DNCR which does not exist, including the personnel in both the State and local Government Offices nationwide;
3. Establish, operate and manage the National Identity Management System (NIMS):
4. perform the enrolment of citizens and legal residents as provided for within the Act;
5. Create and operate a National Identity Database;
6. Issue Unique National Identification Numbers (NIN) to qualified citizens and legal residents

In the United State of America, driver's licenses given by the individual state and regional governments turned into the true identity cards, and are utilized for several distinguishing proof purposes, similar to when buying some particular products, opening bank accounts, and boarding planes. People who don't drive can acquire an ID card with the comparative usefulness from a similar state organization that gives driver's licenses. Furthermore, numerous schools issue understudy and school ID cards. Likewise, the Social Security as presented in 1935 contains a nine digit number appointed to each legitimate inhabitant of the nation by the United States Social Security Administration Service (Akinyemi, 2014).

According to Akinyemi (2014), two reasons were given as intentions in the Social Security.

1. To separate at least two individuals with the indistinguishable names;

2. To structure a government assistance program that may guarantee laborers would have a source of income after they are resigned.

Thus, in each transaction with government and its organizations, everyone gives his Social Security number after its name. This makes identification much simpler. Some of other information like personal home address, phone number, and date of birth, parent's information, and DNA information, driving record, marriage data and even business record of people are stored with the number. In this manner, an entire life history of an individual will be pulled from the PC (by approved government authorities) alongside his Social Security number. The majority of the identity reports have biometrics imbedded in them which could be a recognition system that works by gaining information from an individual and contrasting it and the template set in the database. Contingent on the unique situation, the identity of an individual will be settled in two different ways; verification and identification. In the former, a person to be distinguished presents a case while in the later an individual is recognized without an individual professing to be distinguished. The two terms are conversely used in writing for biometrics recognition (Jain, et al, 2006).

In Nigeria, the idea of a national identity card was first mooted in 1978 during the rule of Olusegun Obasanjo, the then military head of state. It absolutely was conceived to supply a veritable platform for the identification of citizens of the state. There are no apparent advancement a very long time after with greater part of the populace actually deficient with regards to any conventional national identification. The ID card project has failed to deliver genuine cards to numerous Nigerians. It is been loaded with wild scale corruption and stunning outrage that has hindered the accomplishment of the plan. The corruption case involving several government and party officials was never settled while just a few Nigerians got identity card (Levine, 2014). Usually, a national identity undertaking ought to incite excitement from Nigerians who by and large might want a plan that uniquely recognizes them, but the past narrative of squander and sleaze related to the project greatly eroded public confidence on the scheme notwithstanding the obvious advantages it will give. There has been a reestablished drive by the administration of former President Goodluck Jonathan to revive the project which they trust to be a lasting solution of providing identity to the nation's residents. Critics however dissent, contending it's constantly been the indistinguishable line recently acclimated plunder reserves (Ahaefule, 2013).

As stated by Ahaefule (2013), the government had in 2001 granted a contract worth $214m to a consortium led by French firm Sagem, for the gathering of identity cards for every Nigerian citizens. The contract was damaged in 2003 by charges that Nigerian officials collected quite $2m pay-offs to impact the honor of the project while in 2006, an advisory group on harmonization of national identity cards was established with the order "to survey existing cards extends and suggest methods of incorporating them into one multi-application card". It never worked. The nonappearance of a nationally acknowledged positive identification, has made most organizations, corporations and foundations to put up different systems for identification of its members.

For example, banks would require the ownership of one of a national ID card, valid driver's permit, international passport or a voter card along with a utility bill (electricity bill, water bill, house bill, etc.) receipt before opening an account. The Federal Road Safety Corps (FRSC) requires some personal information furthermore as driving skills before issuing a driver’s license.

Cards are given by all way of associations; Universities issue them to staff and students; government issues them to residents; organizations issue them to their staff. The majority of those cards contain some essential information like name, photo of the persons face and a reference number. The chief basic style of these cards is the plastic kind. It is not exceptional these days for institutions requiring their students to put on their ID card at certain times of the day (Olotu, 2014). This card based systems is famous, on account of its overall simple creation and use. Most nations are presently modernizing their ID information base to join biometric identifiers like fingerprints, iris, face, palm prints, voice and DNA.

Biometric identification is considered the mechanized identification of an individual using either a physiological attributes like fingerprint or behavioral attributes like signature. Most biometrics framework spins round the previously mentioned qualities (Jain, et al 2006). They are used in light of the fact that it is accepted for instance, that no two individuals have the identical patterns within the skin of their fingers. (Obiagwu, 2014).

NIMC is charged with the responsibilities of enrolling each person in Nigeria, setting up and keeping up a national identity information database besides giving of a unique identification number and a general multi- purpose card. The commission intends to include biometrics for its activity. It is equally intended to be used as a voter’s card document in future elections (Levine, 2014). It is as yet indistinct how the card are joined as an identification tool in a heterogeneous nation like Nigeria. Expounding on the significance of getting a solid national identity scheme, Professor of Sociology and Head, academic department, University of Lagos, Dr. Adebayo Ninalowo, said it totally was basic to just decide and build up cases to Nigerian citizenship, for the state to meet its commitments to the residents (Ahaefule, 2013). Narrowing the identification and verification process to Nigeria e-governance, it totally was seen that there exists distinctive identity documents being used inside the nation. There is the general ID card given to all or any qualified resident or staff working in any institution, Driver's permit issued by FRSC, Voters card and international passport. Investigation of a large portion of those cards uncover that it will be tampered with. It very well may be forged, and furthermore the inaccessibility of a verification system that empowers the cards details to be matched to a central information database exposes the weakness of the card. This specific flaw has been exploited by fraudsters to perpetrate crimes. It has helped such practices like impersonator and phantom laborers disorder that are pervasive in the greater part of our public areas.

The modernity in some of the identity cards being used by some establishment today needs some specific and often expensive high end tools to read its data thus restricting its usage. Considering these limitations and with the current caution inside the nation to comprehend our neighbor as a results of the safety circumstance, this work proposes a model for secure biometric confirmation in Nigerian e- governance utilizing a multi biometric technique to upgrade the single and bimodal biometric strategy.

Non- availability of fundamental verifiable biometric and demographic information of a boundless greater part of the general population has been a genuine obstacle to national planning, subsequently the hindered movement of national development and advancement inside the public and individual divisions of the economy. To stem this disagreeable tide, the federal government charged the National Identity Management Commission (NIMC), to create and actualize a decent National Identity Management System (NIMS), for Nigeria within three years. Upon completion, NIMS will help national planning, improve national security; encourage financial incorporation, cultivate advancement of internet business and a national payment system, and furthermore synchronize and coordinate integrate pre-existing identity databases into the national identity information base (Fabunmi & Isa, 2008).

The enrolment exercise will precede the issuance of the unique National Identity Numbers and chip-based identity cards, which can progressively drive the adoption of standardized biometric, demographic and confirmation methods across public and personal organizations in key areas of the economy, bringing about harmonization, coordination and interoperability across numerous systems. Usually, the NIN is used by governments for national planning within the areas of employment creation, tax assessment, medical care and furthermore the conveyance of basic public sector services. The private area, particularly, the financial sub-sector also will benefit enormously from this activity which can validate Know-Your-Customer (KYC) processes, subsequently lessening financial violations. Ultimately, this may help minimize the incidence of fraud in Nigeria, since the biometrics of the ten fingers of each enroller are captured in the NIMS database.

**2.5 Biometric Traits**

According to Yanushkevich (2007), biometrics are ordinarily classified as either physiological or behavioural traits. Physiological traits (sometimes called passive traits) allude to fixed or stable human qualities, similar to fingerprints, shape and geometry of face, hands, fingers or ears, the pattern of veins, irises, teeth, samples of DNA. Physiological characteristics are commonly existent on each person and are unmistakable and permanent, except if mishaps, ailments, hereditary imperfections, or maturity have changed or crushed them. Behavioral traits (active qualities) measure human attributes spoke to by aptitudes or capacities performed by a person. These incorporate stride, voice, key-stroke and mark elements.

The accompanying passages depict the characteristics of the two classifications, which are at times assessed dependent on such attributes as:

1. Universality – Each individual ought to have the biometric characteristic.
2. Uniqueness – Any two people ought to vary with respect to the characteristic.
3. Permanence – The biometric ought to be adequately invariant over a particular time of your time.
4. Collectability – The biometric ought to be quantitatively quantifiable.

It is contended by some that none of the human biometric characteristics meets all the above necessities. Albeit each biometric quality has its qualities and downsides; no biometric is "ideal".

**2.5.1 Physiological Traits**

The physiological traits are the fixed human qualities which incorporate however not limited to the following:

* Fingerprint- Analyzing fingertip patterns.
* Facial Recognition- Measuring facial characteristics.
* Hand Geometry- Measuring the shape of the hand.
* Iris recognition- Analyzing features of colored ring of the eye.
* Vascular Patterns- Analyzing vein patterns.
* DNA

**i. Fingerprint Base Technique**: Fingerprint biometrics is generally seen as a precise biometric affirmation strategy. Today, unique finger impression scanners are accessible effectively and dynamically consolidated in workstations and other flexible ICT devices. As stated by Kong et tal,(2009) most finger impression affirmation structures dismember the stand-out case of edges and valleys, and the arrangement of minimal uncommon keeps an eye on the unique imprint, which are known as subtleties. They can be seen and perceived by their sort, by x-and y- coordinates, and by their direction.

Fingerprint scanners can work with contact based or contactless optical structures. The previous is to be found in laptops and works along these lines to automated cameras by getting an advance image of the fingertip using visible light. While such a sensor gives an unassuming and essential solution, it goes with a couple of drawbacks: when a finger contacts or proceeds onward the scanner surface, the adaptable skin distorts. The nature of the caught picture solidly depends on the entirety and heading of weight applied by the client and the unique imprint may appear to be assorted in each catch. Furthermore, when utilized in huge scope applications, for example, a migration work area, extraordinary sterile consideration should be practiced to dodge earth being conveyed from one finger to the next.

By emitting light on or through the finger and getting the reflected or communicated signals, fingerprints can be taken without contact among skin and scanner. To avoid fake finger attacks, a couple of systems use implied live identification innovation, which abuses the sweat development of human bodies. High-amplification focal points and unique light advancements catch the finger's sweat and articulate the finger in any condition. Application organizers need to consider that fingerprints of a little piece of the general population cannot be utilized for biometric acknowledgment. This can be on the grounds that maturity, incidents, genetic reasons, regular or word related reasons (e.g., development workers may have worn fingerprints or a gigantic number of cuts and wounds on their fingerprints that keep developing).

A number of fingerprint based biometric systems have been created by researchers for identifying a person. These systems use fingerprint, thumbprint, palm print, finger veins, and hand geometry based highlights for identity confirmation (Wang, 2007). The features of fingerprint image incorporate principle lines, wrinkles, edges, minutia points, singular points and texture. A low-resolution fingerprint image with less than 100 dpi (dots per inch) can be used to obtain principle lines and wrinkles. A high-resolution fingerprint image with at least 400 dpi can be used to obtain minutiae points, ridges and singular points (Zhu, 2010).

Fingerprints include the ridge, furrows, minutiae points, and orientation of minutiae points, distances between minutiae points, whorl, and curves of fingerprints (Jain, 1997). Hand geometry based identification approaches utilize the geometric form of hand for affirming the identity of an individual. Although, human hands are not unique but, few essential features such as hand length, finger length, finger width, palm length, and palm width may contrast starting with one individual then onto the next individual. In image pre-processing stage we extract the hand outlines and eliminate relics, such as guidance pins; user rings; and overlapping cuffs. In hand silhouettes alignment we compute hand length, finger length, finger width, palm length and palm width. The matching module compares user features with templates stored in the database and generates matching score (Krishnan, 2009). This can be done independently or as a bimodal biometric framework as illustrated in figure 2.5.

****

Figure 2.1: Architecture of a bimodal biometric verification system based on fingerprint/palm print and facial features (Krishnan, 2009).

**ii**. **Facial Recognition**: Humans recognize and perceive faces reliant on the spot, size and state of facial features, for instance, eyes, eyebrows, lips, nose, cheekbones, jawline and jaw. The contrasting electronic ways which manage face affirmation are condensed as geometry incorporated base systems. Various methodologies rely upon image designs and process the connection between a secretly gotten face and in any event one model formats to assess comparability. Most venders of robotized face acknowledgment systems use restrictive estimations to make biometric layouts.

As expressed by Unsang (2018) facial acknowledgment system is a computer driven application for normally recognizing a person from an automated picture. It does that by looking at chosen facial features in the live picture and a facial database.

In this manner, face acknowledgment designs are not interoperable among merchants and therefore the first caught photograph must be kept, as opposed to a prepared to-use format. Because of machine-intelligible visas, the first caught photo is stored on the RFID (radio-frequency identification) chip. When passing an edge or relocation work territory, the getting state uses its own merchant estimation to consider the visa transporter's facial picture caught logically with the data read from the chip. To be seen unequivocally at various edges, it is significant that the layout picture on the chip makes unquestionable different facial features and is taken under certain light and intricacy conditions.

**iii. Iris patterns**: Before isolating and separating an iris plan, the iris must be situated inside an image. Achievement features, for instance, the outer iris limits and the student in the focal point of the eye help to stamp the iris' edges. At the point when discovered, the iris is gotten with the help of a first class camera, which all things considered releases infrared light to illuminate the eye without making hurt the eye or burden. A modernized depiction of the iris features (direction, spatial recurrence, and position) is figured (the Iris Code), stored and – in the application–looked at. It is exceptionally difficult to exactly modify the outside of the iris, and parody attacks (e.g., with orchestrated contact focal points) are recognizable rather no issue by any means. On the downside, iris affirmation is difficult to perform from partitions farther than a meter and it requires dynamic customer investment.

**2.5.2 Limitations of Physiological Features Based Biometrics**

The degradation of fingerprint caused by occupation is a hindrance of fingerprint based identification. The fingerprints might be changed or adjusted by utilizing certain unreasonable methods. Hand geometry based identification system has low exactness since at least two people may have comparative hand geometry (Kumar, 2006). Iris based identification is a safe biometric framework however the obtaining of an iris picture requires more training and expertise and it is hard to catch the right iris picture (Jain, 1997). The DNA identification based framework can't be utilized for online identification. Identical twins may have same DNA sequence thereby making it difficult to have a seamless DNA identification.

Finger veins based biometric identification systems are not relevant for identifying a handicapped individual. Heartbeat based identification system may fail for identifying an individual with strange pulse. Body expressions can't be utilized for recognizing an individual in light of the fact that an individual can undoubtedly duplicate the non-verbal communication of someone else. In palm print based identification system, the area of palm does not remain the same during the life period and deception may exist between palm prints of two people. Identifying a person using ear geometry based identification system has very high false acceptance rate percentage.

**2.5.3 Behavioral Features Based Biometrics**

The behavioral features used for individual identification are gait signature, voice, lip movement, body language, and handwriting and so on. Gait signatures are used for personal identification. In this identification strategy the system catches gait signature with the assistance of a high resolution digital camera. The acquired gait signature is converted into grayscale image. The features of gait signatures are extracted and these features are compared with stored gait signatures of database. Based on coordinating outcomes an individual is either acknowledged or dismissed by the system (Wang, 2007).

Today, numerous biometric advancements are accessible. Among these innovations, voice based identity validation has a unique edge. The human voice is unique in view of physiological and behavioral parts of speech creation. Each human has unique voice. The human voice incorporates various attributes for example rhythm, frequency, pitch, and tone. Each individual has unique voice frequency, tone, pitch, and rhythm. Voice based biometric arrangements make a voice print which is a format of the attributes of unique voice. A particular individual can be identified based on these unique highlights of his/her voice. Voice recognition framework can be arranged into two classifications (Bohm, 2004);

***Category 1****: T*ext-Dependent (In text–dependent method, the person will have to read predefined words, sentences, and specific phrases specified in the system)

***Category 2***: Text-Independent (In text-independent method, the person can speak anything which he wants to speak).

The online voice sample is compared with prerecorded templates. A person’s voice changes overtime with the physical growth and it may also change due to coldness or specific diseases. High level voice matching methods use accents, talking style, and dialects for identifying a person (Bohm, 2004).

**2.5.4 Limitations of Behavioral Features based Biometrics**

The behavioral feature based biometric frameworks have low accuracy, high FAR, and low FRR. The gait signature, lip movement, and body language of an individual can be effortlessly mirrored by another expert. The voice of an individual changes after some time and it might likewise change in frigidity. Scarcely any expert can match their voice frequency and pitch with different people. The voice based technique is not pertinent for distinguishing a deaf person. Therefore, a single behavioral component based biometric system will not be adequate for distinguishing an individual.

**CHAPTER THREE**

**METHODOLOGY**

**3.1 Introduction**

This chapter shows the various research methods used to generate the data in this research work. Various methods of data collection exist, but for this research, the method used involves the collection of primary and secondary data with an in- depth qualitative analysis or evaluation of the two basic physiological biometric (fingerprint and face) traits within local and international standards. Amongst the areas discussed here are; the research population, sample and sampling technique(s), research design, source of data, data collection and process of data analysis. The procedures involved are to enable the researcher to find answers to the research questions, suggest a better and more secure multimodal biometric technique to be adopted by the National Identity Management Commission (NIMC).

This research is an analytical study using quantitative procedures. The research was carried out by administering questionnaires and carrying out an extensive literature review of the subject matter. This method allows data obtained from a sampled population to be analyzed numerically and consequently allows an open opinion to ascertain a general perspective of the suggested multimodal biometric system base technique to be carried out open registration by the commission in order to achieve a better security within its domain and the Nation at large.

**3.2 Method of Data Collection**

The method of data gathering includes both primary and secondary data collection methods. This project's primary source of data was obtained by interviewing and administering questionnaires on individuals who have undergone the NIMC registration and have worked or working with the commission as technical and non-technical staff. Data collected with the aid of survey questionnaires as instruments are considered primary data because they are first-hand data obtained by the researcher from personal experience. The secondary sources of data came from archival and library sources such as books, magazines, journals and the internet.

**3.3 Validity and Reliability of Instruments.**

The research instrument used for this study included a well-structured questionnaire, interview with an in-depth literature review. To ensure the validity and reliability of this study, the researcher thoroughly scrutinized these instruments by reviewing them in terms of their clarity, the appropriateness of the language and expressions to the respondents as well as the appropriateness of the instructions and more importantly the ability of the instrument to gather the necessary and required information.The development of research instruments was done by examining the research objectives and related literature. Reading through the study instruments and confirming proper coverage of all the goals established the instruments' content validity.

* 1. **Sampling and Sampling Techniques**

In common parlance, the population is taken to mean all the people or the total number of people who live in a particular area, city or country. More precisely, however, a population can be described as the totality of all elements, subjects, or members that possess a specified set of one or some common definite attributes. Consequently, the population in this study comprises of the staff of National Identity Management Commission (NIMC) and some citizens that have been enrolled on the NIMC platform residing in Kaduna state. According to National Bureau of Statistics Nigeria , the latest population of Nigeria as at December 2020 is over 200 million people although the UN has placed the population at 206,867,836 million people with Kaduna having over 1,133,503 persons(United Nations world population prospect, 2020)

Primary data was collected in addition to the secondary data basically through a questionnaire. A structured questionnaire was administered to 400 citizens in Kaduna state of different occupations, including students, public servants, self-employed, and civil servants that have been enrolled on the NIMC platform.

In other to ensure that the sample size identified above is actually a representative of the actual population and also to ensure that only those who have registered are given the questionnaire, the simple random sampling techniques were adopted. Random samplings of Four hundred (400) respondents were drawn out of over (1,133,503 million) people leaving in the Twelve (12) wards in Chikun local government area of Kaduna state which includes; Kuriga, Kujama, Gwagwada, Narayi, Sabon Tasha, Nasarawa, Sabon garin Nasarawa, Kakau, Rido, Kunai and Ungwan Yelwa and also having twenty three (23) local government area in total. According to Wikipedia sources, Chikun has an area of 4466km² and a population of about 372,272 persons.

The researcher used the Sloven’s formula in determining the sample size. Below is the equation and working to determine the accurate sample size.

*……………………………………………………………Equation 1*

(Guilford & Fruchter, 1973).

Let N be the population size, and the margin of error ‘e’ denotes the allowed probability of committing an error in selecting a small representative of the population. Hence the sample size ‘n’ can be obtained by the formula above.

Thus:

N = 372,272

e = 0.05

n = 399.57 ≈ 400

n = 400

**3.5 Research Design**

The analytical research design was employed in this research. This research design is a type of survey design that allows data to be obtained from a population to assess some people's view on the lope holes and challenges encountered during the registration and verification process using the fingerprint and face recognition biometric techniques that would otherwise be too expensive to study as a whole.

As part of the process of inspecting the data collected from the field for this study, this section seeks to present the several analyses performed. However, the questionnaire was analyzed using basic statistical techniques of percentage i.e.

% = × 100……………………………………..*Equation 2*

**CHAPTER FOUR**

**RESEARCH ANALYSIS**

**4.1 Introduction**

This chapter focuses on the analysis of results and findings of the study. In the cause of this research, a structured questionnaire was administered and several literature was reviewed in order to carefully and technically analyze biometric technologies based on their operational processes, vulnerabilities and importance in correlation with the National Institute of Standards and Technology (NIST) for equipment used and adopted by the federal government for the enrolment and verification of its citizens.

## 4.2 Respondent Feedback

## This section seeks to analyze and interpret the collected data. It shows how the participants responded to the questions, the frequency of numbers and percentages as well as their answers. The analysis of data is based on the percentage of respondent. As shown from the data obtained, practically every respondent has been enrolled on the NIMC platform, thereby giving the researcher a homogenous feedback. They are also knowledgeable and conscious of their biometric information that was captured, as such all questions are coined to get respective feedback that will suggest the need for Iris biometric technology to be adopted by NIMC.

**4.2.1 Have you been registered on the NIMC platform?**

Out of a total number of 400 target respondent, 350 (100%) responded to have been registered on the NIMC platform as shown in figure 4.1. This criteria was structured to obtain the required data and to ascertain that only those who have registered will be able to give their honest feedback or experience during the enrolment and verification process. This is the first process in getting the NIN as every individual is expected to either walk in to the nearest enrollment center or register online by submitting his/her basic information such as names, date of birth etc. before proceeding with the biometric data capture.

Figure 4.1: Number of Respondent registered on the NIMC platform.

**4.2.2 Was your Biometric data captured during registration?**

In other to avoid any form of doubt or uncertainty with respect to respondent feedback, the term “Biometrics” was clearly defined. As shown in figure 4.2, 336 (96%) respondent, acknowledged that their biometric (fingerprint and face) data was captured during the registration process. 14 (4%) respondent gave a pending response which shows that their registration is not completely done. However, there is no recorded percentage (0%) of respondent that said none of their data was captured which is key to deduce that biometrics is an essential element in the NIMC registration process.

Figure 4.2: Respondent’s knowledge of the research subject.

**4.2.3 Enrollment age of Respondent.**

The Questionnaire was structured and administered to people of different age according to the National Identity Management Commission (NIMC) age standard. Nationals from 6month old to an adult age are eligible to get enrolled, since biometric formation starts at an early age in life. Figure 4.3 below shows a pictorial representation of individual response. From a total of 350 respondent, 28(8%) respondent are within the age boundary of 6months to 10years, 84(24%) persons from 11-20years, 126(36%) persons from 21-40years, 56(16%) persons from 41-60years and 60years above also responded.

Figure 4.3: Survey respondent age.

**4.2.4 Respondent Biometric Data Captured upon Enrollment.**

From the available 350 respondent, responses obtained to illustrate which biometric data NIMC captured are shown in figure 4.4 below. As shown from the bar chart below, 175 persons and 171 persons both responded to fingerprint and face biometric data captured during enrolment. This consequently gives room for this research work and suggest the introduction and adoption of Iris biometric data capture. This is so, as both (fingerprint and facial biometrics) pose to have an underlying security vulnerabilities associated with them such as spoofing and

Figure 4.4: Respondent Biometric data capture

**4.2.5 Respondent View on Fingerprint Biometric Data Capture Process.**

From figure 4.5, 169 (48.3%) persons claimed that the process of fingerprint data capture was a normal process which implies being approximately average or within certain tolerable limits in operations. 117 (33.4%) persons claimed the process was easy and seamlessly done. 54 (15.4%) persons claim to have a difficult experience upon enrolment using their fingerprint which could be due to a distorted minutiae point while the remaining 10(2.9%) claimed to have an extremely difficult experience during the fingerprint data capture which could result to a rescheduling or referral to a different registration center. This reason could be due to a lot of factors ranging from distorted fingerprint to equipment inefficiency.

Figure 4.5: Respondent View on Fingerprint Data capture process

**4.2.6 Respondent View on Face Biometric Data Capture Process.**

The face biometric data capture has its own underlying challenges as illustrated in figure 4.6 below. From the figure, it is seen that 162 person (46.3%) claimed to have an easy and seamless face capture, 139 (39.7%) respondent claim to have a normal or approximately average experience during the face biometric data capture during registration. While 44(12.6%) and 5(1.4%) persons had a difficult and extremely difficult experience respectively which could be due to several limiting factors as age, light intensity, equipment malfunction and so on.

Figure 4.6: Respondent View on Face Biometric Data capture process

**4.2.7 Respondent View on Possible Factors that Affects Face and Fingerprint Enrollment and Verification.**

From a feedback obtained from 350 respondent, certain biological factors like facial marks, age, distorted fingers, face structure, facial skin and facial expression changes with change in age of a person affect enrollment and verification process as experienced by those who have been enrolled on the NIMC platform. Figure 4.7 gives a pictorial representation of respondent view as 108 (31%) persons gave a hypothetical view and were indifferent on their experience to as whether or not such factors aforementioned affected them. 146 (42%) person believed there are no limiting factors to fingerprint and face biometric capture process while the remaining 96(27%) persons agree that such factors mentioned above can affect fingerprint and facial biometric data capture.

Figure 4.8 similarly shows respondent opinion on whether or not environmental factors like temperature, humidity, light intensity etc. also affects biometric data capture of fingerprint and facial recognition. As seen in figure 4.8, 174(50%) respondent believes that environmental affects biometric data capture; 94(27%) respondents believes environmental factors have no influence on biometric data capture and the remaining 82(23%) were indifferent on their view. However, further evaluation will show a corresponding advantages and disadvantages and will further expose such factors.

Figure 4.7: Respondent view on Biological factors that affects face and fingerprint biometric data capture

Figure 4.8: Respondent view on Environmental factors that affects face and fingerprint biometric data capture

**4.3 Analysis of Fingerprint Identification Devices**

As stated by Lockie (2006), a high-resolution fingerprint device called P3400 has been utilized. That is a little and monetarily less expensive fingerprint reader brought by Zvetco inc. This device can create 500 dpi images and is built of extraordinary aluminum. It is geared with a 6-foot USB cable and is highly utilized with most biometric security access software packages. (Lockie, 2006).

The compact guardian consists of capabilities which include patented automatic capture capability and ideal rolling era, making it perfect for foolproof fingerprint acquisition in high-volume processing environments. The device can collect quality fingerprints at high resolution (500 dpi) in few seconds and meets overall prerequisites that watch government necessities in numerous countries.

Such a scanner used depends on the utility and environment where it is to be applied. It is preferred to have scanners that are merchandise licensed for compliance with the government and National Institute of Standard and Technology (NIST). These structures incorporate information concerning fingerprint image resolution, length (place), the number of pixels, geometric exactness, dark level quantization and gray variety, spatial frequency response, and sign to-noise ratio (SNR). Table 4.1 shows a summary of fingerprint biometric guidelines as used by National Identity Management Commission (NIMC).

Table 4.1: Summary of Fingerprint Biometric Standards

|  |  |
| --- | --- |
| *Key Decisions* | *Summary of Decision* |
| **Enrolment** |  |
| Image Capture  Plain or Rolled | Plain, Live Scan |
| Number of Fingers,  Fingerprint in Rural Areas | Ten.  Absence of fingers and presence of worn out and Disabilities fingerprints.  Capture other biometric identifiers. |
| Device Characteristics | In covering scan resolution pixel depth and dynamic range, the biometric sample captured during enrolment needs to be the best sample possible. |
| Quality Check | Yes-Specified as best practice |
| Operational Operator | Assistance, Corrective Measure, and 5 retries. |
| Storage and Transmission |  |
| Compression | Uncompressed images strongly recommended. |
| **Authentication** |  |
| Image Capture | Same as enrolment |
| Number of Fingers | No minimum or maximum. A single finger will be sufficient to provide the minimum standard of accuracy requirements. |
| Any Finger option | Any finger. |
| Retry | A timeout should be implemented in service after five  (5) attempts |
| Device Characteristics | A standard will be defined for the scanners used in the authentication process. |
| Compression | JPEG 2000 compression recommended compression ratio to be less than 15:1. |
| Minutiae Format | ISO/IEC 19794-2:2005, ANSI INCITS 381-2004, and the  MINEX (I or II) |

**4.3.1 Preprocessing of Fingerprint Image**

In a fingerprint image which is obtained from any fingerprint device, there are chances that the image may be distorted or it may contain some noise disturbances in it. In preprocessing step we aim at the removal of these noise disturbances.

Jain *et al.* (2005) have suggested several methods, which can be used for our purpose of noise removal. These two basic tasks that are to be accomplished during this step are:

**Step 1:** Joining the broken ridges in the inner part of the thumbprint image.

**Step 2:** Smoothing the ridges so that the thumbprint images can be used for the purpose of pattern recognition.

**4.3.2 Analyzing Key Features of Fingerprint Based Techniques**

The fingerprints are one of the most unique patterns found on human body. It is being utilized for identifying and separating one individual from the other. The fingerprint images are comprised of friction ridges of human fingers. A friction ridge is the raised portion of the epidermis (the external layer of the skin) on the palm or on the foot bottom. These are additionally called "epidermal ridges". The palm comprises of a considerable lot of these connected or broken ridges, forming a definite pattern. The ridges are unique for each individual

The ridges and minutiae are the essential parts of fingerprint. It is exceptionally hard to alter the patterns of ridges and minutiae points for a thumbprint image. Essentially, the edge qualities can be characterized into two classes: the first is the global component, and these features are one that we can see through our naked eyes. The global features incorporate the essential ridge patterns, pattern areas, core areas, deltas, type lines and ridge counts. The second component arrangement incorporates minutiae patterns which needs magnifying devices for reading are called minutiae points. The minutiae points include exceptionally small unique qualities of fingerprint ridges that are used for individual identification. It is possible for two people to have identical global features yet at the same time they will have different fingerprints.

The minutiae organizes, orientation angles and minutiae distance based strategies, compare fuzzy set values of a fingerprint or a palm print image though cores, deltas, and focus point separation based strategy analyze the patterns and orientations of two images. Minutiae tree based technique builds a minutiae tree for fingerprints and palm print pictures and this minutiae tree will be contrasted and the minutiae tree of another online image.



Figure 4.9: A scanned fingerprint image; its minutiae point orientation field and authentication process (Jain, 2007)

**4.3.3 Advantages and Disadvantages of Fingerprint Base Technique**

The benefits of fingerprint base technique incorporates:

* Very high accuracy.
* Is the most economical biometric PC client verification method.
* It is one of the most evolved biometrics
* Easy to use.
* Small extra space required for the biometric template, decreasing the size of the database memory required
* It is standardized.

Similarly, fingerprint verification and authentication has a comparing drawbacks which incorporates:

* For a few people it is intrusive, in light of the fact that is as still related to criminal identification.
* It can commit errors with the dryness or dirt of the finger's skin, as well as with the age (it is not appropriate with kids, because the size of their fingerprint changes rapidly).

**4.4 Analysis of Facial Recognition Technique**

Face recognition system analyzes the face on static images and video-based methodologies. Age is a significant attribute of human face. Identification and verification issues might be solved by utilizing face recognition systems.

Face recognition is used as a personal identification strategy in the areas of media security, home security, and searching for missing people (Wang, 2007). Face based recognition techniques store face images through a high definition digital camcorder and uniquely identify a person based on face metric and Eigen face properties. A human face can be effortlessly changed through medical procedure or mask. The face of an individual changes from youth to become mature age citizen (Ko, 2005). In this way, face recognition based system is definitely not a robust system for personal identification. As shown in Table 4.2, the National Identity Management Commission precluded certain standards to accomplish a consistent enrolment and verification process.

Table 4.2: Summary of Face Biometric Standards

|  |  |
| --- | --- |
| *Key Decisions* | *Summary of Decision* |
| **Enrolment** |  |
| Face Image Capture  Tribal Marks | Full frontal 24bit colour images  Well focused eye / nose / mouth / forehead / chin region.  Capture of tribal marks. |
| Digital/Photographic  Requirement | Auto forms and auto-capture functions for capture device |
| Expression | Neutral face expression.  Mouth closed.  Eyes open. |
| Illumination | Sufficient illumination.  Equally distributed illumination.  No shadows |
| Eye Glasses | If glasses are worn, it should be clear and transparent so that pupils and iris are visible |
| Accessories | Head attire is strongly discouraged.  Religious accessories may be permitted (e.g. hijabs).  Medical accessories may be permitted (e.g. eye patches).  All facial features from bottom of the chin to top of the forehead (including both edges of the applicant’s face) are clearly shown. |
| Operational | Operators should be trained to obtain the best possible face image that satisfies requirements. |
| Quality Check | The quality assessment algorithms should encode  parameters like illumination, pose, blur, nose,  resolution, inter-eye distance, image height and width and horizontal vertical position of the face |
| Storage and Compression | Uncompressed images should be stored in database to preserve the quality. |
| **Authentication** |  |
| Image Capture | Same as enrolment |
| Compression | JPEG 2000 compression ratio should not be less than 11KB. |
| Number of images | For both manual and authentication, a single full frontal face image is sufficient. |

**4.4.1 Preprocessing of Face Image**

In the face recognition field, no physical contact is required for identification. Commonly available sensors; like cameras. There are a lot of existing information to permit background and/or watch-list checks. It is also easy for people to verify results. There are a couple of disadvantages to face recognition, such that the face can be obstructed by hair, glasses, hats, scarves and so on. It is also delicate to changes in lightning, appearance, and stances. In addition to that, the face itself changes after some time.

**4.4.2 Basis for Facial Recognition Identification**

Several face recognition techniques, such as principal components analysis, active appearance models, or elastic bunch graph matching, can be applied for biometric verification.

Face is directly associated with identity, gender, and age group. Face recognition comprises of two aspects (Jain, 1998).

* ***Aspect 1****:* Face Appearance (In face appearance, the basic aspects are attractiveness, age, face structure, and facial skin).
* ***Aspect 2****:* Facial Expression (The facial expression changes with change in age of a person. Facial expression includes pose and changes in face expression).

**4.4.3 Advantages and Disadvantages of Facial Recognition Technique**

The merits of facial recognition incorporates:

* Non-intrusive.
* Cheap technology.

While the demerits of facial recognition includes:

* 2D recognition is influenced by changes in lighting, the individual's hair, the age, and if the individual wear glasses.
* Requires camera equipment for user identification; in this way, it is not probably going to get well known until most PCs include cameras as standard hardware.

**4.5 Analysis of Iris Recognition Identification**

Iris image is used as a means of secure identification of an individual. In iris image-based system of personal identification we use human eyes as the basis of personal identification. In this part we discuss the realities of how we can productively utilize iris images so as to uniquely identify people. Most importantly we have to acquire the sample of iris image. When the iris image is acquired, then in the following stage we eliminate noise disturbances of the image and extract that specific segment of the image that is particular and clearly recognizable as it is discussed in chapter three of this research.

This process is called the extraction of iris image. Subsequent to finishing the extraction, we continue towards the compression of iris image. When the compression of iris image is complete then at last we store the compressed iris image for further online comparison and identification. Base on the investigation carried out to accomplish an accurate Iris image capture, the commission has a few principles it must cling to during the enrollment and verification process. Table 4.3 underneath gives a summary of Iris biometric standard.

Table 4.3: Summary of Iris Biometric Standards

|  |  |
| --- | --- |
| *Key Decisions* | *Summary of Decision* |
| **Enrolment** |  |
| Image | Two eyes, minimum 140 pixel image diameter (170 pixel),image margin 50% left and right,25% top and button of iris diameter. |
| Compression and Storage | 150 19794-6(2010) data format standard JPEG 2000 or  PNG lossless compression. |
| Quality Assessment | Per IREX11 recommendation. |
| Segmentation | Non-linear segmentation algorithm. |
| Device characteristics | Tethered, auto focus, continuous image capture,  expose< 33millisecond |
| Operational | Operator controlled strongly preferred No direct natural or artificial light reflection in the eye, indoor. |

**4.5.1 Basis for Iris Based Biometric Technique**

Iris is used for personal identification in highly secured zones e.g. nuclear reactors. An iris image contains a large number of visible pixel patterns which are unique for an individual and these patterns remain stable with age. The left and right iris images are different for the same person. Iris recognition system includes image acquisition, iris localization, and matching iris patterns.

The iris image based personal identification technique can be used for the following purposes: National ID Card, international Passport, Smartcard, Criminal Identification, Automated Banking, Credit Card, Government Benefit Distribution, Home Security System, and Confidential Database Access but, the iris image of a person takes a large amount of memory approximately 450KB (Jain, 1999; Shih, 2002). Iris recognition method scans the iris image with the help of digital camera and authenticates a person on the basis of iris characteristics.

Iris based identification is secure and accurate because, iris image doesn’t change for the whole life of a person. The iris image fully develops in the first six months after the birth of a child (Bowyer, 2008). An Iris based identification system includes following four basic steps for identifying a person (Belkin, 2003; Bowyer, 2008):

***Step 1****:* Image Acquisition means capturing the iris image using a high resolution camera.

***Step 2****:* Image Preprocessing includes converting the image to a gray scale image and removing noise disturbances.

***Step 3****:* Template matching compares the user templates with templates of database using a matching metric**.**

***Step 4****:* Authentication uses the matching metric and declares a person either an authentic person or an imposter.

In extraction phase we remove the unwanted areas of iris image and obtain the parts that are useful for the purpose of compression. The extraction phase is called the segmentation phase. The unwanted regions of image include eyelashes, eyebrows, pupil and skin, etc. Hence, we need to remove these disturbances. In order to extract the iris ring we first need to identify the boundaries of iris ring. The iris ring is basically identified by two concentric circles. The inner circle marks the inner boundary of iris ring and outer circle marks the outer boundary. The identification of inner and outer boundaries is a difficult task in the process of iris ring extraction.

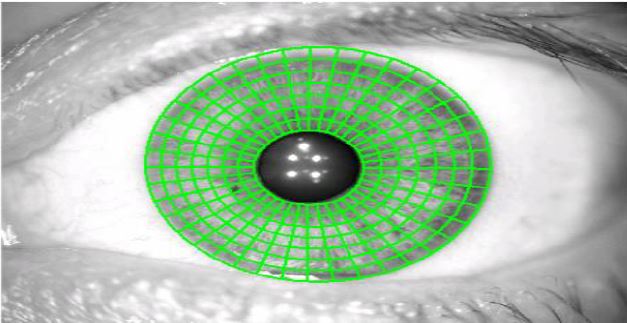


Figure 4.10: Iris image segmentation (Mishra et al., 2011)

Therefore, some special methods need to be adopted in order to accomplish the identification of boundaries. Before, we can identify inner and outer boundaries of the iris ring (which are generally circles), we need to identify the center of the iris ring (the center of the iris ring may be different from the geometrical center of the image) (Mishra *et al.*, 2011). In order to find out the center of the iris ring we first trace the inner circle. The inner circle marks the end of the pupil (which is the inner black portion of the eye) and beginning of the iris ring which consists of a combination of various colors. There is a clear distinction between regions of pupil and actual iris. Hence, it is easy to detect this circle by making use of already defined segmentation techniques.

**4.5.2 Advantages and Disadvantages of Iris Base Technique**

The advantages of the Iris base technique includes:

* Very high accuracy.
* The eye from a dead person would deteriorate too fast to be useful, so no additional precautions needs to be taken with retinal scans to be certain the user is a living person.
* Highly protected, internal organ of the eye.
* Externally visible; patterns imaged from a distance.
* Iris patterns have a high level of randomness
* Uniqueness: set by combinatorial complexity
* Limited hereditary penetrance of iris patterns
* Patterns obviously stable all through life
* Search speed: 100,000 Iris Codes per second on 300MHz CPU

The disadvantages of the iris base strategy includes:

* Very intrusive and costly
* It has the stigma of consumer's thinking it is potentially harmful to the eye.
* Comparisons of template records can take as much as 10 seconds, depending on the size of the database.

**4.6 Why Multi-biometric Systems are Important.**

Each physiological and behavioral characteristics has its own limitations for example lip motion, body language, and voice of an individual can be copied without any problem. The physiological features like palm prints, hand geometry, finger veins, and pulses have extremely high false acceptance rate. Thus, a single biometric feature based approach is not reliable and secure. It cannot identify a specific individual independently. Therefore, a single feature based biometric system will not be sufficient for secure identification of an individual. Hence, we have to combine at least two physiological and behavioral attributes or two-three physiological attributes for building up a secure multi-biometric identification system. The multi-biometric systems have high accuracy and low false rejection rate.

**4.7 Multi-Biometric System Based Identification Methods**

A single biometric system based model is not adequate for foolproof individual identification since it might experience the ill effects of numerous issues for example sensitivity to noise, intra-class variability, data quality, non-universality (due to incorrect data), intra-class variations (due to incorrect interaction with sensor), inter-class similarities (due to overlap), and spoof attacks (Doroteo, 2006; Ko, 2005; Singh, 2011). Consequently, we have to combine at least two biometric features for foolproof individual identification. Few of the well-known and established biometric feature combinations are: palate and DNA, heartbeat - head and voice, iris - DNA and thumbprint, voice - lip motion and head developments, Iris - Veins and hand Geometry.

Numerous cases emerge in which a single identification system was inadequate in doing the work of foolproof individual identification. Instances of these cases are identification of identical twins and identification of a dead individual. On account of indistinguishable twins it may be the cases that face structure or thumbprint may fail to effectively identify the individual's identity. Hence, we can say that a single biometric identification system may not be adequate to complete the assignment of foolproof individual identification. Circumstances may emerge in which we have to join at least two identification techniques together for individual and national identification. Prior to integrating at least two systems, we have to obviously choose the following factors:

***Factor 1***: We need to clearly specify different identification systems with which our incorporated system should work.

***Factor 2***: We have to identify the conditions where the integrated system is supposed to switch from one identification method to another.

The identification of both factors will be critical for the construction of an algorithm which will oversee the general working principle of the integrated system. In carrying out the enrolment process by NIMC, the face of a person is identified first. If the facial recognition method fails to identify a person then we switch to fingerprint identification. If the combination of fingerprint and facial recognition methods fail to identify a person then we move to a multimodal verification involving the face, fingerprint and iris for foolproof identification.

**CHAPTER FIVE**

**CONCLUSION AND RECOMMENDATIONS**

**5.0 Introduction**

This chapter summarizes the research work, present areas of applications, highlight the contribution of the research work to the Federal Government through the National Identity Management Commission (NIMC) and general body of knowledge. It further recommends futue research to be carried out in biometrics to improve biometric security in the Nation. And finally went ahead to draw notable conclusions.

**5.1 Summary**

In this research work the researcher delve into the major biometric technology (fingerprint and face) adopted by NIMC, analyzed their security vulnerabilities through an extensive literature review and a structured questionnaire and consequently proposed a new Iris technology to be integrated into the preexisting biometric technologies to enhance biometric security and help in achieving a centralized biometric database

**5.2 Conclusion**

Biometrics technology has proven to be an emerging and reemerging technology that has helped in providing seamless and easy human identification across the world. The abduction of biometric technology has played a vital role in ensuring national security. Today criminal act has gone beyond the conventional act to a cyber-domain hence, making it almost difficult to track and identify perpetrators since it is an extremely large domain and operations in such domains a practically complex.

There are many mature biometric systems available now. Proper design and implementation of the biometric system can indeed increase the overall security. There are numerous conditions that must be taken into account when designing a secure biometric system. First, it is necessary to realize that biometrics is not secrets. Second, it is necessary to trust the input device and make the communication link secure. Third, the input device needs to be verified, as a slight malfunctioning of the device leads to a total denial or authentication of a person’s biometrics. Biometrics, when properly implemented, not only increase security but also often are easier to use and less costly to administer than the less secure alternatives. Biometrics can’t be forgotten or left at home and they don’t have to be changed periodically like passwords.

**5.3 Recommendations**

Amongst the several biometric authentication system discussed in this work, the use of DNA for verification and authentication is completely secured since it involves some sort of genetic analysis. It is however expensive, and cannot be used for the identification of twins with the same DNA structure and it is time consuming as most organizations lacks the technical knowhow on the equipment’s used.

Therefore, it is recommended for the implementation of the iris scan in conjunction with the fingerprint and face recognition by the National Identity Management Commission (NIMC). This is of utmost importance as it helps to establish a more secure biometric design and database. The Iris scan adoption tends to address the disadvantages of fingerprint and facial recognition used by the National Identity Management Commission (NIMC) to ensuring national security.

This will subsequently help in enhancing the security of the Nigerian National Identity Management System database and can be adopted by the National Communication Commission (NCC) and the Independent National Electoral Commission (INEC) in combating election shortcomings.

**REFERENCES**

Akinyemi Akinlabi, (2014), *Nigerian National Identification Card –Costs and Benefits*. Available at <http://www.gamji.com/article6000/NEWS6202.htm> Viewed

Everest Ahaefule, (2013), *How National Identification Management System Will Stimulate Development*, Available <http://www.punchng.com/business/close-up-on-ict/how-national-identification-management-system-will-stimulate-development/> Viewed

Fabunmi, M., Isah, E.A., (2008), “*Determinant Factors for Planning Students Records Retrieval in Nigerian Universities” in Revitalization of African Higher Education*. Ibadan, Herp-Network, Available [http://herp-net.org/Revitalization-of-African-Higher-Education/Chapter29.pdf Viewed Dec.5](http://herp-net.org/Revitalization-of-African-Higher-Education/Chapter29.pdf%20%20%20Viewed%20Dec.5), 2020

Jain, A.K., Ross, A., Pankanti, S.,(2006), *Biometrics: a Tool for Information Security*. IEEE Transactions on Information Forensic and Security, Vol. 1, 2006pg365-367 retrieved from <http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/JainRossPankanti_BiometricsInfoSec_TIFS06.pdf>

Levine, C. A, (2014), *National Identity Card: Investing or Infesting Nigeria Image?*  Available at <http://nigeriaworld.com/feature/publication/arizona/100108.html>

Unsang P., Yiying T., Anil K. J. (2018) - Face Recognition with Temporal Invariance: A 3D Aging Model, 8th IEEE Int'l Conference on Automatic Face and Gesture Recognition, Amsterdam, Netherlands, September, 2019.

Ross A., Jain K. 2013 – A Learning user specific parameters in a multibiometric system. In: Proc. Internat. Conf. on Image Processing, Rochester, New York, 2013.

Jain A. K., Ross A. - Information Fusion in Biometrics, Pattern Recognition letters, Vol. 24, pp. 2115- 2125, 2013.

Obiagwu Kodilinye, (2014), *Nigeria: South East States at Full Alert Over Insecurity,* Available on <http://allafrica.com/stories/201407151676.html>

Olotu B. (2014), Nigeria: South East States at Full Alert Over Insucurity, Retrieved from (<http://myschool.com.ng/aaua/news/27079/aaua-important-notice-to-students-on-identity-cards.html>.)

Roger Clarke, (2013), *Human Identification in Information Systems: Management Challenges and Public Policy Issues*. Retrieved from htpp://www.rogerclarke.com/DV/HumanID.html.

Wayman, J.L., Alyea, L., (2000), *Picking the Best Biometric for your Application National Biometrictest Centre Collected Works*, Available on <https://www.nimc.gov.ng/>

Lockie, M. (2006). Fakta stores go biometric in Denmark. *Biometric Technology Today*.

S. N Yanushkevich, Fundamentals of Biometrics System Design *International Journal of Science*

*and Advanced Technology*, **(**2007**)**

Kong A, Zhang D, Kamel M (2009) A survey of palmprint recognition. Pattern Recognition 7:

1408-1418.

Osho P.S, Onoja M.A, (2015), National Cyber Security Policy and Strategy of Nigeria: A

Qualitative Analysis.

Odumesi, J. O. (2014). Combating the Menace of Cybercrime. *International Journal of*

*Computer Science and Mobile Computing*, *3*(6), 980 – 991.

Loader, B. D. and Thomas, D. (2000). Introduction. In B. D. Loader and D. Thomas *Cyber crime:*

*Law enforcement, surveillance and security in the information age* (pp. 1 –14). New York,

USA: Routledge.

Wayman J. L. Federal biometric technology legislation. IEEE Computer 33(2):76–80, 2000.

Ko, T. and Krishnan, R. [2009] “Fingerprint and face identification for large user population,”

*JSCI* **1**(3), 87–92.

Mishra, K. N., Agrawal, A., Srivsatava, P. C., Tripathi, V. and Gupta, V. [2011] “An efficient

eigen values based technique for online iris image compression and identification,” *Int. J. Inf. Acquis.* **8**(2).

Wang, P. S. P. and Yanushkevich, S. N. [2007] “Biometric technologies and applications,” *Int.*

*Con. Artificial Intelligence and Applications, Part of the 25th Multi-Conference on Applied Informatics, Innsbruck, Austria.*

Belkin M., and Niyogi P., 2003. *Laplace eigen maps for dimensionality reduction and data*

*representation,* Neural Computation, Vol. 15,No.6, 373-396.

Bohm Igor, and Tester Florian, 2004. Biometric Systems: Report, Department of Telecooperation,

University of Linz, Austria, pp. 1-7.

Bowyer Kevin W., Hollingsworth Karen, and Flynn Partrick J., 2008. *Image understanding for*

*iris biometrics: A survey*, Computer Vision and Image Understanding, Elsevier, Vol. 110, 281-307.

Daugman John, 2004. *How iris recognition works,* IEEE Transaction on Circuits and Systems for

Video Technology, Vol. 14, No. 1, 21-30.

Guilford, J. P., & Fruchter, B. (1973). Fundamental statistics in psychology and education

(5th ed.). McGraw-Hill

Daugman John, 2007. *New methods in iris recognition*, IEEE Trans. on Systems, Man, Cybernetics

B, Vol. 37, No. 5, 1167-1175.

Doroteo T. Toledano, 2006. *Usability evaluation of multi-modal biometric verification systems,*

Interacting with Computers, Elsevier, Vol. 18,1101-1122.

Jain Anil K., Prabhakar S., and Pankanti S., 2000. *Can identical twins be discriminated based on*

*fingerprints?,* Proc. IEEE, Vol. 85, No. 9, 1 – 16.

Bala S., & Ouédraogo E., 2018- National Security Strategy Development, Nigeria Case study.

Working paper (preliminary draft)

United Nations population prospects (2020) Nigeria Metro Area Population 1950-2021

<https://www.macrotrends.net/cities/22004/kaduna/population>, [www.macrotrends.net](http://www.macrotrends.net). Retrieved 2021-07-21.

Hong L., & Jain A. 2018- Integrating faces and fingerprints for personal identification, In Proceedings 3“d Asian Conference on Computer Vision, pp. 16-23 Hong Kong, China, 2018.

**Program Appendix 1**

**QUESTIONNAIRE**

**NIGERIAN DEFENCE ACADEMY KADUNA**

**DEPARTMENT OF INTELLIGENCE AND CYBERSECURITY**

**FACULTY OF MILITARY SCIENCE AND INTERDISCIPLINARY STUDIES**

**MULTIBIOMETRIC SYSTEM BASED TECHNIQUE AS A FACTOR TO ENSURING NATIONAL SECURITY STRATEGY; A CASE STUDY OF NATIONAL IDENTITY MANAGEMENT COMMISSION. (NIMC)- KADUNA STATE.**

Dear Respondent,

This is a questionnaire on the topic; ***Multibiometric System Based Technique as a Factor to Ensuring National Security Strategy; A Case Study of National Identity Management Commission. (NIMC)- Kaduna State***, structured by ODIDO GODWIN of the department of Intelligence and Cyber Security, Nigerian Defence Academy, Kaduna, in partial fulfilment for the award of a Masters degree in Cybersecurity.

1. Have you been registered on the NIMC platform?

* Yes
* No

1. Biometric data are basic human behavioural and or physiological attributes like fingerprint, face, voice etc.

Was your Biometric data captured during registration by the officers of NIMC?

* Yes
* No
* Pending

1. At what age were you registered?

* 6month – 10years
* 11years ­– 20years
* 21years – 40years
* 41 years – 60years
* 61years above

1. Which of your Biometric data or information was captured? Tick appropriately.

* Face
* Voice
* Fingerprint
* Iris
* Deoxyribonucleic acid (DNA)
* Walking style

1. Kindly rate the enrolment (registration) process during fingerprint capture.

* Easy
* Normal
* Difficult
* Extremely difficult.

1. Kindly rate the enrolment (registration) process during face capture.

* Easy
* Normal
* Difficult
* Extremely difficult

1. Would you say factors age, facial marks etc. will affect face and fingerprint enrolment and verification?

* Yes
* No

1. Do you think environmental factors like weather, humidity, temperature, light intensity etc. will influence the capturing process?

* Yes
* No

1. Would you consider any form of additional biometric technology be added to the fingerprint and face cognition biometric technology and adopted by the NIMC?

* Yes
* No

1. Do you consider your biometric data obtained by NIMC will help in ensuring national security?

* Yes
* No