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

**BY**

**ODIDO GODWIN**

**PRESENTATION OUTLINE**

* **ABSTRACT**
* **INTRODUCTION**
* **LITERATURE REVIEW**
* **CONCLUSION AND RECOMMENDATION**

**ABSTRACT**

Due to contemporary global trends in governance, it has become a serious challenge to verify the identity of citizens and non-citizens of a particular country. This is especially true of developing countries with high influx like Nigeria. More often than not, people falsify their ID cards either to immigrate, emigrate, or achieve other personal aims. In recent time, the NIMC (National Identity Management commission) started a nationwide registration of citizens to curb identity falsification. This no doubt will create a centralized database of citizens and enhance security challenges in identification and verification. However, the question is, how can peoples identify be verified without the threat of identity theft? This is the thrust of this research as it seeks to suggest a multi biometric system-based technique of identification and verification using the fingerprint, facial and iris scan verification system. This will beyond reasonable doubt address the issue of identity theft and spoofing upon verification, hence giving the nation a centralized biometric database where other security agencies can obtain or extract her citizen biometric data for uniformity and easy identification. The work was intended to achieve the following objectives: To evaluate fingerprint and facial biometric technology as used by NIMC; to evaluate Iris biometric technology; to evaluate a multi-biometric system-based technique by introducing a unique Iris biometric technique for fool proof identification and verification in order to ensure National security strategy is achieved. The research was analytical as relevant data were collected from both primary and secondary sources. The respondent data was obtained and analyzed using percentage method, showing the registered respondent feedback on the biometric registration challenges encountered. 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.

* **INTRODUCTION**
* The term biometric is characterized from two Greek words 'bio' signifies life and 'metric' signifies estimation
* Biometrics is defined as the unique (personal) physiological or behavioral characteristics or traits of human body.
* The different biometric perspectives used for individual identification are: ***fingerprints, face***, hand geometry, palm print, finger veins, gait signature, DNA acknowledgment, **Iris**, facial appearance, voice and so forth.
* NIMC Act of 2007 was created to handle citizens and legally authorized individuals identity enrolment and verification using the Fingerprint and Face biometric data and converting it into the present day NIN

**STATEMENT OF PROBLEM**

* A number of different types of cyber-attacks and conventional crimes are possible and hardly traceable
* 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.
* In order to achieve this, the research aim to assess the NIMC biometric system and propose the need to adopt a unique **Iris biometric technology** to complement the pre-existing facial and fingerprint enrollment and verification process which pose to have lots of vulnerabilities associated example identity theft.
* This consequently will differ in a way of biometric data collections from different agencies (private and government) thereby solving the problem of **Centralized database**

**AIM AND OBJECTIVES**

The aim of this work is to evaluate NIMC biometric system and propose an Iris recognition technique that will enhance their biometric systems.

The objectives of this research work include:

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

**NATIONAL CYBER SECURITY STRATEGY.**

" 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".

* Define minimum standard and technical requirements to safeguarding personal information from been compromised by NIMC or other government and private agencies.
* To find out and keep up a dependable information communication and transaction condition by giving digital certificate management administrations with global acknowledgment. Improve security of electronic communications and transactions.

**NATIONAL IDENTITY MANAGEMENT COMMISSION (NIMC)**

The NIMC Act 2007 provides for the establishment of the NIMC, its was created to replace the Department of National Civic Registration (DNCR) to do the following among other functions:

* Primarily to create legal institution for identification.
* Perform enrolment of citizens
* Create National Identity database
* Issue National Identification Number  (NIN) to citizen and legal residents.

**WHY INTEGRATE THE IRIS BASED TECHNIQUE?**

Although it is Very intrusive and costly ; It has the stigma of people 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.

* 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.
* **Uniqueness**: set by combinatorial complexity
* **Limited hereditary penetrance** of iris patterns
* Patterns obviously **stable all through life**
* **Basis for Iris Based Biometric Technique**
* ***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.

**WHY MULTI-BIOMETRIC SYSTEMS?**

* The physiological features like palm prints, hand geometry, finger veins, and pulses have **extremely high false acceptance rate (FAR)**. Thus, a single biometric feature based approach is not reliable and secure.
* A single biometric system base is susceptible to 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 identity theft.

**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.
* 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.

**RECOMMENDATIONS**

* 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.
* Government should invest massively in Biometric technology and forensic studies, this will help to easily apprehend perpetrators of crime and threat agents.
* Further research should be carried out on multi-biometric design algorithm and operations.