

Biometric Database – A Tool to Fight Corruption in a Developing Nation

Ekwonwune Emmanuel Nwabueze¹, Sam Okeke Doris C.², Etim Emmanuel Okon³, Egwuonwu Deborah, Uloaku⁴

Department of Computer Science, Imo State University, Owerri, Nigeria¹

Department of Computer Science, Abia Polytechnic, Aba, Nigeria^{2,3,4}

ABSTRACT: This piece of work was motivated by the lack of Harmonized Biometric Database where all the activities of government ministries, Department and Agencies (MDAs) are pooled together to capture everyone in the country to help government fight corruption, reduce cost of governance and chat a better path for a progressive nation. This paper therefore aims at considering different approaches to have a common database for building a Biometric institution about the citizenry to fight corruption at the work place. The paper discusses some of the Biometric physiological and behavioural Biometric Techniques used in identification purposes, design of Biometric database and application among others. It will be observed that a good Biometric Database will be sine qua non for government and other cooperate organization in the areas of encouraging good governance, fighting corruption, reduced cost of governance, chatting a better path for a progressive nation etc.

KEYWORDS: Biometrics, Corruption, Database, Government, Security, Techniques,

I. INTRODUCTION

In Nigeria, the absence of a national database for citizens is being taken care of through the issuance of National Identity Cards, Permanent Voter Cards, SIM card registration and recently, the bank verification number exercise authorized by the Central Bank of Nigeria, CBN. All these are made relatively easy through the deployment of ICT. It can be assumed that in the future, all these form of biometric information can be harmonized into a single platform as a statistical/forensic database.

In the opinion of Onyemenam Chris [1], as government Ministries, Departments and Agencies (MDAs) began to migrate from manual records to semi-automated and electronic processing and with the **advent of biometric identification and smart card technology**, the quest for data capture activities grew along with various kinds of upgrades. For now, their functions are specific operating in specific institutions also, whether private or public. They do not fit other purpose or purposes, aside from the one that led to the creation of that particular institution. To assume that they work together is to be uncharitably imprudent. Chris maintain that they do not 'cover' the entire population, (except the national identity card), they just define specific subsets of the population and talk only of eligibility for a service or something - each of these functional identification schemes involves 'Identity Management' in one form or the other. The concept of biometric data arrangement, which is the application of statistical techniques to biological data using measurable, biological characteristics such as fingerprints or iris patterns to identify a person to an electronic system, inter alia is not new as such in that a number of these function-specific institutions among MDAs have been in that business for some time now in Nigeria. However, what is lacking, according to Chris, is a harmonized database of a biometric arrangement, where all the activities of these function-specific agencies are pooled together under one umbrella aimed at capturing everyone living in the Nigerian state. Such arrangement will help government to fight corruption, reduce cost of governance and chat a better path for a progressive nation.

Before now, government has established a number of its institutions concerned with identity issues. In Vanguard Publication of 2015 Ogodo [2], was of the opinion that they include:, Federal Road Safety Corps (FRSC), established in 2009 for the issuance of Driver's License, Permanent Voters Card, (INEC), 2014, Tax Identification Card,

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

(JTB/FIRS), in 2014, Pension Card, (PenCom), in 2013, Residency Cards, e-Passport, (Nigeria Immigration Service), in 2006, National Identity Cards, (NIMC), in 2014, Bank Verification Number Card, by CBN/NIBSS, in 2015, among others. Ogodo added that it is not in doubt that the above – mentioned governmental Agencies work are function-specific institutions, whether private or public. They do not fit other purpose, aside from the one each of them is meant for.

Thus, Nigeria's identity ecosystem has experienced stunted growth largely due to lack of a central national identity infrastructure, the limited efforts of managers of functional identity schemes towards fostering a harmonized and integrated identity eco-system and therefore the duplication of identity life cycle activities, the poor appreciation of the concepts of and distinction between 'National Identity' and a 'Functional Identity', how both are developed, maintained, interrelated and used for socio-economic development purpose.

For the reasons adduced above, the Nigeria Computer Society (NCS) [3] has therefore thrown its weight behind the recent directive by President Muhammadu Buhari on Ministry, Department and Agencies, (MDAs) to harmonize the collection and usage of biometric data instead of replicating efforts. This directive by President Buhari, according to the NCS President, Prof. Sola Aderounmu was very timely considering the huge cost implication biometric exercises have caused tax payers in the past especially in terms of cost of data acquisition, cost of personnel, cost of storage of acquired data and cost of making such data available.

According to Vanguard Newspaper of August 2015 [], Prof. Aderounmu posits thus; “Therefore it delights us as a Society that this cooperative model of data acquisition but vested in one agency of government is being embraced. It is a right and fundamental step towards a true e-government society and will assist in the fight against crimes when agencies drew data from the same database. “We however wish to emphasize on the need to evolve enabling technology and legal framework for storing, protecting and making available the data acquired and to safeguard the privacy of citizens’ personal identifiable information (PII) such that the data are not in any way used for adversarial purposes. NCS is ready and willing to render technical assistance and support in the monitoring of the capability deployment of this enviable project.”

The nuances of Prof. Sola Aderounmu above have further reiterated the importance of a harmonized database for the Nigerian state and the actualization of effective and efficient e-government in the country. All these will in addition fight an endemic corruption that has eaten the fabrics of this society and elsewhere in the world. This research will therefore encourage good governance and a better society through its findings and recommendations.

II. RELATED WORK

Corruption could be said to be extreme immorality or depravity. Microsoft Encarta (2009) [4], describes Corruption as wrongdoing by those in a special position of trust.

Furthermore, Obafemi Awolowo (1909 - 1987) in: ‘Nigerian lawyer and politician, August 18, 1975.’ Said: “It will, I believe, be generally agreed that ERADICATION OF CORRUPTION from any society is not just a difficult task: *it is without dispute, an impossible objective.*” But Lord Acton (1834 - 1902), a British historian, April 3, 1887 in a in: ‘*Letter to Bishop Mandell Creighton*’ Posits: “Power tends to corrupt, and absolute power corrupts absolutely”.

From the above, one sees the embarrassing posture of corruption in the psyche of the ancient and modern; hence the position of the Nigerian president, Mohammad Buhari in calling for its eradication in the public service through a biometric database harmonization system in the republic.

The Concept of Biometric Techniques

According to Ekwonwune et al [5], Biometrics is a means of identifying somebody or an electronic system through some measurable, behavioral or biological characteristics such as fingerprints, voice or iris, patterns, a password etc for the singular aim of distinguishing between a specific individual and an impostor. They are of the view that in computer technology, biometrics relates to identity confirmation and security techniques that rely on measurable, individual

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

biological features that recognize or verify the identity of individuals through automated means. Biometric systems are the automatic methods for identifying a person on the basis of some biological or behavioral characteristic of the person. Therefore, biometrics is more reliable and more capable in distinguishing between a specific individual and an impostor than any technique based on identification (ID) document or a password.

There are a number of simple, widely available means of personal identification, including photo ID cards and secret passwords which may be compromised easily [6]. Similarly, passwords or personal identification numbers (PINs) may be forgotten or guessed by others. However, in that same opinion, Biometric Systems provide automatic personal identification on the basis of a physical or behavioural feature that is distinctive to each individual.

III. DESIGN OF A BIOMETRIC DATABASE SYSTEM

Automatic personal identification is the process by which a biometric system associates a particular person with a specific identity. Identification may be in the form of verification or recognition. In verification the system authenticates a claimed identity. In other words, the system verifies a claim that a person is who he or she says he or she is. In recognition the system determines the identity of a given person from a database of persons known to it. It is easier to design a biometric system for verification than for recognition. A verification system authenticates a person's claimed identity by comparing the particular biometric characteristic being used for identification against biometric measurements of the claimed identity that have been previously stored in the system. In a recognition system, the biometric characteristic being used is compared against the corresponding biometric measurements of all identities stored in the system. For example, a thumbprint from a person who wishes to enter a secured room is compared against the thumbprints of all persons who are authorized to enter the room. A biometric system is essentially a pattern-recognition system that makes personal identification possible. It does so by establishing the authenticity of a specific biological or behavioral characteristic of the user, that is, the person who is being identified.

The enrollment module equips the system to identify a given person. During enrollment [6], a biometric sensor scans a characteristic of the user to acquire a digital representation of the characteristic, such as a digital image of the person's face. A computer program known as a feature extractor then processes the digital representation to generate a more compact representation called a template. With a facial image, for example, the template of features may include the size and relative positions of the eyes, nose, and mouth. The template for each user is stored in the system's database or recorded on a *smart card*, which is a small plastic card containing a microchip that can store personal data. If the template is recorded on a smart card, the card is issued to the user. To be identified as the true user, the cardholder must match the characteristic recorded on the card. The identification module recognizes the person. During identification, as [6], posits, the biometric sensor scans the characteristic of the person to be identified and converts it into the same digital format as the template. The sensor also inputs the resulting representation into a feature matcher, another computer program. The feature matcher compares the representation against the template. A verification system will conclude that the person is correctly identified when the scanned characteristic and the stored template for the claimed identity are the same. Otherwise it will reject the person. A recognition system will assign the user the identity associated with the correctly matched template when the scanned characteristic and a characteristic on a stored template are the same. However, if the scanned characteristic does not match any stored template, the system will reject the person.

According to Alexandre F. and Vincent B. [7], Biometric Techniques can be divided into physiological and behavioural as shown below:

1. Physiological biometric

- Fingerprints

This is the most known method that belongs to this category which is also the oldest biometric authentication approach based on the recognition of someone's fingerprint, by analyzing its characteristics. There are two different techniques to capture fingerprints; scanning optically the finger and using electrical charges that determines which parts of the finger are directly in contact with the sensor and which are not

- Eyes

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

There are two methods using the eyes characteristics for authentication the retinal recognition whereby the user has to look in a device that performs a laser-scanning of his retina for the analyzes the blood vessels configuration of the acquired retinal picture and the iris recognition which is scanned by the camera and the acquired picture is analyzed by the device, and contains 266 different spots. The Iris recognition is said to be the most reliable biometric authentication method while the Retinal recognition can fool the authentication system.

- DNA

To perform a DNA analysis the user has to give some of his cells, for example by giving a hair, or some skin. Analyzing DNA takes a long time and that is why it is not used as an authentication method.

- Face

This method is based on the faces recognition and uses a simple device like camera, even a web cam with low resolution in which case, the user stands in front of the camera, and then the device computes a digital representation based on some features of the face. The representation is compared with one which is stored in a database, and if there is a match, the user is authenticated. It is easy to setup, and cheap to implement because all you need is a cheap camera and a well-done software.

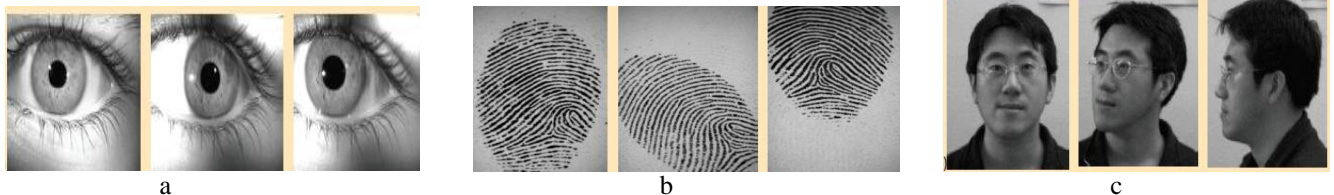


Figure 1: Inherent variability between biometric samples of the same individual. (a) Variations in fingerprint patterns of the same finger due to differences in finger placement on the sensor. (b) Variations in face images of the same person due to changes in pose. (c) Variations in iris images of the same eye due to differences in pupil dilation and gaze direction. **Source:** [8]

- Handprints

This method is based on the recognition of the handprints and the device is a scanner that extracts a picture of a user's hand whereby some characteristics like length of the fingers, distance between them or their relative position are computed, based on the picture. These characteristics are used to match with an entry in the database.

- Voice

This method is based on the recognition of someone's voice whereby the user speaks in a microphone, and voice is recorded and computed. It is done by using some frequency analysis of the voice. It is less accurate than other biometrics authentication methods, easily fooled and some errors can occur.

There are several others physiological biometrics, such as lips or earlobes recognition, sweat ore odor analysis, blood analysis and so on.

These biometric methods are less used and have to improve before they can be used.

2. Behavioral biometric

- Signature

The analysis of signature is also a biometrical authentication solution with tactile screen device. The user performs a signature with a "pen" on this tactile screen. The parameters that are computed for the authentication are the shape of the signature, the time taken to do it, the stroke order and the pen pressure.

- Gait

This behavioural biometrics works by analyzing how a person is walking. A camera films the user walking, and by computing some mathematical function on the inclination of the legs, the frequency of the balancing of the body, it gives you a good authentication method. You can use this at distance, and then it can be used as a security system.

- Keystrokes

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Keystrokes analysis provides an authentication method which works more or less like the signature biometric, by analyzing the way a user is typing on a keyboard. It measures how long a user holds a key, and how long it takes to the user to switch from one key to another.

According to Alexsandra F and Vincent B, all these methods follow a common scheme: Some part or behavior of someone is digitalized, transforms in data that follows a template so it can be compared to entries in a database and then authenticate or not a user. The size of this template is a part of the strength of a biometrics. For example fingerprints have templates at least of 150 bytes, and iris gives a template of 512 bytes.

IV. APPLICATIONS OF BIOMETRICS

Biometrics is a rapidly evolving technology that is widely used in law-enforcement applications such as the identification of criminals and the maintenance of security in prisons. Outside of law enforcement there are many areas where biometrics can improve security and prevent fraud, such as in ATMs and driver licensing. However, there are privacy concerns for citizens in terms of how, and by whom, their biological and behavioral characteristics are monitored or used.

Many private companies and government agencies are seriously considering biometrics [9] for adoption in a broad range of applications outside of law enforcement. It is estimated that losses due to identity fraud in welfare disbursements, credit card transactions, cellular telephone calls, and ATM withdrawals total over \$6 billion every year. For this reason, various organizations are adopting automated systems for identity authentication to improve customer satisfaction, increase cost savings, and improve operating efficiency. ATMs are a good example of the need for better identity authentication.

Electronic commerce and electronic banking are two of the most important areas where applications of biometrics have emerged. Advances in the technology used for electronic transactions have opened these areas to biometrics. In the opinion of Chris, various government agencies have considered using biometrics. In benefits distribution programs such as welfare disbursement, biometrics could bring about substantial savings by deterring the same person from filing multiple claims. Personal identification based on hand geometry could permit faster processing of passengers at immigration checkpoints. Biometric-based voter registration and driver licensing could prevent fraud in those processes.

According to Leadership Newspaper [10] Federal ministries, department and agencies (MDAs) that are implementing identity database related projects have begun complying with the presidential directive on harmonization and integration of Biometric Databases with the national Identity Management System (NIMS) housed in the National Identity Management Commission (NIMC).

V. NCC AND NATIONAL BIOMETRIC DATABASE

Telecommunications forms a vital hub for any modern society. It is an essential infrastructure, which stimulates the development of other sectors such as commerce, industry, agriculture, education, health, banking, defense, transportation, and social interaction and that is why Tosin Akinjobi [11], writes: "With the implementation of the National Telecommunications Policy, Nigeria's telecoms industry has undergone significant development in the last 15 years". He posits that the successful take-off of digital mobile telephone services using the global system for mobile communications (GSM) technology rapidly escalated active telephone lines from about 400, 000 in mid-2001, to about 136 million and still growing as at now. Tosin Akinjobi posits that in order to be consistent with new developments and emerging trends locally and internationally, the Nigerian Communications Commission (NCC), was established by Decree 75 of 1992 with the objective of the National Telecommunications Policy is to achieve the modernization and rapid expansion of Nigeria's telecommunications network and services to enhance national economic and social development.

According to him, in February 2014 the Central Bank of Nigeria (CBN), as part of its efforts to develop "a safe reliable and efficient payments system, launched the Bank Verification Number (BVN) project which requires all bank customers to complete biometric registration and obtain a BVN, through which all transactions by that particular customer may be verified. In September 2014, the CBN directed that all bank customers must have a BVN by June

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

2015, and that from March 2015 only customers with BVNs will be permitted to make transactions in excess of N100 million (approximately \$500,000). With this policy, banks are now among institutions that hold biometric data of citizens.

Tosin also was of the opinion that the NCC also requires that every single active mobile telephone number has the owner's biometric data registered. The SIM card registration exercise has been running since the past two years to build a database of telephone subscribers as well as assist in crime monitoring and control.

Registered voters are also entitled to receive permanent voter cards after the Independent National Electoral Commission (INEC) has captured their biometric data. Also, the National Identity Management Commission is biometrically assembling the data including photographs, fingerprints, and geo and bio data of citizens as a way of officially documenting Nigerians. Other forms of digital data capturing include the issuance of passports and driver's licenses.

VI. RECOMMENDATIONS

From the foregoing, this piece of work recommend as follows:

1. That the federal government of Nigeria institutes without delay necessary policies that will strengthen the anti – graft agencies in the fight against corruption.
2. That the Federal House of Assembly makes necessary laws to legalize database harmonization policy in the country's e-government system so as to engender sanity in database management, reduce cost of governance and maintain efficiency in information and technology management in Nigeria.
3. That government makes effort in training and re-training of her staff vertically and horizontally with the single aim of making the workers current in ever evolving information technology globally.
4. That effort be made to evolve Management By Objective (MBO) in the nation's work system because MBO policy will encourage the work force to be more accountable and responsible in operational management of their MDAs.
5. That government at all level increase budgets for the acquisition of all that is required to make Info-Tech and e-government to work in their various establishments, inter alia.
6. That government removes the idea of function-specific arrangement in its biometric database identity capturing exercises and in its place maintains a harmonized database arrangement.

VII. CONCLUSION

In this work, we have attempted to advance the course national biometric database harmonization infrastructure by examining various options that can make it succeed. It looked into the concept of the cankerworm called corruption and how it has to some extent affected those fabrics of the nation's ICT management. The idea of a biometric system was also x-rayed with a view to finding ways through which an integrated or harmonized database arrangement can benefit the system by eliminating corruption, reducing cost and maintaining effective and efficient workforce. In the end, it is hoped that there will be a harmonized database of a biometric arrangement, where all the activities of these function-specific agencies are pooled together under one umbrella aimed at capturing everyone living in the Nigerian state. Such arrangement will help government to fight corruption, reduce cost of governance and chat a better path for a progressive nation.

REFERENCES

- [1] Onyemenam Chris (2015); National Identity' And Data Capture Activities In Nigeria; National Identity Management Commission; Daily Independent Of 25 Aug 2015
- [2] Ogbodo (2015) : Harmonization Of National Biometric Database Will Fight Corruption – NCS; Vanguard Newspaper; August 16, 2015
- [3] NCS Nigeria (2015): Harmonization Of National Biometric Database'll Reduce Corruption – NCS, All Africa Wednesday 19th August, 2015

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

- [4] Niccolò Vivarelli (1994): Collier's Year Book, 1994; Newsweek, In Microsoft ® Encarta ® 2009. © 1993-2008;
- [5] Ekwonwune et al (2016), Vulnerability of Biometric Authentication System, a published article in the International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, March, 2016
- [6] <http://video-lessonoffer.blogspot.com.ng/p/biometrics-i-introduction-biometrics.html>
- [7] Alexandre F. and Vincent B. (2005), 'Biometric Authentication', a published Assignment in IT – University, KISTA
- [8] Anil J. and Nandakumar K. (2012), Biometric Authentication System Security and User Privacy, IEEE Computer Society.
- [9] Onyemenam Chris (2015); Harmonization Of National Biometric Database Will Fight Corruption – NCS; Sun, Aug 16, 2015
- [10] Leadership Newspapers (2014), Harmonization of Biometric Database: MDAs Complying with m SGAF's Circular.
- [11] Akinjobi Tosin (2015); Ncc And Nigeria's Biometric Database ; Daily Independent, Nigerian Newspaper. March 14, 2015; <Http://Linkis.Com/Htwwa>