Multi –Mode Biometric Solution for Examination Malpractices in Nigerian Schools.

Olufemi Sunday Adeoye
Department of Computer Science
University of Uyo

ABSTRACT

The major technique for admitting students to an examination over the years has been through the presentation of a token. The student possesses a physical and portable device which contains the user identity. Examples of such devices include ID cards, Library Cards, Fees Clearance Cards, Photo Cards, etc. However, this method of authenticating a student for an examination has an obvious problem. The problem is that object can be misplaced, stolen, forgotten at home or somewhere, and ID card can also be faked. This paper presents a multi-mode biometrics (fingerprint and face) solution to the problem of examination malpractice in Nigerian schools. The appearance of both fingerprint scanner and web cam on modern laptop and notebook computers motivate the writing of this paper.

Keywords: *Multi-mode Biometric, Examination Malpractices, Enrolment, Identification, Verification, Biometric Fusion.*

1.0 Introduction

Multi-mode involves the use of more than one biometric factor or modality as a means of security. Multi-mode authentication is the use of more than one biometric modalities to authenticate or verify the identity of a person or other entity. Every biometric modality has its own flaws hence the use of multi-mode biometric to address examination malpractices in Nigerian schools. For instance fingerprint of a person keep on changing from time to time especially for those who are involved in hard labour works such as bricklaying. This can lead to the security device having problem in identifying a person’s fingerprint. The age and occupation of a person can cause sensors difficulty in capturing a complete and accurate fingerprint image.

Face is another popular biometric that has been used over the years. In fact, it is the oldest method through which human beings have been identifying themselves. The emergence of web cam on laptop and notebook computers has made facial automation possible. Facial recognition is not without it own flaw(s). The most prominent of such flaw is that the face can easily be disguised or even obstructed by hair, glasses, hats, face plastic surgery, etc. This reduces the reliability of face biometric security to a great extent. Face biometric is also sensitive to changes in lighting, expression, and poses. Finally, the face keeps on changing over time and this can be another problem.

Automatic personal identification system based solely on fingerprint or faces is often not able to meet the system performance requirements [13, 26, 28]. This is why this paper combines fingerprint and face recognition in order to utilize the features of the two. Self recognition is said to be fast but reliable while fingerprint verification is reliable but inefficient in database retrieval. The limitations of unimodal biometric systems can be overcome by using multimodal biometric systems [13]. Multimodal biometric system uses multiple applications to capture different types of biometrics. This allows the fusion of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements. An effective fusion scheme is required to combine the information presented by individual modalities. Biometric fusion combines biometric characteristics and can improve accuracy, robustness, fault tolerance and efficiency of multi biometric system. According to Anastasis et al, three levels of fusion are possible (a) fusion at the feature extraction (b) fusion at the marching score level and (c) fusion at the decision level. In the case of fusion at the feature extraction, the features obtained from each biometric is used to compute a multimodal feature vector which is used for the biometric authentication. The second approach involves fusion at the matching score level. For each biometric, the user is validated and a marching score indicating the proximity of the feature vector with trained model is calculated. These scores are then combined in order to verify the claimed identity. The third approach is the fusion at the decision or output level. The final decision is the fusion of individual accepts or rejects decisions taken by each biometric method.

2.0 Biometrics

Biometrics comes from the Greek bios (life) and metrikos (measure). A biometric is a measurable physical or behavioural characteristic of a human being. Hence, biometric are measures of people. They are proposed for use in recognizing identity or authenticating claims of identity. Biometrics are technologies that produce and process measures of people. Biometrics is an automatic method for identifying a person on the basis of some biological or behavioural characteristic of the person. Many biological characteristics such as fingerprints and behavioural characteristics, such as voice patterns are distinctive to each person. Therefore, biometrics is more reliable and more capable in distinguishing between a specific individual and an impostor than any technique based on an identification (ID) document (e.g., ID cards, Photo cards, Library cards, Fee clearance cards) or a password.

In computer technology, biometrics relates to identity - confirmation and security techniques that rely on measurable individual biological characteristics. For example, fingerprints, handprints or voice patterns might be used to enable access to a computer, to a room or to an electronic commerce account. In general, there are three levels of computer security schemes. Level 1 relies on something a person carries, such as ID card with a photograph. Level 2 relies on something a person knows such as a password or a code number (e.g. PIN). Level 3, the highest level, relies on something that is a part of a person's biological makeup or behaviour, such as a fingerprint, a facial image, or a signature. There are a number of simple, widely available mans of personal identification, including Photo ID cards and Secret passwords or Personal Identification Number (PIN). While these simple means of identification work most of the time, they may be compromised easily. For example, ID cards may be lost, stolen, or copied. Similarly, passwords or personal identification numbers (PINs) may be forgotten or guessed by others. However, biometric systems provide automatic personal identification on the basis of a physical or behavioural feature that is distinctive to each individual.

The concept of biometrics perhaps has its origin with the human use of facial features to identify other people. It can be said to have its link to the traditional method of human identification. Modern biometrics, however, started in the 1880s when Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, France, developed a method of identification based on a number of bodily measurements. One of the most well-known biometric characteristics is the fingerprint. British scientist Sir Francis Galton proposed the use of fingerprints for identification purposes in the late 19th century. He wrote a detailed study of fingerprints in which he presented a new classification system using prints of all ten fingers, which is the basis of identification systems still in use [11]. British police official Sir Richard Edward Henry introduced fingerprinting in the 1890s as a means of identifying criminals. Automatic fingerprint - based identification systems have been commercially available since the early 1960s. Until the 1990s these systems were used primarily by the police and in certain security applications [11].

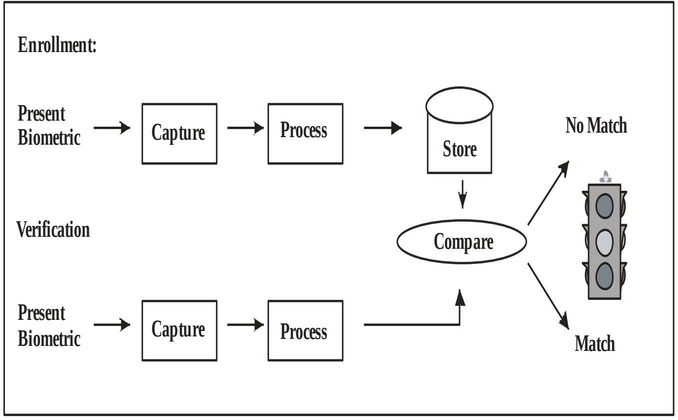

Fig. 1: Typical biometric enrolment and matching process.

2.1 Fingerprint Biometrics Identification

Human beings have used fingerprint for personal identification for centuries and they have used them for criminal investigations for more than 100 years. The validity for fingerprint as a basis for personal identification is thus well established.

A fingerprint is the pattern of ridges and furrows on the surface of a fingertip. No two persons have exactly the same arrangement of patterns, and the patterns of any one individual remain unchanged throughout life. Fingerprints are so distinct that even the prints of identical twins are different. The prints on each finger of the same person are also different. The biometric fingerprint sensor takes a digital picture of a fingerprint. The fingerprint scan detects the ridges and valleys of a fingerprint and converts them into ones and zeroes.

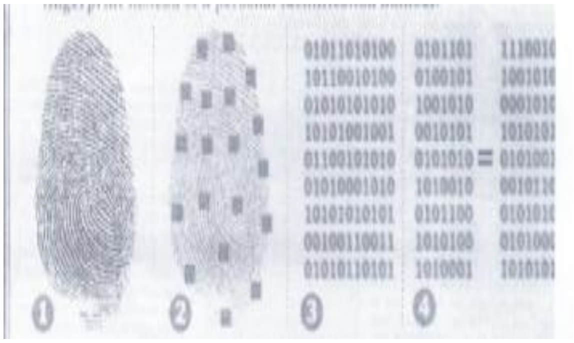

Fig. 2: Conversion of fingerprints to Binary Digits

Complex algorithms analyze this raw biometric scan to identify characteristics of the fingerprint, known as "minutiae". Minutiae are stored in a fingerprint template (a data file usually smaller than the initial scans). Up to 200 minutiae are stored in a template, but only a subset of these (10 to 20 minutiae) has to match for identification or verification in most systems. For smart card systems, approximately 40 minutiae are stored, because of space restrictions [19].

Small ridges form on a person's hands and feet before they are born and do not change throughout life. These ridges are formed during the third and fourth month of fetal development. Fingerprint of cloned monkeys, just like identical twin humans have completely different fingerprint. The ridges on the hands and feet have three characteristics

- ridge endings
- bifurcations - a Y shaped split of one ridge into two
- dots – short ridges that looks like dots.

Under a microscope the fingerprint has unique characteristics known as minutiae points. Common minutiae points are the intersections of bifurcations and ending points of fingerprint ridges. With the advent of Automated Fingerprint Identification Systems (AFIS), a fingerprint can be compared against every fingerprint in the entire database. No two fingerprints have been found to have the same individual characteristics in the same unit relationship [33].

A fingerprint device is typically a self-contained sensor that supports two key functions:

- a sensor for capturing a fingerprint
- the ability to communicate the digital image to the host processor via an interface such as USB or serial.

Some key features of fingerprint sensor devices are:

- high- speed USB interface;
- high quality image capture and encrypted image data;
- plug- and- play
- Self- calibrating, rugged, small footprint;
- no external interface or power supply required; and
- support for Windows NT 4.0, Windows 2000, Windows 98 and 95 OSR 2.1(USB), Windows XP and Windows Vista.

2.2 Facial Biometrics

The most familiar biometric technique is facial recognition. Human beings use facial recognition all the time to identify other people. As a result, in the field of biometrics, facial recognition is one of the most active areas of research. Applications of this research range from the design of system that identify people from still - photograph images of their faces to the design of systems that recognize active and changing facial images against a cluttered background. More advanced systems can recognize a particular individual in a video tape or a movie.

Facial recognition analyzes the characteristics of a person's face images input through a digital video camera. It measures the overall facial structure, including distances between eyes, nose, mouth and jaw edges. These measurements are retained in a database and used as a comparison when a user stands before the camera. This biometric has been widely, and perhaps wildly, touted as a fantastic system for recognizing potential threats (whether terrorist, scam artist or known criminal).

One of the strongest positive aspects of facial recognition is that it is non-intrusive. Verification or identification can be accomplished from two feet away or more, and without requiring the user to wait for long periods of time or do anything more than look at the camera. The inherent difficulties in making a positive identification (lighting requirements, facial position etc) are larger than most people realize and seems to make this biometric a better choice for verification systems, rather than identification.

Facial recognition software translates the characteristics of a face into a unique set of numbers - this is referred to as "eigenface". The eigenface is used by both identification and verification systems for facial comparisons made in real-time. Identification involves a one-to-many comparison of an individual's face against all faces in a database in order to determine the identity; and verification is characterized as a one -to- one match of an individual's face to his or her stored image for the purpose of confirming identity [33].

The brain deals with visual information much as computer algorithms compress files. Because everyone has two eyes, a nose and lips, the brain extracts only those features that typically show deviations from the norm, such as the bridge of the nose or the upper cheekbones. The rest it fills in. Facial recognition software today can instantly calculate an individual's eigenface from either live video or a still digital image, and then search a database of millions in only a few seconds in order to find similar or matching images. The challenge is to support rapid and accurate real-time acquisition as well as its scalability to databases containing millions of faces [31].

2.3 Examination Malpractices

Examination malpractice has been defined as a deliberate wrong doing contrary to official examination rules designed to place a candidate at an unfair advantage or disadvantage.

Examination malpractices has also been viewed as the act of omission or commission that contravenes those West Africa Examination Council rules and regulations to the extents of undermining validity and reliability of the text and ultimately the integrity of the certificates issues by West African Examination Council. From the psychological view examination malpractice is all forms of cheating which directly or indirectly false the ability of the students [2, 31].

Examination malpractice has long graduated from the normal giraffing at neighbors' work, using key points, notes or textbooks or copying on sheets of papers referred to as "microchips", or "ekpo", or copying on desks or laps also known as "desktop publishing" and "laptop publishing", respectively to a more advanced and more organized system of buying questions from examination bodies or corrupt bank officials or individual entrusted with the safe keeping of examination question papers [30].

Also, syndicates have been able to arrange "special" centers for their "special candidates", enrolled for the examination at exorbitant and unapproved fees with the connivance of examination bodies for the easy perpetration of malpractice. These "miracle" centers enjoy the patronage of some corrupt school administrators and examination officers.

These syndicates have made it very easy for somebody to acquire a Senior School Certificate of Education or a University degree without necessarily entering the examination hall. "Mercenaries" abound to impersonate the candidates without adverse consequence. This trend has, sadly, crept into international examinations like British and the American-sponsored examinations (City and Guilds, SAT, TOEFL, etc) organized in Nigeria. These syndicates have also devised mind-boggling means of impersonating and cheating during these examinations [2, 30].

2.4 Manifestation of Examination Malpractice in Nigeria

Examination malpractice is not a new phenomenon in Nigeria, as well as indeed in any part of the world. The first examination malpractice in Nigeria was reported in 1914, when there was a leakage of question into the Senior Cambridge local examination; others traced the origin of examination malpractices to the wave of cancellation of Nigeria's candidate paper in 1948 because it posses on history during the 1940 matriculation examination to then "Yaba"-Nigeria technical [31]. The most pronounce, malpractice in Nigeria in early examination was that of 1964 that was tagged "expo" subsequently in 1970, 1973, 1974, 1979, 1981, 1988 and 1991 followed. Since 1991 to date examination has taken advance and more sophisticated dimensions, records are been emerged yearly indicating high or low percentage in examination malpractice in the Nationals core examination (external) West African Examination Council and JAMB [9, 23].
To prove this point, investigation has revealed that thirty out of one hundred and sixty-six examination towns were involved in cheating and malpractice while forty-five thousand four hundred and four-eight candidates seeking University admission had their results cancelled in year 2002 because of examination malpractice [30, 31].

Referring to the examination fraud in the country the former president of Nigeria, "Chief Olusegun Obasanjo" said students in the country perceived education as a means of getting a meal ticket and getting a job; the former president further argued that the perception or orientation must change so that students would appreciate the intrinsic value of education, which is the total development of the individual to be able to make meaningful contributions to the family, community and the country at large [30].

Even though various strategies, such as Post UME test, setting of different versions of questions for the same examination, the use of photo cards and involving more hands in examination supervision, have been used over the years to stop examination malpractices, the area of impersonation still remains. This is why this paper focuses on the use of multimode biometrics to offer solution for examination malpractices in Nigerian schools.

3.0 Multimode Biometric Solution for Examination Malpractices

Individual student must first register their form of identity with the system by means of capturing raw biometrics to be used in the system. This process, which is called enrolment, composed of the following phases: capture, process and enroll [11]. A raw biometric of each student is captured by the biometric sensing device, characteristics that are unique to individual and distinguish each student from another are extracted from the raw biometric transformed into a biometric template. The template is then stored in a suitable storage medium such as a database on a disk storage device or on a portable device such as a smart card, whereby later comparisons can be made easily. Once enrolment is complete, the system can authenticate individual student by means of using the stored template.

The major key elements of all biometric systems are enrolment and matching.

3.1 Enrolment

Enrolment is the process whereby a user's initial biometric sample or samples are collected, assessed, processed and stored for ongoing use in a biometric system. Enrolment takes place in both one to one (1:1) and one to many (1: N) systems. If users are experiencing problems with biometric systems, they may need to re-enroll to gather higher quality data [18].

Enrolment is the most important process in overall biometrics. It is the moment when the computer first "gets to know" the person who is later to be identified. The more and the better information the system gets, the better will be the accuracy for recognition.

Technically spoken, enrolment is a process in a biometric system with the following input/output (I/O).

INPUT- samples of the person's characteristics (e.g. face images for face recognition, fingerprint for finger recognition, spoken words for voice recognition, etc).

OUTPUT- The "biometric template", the extracted information of the input samples describing the person's characteristics.

For this approach to function effectively, every student at the point of admission is enrolled into the student's database. The picture (mainly the face) and the fingerprint of each student are enrolled along with their corresponding names. Most laptops produce nowadays, because they come with built-in web cam and fingerprint scanner, can allow for multi modal enrolment. The face will be captured by the web cam and the finger will be captured by the fingerprint scanner or reader. The school authority must allow for good enrolment- a situation when user gives different samples to the system within the full range of variety that this person normally exhibits.

Enrolment can be done through any enrolment application or through enrolment wizard that comes with your computer system. A very large storage device should be provided for storing the biometric template(s) of the students since this will definitely take a large memory. The template may be stored within the biometric device or remotely in a central repository. Storing the template in a central repository is a good option in a high-performance, secure environment. The size of the biometric template varies from one vendor product to the next and is typically between 9 bytes and 1.5 kilobytes.

The task of the enrolment is the creation or management of a user‘s biometric template. If enrolment wizard is used, it guides the user to make a sufficient number of recordings, to review those recordings, test the result of the training, and finally store the biometric template in the database.

3.2 Matching

This is the process of comparing submitted biometric sample against one (verification) or many (identification) templates in the system's database. Matching involves two process i.e. identification and verification.

Matching will be done during the examination period. Each student's fingerprint and facial picture is taken at the point of entry into the examination and is compared against the template already stored in the student's database.

3.3 Biometric Recognition- Identification

Biometric recognition can be used in identification mode, where the biometric system identifies a student from the entire enrolled population of student by searching a database for a match based solely on the biometrics. Identification can be used to discover the identity of a student when the identity is unknown (the student makes no claim of the identity). For the process of identification a central database is necessary to hold records for all students known to the system; without a database of records, the process of identification is not possible.

When a student comes to be identified, he provides a live biometric sample, e.g. a fingerprint or a face is scanned. The data is processed and the resulting biometric template is compared against all entries in the database to find a match (or a list of possible matches). The system then returns as a response either the match (or list of possible matches) it has found, or that there is no match against the enrolled population of student.

3.4 Biometric Recognition – Verification

Verification is a test to ensure whether a student is really he or she claims to be. Two types of verification can be envisaged: with centralized storage or distributed storage.

3.5 Verification with Centralized Storage

If a centralized database exists (produced once at enrolled and updated with each additional student) where all biometric data and the associated identities are stored, the biometric sample of the claimed identity is retrieved from the database. This is then compared to the live sample provided by the student, resulting in a match or a non-match. The matching can be done locally on the device temporarily storing the acquired sample or remotely by the hardware that stores the sample acquired during enrolment.

3.4.2 Verification with Distributed Storage

Biometric data can also be stored in a distributed system in which case student's templates are stored department by department. This has an advantage of allowing student data to be monitored departmentally and at fast rate. This allows for fast identification since the data of students in each department can never be as large as the one in central database storage.

3.4.3 Biometric Fusion Scheme

Information presented by multiple traits (such as fingerprint and face in this paper) may be consolidated at various levels. At the feature extraction level, the data obtained from each sensor is used to compute a feature vector. Since data from various traits are independent of each other they can be concatenated to a new vector with higher dimensionality that represents a person's identity in a new hyperspace. This new vector is then used in the matching and decision-making modules of the biometric system. At the matching score level, each individual system provides a matching score and those scores are combined to affirm the authenticity of the claimed identity. At the decision level or output level, each individual system provides multiple biometric data and the resulting vectors are individually classified into two classes – accept or reject. The final decision is the fusion of individual accepts or rejects decisions taken by each biometric method [21, 22].

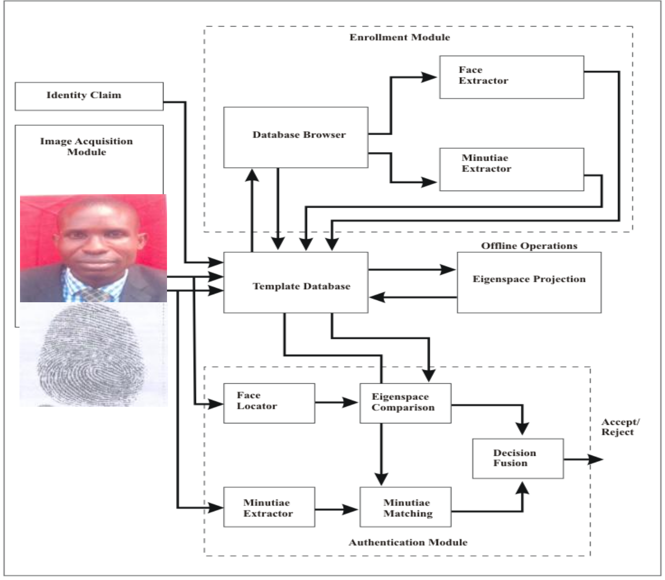

Fig. 3: Architecture of a Multi-mode identity authentication system

The architecture of an automatic multi-mode identity authentication system is shown in the figure above. It consists of five components: (i) Image Acquisition Module, (ii)

Template Database, (iii) Enrolment Module, (iv) Authentication Module, and (v) Decision Fusion.

The image acquisition module provides mechanisms for a student to indicate his/her identity claim and input his/her fingerprint and facial image into the system. The template database consists of a collection of records, each of which corresponds to a student authorized to take a particular course or examination. Each record contains the following fields which are used for authentication purposes: (i) user name, (ii) minutiae template of a student's fingerprint and eigenface, and (iii) other information.

The task of enrolment module is to enroll students and both their fingerprints and facial images into the template database. When the fingerprint, facial image and the user name of a student to be enrolled are fed to the enrolment module, a minutiae extraction and eigenface extraction algorithms are applied to the fingerprint images and facial images which made the minutiae patterns and eigenface to be extracted. A quality checking algorithm is used to ensure that the records in the system database only consists of templates of good quality in which a significant number of genuine minutiae and eigenface may be detected. If a fingerprint and facial image is of poor qualities, they are enhanced to improve the clarity of ridge/valley or face structures and mask out all the regions that cannot be reliably recovered. The enhanced fingerprint and facial image are fed to the minutiae and eigenface extractors respectively.
The task of authentication module is to authenticate the claimed identity of the student who intends to take a particular examination. The student to be authenticated indicates his/her identity and place his/her finger on the fingerprint scanner as well as positioning his/her face properly on the web cam; a digital image of his/her fingerprint and face are captured; minutiae pattern is extracted from the captured fingerprint; eigenface is extracted from the captured facial images and fed to a matching algorithms which matches them against the student's minutiae and eigenface stored in the template database to establish the identity.

The decision fusion combines the features of both the fingerprint and the face for each student to accept or reject decisions taken by each biometric method.

4.0 Conclusion

Biometrics is the technology of the millennium. It has been used in different areas of life to provide security. This paper clearly reveals that biometrics can also be used in the school system to curb examination malpractices which is a rampant cankerworm that has eaten in-dept into every fabric of our educational system. Incorporating biometrics identity verification in the school system will not only help to monitor the attendance of students in lectures but will also help to check examination malpractices (impersonation). The rational for multimodal user authentication is that no single biometrics is generally considered sufficiently accurate, universal, and user acceptable for any given application.

5.0 Recommendation and Next Step

Using biometrics for identifying human beings offer some unique advantages. Biometrics can be used to identify you as you. Biometrics holds the promise of fast, easy – to – use, accurate, reliable, and less expensive authentication for a variety of applications. Therefore, with the alarming rate of examination malpractices in Nigeria schools, it is important that biometrics be employed to identify students into the examination hall to check impersonation. It is also certain that in the nearest future biometrics will be used in all necessary areas where proper authentication is unavoidable.

6.0 REFERENCES

[1] Adamu, M (2001). "Examination Malpractice" A Paper Presented at the Annual Special and Prize Giving Day Ceremony of Federal Government, Daura Katsina State.

[2] Ajibola Olushola, *Advocates of Examination Malpractices*, EzineArticles.com, 2009

[3] Alex, T.E. (2009). *Examination Malpractices are Disturbing*, September 25, 2009 Newshoundjoansleaue a command Go to commands.

[4] Anastasis Kounoudes et al, POLYBIO: Multimodal Biometric Data Acquisition Platform and Security System.

[5] Bernard, M.O (1998). Examination Malpractice in Tertiary Institution in Nigeria: Types, Causes, Effects and Solution. Unpublished.

[6] Brinerd, C. (1978). Piaget's Theory of Intelligence. Englewood Cliffs. NJ. Practice-Hall.

[7] Brunelli, R., Falavigna, D. *Person Identification using Multiple Cues*. IEEE Trans. On Pattern Analysis and Machine Intelligence, vol. 12, No 10, pp 955-966 (1995).

[8] Castle, E.G. (1982). Principles of Education for Teacher. Ibadan Evans Books.

[9] Chinedu Ugwu. The Menace of Examination Malpractice (July 16, 2008) Unpublished.

[10] Editorial commentary (1990). "Aiding Examination Malpractice. Daily star. December 19 pg.3

[11] Galton ,F., *Person Identification and Description*. Nature 38, 201-202 (1888).

[12] Hogan, M. (2003), *Are you who you claim to be?* National Institute of Standards and Technology, International Standards Organization. http://www.iso.ch/iso/en/commcentre/isobulletin/articles/2003/pdf/biometrics03-03.pdf

[13] Hong L., Jain A. K., Pankanti S., *Can Multibiometrics Improve Performance?*, In Proc. AutoID'99, Summit, NJ, October 1999, pp. 59 – 64.

[14] http://techbiometric.com/biometric-products/biometric-sensor/

[15] http://techbiometric.com/biometric-products/face-recognition/

[16] http://techbiometric.com/biometric-products/fingerprint-reader/

[17] Jain A. K., A. Ross, S. Prabhakar, *An Introduction to Biometric Recognition*, IEEE Trans. on Circuits and Systems for Video Technology, Vol.14 No. 1, pp 4-19, January 2004.

[18] IBG, www.biometricgroup.com

[19] Smart.card.reader@cardwerk.com

[20] Jain, A. K., Ross, A., *Multibiometric Systems*. Communication of the ACM, Special Issue on Multimodal Interfaces (2004).

[21] Jain A. K., Prabhakar S., and Hong L., *A Multichannel Approach to Fingerprint Classification, Proc. Of Indian Conference on computer Vision, Graphics, and Image Processing* (ICVGIP '98), New Delhi, India, December 21-23, 1998.

[22] Kresmir Delac, Mislav Grgic. *A survey of Biometric Recognition Methods*, 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 JUNE 2004, Zadar, Croatia.

[23] Linus, H. (1999). *Scourge of Examination Malpractice in Public Examination*. Success Magazine. Vol.1.

[24] Maltoni D., Maio D., Jain A. K., Prabhakar S., Handbook of Fingerprint Recognition, Springer, 2003.

[25] Prabhakar S., S. Pankanti, A.K Jain. *Biometric Recognition : Security and Privacy Concerns*, IEEE Security and Privacy, March/April 2003, pp.33-42

[26] Ross A., A.K. Jain, *Information Fusion in Biometrics*, Pattern Recognition Letter 24 (2003) 2115-2125, available at http://www.computerscienceweb.com/.

[27] Ross, A, Nandakumar, K., Jain, A.K., Handbook of Multibiometrics. Springer, New York, USA, 1st edition (2006).

[28] Ross, A. ,Jain, A .K., *Identification Information fusion in Biometrics*. Pattern Recognition Letters 24, 2115-2125 (2003).

[29] Ross, A., *An Introduction to Multibiometrics*. In : Proc. Of the 15th European Signal Processing Conference (EUSIPCO), Poznan. Poland (2007).

[30] Saintmoses Eromosele (May 12, 2008). *Taming the Menace of Examination Malpractice in Nigeria*, Unpublished.

[31] Shonekan, M. O. (1996), Various forms of Examination Malpractice and WAEC Penalties for Them. Paper Presented at the Symposium Organized by the Federal Ministry of Education on "Character Formation in secondary Schools", May 22, National Theatre, Lagos.

[32] Tistarelli M., Bigun J., Grosso E., (Eds): Biometrics School 2003, LNCS 3161, pp. 43 – 68, 2005. Springer-Verlag Berlin Heidelberg.

[33] Uday O. Ali Pabrai (2001). *Biometrics for PC – User Authentication: A Primer*, ecfirst.com