ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

A Biometric Authentication Approach to Examination Conduct in Nigerian Universities

Ekwonwune Emmanuel N[1], Okonkwo Thaddeus Ogadimma[2]

Department of Computer Science, Imo State University, Owerri Nigeria[1,2]

ABSTRACT: The unethical manner associated with the examination is a grim issue that require the stakeholders in academic area to seek for alternative means of authenticating student for examination because, the manual paper-based clearance process is fundamentally flawed. The process of allowing students to sit for an examination in most universities has been through the presentation of medium of identification such as ID cards, library cards, fees clearance cards, photo cards, etc. This piece of work is motivated by the fact that the method of authenticating a students for an examination has an obvious problem such as presentation of fake clearance card, impersonation and so on. The aim of this work therefore is to design a program that will address issues of exam misconducts such as impersonation and revealed the effectiveness of biometric system using fingerprint in conducting examination clearance. The method that will be used involves structured system analysis and methodology (SSADM). The proposed system used fingerprint biometric approach, the system recognizes an individual by comparing his/her biometrics with every record in the database rather than old manual method in use. The expected result from the system is that the new system will compulsorily prompt for biometric (fingerprint) in order to allow student gain access into the system for authentication and identification of the real student before entering into examination hall.

KEYWORDS*:* Biometrics, Authentication, Examination, Fingerprint, Exam Malpractice, Technology

1. INTRODUCTION

Biometric approach has become a prominent option and secured means of authentication capable of sustaining the emerging universal computing.

All academic institutions have certain criteria for admitting students into examination hall. That is why keeping the accurate record of attendance and fees payments are very important. In almost all institutions in the developing countries, clearance is usually done manually using paper sheets and old file system approach.

Biometric identification of a person is fast, easy-to-use, precise, trustworthy and economical over traditional knowledge-based and manual methods. A biometric system contains mainly an image capturing module, a feature extraction module and a pattern matching module. An image capturing module acquires the raw biometric data of a person using a sensor. Utilizing suitable algorithm/s feature extraction module improves the quality of the captured image. Database module stores the biometric template information of enrolled Persons. Pattern matching module compares the extracted features with the stored templates, which in-turn generates match score.

This approach discourages fraud, impersonation during the examination unlike the paper clearance approaches which encourage fraud, impersonation etc. As the level of security breaches and transaction fraud increases, the need for highly secured identification and personal verification technology is fast becoming apparent **[1].**

The relevance of biometrics in modern society has been reinforced by the need for large-scale identity management systems whose functionality relies on the accurate determination of an individual's identity in the context of several different applications. Biometrics offers a secured method of access to sensitive services and obviates the need to carry a token, card or to remember several passwords.

Biometric techniques also reduce the risk of lost, forgotten or copied passwords, stolen tokens or even shoulder attacks, yet despite these obvious benefits, most biometric techniques are not pervasive in everyday life **[2].**

There are some significant reasons for this. The cost of deployment of many techniques is very high; potentially requiring specialist analytical software and machines with the computing power to run it. There is a lack of

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

standardization of many methods, and the wide variance of algorithms results in different performance levels from comparable equipment. Additionally, end users may refuse to use some types of biometric identification due to possible hygiene misunderstandings, cultural differences or ethical issues **[3].**

The exception to this antipathy towards biometrics is fingerprint recognition (FR) a well-known technique to identify individuals by comparing fingerprints features with a pre-defined template which most people are familiar with nowadays. FR is widely used today in places such as airports and legal system, and it is built into devices such as laptops. Lot of work has been showcased in literatures, which aim at identify and qualify the best methods and algorithms for FR than any other biometric system; however there is still not a categorical standard algorithm for FR systems.

Despite this, identification or authentication through FR still has three main advantages **[4]:**

i. Low cost of deployment (cost effective).
ii. Simple to implement and use.
iii. User must be physically available at the point of identification or verification.

Biometrics system can be used in two ways: verification or identification. When a biometric is used to verify whether a person is who he or she claims to be, that verification is frequently referred to as “one-to-one” matching. Identification, by contrast, is known as “one-to-many” matching. In identification, a person’s presented biometric is compared with all biometric templates within a database in order to get a match**.**

According to **[6], r**esearch on biometric methods has gained renewed attention in recent years brought on by an increase in security concerns. The recent world attitude towards terrorism has influenced people and their governments to take action and be more proactive in security issues. This need for security also extends to the need for individuals to protect, among other things, their working environments, homes, personal possessions and assets. Many biometric techniques have been developed and are being improved with the most successful being applied in everyday law enforcement and security applications. Biometric methods include several state-of-the-art techniques. Among them, fingerprint recognition is considered to be the most powerful technique for utmost security authentication. Advances in sensor technology and an increasing demand for biometrics are driving a burgeoning biometric industry to develop new technologies. As commercial incentives increase, many new technologies for person identification are being developed, each with its own strengths and weaknesses and a potential niche market.

Biometrics is the use of measurable, biological characteristics such as finger prints or iris patterns to identify a person to an electronic system. Once these measurements have been taken, they may then be used to authenticate an individual or user. This is done by comparing the sampled biometric against a template taken earlier.

[6] defined the term “Biometrics” is derived from the Greek words “bio” (life) and “metrics” (to measure)

Biometrics is the use of measurable, biological characteristics such as fingerprints, or iris patterns to identify a person to an electronic system. Biometrics is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

[7] further described Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. A physiological biometric would identify by one’s voice, DNA, hand print or behavior

II. STATEMENT OF PROBLEM

The rate of problems encountered in conducting universities examination is too high and the approach used on it is to poor. Such problems include:

1. Student impersonation
2. In secured authentication of students
3. Manual verification of students

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

III. AIM AND OBJECTIVES OF STUDY

The ultimate Aim of this research study is to design an approach to examination conduct in Nigerian universities the following objectives are here by undertaken:

1. To create a system that is capable of tracking impersonators in the examination system using finger print biometrics.
2. To reduce rate of corruption in the educational sector and increase the rate of self-confidence on students.
3. To demonstrate the possibility of computer technology in the satisfaction of human needs and also enforce strict security measures that ensure unregistered students do not write exams for other registered students.

.

IV. THEORETICAL BACKGROUND

[8] Fingerprints have certain natural traits that make them ideal for use in biometric Systems. Fingerprints are developed between the first and second trimester and Remain unchanged (barring any damage or scarring) until death. Fingerprints are Unique. No two people on record have been found to have the same fingerprints. Fingerprint identification has been used by law enforcement agencies for many Years. But this type of one-to-many match is seldom used for commercial Purposes. Most fingerprint systems operate in authentication, rather than Identification, mode. Fingerprint scanning can be done in several different ways. Some systems scan the distinct marks on the finger called minutiae points (similar to the traditionally used police method).

Currently, there are mainly nine different biometric techniques that are either widely used or under investigation, Including face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice print, and facial thermo grams Although each of these techniques, to a certain extent, satisfies the above requirements and has been used in practical systems or has the potential to become a valid biometric technique, not many of them are acceptable (in a court of law) as indisputable Evidence of identity. For example, despite the fact that extensive studies have been conducted on automatic face recognition and that a number of face recognition systems are available it has not yet been proven that face can be used reliably to establish/verify identity. Without any other information about the people in it will be extremely difficult for both a human and a face-recognition system to conclude that the different faces shown in are disguised versions of the same person. So far, the only legally acceptable, readily automated, and mature biometric technique is the automatic fingerprint identification technique, which has been used and accepted. In forensics since the early 1970‘s. Although signatures also are legally acceptable biometrics, they rank a distant second to fingerprints due to issues involved with accuracy, forgery, and behavioral variability.

The biometrics community is slow in establishing benchmarks for biometric systems. Although benchmark results on standard data bases in themselves are useful only to a limited extent and may result in excessive tuning of the system parameters to–improve the system performance, they constitute a good starting point for comparison of the gross performance characteristics of the systems. No metric is sufficiently adequate to give a reliable and convincing indication of the identification accuracy of a biometric system. A decision made by a biometric system is either, called genuine distribution and impostor distribution, respectively. For each type of decision, there are two possible decision outcomes, true or false. Therefore, there are a total of four possible outcomes:

1. A genuine individual is accepted,
2. A genuine individual is rejected,
3. An impostor is rejected ,and
4. An impostor is accepted.

Outcomes 1) and 3) are correct, whereas 2) and 4) are incorrect. In principle, we can use the false (impostor) acceptance rate (FAR), the false (genuine individual) reject rate (FRR), and the equal error rate (EER) 2 to indicate the identification accuracy of a biometric system.

[9] a fingerprint is the reproduction of a fingerprint epidermis, produced when a finger is pressed against as smooth surface. The most evident structural characteristic of a fingerprint is a pattern of interleaved ridges and valleys; in a finger print image.

Ridges (also called ridge lines) are dark whereas valleys are bright. Injuries such as superficial burns, abrasions, or cuts do not affect the underlying ridge structure and the original pattern is duplicated in any new skin that grows.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Ridges and valleys run in parallel; sometimes they bifurcate and sometimes they terminate. When analyzed at the global level, the fingerprint pattern exhibits one or more regions where the ridge lines assume distinctive shapes (characterized**).**

Authentication

[11] an essential aspect of security is the ideology of authentication the ability to prove that someone or something is what it claims to be. In the systems 'security Realm there is three commonly accepted types of user authentication:

1. Something you have : digital certificates, tokens, smart cards and keys
2. Something you know : passwords, personal identification numbers (PIN), or some other piece of personal information such as your pet's Name or mother's maiden name
3. Something you are a biological trait (a biometric)

Examination Malpractice

Examination malpractice is any wrong doing before, during or after any examination. Although one may not be able to rule out examination malpractice in the past, the current trend is alarming and calls for proper management in order to rid the school system of its consequences. Whereas in the past, students tended to hide the acts, now they advertise them with positive blatancy.

[11] opined that the interest in non-intellectual factors would Seem to have stemmed from the idea that–the human being is a complex whole That is, man is made up of intellectual, emotional, affective and psychological Traits. For them to develop and reach their full potential in life, these traits must be understood, harnessed, and be catered for by the school. Students Involvement examination malpractices have become perennial and institutionalized. It is a testimonial to the flawed process of admission into Secondary schools and tertiary institutions. It has invariably, reflected in the Multifaceted crises in the nation's educational system. Moral instruction is the detailed information, which concerns the principles of right and wrong behaviors.

V. METHODOLOGY

In this section, I described the methodology used for the software design and also analyzed the system. The system strengths and weaknesses were also viewed to determine areas for improvement. To actualized this the Software Engineering Methodology called Structured System Analysis and Design Methodology (SSADM) was used while Top down Software design approach will be followed.

The biometric identification consists of two stages: Enrollment and Authentication

Structured System Analysis and Design Methodology (SSADM).

While using the system structured analysis and design methodology **SSADM** the following sequence of step were carried out and they include

(I) **Problem identification:** Here Researcher tries to understand the problem facing Imo State University Owerri in handling and conducting their students' examination.

(II) **Investigation or fact findings:** A thorough investigation will be carried out on the present system that exist in the university by me this is to enable me finds out the facts about it before trying to improve on it. For good job to be achieve I shall logically go through the various phases of the institute, so as to get accurate data collections. The method for data collections shall be: evaluating all forms, interviewing through oral and written method (questionnaires), observation method and studying of procedural manuals.

(III) **Analysis:** the analysis of the data gathered will be established. We will try to know how quickly and cheap is the present system, how does it meet the objectives and its problem spots.

(IV) **Design**: we structured the system under study, following the specification of processing requirement such as input files, master files and segmentation of these processes into programs.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

(V) **Implementation**: The new system shall be into in use. The software program and it modules will be tested to see if it does correctly everything it intends to do. Change over procedure will be **parallel and pilot approach.**

Weaknesses of the Existing System

Several problems tend to exist within the use of the system and as such include:

- Inefficient to comprehend the act of exam impersonation
- The process of authorization was done manually. This is a concept of what you have which can be manipulated at any time by the students.
- Matching to establish security measures occurs through the physical eye and this is a very big problem and requires great power of recognition, hence an impersonator can be present without recognition.

Expectation of the New System

It is expected that the new system will provide solutions to the weakness observed in the present system above by providing fast and reliable means of conducting examination through the use finger print biometric authentication software for student exam clearance.

High Level Model of the Proposed System

Here the top – down approach is used. The design approach is structured or modular, in which the whole system is broken into different functional component or modules, which are then separately design to flow from top hierarchy to the bottom. The top-down design of the program structure was presented as:

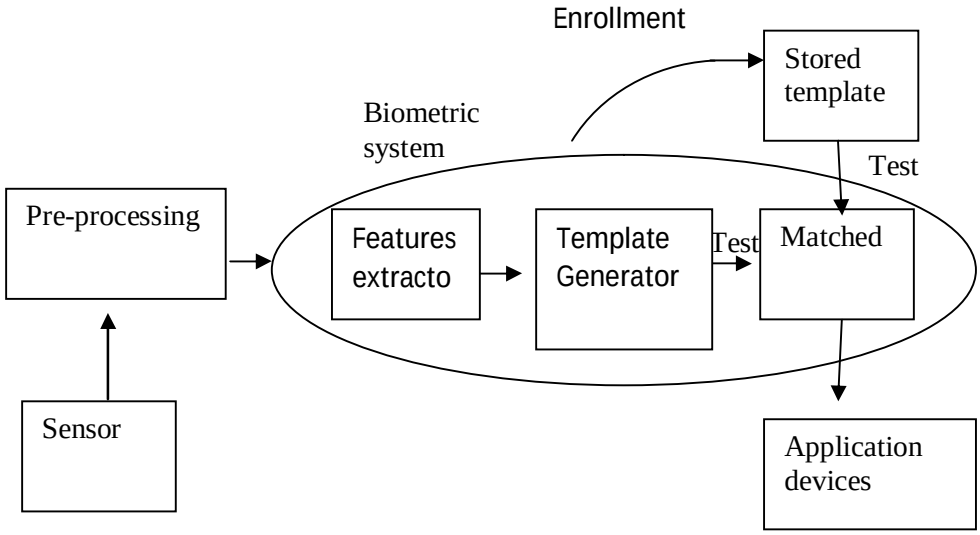

Fig 1: High Level Model

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

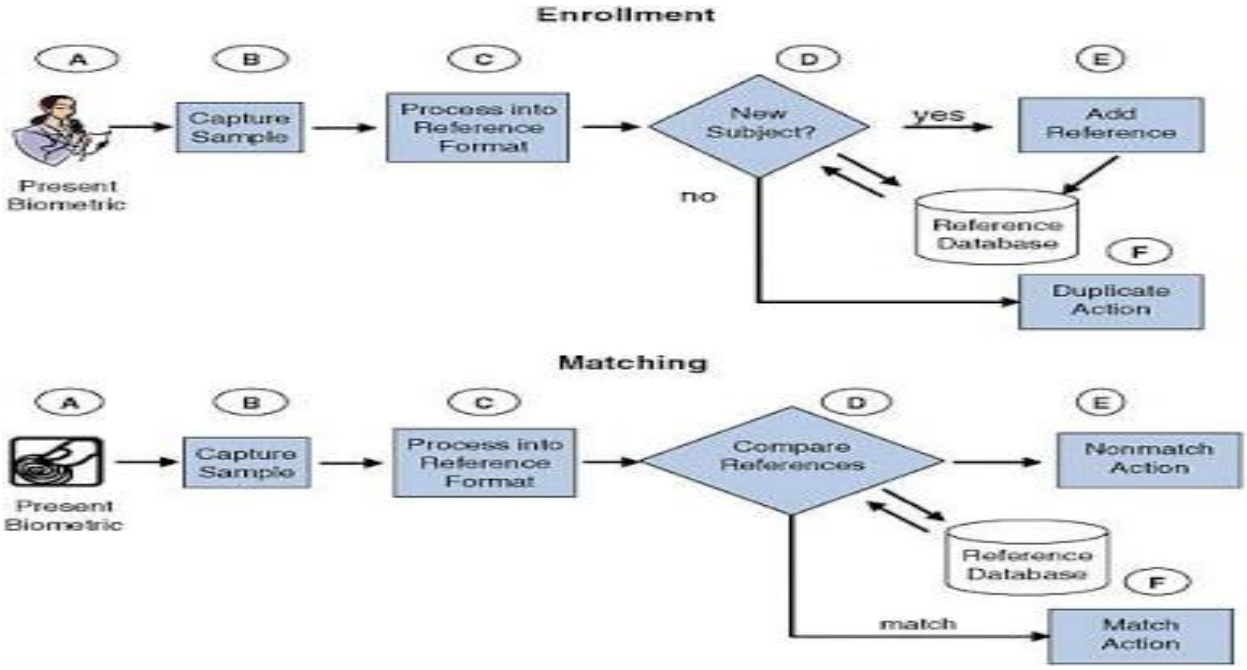

Fig 2: High-level model for enrollment and matching

Sources: www.researchgate.net

VI. CONCLUSION

Biometric authentication approach (BAA) is a better substitute for the identity cards in verifying Student identity. This study revealed that BAA is more secured, credible and error free to checkmate student malpractices, impersonation and other unlawful acts as compared to existing manual-paper based. Various researches have shown the porosity of identity cards in uniquely identifying individual in the face of sophisticated forgery technology but the natural uniqueness in the use of fingerprint makes it a reliable access control technique thereby eliminating impersonation in examination and the issue of fake clearance cards. This study has established the effectiveness of examination clearance using biometric system. The obvious shortcoming in the manual paper based is addressed. The study will go a long way in addressing the issues of examination malpractices, impersonation, and fake clearance in our educational institution. The system can be linked with the school's central database so that the student registration phase can be eliminated and the bio-data can directly be accessed from the database.

REFERENCES

[1] Alane K. and Ari, S. (2004). Biometric Technologies: Security, Legal and Policy Implications. USA Center for Democracy and Technology and the Heritage Foundation.
[2] Salil Prabhakar and Anil K. Jain (2003). Biometric Recognition: "Security and Privacy Concerns" IEEE Security & Privacy March/April, 2003.
[3] Farzad, P. (2012) Fingerprint-based student Attendance Register. MSc Dissertation. University of Bedfordshire.
[4] Maltoni, D, K. Jain, A. and Prabhakar, S., (2010). Handbook of Fingerprint Recognition. Second edition.Springer publishers London.
[5] Ezema, Eneh J.N, and I. Amanze (2015). Fingerprint Based Attendance Management System. International Journal of Scientific & Engineering Research, Volume 6, Issue 7, July-2015. ISSN 2229-5518
[6] https://arxiv.org/ftp/arxiv/papers/1107/1107.3194.pdf
[7] Lawson and Olaniyi (2011) Introduction to Biometrics Technology. McGraw Book Company London.
[8] Saheed Y.K, AliyuJubril, (2015). A Framework for Examination Clearance Using Biometrics System. Multidisciplinary Innovations & Technology Transfer (MINTT) Conference UNIBEN 2015. Book of Proceedings. Series 8, pp. 107 – 116.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

[9] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.2569 &rep=rep1&type=pdf
[10] Cavoukian, A. (2008). Fingerprint Biometrics Address Privacy before Deployment. Toronto Information and Privacy Commissioner of Ontario.
[11] Okwilagwe, H. (2001)Security and Access Control using Biometrics Technologies. 1st edition Boston: engage Learning Winnipeg.
[12] www.researchgate.net