DESIGN AND MODELING OF A STUDENT VERIFICATION SYSTEM IN AN EXAMINATION IN NIGERIA USING BIOMETRIC FINGERPRINT TECHNOLOGY

***Ahmed Baita Garko[1] and Abdulaziz Ahmad[2]**
[1]Department of Computer Science, Federal University Dutse – Nigeria
[2]Department of Computer Science, Northwest University, Kano – Nigeria
*Correspondent Author's E-mail: abgarko@fud.edu.ng

Abstract
With the current advances in Information Technology, there are lots of technologies being used in the 21st century. Different software and hardware are created in order to save and retrieve data and information in some computerized systems. One of these systems is the one we designed and modeled in this paper. This paper proposed a system that will help in identifying and verifying student during examinations with a view of minimizing exams malpractice. Currently, in most schools in Nigeria students' verification is carried out manually whereby a student will be issued with an examination card for verification or by using his/her id- card. A lot of problems happen whereby some students are in habit of hiring some people to come and sit for their exams in which same id-card is pirated, and at times very difficult for the invigilators to identify due to the number of students sitting for the examination. The introduction of fingerprint based exam verification system in this paper will help to easily identify students that registered for a particular course and can easily identify students that are eligible to enter the exam hall. Each student's information will be saved in the database which will help the staff to carry out their verification and identification exercise efficiently and is more secured. However, for student to be verified using the system they should make sure they have registered for all the courses they supposed to take during a particular session and they must have 75% of attendance for him/her to be eligible to sit for the exam. Prototyping software development methodology was adopted in this paper; Visual Basic 6.0 was used to design the interfaces and Mysql was used as the back-end. Finally, only the verified students are allowed to sit for the exam. The output from the system shows that, the proposed framework is more secured, more efficient, and has better performance when compared with the manual system of students' verification.

Keywords: Information Technology, Examination, Fingerprint, Biometric System

Introduction

Formal examination can rightly be defined as the assessment of a person‘s performance, when confronted with a series of questions, problems, or tasks set to him, in order to ascertain the amount of knowledge that s/he has acquired, the extent to which s/he is able to utilize it, or the quality and effectiveness of the skills s/he has developed. Examinations have also increasingly employed for the selection of recruits to the civil service, and the professions, and to posts in industry and commerce. Over the ages, standardized testing has been the most common methodology, yet the validity and credibility of the expanded range of contemporary assessment techniques have called into question.

There are two types of system, which help automatically in establishment of identity of a person:

i. Authentication (verification) systems
ii. An identification systems

In a verification system, a person desired to be identified submits an identity claim to the system, usually via a magnetic stripe card, login name, smart card, etc., and the system either rejects or accepts the submitted claim of identity (Am I who I claim I am?). In an identification system, the system establishes a subject‘s identity (or fails if the subject is not enrolled in the system database) without the subject‘s having to claim an identity (Who am I?).

The focus of this paper is channeled towards the development of examination verification system and this system would strictly function with the unique feature of identification by means of fingerprint. Verification system based on fingerprints, and the terms verification, authentication, and identification are used in a loose sense and synonymously. Accurate automatic personal identification is becoming more and more important to the operation of our increasingly electronically interconnected information society. Traditional automatic personal identification technologies to verify the identity of a person, which use something that you know, such as a personal identification number (PIN), or something that you have, such as an identification (ID) card, key, etc. are no longer considered reliable enough to satisfy the security requirements of electronic transactions or school management system. All of these techniques suffer from a common problem of inability to differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of the authorized person.

Biometrics is a technology that (uniquely) identifies a person based on his physiological or behavioral characteristics. It can be used to achieve a positive identification with a very high level of confidence, such as an error rate of 0.001%. Fingerprint technology using biometrics employs certain advantage of eradicating the problem of examination impersonation by allowing the measure of what you are to perform the security activities of student participation in the examinations.

Statement of Problem

Some of the problems we encounter in the current system of students verification and identification during examinations are:

i. Student impersonation
ii. Insecure authentication of students
iii. Inefficiency of the process due to students' population or size of a class
iv. The tedious nature of the manual process

Related Works

Examination malpractice is any wrong doing before, during or after any examination [3]. 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. The things that others thought right to draw a veil across, the modern biographer reveals with all the gusto of a showman it was traced back examinational practice to 1914. He further reported that in the University of Maiduguri, about 25% of the students interviewed admitted to have engaged in one form of examination malpractice. Examination malpractice occurs in both internal and external examinations. In short, it has become an epidemic in the nation's educational system, which needs a prompt attention. The situation of examination malpractice is so embarrassing to the nation that the federal military government in 1984 promulgated Decree 20 to deal with it. Parts of the Decree reads as: "*Any person who fraudulently or with intent to cheat or secure any unfair advantage to himself or any other person or in abuse of his office, produces and sells or buys or otherwise deals with any question paper intended for the examination of persons at any examination or commits any of the offences specified in section 3(2 7) (c) of this Decree, shall be guilty of an offence and on conviction be sentenced to 21 years imprisonment* " [3].

Students are likely to cheat when they are not prepared for examinations [3]. It was also reported that university lecturers are of the opinion that inadequate teaching and learning facilities, poor conditions of service of teacher's fear of failure by students and admission of unqualified candidates into universities are responsible for examination malpractices [8]. A Researcher categorized the reasons for examination malpractices into psychological and sociological causes. The over dependence on certification has led to mad ruche by the populace and the resultant effect is that people either acquire certificates legally or otherwise. This messy situation is having a negative effect on the nation's quality of education and the kind of certificates issued to students at different levels. So many people can no longer defend their certificates. He 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. Student's involvement in examination malpractices have become perennial and institutionalized [11].

According to [3] year-in-year-out; students come up with new dimensions of examination malpractices. This is the reason why drastic steps must be taken. The instances of examination malpractices vary. They range from impersonation, leakage of questions, tampering with results, and computer fraud to fraudulent practices by invigilators, officials and security personnel charged with supervising examinations. Parents are not left out of the business. Some of these dimensions are discuss below:

i. **Bringing of foreign materials into examination hall:** this is a situation where students bring into the examination hall notes, textbooks, and other prepared materials. The method has nicknamed as "hide and seek microchip, tattoo or magic desk". Sometimes students bring into the hall unauthorized materials like sophisticated and scientific calculators or four figure tables. Some methods like contraband, bullet, super print, escort, missiles, and pregnant biros and so on [3, 11].

ii. **Assistance from educational stakeholders:** Examination stakeholders include parents, teachers, lecturers, supervisors, security agents, printers and staff of examination bodies. Some parents go to any length in buying question papers for their children while some others even buy certificates for their children. Supervisors colluding with teachers, school principals or students by allowing teachers to come around to teach the students during the examination period; lecturers or teachers releasing question papers, giving underserved marks, or allowing students to illegally re-take examination papers. Security agents, printers and staff of examination bodies also sell question papers [3].

iii. **Impersonation:** this is a situation where a candidate sits in an examination for another candidate, thereby pretending to be the real or original candidate. Impersonation is becoming very rampant, even among school candidates. Various methods that have been devised by students [11, 15, 3] and these include:

   a. Entry for similar subjects: the plot is hatched right from the entry stage by making the impersonator to enter for the same subjects and sit for the examinations in the hall with the candidate; he writes the candidate's name and number on his booklet while the candidate writes the impersonator's and they exchange scripts before submitting.
   b. Multiple entries: that is candidates entering for the same examination in several parts of the locality. It has also been observed that several candidates struggle unnecessarily for live question papers at the beginning of a paper, which have then passed to touts for assistance. In addition, candidates deliberately come into the hall with the sole aim of smuggling the question paper out as soon as the paper starts and bringing the solution inside later.

What Is Biometrics?

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 [1, 2, 5, 9]. 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 or handprint. Behavioral biometrics relates to the behavior of a person, including but not limited to: typing rhythm, gait, and voice. Some

researchers have coined the term behavioral metrics to describe the latter class of biometrics. Traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods. However, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information [5].

Biometric Functionality

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Universality means that every person using a system should possess the trait. Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another. Permanence relates to the manner in which a trait varies over time. More specifically, a trait with good permanence will be reasonably invariant over time with respect to the specific matching algorithm [5, 7].

Commonly Used Biometrics

Biometric technologies enable automatic personal recognition based on physiological or behavioral characteristics. Biometric is the automated identification or verification of human identity through the measurement of repeatable physiological and behavioral characteristics [4]. Selection of biometrics in any practical application depends upon the characteristic measurements and user requirements. We should consider Performance, Acceptability, Circumvention, Robustness, Population coverage, Size, Identity theft deterrence in selecting a particular biometric. Selection of biometric based on user requirement considers Sensor availability, Device availability, Computational time and reliability, Cost, Sensor area and power consumption [9, 14, 16].

i. Hand Geometry

Hand geometry involves the analysis and measuring of the hand and fingers [9]. The user places their hand on the reader with their fingers in designated positions. A camera is then used to capture both a top view, which gives the length and width, as well as a side view, which gives the thickness. Hand geometry is one of the most established uses of biometrics today. It is accurate and fast.

ii. Retinal Scanning

Retinal scanning involves using a low intensity light to scan the unique pattern found in the retina portion of the eye. An optical coupler is used to produce the light, which analyzes the layer of blood vessels found at the back of the eye. It requires the user to position their eye at the reader and focus on a central point. This is not always convenient for those who wear glasses and some find the idea of a light scanning their eye intrusive, although it is not painful

and poses no known danger. Retinal scanning devices are often used in areas where high security is needed and where less consideration is given to convenience and comfort of the user [8].

iii. Iris Scanning

Iris scanning technology is commonly thought of as the most secure or strong biometric system. This is because the iris contains a very complex pattern and large number of measurable characteristics that make it practically impossible to replicate. Even a person‘s right and left iris patterns are different. For iris scanning, a camera is used to record a digital image of the user‘s iris. Contact lenses and glasses do not interfere with the scan. And unlike retinal scanning, there is no intrusive light beamed into the individual‘s eye. Among all biometric technologies, iris scanning has the most potential for further development [6].

iv. Voice Verification

Voice verification uses a microphone-recording device to capture a sample of a user‘s voiceprint. Measurements of a number of characteristics were taking, including cadence, pitch, and tone. Voice verification considers a hybrid of physical and behavioral biometric types. On the physical side, the shape of your throat and larynx helps to predetermine your voiceprint. But then again, your experiences help influence such things as inflect and dialect. In addition, although difficult to do, it is possible that one could alter their voiceprint. Additionally, it is important to make sure that the distinction between voice verification and voice recognition is understood. Voice recognition is software that is able to decipher words that has been spoken, and is not an authentication technique. Voice verification is simple to implement. Because most workstations come with a microphone of some sort, pre-installed, new hardware is usually not needed. It may also be implemented using current telephone systems. Voice verification has run into some opposition and has been accused of being hard to use from an end user perspective [7]. At times, it is difficult to enroll in the system as background noises, and static as well as the common cold can cause problems at enrollment and during verification.

v. Signature Verification

Signature verification involves the use of a special pen, tablet, or both to capture the way a person signs their name. Although the final appearance of the signature is important, a number of other attributes are captured as well [16]. These include speed, velocity, pressure, angle of the pen as well as the number of times the pen is lifted from the pad. Signature verification has been considered very accurate. Additionally, most users will not object to providing their signature for verification, as they are used to identifying themselves by signature all the time (i.e. credit card slips, checks, etc.).

vi. Facial Recognition

Facial recognition utilizes distinctive features of the face to authenticate users. A camera of some sort (digital, video or thermal) is used to capture the features. This includes such things as the upper outlines of the eye sockets, the cheekbones, the sides of the mouth, and the location of the nose and eyes. Video facial recognition maps out a number of points on the face or creates a three dimensional image to be used for comparison. The user is usually required to stand a few feet away and most systems are capable of compensating for expressions, glasses, hats and beards. Poor lighting can cause problems so most systems will need to be placed in well-lit areas. Thermal recognition systems use an infrared camera to scan faces and create a digital map of their thermal patterns. This digital image is known as a thermo gram. Branching blood vessels under the skin, which are hotter than the surrounding tissue, are responsible for creating the hot spots that the infrared camera picks up. Much like fingerprints, no two people are known to have the same thermo gram [2].

vii. Fingerprint Verification

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. 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). The positioning of pores and straight pattern matching may also be used. More recent developments include the use of moiré fringe patterns (superimposing of lines and grids to capture three dimensional surface shape) as well as ultrasound. Fingerprint systems should be kept clean as smudges or dirt and grime may cause problems for the reader [4, 6].

Methodology

In order to attain quite reasonable acceptance of the research work we made use of the internationally accepted software engineering model, this system is designed using the SSADM (Structured System Analysis and Design Methodology) and Prototype Model which are object oriented.

The SSADM Approach

The SSADM is a system approach to the analysis and design of information system. It involves the application of a sequence of analysis, documentation and design tasks concerned with the analysis of the current system logical data design, logical process design.

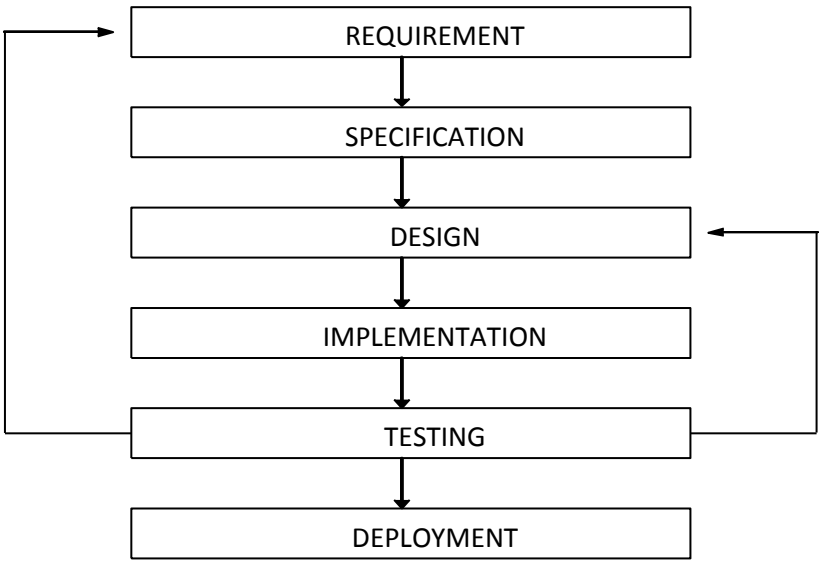

Figure 1: The SSADM Approach [12]

Prototyping is a development approach used to improve planning and execution of software projects by developing executable software systems (prototypes) for experimental purposes. It is very suitable for gaining experience in new application areas and for supporting incremental or evolutionary software development. Prototyping has many objectives including evaluation of the design, functionality and user interface. This paper focuses on the user interface aspect with some linkage to the functionality. A function defined in the specification may seem useful and well defined but when the users finally try to use the application they find that their view was incorrect. Prototypes thus let user validate and evaluate their requirements and thus, users can discover requirements omissions early in the process. Rapid Application Development Methodology uses development of the prototypes by the software team, working closely with the users in the requirements identification phase. Moreover, prototype model helps to gain a better understanding of the user's requirements, to gain a better understanding of development technologies, allow the customer to explore possibilities, to investigate the feasibility of a development project.

The Prototyping Process

There have been many suggestions over the years as to how prototyping should carry out. He describes a basic model as shown in figure 2:

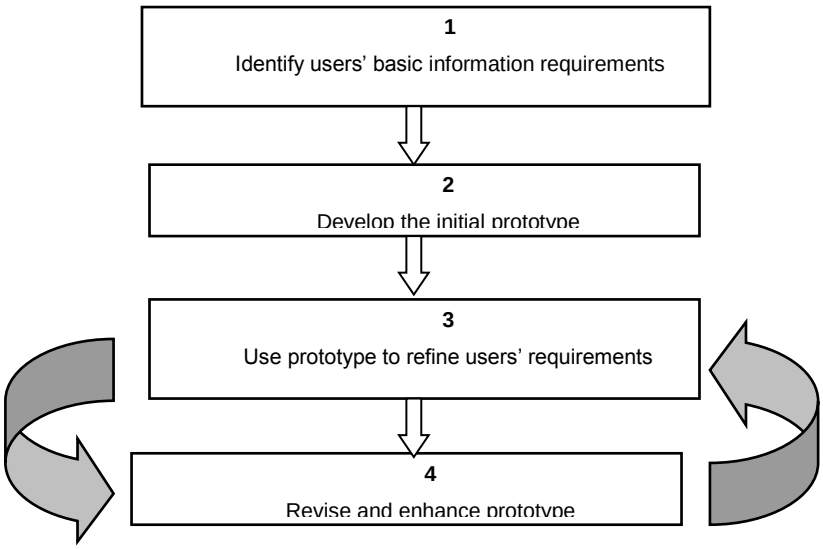

Figure 2: General Prototyping Process [12]

Use-case Diagram of the Proposed System

The figure 3 below shows the various users of the proposed system together with their various use cases.

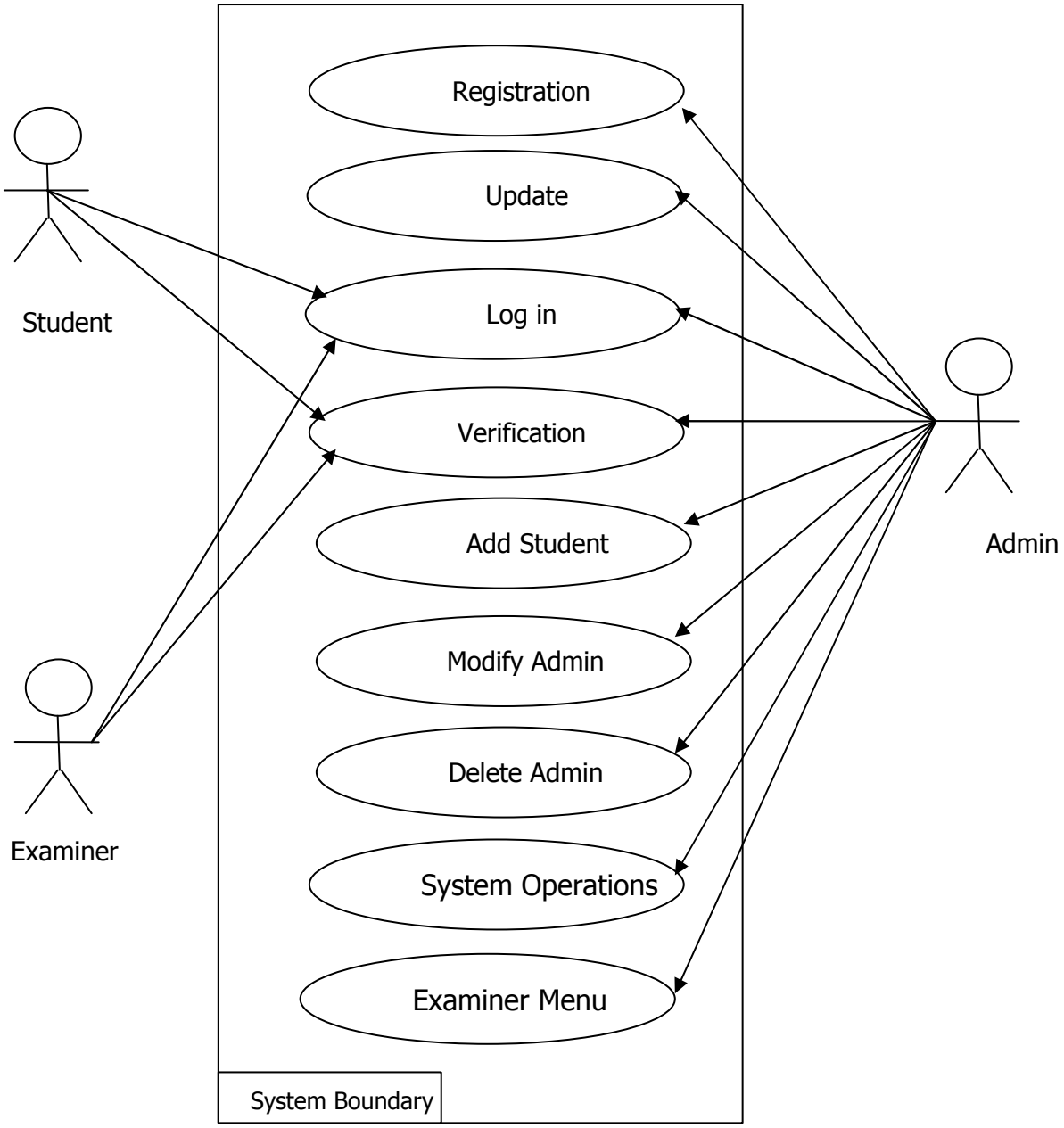

Figure 3: Use-case Diagram of the Proposed System

The Biometric Access System

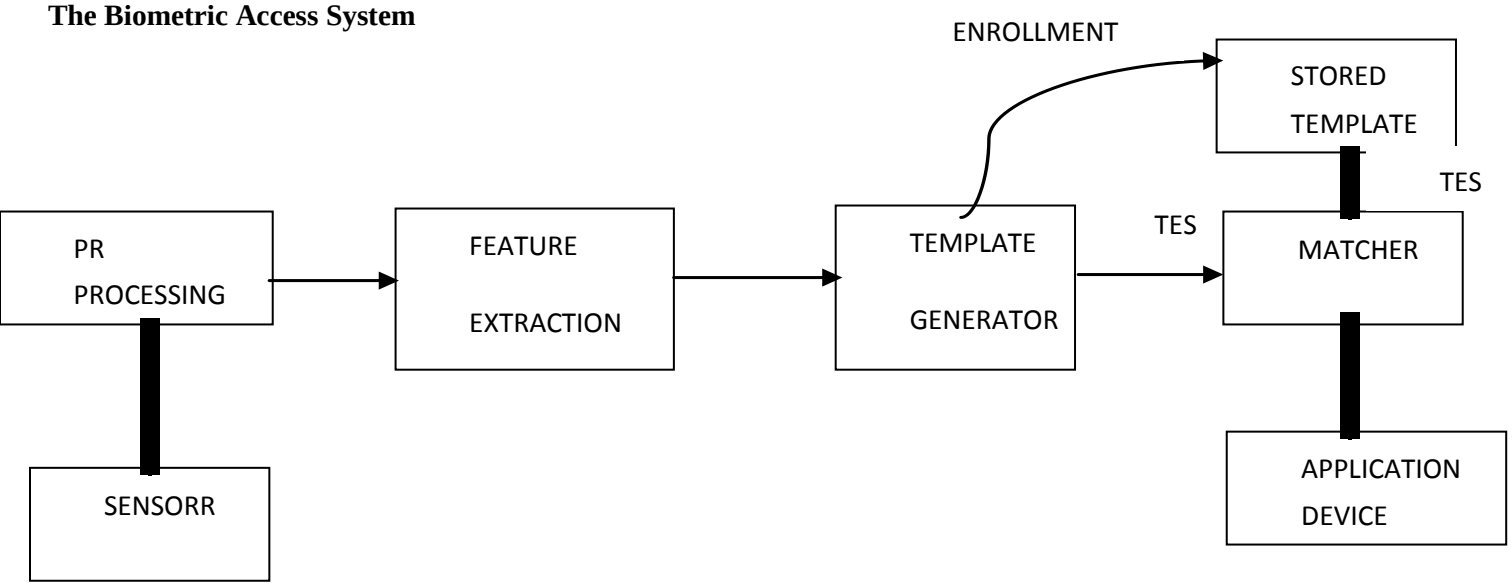

Figure 4: Conceptual Design Describing How to Access the System

The diagram above shows a simple block diagram of a biometric system. The main operations the system can perform are enrollment and test. During the enrollment, biometric information from an individual is stored. During the test, biometric information is detected and compared with the stored information. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and our system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. For the sake of our discussion, the sensor may be a fingerprint capture device, which provides an interface where the user thumbprints. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise or image), to use some kind of normalization, etc. The above feature is built into the capture device. In the third block, features needed are extracted. This step is an important step, as the correct features need to be extracted and in the optimal way. A vector of numbers or an image with particular properties has to be used to create a template. A template is a synthesis of all the characteristics extracted from the source, in the optimal size to allow for adequate identification. If enrollment is being performed the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in area).

Architectural Design of the System

The architecture of our automatic identity authentication system as shown in Figure 3.6.4; it consists of four components: user interface, system database, enrollment module, and authentication module. The user interface provides mechanisms for a user to indicate his/her identity and input his/her fingerprints into the system. The system database consists of a collection of records each of which corresponds to an authorized person that has access to the system. Each record contains the following fields that are used for authentication purpose: user name of the person, minutiae templates of the person's fingerprint, and other information.

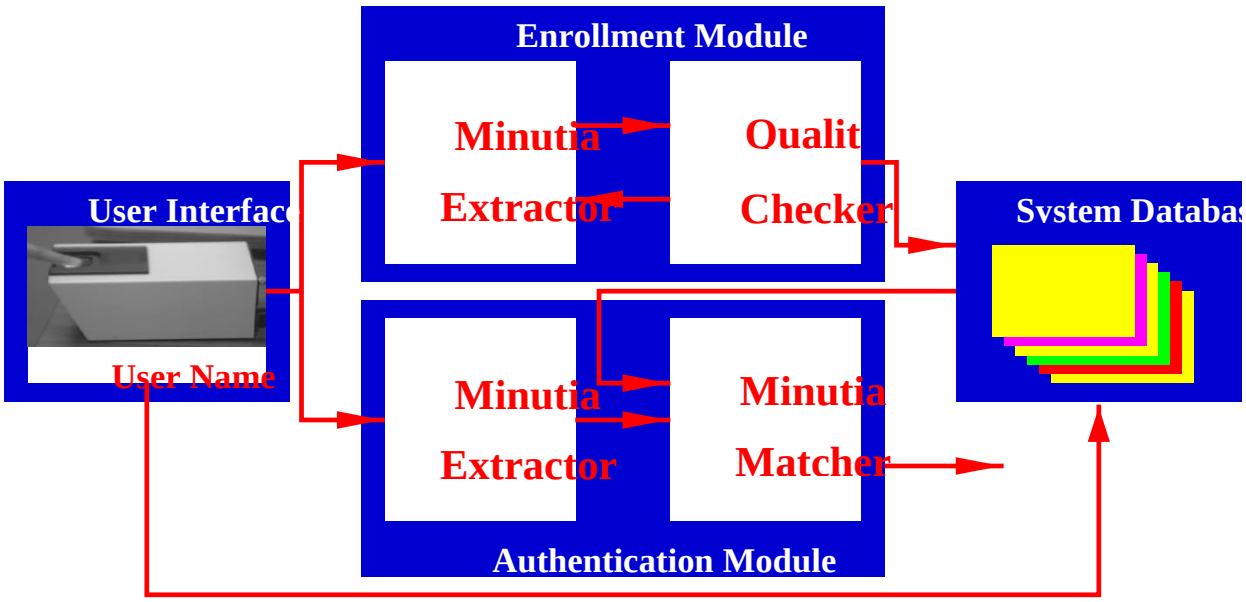

Figure 5: Architecture Design of the system

Some sample interfaces of the proposed system

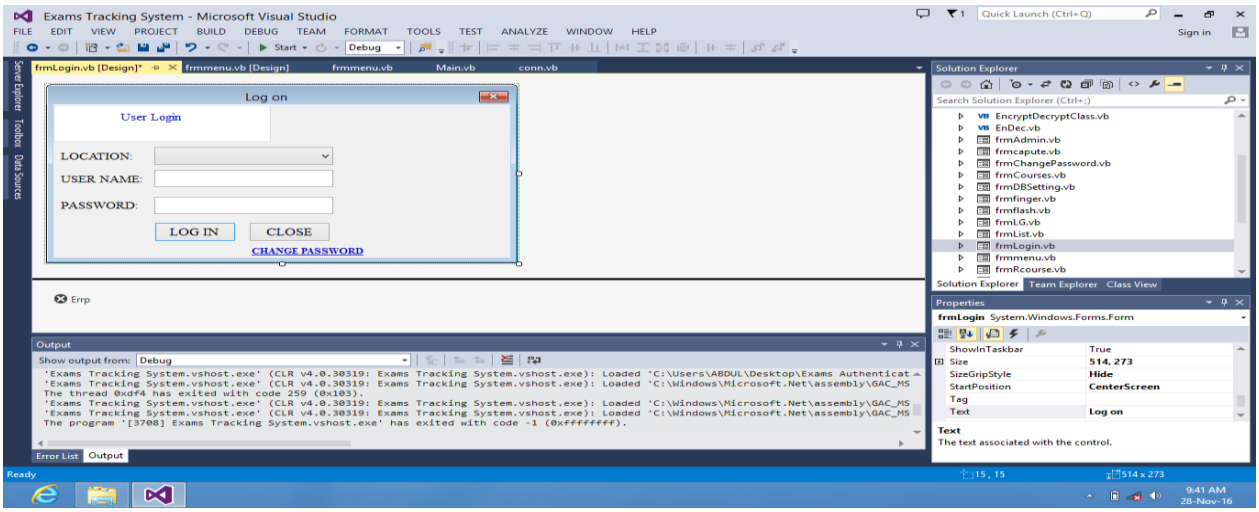

Figure 6: An Interface of Login Page

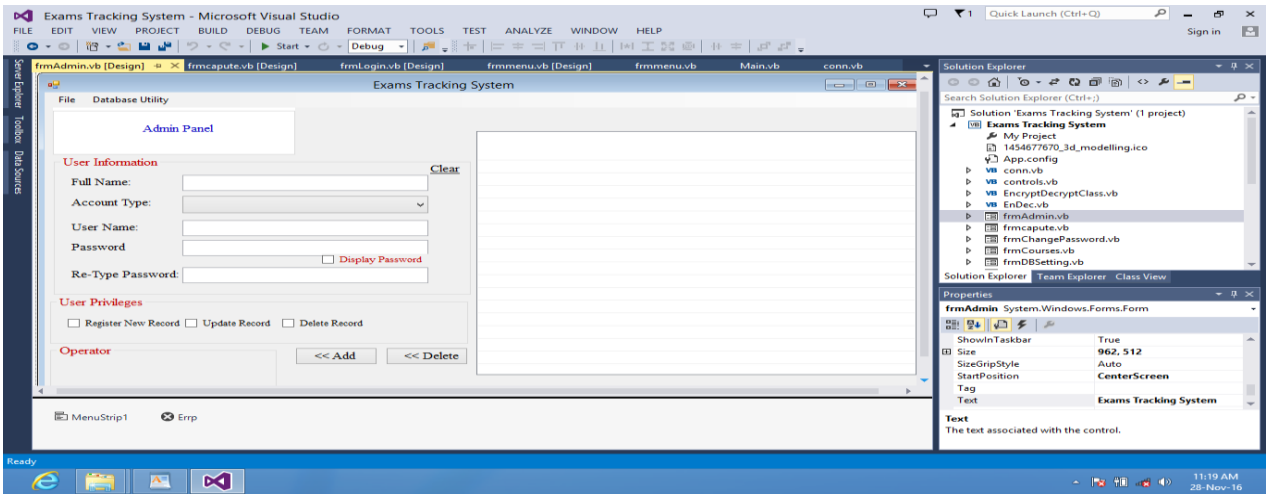

Figure 7: An Interface of Login Admin Panel

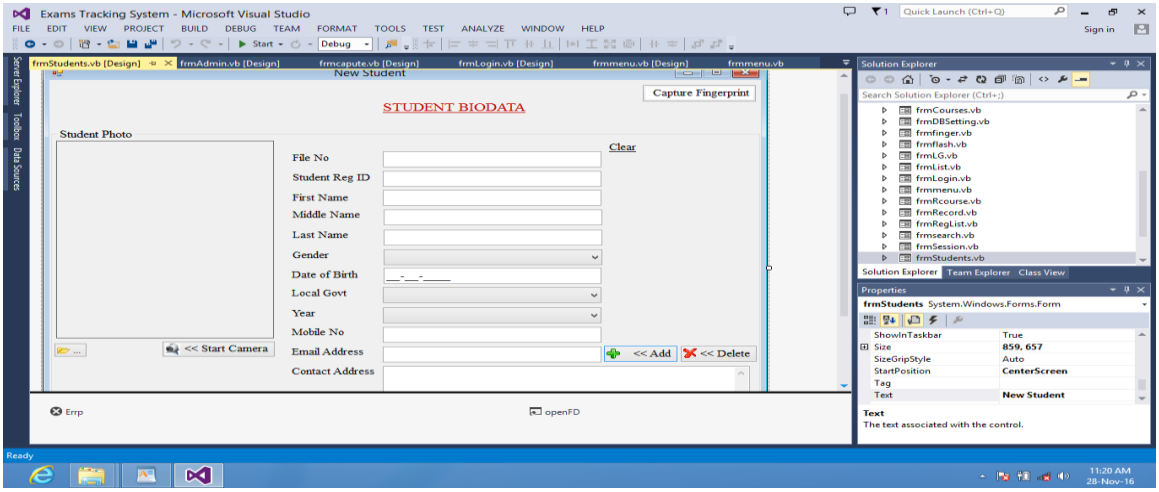

Figure 8: An Interface of Student Bio data

Discussions

The system was evaluated using usability testing. The usability testing technique is a technique for ensuring that the intended users of the system can carry out the intended task efficiently, effectively and satisfactorily. The following tests are carried out to evaluate the developed solution:

i. Test of Biometric Efficiency
ii. Speed of Identification and Authentication
iii. Test of General Requirement

i. Test of biometric efficiency: False Accept Rate (FAR) and False Reject Rate (FRR) are the error rates which are used to express matching satisfaction. The parameters used to measure these error rates include;

a. False Accept: False Accept is a situation where wrong fingerprint is accepted as valid for an individual during verification.

b. False Reject: False Reject is a situation where the system fails to match the valid fingerprint of an individual.
c. True Accept: True Accept is when a fingerprint matches with the fingerprint of same individual.
d. True Reject: Is said to occur when the system rejects a wrong fingerprint in the process of verifying an individual.

ii. Speed of identification and authentication: This test is used to measure the average time it takes to record student attendance and also to authenticate student entrance into examination venue in comparison with manual system.

iii. Test of general requirements: The software developed is also tested and evaluated based on the following criteria:

a. Ease of Enrollment
b. Adherence to Rules for Examination eligibility
c. Ease of viewing records of students

Conclusion

The proposed system has proved to be more successful when compared with manual systems. The genuineness in the use of fingerprint makes it a reliable access control technique. The fact that a user no longer needs to carry identity cards and other documents for identification explain the ease of use. Student verification system redefines the manual verification system, hence averts academic fraud and illegal studentship certificate and document.

References

1. Z. R. Li and D. P. Zhang, "A fingerprint recognition system with micro-computer," inProc. 6th ICPR,Montreal, Canada, 1984, pp. 939–941.

2. R. Clarke, "Human identification in information systems: Management challenges and public policy issues," Info. Technol. People, vol. 7, no. 4, pp. 6–37, 1994.

3. Two Day Summit on Examination Malpractice in Nigeria Organized Faculty of Education, Ambrose Alli University, Ekpoma, November 10-12, 2014. In Proceedings of the Sixth International Conference on Cognitive

4. Griaule Biometrics LTDA. 2007. *Fingerprint SDK2007 Developer's Manual.* http://www.griaulebiometrics.com

5. Beyond LSI, Inc. 2005. "Fingerprint Technology".August, 2005. http://www.beyondlsi.com.

6. L. o'Gorman. "Fingerprint Verification" in Biometrics: personal Identification in Education sector, pp.45-66. Kluwer academic Publishers. 2001

7. R Clarke. "Human Identification in information system": Management challenges and public issues, info. Technol. People, Vol.7, pp. 7-38, 1997.

8. Suhansa, R., George, Y. and Ronald, W. (2011). Student's verification system for Online Assessments: Botstering Quality and interigty of Distrance Learning. Journal of Industrial Technology. Volume 27 Number 3. P1-8.

9. Alotaibi, S (2010). "Using biometrics authentication via fingerprint recognition in e -exams in e-learning environment", The 4th Saudi International Conference, The University of Manchester, UK.

10. Barnes M., Clarke, D. & Stephens, W. (2000) Assessment as the engine of systemic reform. Journal of Curriculum Studies 32 (5), pp. 623-650. .

11. Boston. (2002). The concept of formative assessment. Practical Assessment research & Evaluation, 8(9).

12. El-Ghareeb. (2009). "e -Learning and Management Information Systems, Universities Need Both", e -Learn Magazine, September 2009.

13. EPPI. (2002). A systematic Review of the Impact of Summative Assessment and Tests on Students' Motivation for Learning. University of London: Evidence for Policy & Practice Information & Coordinating Centre

14. Hayes B., Ringwood J., editors. Authenticating student work in an e-learning programme via speaker recognition. 3rd International Conference on Signals, Circuits and Systems (SCS) 2009: IEEE.

15. Heinrich E. Milne, J. & Moore, M. (2009). 'An Investigation into E -Tool Use for Formative Assignment Assessment – Status and Recommendations'.

16. Hernandez. J.A., Ortiz, A.O., Andaverde, J.& Burlak, G. (2008). 'Biometrics in Online Assessments: A Study Case in High School Students'.