ISSN:
Print - 2277 - 0593
Online - 2315 - 7461
© FUNAAB 2012

Journal of Natural Science, Engineering and Technology

A BIOMETRIC AUTHENTICATION SYSTEM FOR ELECTRONIC EXAMINATION

***[1]A.J. IKUOMOLA [2] O. A. AROWOLO**

*1 Department of Mathematical Sciences, Ondo State University of Science and Technology, Okitipupa, Ondo State, Nigeria.
2 Department of Computer Science, Tai Solarin College of Education, Omu Ijebu. Nigeria.
***Corresponding author**: deronikug@yahoo.com **Tel:** +2347062843043

ABSTRACT

Electronic examination system was introduced into the examination system to overcome the stress and the time consumption factors commonly experienced in the traditional paper-based examination system. In both the traditional and the e-examination system, eligible students are allowed to write examination only after they have been manually authenticated by invigilators. However, impersonation problem persist owing to human or examiner error which occur when examiners cannot distinctively distinguish each student (e.g. in the case of twins). This paper attempts to address the problem by proposing fingerprint biometric authentication technologies to curb unethical conduct during electronic examination. The fingerprint biometric device has the ability of identifying unique biological characteristics of student. The e-examination system is made up of four phases; Registration, Verification, Examination and Submission phases. Two categories of software were used: the system software and the application software. The system software consists of the operating system which is Windows XP professional Service Pack 2 and the application software architecture is C# programming language. C# is a multi-paradigm programming language encompassing strong typing, imperative, declarative, functional, procedural, generic, object-oriented (class-based) and component-oriented programming disciplines. C# was used to implement the design because of its interactiveness and good functionalities in graphical outputs. Testing the new design with data, the result shows a system that can administer examination effectively.

Keywords: *Adaptive, Artificial Neural Network, Fuzzy, Performance*

INTRODUCTION

Prior to about a decade ago, the only mode adopted by all educational institutions for conducting examination is the traditional paper-based examination system. In this examination system, students are usually presented with question sheet(s) containing a set of questions. The educational institution also makes provision for answer sheets on which the students fill in their answers. In traditional paper-based examination system, eligible students are usually authenticated or checked-in manually by the examiners. Examiners are also saddled with the responsibility of ensuring that students comply with the rules of examination conduct. There is non-anonymity of teachers in traditional paper-based examination system i.e. students have knowledge of who will mark their answer sheets, hence they can bribe or threaten them in order to receive better grades.

In recent years, another way of conducting examinations has been developed differing

from the traditional paper-based system. This other system involves the use of electrical device (computer system) to disseminate questions, collect and mark answers provided by students. In a more precise terminology, it is referred to as e**lectronic examination system**. Ayo *et al.* (2007) define e-examination as a system that "involves the conduct of examinations through the web or the intranet". Awosiyan (2010) quoting Prof. Olu Jegede, the former Vice-Chancellor of NOUN, says that: e-examination was introduced to address series of anomalies being encountered in the manual tests. He said that the e-examination would remove all human errors recorded in manual examination and create opportunity for students to access their results immediately.... With this, we have removed so many hiccups in the compilation of answer scripts and movement of examination papers from one part of the country to another. The examination is conducted now through the net." ... it would be difficult for students to carry out any form of examination malpractice.

Electronic examination is of great interest from both educational and pedagogical points of view. It is aimed to resolve many questions and limitations in the conventional or traditional examination. It is flexible and handy to use with complete question types and excellent security strategy so as to make e-examination automatic and reduce the cost. It can be used for all kinds of different scaled e-examination in different subjects' primary, secondary and tertiary institutions and in class examinations or exercises (Ikuomola and Olayanju, 2010). Conducting examination through the use of computer system is made possible by the advent of web applications into the computing technology. Web applications has contributed a significant revolution in not only the social life of web users, but also the traditional system of education and examination. Web-based testing and assessment has become one important area of application of the web technology. Many institutions are beginning to re-evaluate their traditional methods of conducting examination and have started considering using electronic method because of the fact that it offers greater flexibility than the traditional/manual approach. Flexibility in electronic examination system is seen in its use to offer examination at different times to students and in different locations. More importantly, questions are shuffled having the same structure and level but different contents.

Basically, the electronic examination (e-examination for short) system involves the conduct of examinations through the web or the intranet. Its aim is to reduce the large proportion of workload on examination, grading and reviewing. The set of questions often used in the e-examination system are multiple choice objective tests and quizzes that can be formally and easily evaluated online. In essence, e-exam system provides the existence of an examination system where all exam stages are performed electronically.

The problems associated with the conduct of e-examination are impersonation in the examination hall and repetition of examination sessions by students:

In the context of examination, impersonation is doing examination on behalf of someone else. From research, it has been deduced that the main reason why impersonation has become very rampant in the educational system is because of the desire of student to pass at all cost. In traditional paper-based

examination system, exam takers are usually identified by examiners. It is the responsibility of examiners to make sure that each person checked into the examination hall is really supposed to be taking the examination he has been checked in for. The aim of doing this is to reduce this impersonation problem but it has been discovered, however, that the problem still persists owing to human (examiner) error. The human error comes into play when examiners cannot distinctively identify each student (e.g. in the case of twins).

The structure of e-examination is such that the bulk of questions in the database is shuffled and a specific number of questions is selected and presented before each student. Each student gets access to his/her own portion of the multiple questions by logging in using his/her matriculation number in the space provided. The problem of multiple examination sessions is encountered when a student restarts/refreshes the system he is working on realizing that he cannot successfully answer the set of questions he has been offered. By doing so, he is presented a new set of questions.

In order to solve these problems a biometric authentication system for e-examination was proposed. Finger biometric can be a suitable solution for rapid authentication of users. Fingerprints can be used for authenticating students' submissions of exams via the use of biometric devices because Fingerprints are a permanent attribute unique to an individual.
Williams (2002) pointed out that fingerprints have been universally acceptable in the legal system worldwide.

LITRATURE REVIEW

According to Tabitha *et al.* (2006), biometrics is defined as "the application of computational methods to biological features, especially with regard to the study of unique biological characteristics of humans. Such unique biological characteristics relies on individual humane identities such as DNA, voice, retinal and iris, fingerprints, facial images, hand prints or other unique biological characteristics. Moreover, Pons (2006) notes that biometric devices are technological devices that utilize an individual's unique physical or behavioral characteristic to identify and authenticate the individual precisely. Essentially, biometric technologies operate by scanning a biological characteristic and matching it with the stored data. Jain *et al.* (2000) noted that a biometric system is "essentially a pattern recognition system that makes a personal identification by establishing the authenticity of a specific physiological or behavioral characteristic possessed by the user". Coventry *et al.* (2003) discussed the usability aspect of authentication systems and noted that it is a "tradeoff between usability, memorability and security". Coventry *et al.* (2003) maintained that most biometric systems include a digital identifier, a template and a recognition algorithm and they follow similar matching processes. However, they maintained that biometric systems can be separated into physiological biometric (finger, iris) as well as behavioral biometric (voice, key board typing behavior). Biometric systems performance can be assessed by employing statistical methods in which accuracy is calculated.

Although biometric systems are relatively reliable, Coventry *et al.* (2003) asserted that system malfunction stems from users' lack of establishing the biometric during the initial stage as well as potential interruptions during transmission of the biometric image in the validation process. Subsequently, they con-

cluded that although the tradeoff between security and usability aspects remains, biometric systems can facilitate automatic verification for public environments.

Pons (2006) maintained that fingerprints biometric scans are the most commonly used biometric solution as they are less expensive compared with other biometric solutions. According to Jain *et al.* (2000), a fingerprint is a unique "pattern of ridges and furrows on the surface of a fingertip, the formation of which is determined during the fetal period". Fingerprints are unique for each individual, where even identical twins have different fingerprints. Several scholars documented the increase popularity of fingerprint biometric-based systems and their decline in costs (Pons, 2006). Similarly, fingerprints can be used for authenticating students' submissions of exams via the use of biometric devices. Furthermore, Williams (2002) pointed out that fingerprints have been universally acceptable in the legal system worldwide. Fingerprints are a permanent attribute unique to an individual. Fingerprints can be scanned, transmitted and matched with the aid of a simple device. McGinity (2005) pointed out that biometric have been commonly employed in replacing conventional password systems. Biometric devices enable portable scanning and rapid identification. Thus, finger biometric can be a suitable solution for rapid authentication of users. Using a portable device, users can scan their fingerprints and send a print image via the Internet to the University's network. The network will consist of an authentication server that will house a database of students' fingerprints images. The server will then process the matching of the transmitted print image with a stored copy of the fingerprint (called "template"). Following that, the server will generate a matching result. Thus, McGinity (2005) predicted that fingerprints based biometric would become a household activity in the near future. Yang and Verbauwhede (2003) proposed a secured technique for matching fingerprints in a biometric system. Similarly to McGinity (2005), they argued that biometric systems enhance security far more than the current systems. Biometric systems are more accurate as well as simpler to operate compared with passwords systems. Yang and Verbauwhede (2003) described a fingerprint based biometric system in which the fingerprint template is kept in a server during initiation. Upon scanning the finger, an input device scans a biometric signal and transmits it to a server where it is processed for matching. In an effort to shield the system against security compromises, they recommended processing the matching of fingerprints images in an embedded device rather than the server and only transmitting the results to the servers. Furthermore, they suggested encrypting the fingerprint template prior to storing it on the server. Fingerprints templates can be decrypted whenever a matching process occurs. Yang and Verbauwhede (2003) provided additional solutions useful for building up multiple layers of security in fingerprint based biometric systems.

DESIGN METHODOLOGY

Architecture for Biometric Authentication System for Electronic-Examination

The architecture for the biometric authentication system for electronic examination is shown in Figure 1. The architecture is made up of the registration phase, verification phase, examination phase and submission phase.

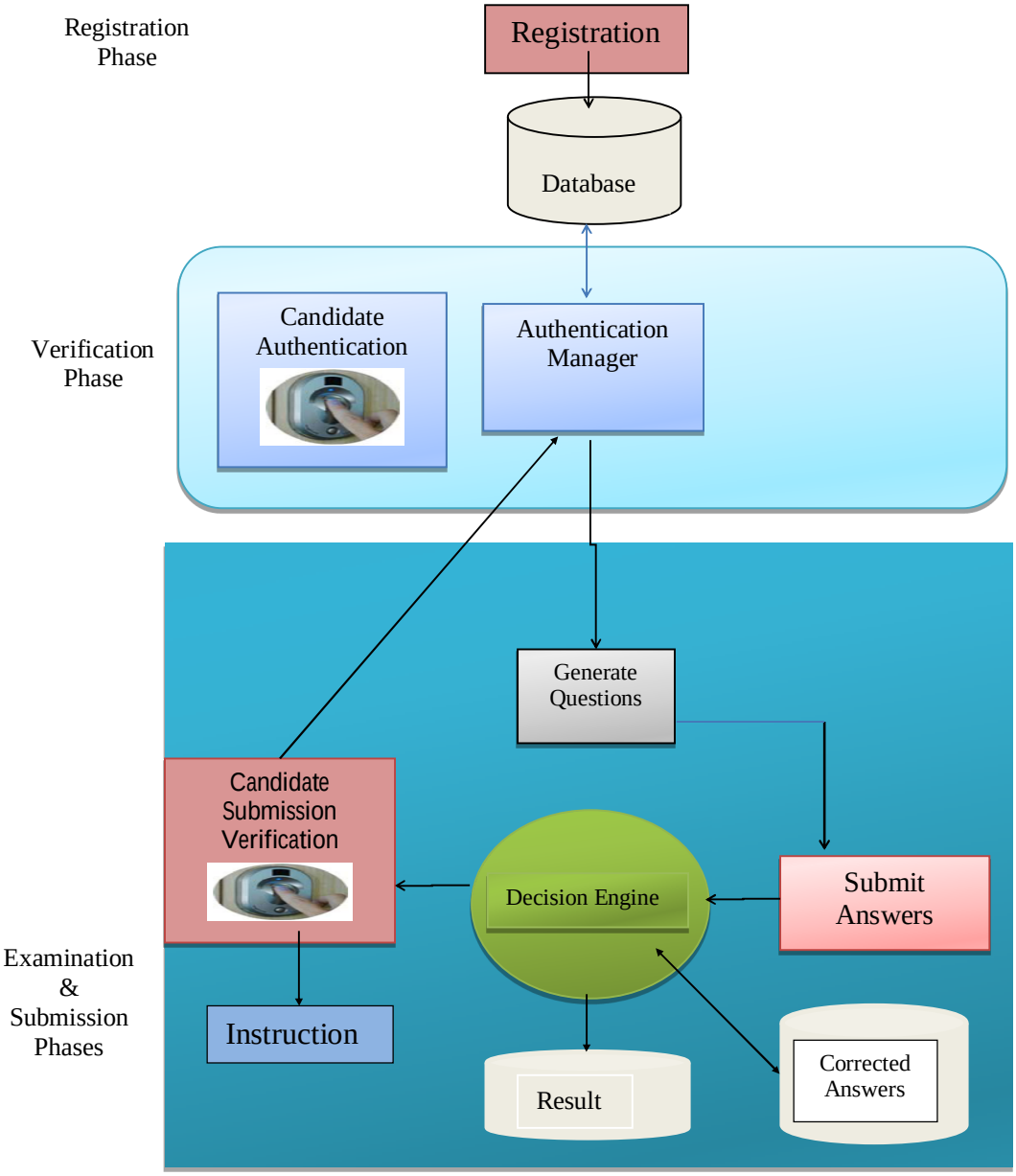


Figure 1: Biometric Authentication System for Electronic-Examination

Registration Phase

At this stage, students will be required to show up at the ICT centre to register their data such as courses offered for the semester, name, matriculation number and fingerprint. Image of each student's fingerprint is captured using fingerprint sensors in fingerprint identification devices. The information collected from each student is afterwards stored in the database. The essence of storing the collected information in the database is to be able to recall them for comparison when the student moves on into the verification stage during examination. The registered fingerprint pattern serves as each student's unique password which enables him to gain access to the set of questions for each examination he is to write

Verification Phase

In this stage, students will first be requested to fill in their matriculation number and name after which they will be required to place their right thumbs on a fingerprint identification device. The purpose of having them place their fingerprints on the device is to make sure that the student writing the examination is actually the one that is supposed to write it. A student will only have been able to successfully pass through this stage if he has passed through the initial stage (registration stage). In verification phase, there exists an interconnection structure between the fingerprint identification device, database and the authentication manager. The fingerprint identification device is responsible for capturing input fingerprint patterns and presenting them for comparison. It places the input pattern before the authentication manager which has the responsibility of checking the database to see if the input fingerprint matches one already existing in the database. If a student's fingerprint pattern matches an already existing one, the student moves to the next stage which is the examination phase. In the case where no match was found, the student is denied access into the examination phase.

Examination Phase

Students gain entry into this stage haven passed through both the registration and the verification phases. Every student that gets access into this phase is considered a legitimate student, that is, the student's information already exists in the database. Examination phase is where students are faced with the set of questions they are expected to find answers to. After providing answers to their set of questions, they proceed to the next stage which is the submission phase.

Submission Phase

Submission phase comes up after the student is through with the examination phase and wants to submit. In this phase, the use of biometrics comes into play again. The essence of using biometrics in this phase is to ensure that the student that started the examination was actually the one that concluded it. After the student is through with the question, he clicks the submit button and receives an instruction to place his right thumb on the biometric device to conclude his submission. The authentication manager, at this stage, is programmed to compare the fingerprint of the student that started the examination with that of the student that is attempting to submit. If the fingerprints match, the student receives an instruction to proceed to the examiners desk to collect a receipt of attendance. In the case where the fingerprints do not match, submission is denied.

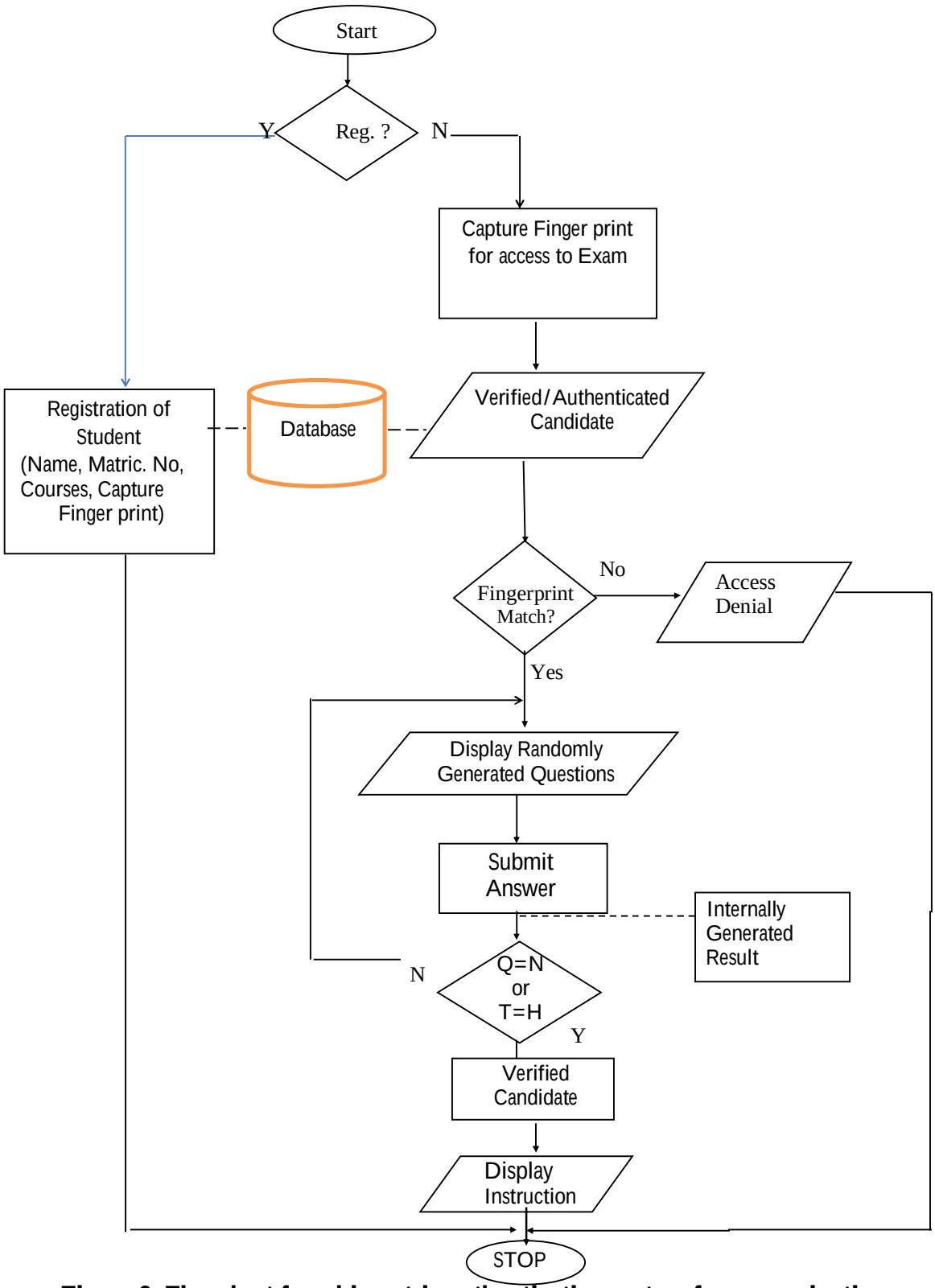


Figure 2. Flowchart for a biometric authentication system for e-examination

IMPLEMENTATION AND RESULTS

Implementation Procedure

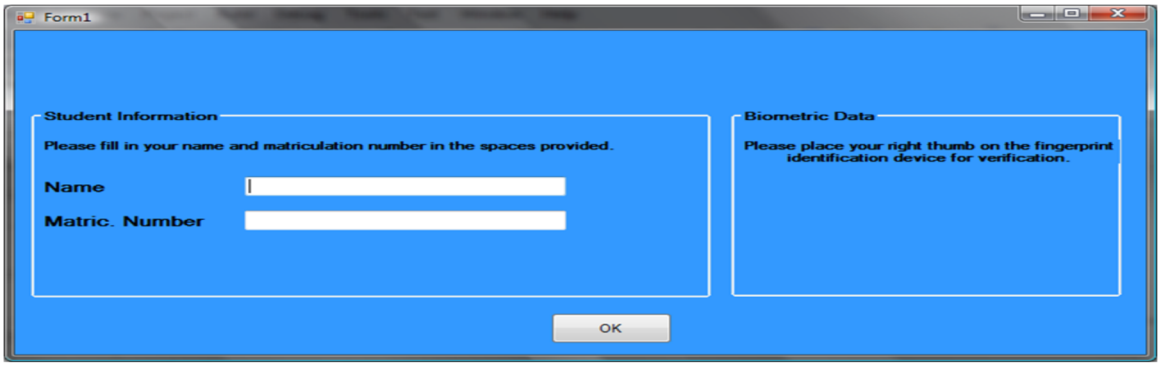
The two (2) categories of software used are the system software and the application software. The system software consists of the operating system which is Windows XP professional Service Pack 2 and the application software architecture is C# programming language. The data used for the implementation was collected from the past questions of Federal University of Agriculture Abeokuta, Ogun State.

Results and Discussion

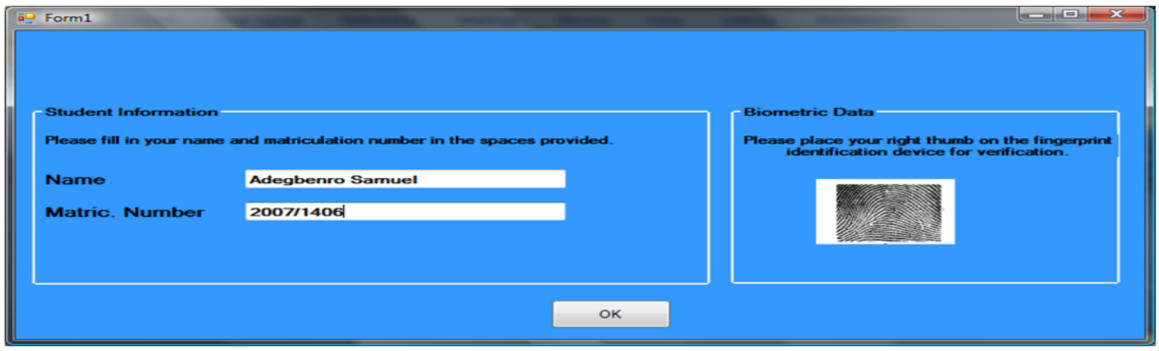
In this work, the running and testing of the design was carried out and the interface designs are shown.

Interface Design

Figures 3 a & b show the candidate console. Before a Candidate can access the e-examination area; he/she must have been authenticated by the system. Authentication requires the placing of the candidate's right thumb on the fingerprint biometric device. On the Console in Figure 3a, the student is expected to enter his/her name, matric. number and then place his/her right thumb on the fingerprint identification device attached to the system for verification.



In Figure 3b, the fingerprint pattern shows up immediately the student clicks OK in the former stage.



(b)

Figures 3a & b: Candidate Console for Verification

Figure 4 shows that the student is a registered candidate and the information about the candidate such as the name, matric. number and photograph are in the database

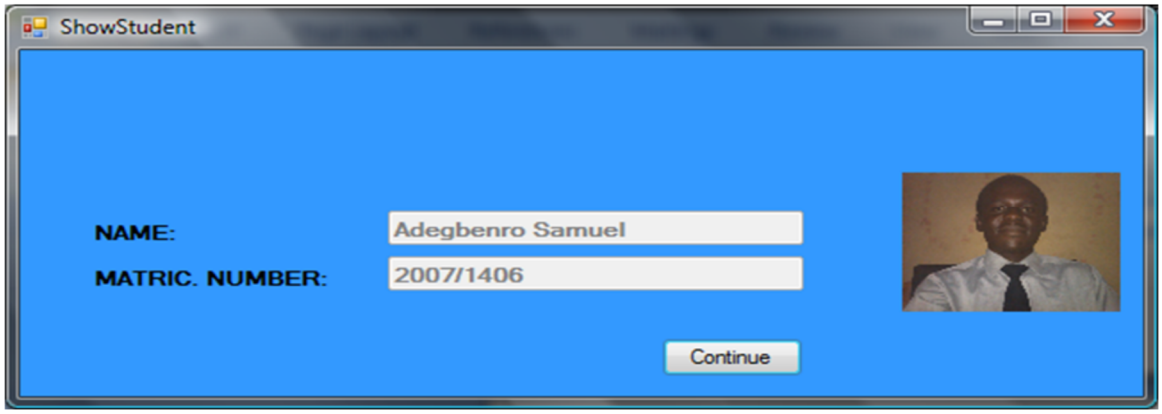


Figure 4: Verified Candidate

Figure 5 is a message interface that shows up after the student clicks on continue in the previous stage. Clicking OK in this stage will prompt the student to the set of examination questions.

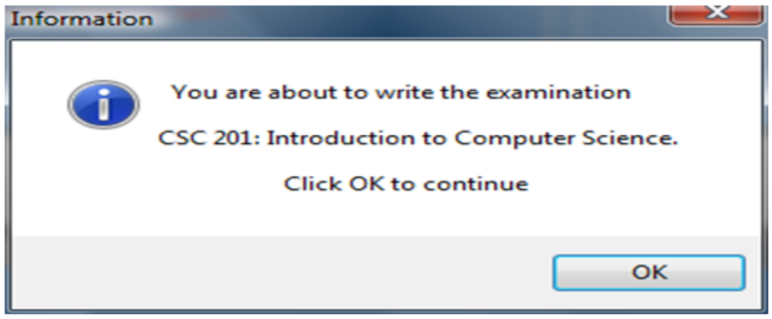


Figure 5: Prompt message

Figure 6 shows the internally generated N-types examination questions set for CSC 201 course.

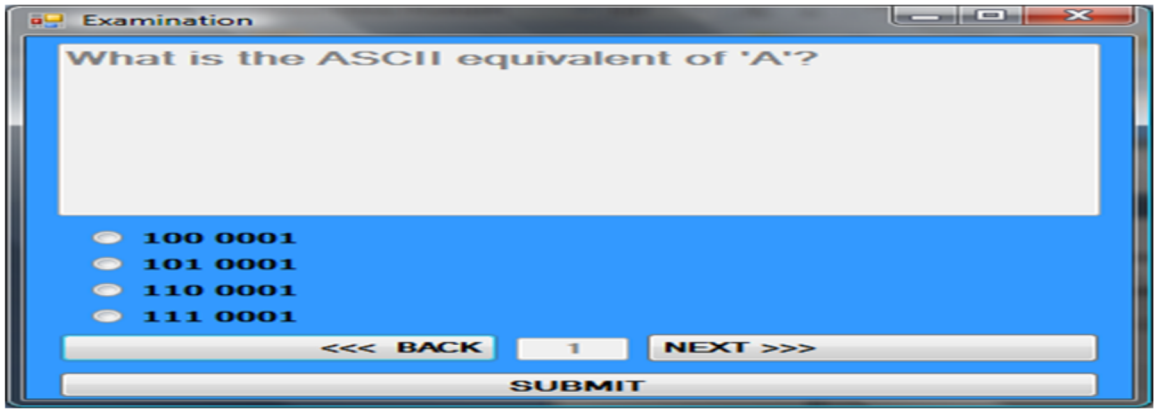


Figure 6: Question Sets

After the whole questions have been treated, the candidate can then submit his/her work by clicking on the SUBMIT button where he/she will be prompted again to place his/her right thumb on the fingerprint device for submission authentication as shown in Figure 7.

Figure 7: Submission Authentication

Figure 8 screenshot comes up after the student has successfully completed the examination process

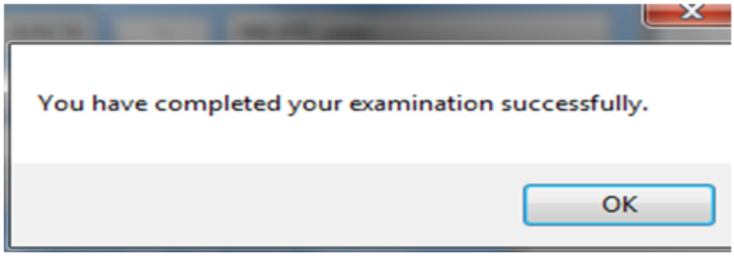


Figure 8: Successful Message

CONCLUSION

Traditional means of authentication, primarily passwords and personal identification numbers (PINs) or matric. numbers have dominated computing. This means of authentication is not effective in e-Exam because impersonation problem persists owing to human or examiner error which occurs when examiners cannot distinctively distinguish each student. We have been able to design and implement a biometric authentication system for e-Examination system, using finger biometric authentication system that is able to address a major issue of impersonation and cheating in e-Exam. This new design can successfully administer an examination process effectively.

REFERENCES

Ayo C. K., Akinyemi I. O., Adebiyi A. A. and Ekong U. O. 2007. "The prospects of e-examination implementation in Nigeria." *Turkish Online Journal of Distance Education-TOJDE*, 8(4): 126

Awosiyan, K. 2010. Stress and success of NOUN examination. Nigerian Tribune, July 1, p.10.

Coventry, L., De Angeli, A., and Johnson, G. 2003. Usability of large scale public systems: Usability and biometric verification at the ATM interface. *Proceedings of the Conference on Human Factors in Computing Systems.* Florida, USA, 153-160.

Ikuomola A. J. and Olayanju T. A. (2010). N-Types Electronic Examination System : An Effective Approach for Combating Examination Malpractice. *Journal of Natural Sciences, Engineering and Technology, 9(2): 2010*

Jain, A., Hong, L., and Pankanti, S. (2000). Biometric identification. *Communications of the ACM, 43*(2): 91–98.

McGinity, M. (2005). Staying connected: Let your fingers do the talking. *Communications of the ACM, 48*(1): 21-23.

Pons, A. P. (2006). Biometric marketing :targeting the online consumer. *Communications of the ACM, 49*(8): 60-65.

Tabitha J., Pirim, T., Boswell, K., Reithel, B, and Barkhi, R. (2006). Determining the intention to use biometric devices: an application and extension of the technology acceptance model. *Journal of Organizational and End User Computing, 18*(3): 1-25.

Williams, J. M. (2002). New security paradigms. *Proceedings of the 2002 Workshop on New Security Paradigms*, Virginia Beach, Virginia, Pp. 97-107.

Yang, S., & Verbauwhede, I. M. (2003). A secure fingerprint matching technique. *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, California, USA 89-94.

(Manuscript received: 28th September, 2012; accepted: 18th November, 2013).