Fingerprint Based Approach for Examination Clearance in Higher Institutions

Yakub K. Saheed, Moshood A. Hambali, Ismaeel A. Adeniji and Akeem F. Kadri

1Department of Physical Sciences, Al-Hikmah University, Ilorin, Nigeria
2Department of Computer Sciences, Federal University, Wukari, Nigeria
3Department of Computer Science, University of Ilorin, Ilorin, Nigeria
4Department of Computer Science, Kwara State University, Malete, Nigeria

yksaheed@alhikmah.edu.ng|hambali@fuwukari.edu.ng|herdeynig@gmail.com|akeem.kadri@yahoo.com

Abstract— Biometric techniques have become a prominent option and secured means of authentication capable of sustaining the emerging ubiquitous computing. The process for allowing students to sit for an examination has been through the presentation of medium of identification such as ID cards, library cards, fees clearance cards, photo cards, etc. This method of authenticating a student for an examination has an obvious problem such as presentation of fake clearance card, impersonation and so on. 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. This paper addressed all the aforementioned shortcomings and revealed the effectiveness of biometric system using fingerprint for examination clearance. The proposed examination clearance system used fingerprint identification. In identification, the system recognizes an individual by comparing his/her biometrics with every record in the database.

Keywords— Biometric Recognition, Clearance, Enrollment, Examination, Fingerprint Identification

INTRODUCTION

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. These paper clearance approaches encourage fraud, impersonation during the examination. As the level of security breaches and transaction fraud increases, the need for highly secured identification and personal verification technology is fast becoming apparent (Paul, Alane and Ari, 2004). Many organizations are trying to identify accurate, safe, and reliable techniques to protect access rights to their existing services or operations. Biometrics is the best answer to these concerns.

Biometric recognition techniques have emerged as most promising option for securing valuable information or system based on their physiological and/or behavioural characteristics. Because of the fact that individual’s biological traits cannot be forgotten, forged, misplaced or stolen (Hambali and Jimoh, 2015). 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 (Salil, Sharath and Anil, 2003). 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 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 (Farzad, 2012).

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 (Maltoni, Jain and Prabhakar 2009; Newman, 2010):

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 (Paul et al., 2004).

2 LITERATURE REVIEW

2.1 Overview of related work

Ezema, Joe-Uzuegbu, Eneh, and Amanze (2015) proposed fingerprint attendance system designed to also operate as a standalone and handheld system without the use of a computer, unlike other fingerprint attendance systems. Only administrator can register student in Ezema et al (2015), paper which is observed as the problem of this work. Rufai, Adigun and Yekini (2012) proposed a biometric model for examination screening and attendance monitoring in Yaba College of Technology (Yaba Tech). The existing examination screening process in Yaba Tech was provided and analysed. An abstract transition model that is based on the concept of automata was proposed. This Biometric Examination Screening and Attendance Monitoring System (BESAMS) model was conceptualized as a finite state machine.

Shoewu, Olaniyi and Lawson in (2011) work on an electronic card-based solution to the lecture attendance problem in higher institutions in the developing countries. This system used a single-chip computer based on subsystems interfaced serially to the serial port of the digital computer. Some of the limitations of this system are that not all computer systems possess serial port and the smart card can be easily misplaced/lost by the user which will prevent the user from gaining access to the system. Mahyidin (2008) also proposed student attendance management system using Radio Frequency Identification (RFID). The system is based on student card in order to grant or denial the student from taking attendance. This technique also did not identify individual based on who he/she is which therefore, can lead to impersonation.

Geetha (2010) designed an embedded application for fingerprint verification system. An extensive study of fingerprint verification was presented. The researcher implemented this project on the ZF Microsystems based single board computer with Cyrix Media GX based processor and coprocessor with a bus speed of 180MHz. The board only support Windows 3.11, 95/98, and Red Hat Linux 4.0. Survey investigation and analysis of the current method of paper-based examination clearance in some higher institutions also has the challenge of impersonation of another user with genuine card. Due to the inefficiency of traditional methods of clearance, a more secured and accurate biometric based model is needed to be formulated and implemented.

2.2 Materials and Method

In this study, we proposed to formulate and implement a simplified, efficient and reliable model for managing students examination clearance based on biometric fingerprint identification in higher institutions of learning.

2.3 Methodology

The proposed Biometric Examination Clearance (BEC) system uses fingerprint identification. In identification, the system recognizes individual by comparing his/her biometrics with every record in the database. In general, biometric identification consists of two stages:

i. Enrolment
ii. Authentication

During enrolment, the fingerprint of the user is captured (using a fingerprint reader, which are likely to be an optical scanner device, solid state or an ultrasound sensor or other suitable device) and the unique features are extracted and stored in database as a template for the subject along with the student ID. The objective of the enrolment module is to admit a student using his/her ID and fingerprints into a database after feature extraction.

These features form a template that is used to determine the identity of the student, formulating the process of authentication. The enrolment process is carried out by an administrator. During authentication, the fingerprint of the user is captured again and the extracted features are compared with the stored features in the database to determine a match. Features extraction performs some transformation of original features to generate other features that are more significant (Samina, Tehmina and Shamila, 2014). The identification accuracy of a biometric system is measured with the false (impostor) acceptance rate (FAR) and the false (genuine individual) reject rate (FRR). Flowchart for the BEC system is depicted in Fig 1.

The study adopted a qualitative research method. The model was implemented using Java programming language and the back-end makes use of MySQL as the database as well as the template. SecuGen fingerprint scanner was used to capture live fingerprint image.

3 Results

Generally, during examination period student produce evidence of school fees and registration forms to obtain clearance card in order to allow sitting for exam. But for FEC, an administrator sign in using his/her password and enroll student through the system.
The proposed fingerprint student BEC has four sections (Enrolment, Verification, Registration and Exams). The first section is where the administrator enroll the student’s bio-data, capture the fingerprint and passport photo. Figures 4 and 5 show the details.

After the enrolment stage and student’s bio-data registration, the verification can be done later most especially when it is time for examination to verify the authentication of student, in order to get admitted into examination hall.

4 PERFORMANCE METRICS

Although only user qualitative evaluation was carried out on the developed system, the following can be applied when using a automated evaluation approach.

True Acceptance Rate (TAR) / True Match Rate (TMR): This measures represents the degree that the biometric system is able to correctly match the biometric information from the same person. We try to maximize this measure.
False Acceptance Rate (FAR) / False Match Rate (FMR): This measure represents the degree or frequency where biometric information from one person is falsely reported to match the biometric information from another person. In this work we attempt to minimize this measure.

True Rejection Rate (TRR) / True Non-Match Rate (TNMR): This measure represents the frequency of cases when biometric information from one person is correctly not matched to any records in a database because, in fact, that person is not in the database. We maximize this measure in this work.

False Rejection Rate (FRR) / False Non-Match Rate (FNMR): This measure represents the frequency of cases when biometric information is not matched against any records in a database when it should have been matched because the person is, in fact, in the database. We attempt to minimize this measure.

Our observations during the evaluation show that many of the false-rejections were due to user error caused by unfamiliarity with the system. Thus, were the systems being used on a daily basis as part of their job, performance would be noticeably better.

4. CONCLUSION
Biometric access is a better substitute for the clearance cards in verifying user’s identity. This study revealed that BEC 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 among others. 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
Boatwright, M. and Lou,X., (2007). What Do We Know About Biometrics Authentication? Information Security Curriculum Development Conference, 28 - 29 September 2007, ACM.
Cavoukian, A.( 2008). Fingerprint Biometrics: Address Privacy Before Deployment. Toronto Information and Privacy Commissioner of Ontario.
Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, (2003). The Handbook of Fingerprint Recognition. Springer Science.
Ezema L.S., Joe-Uzuegbu C.K.A., Eneh J.K., and I. Amanze (2015). Fingerprint Based Attendance Management System. International Journal of Scientific & Engineering Research, Volume 6, Issue 7, July-2015. ISSN 2229-5518
Farzad, P. (2012) Fingerprint-based student Attendance Register. MSc Dissertation. University of Bedfordshire.
Geetha, M. R. (2010). ZF Microsystem Based Embedded System Application for Fingerprint Verification.California: Department of Electrical and Electronic Engineering, California State University, Sacramento.
Hambali, M. A & Jimoh R. G (2015). Performance Evaluation of Principal Component Analysis and Independent Component Analysis Algorithms for Facial Recognition. Journal of Advances in ScientificResearch & Its Application (JASRA). 2, pp. 47 – 62.
Mahyidin, M. (2008). Student Attendance Using RFID System. Thesis, Electrical and Electronics Engineering Department, University of Malaysia Pahang. Retrieved March 2nd, 2013 from http://umpir.ump.edu.my/345/1/3275Firdaus.pdf.
Maltoni, D., K. Jain, A. and Prabhakar, S., (2009). Handbook of Fingerprint Recognition. Second edn. London. Springer.
Nawaz, T., Pervaiz S., and Azhar-Ud-Din A.K. (2009). Development of Academic Attendance Monitoring System Using Fingerprint Identification.
Newman, R., (2010).Security and Access Control using Biometrics Technologies. 1st edu. Boston: cengage Learning.
Paul, R., Alane, K. and Ari, S. (2004). Biometric Technologies: Security, Legal and Policy Implications. USA: Center for Democracy and Technology and the Heritage Foundation.
Rufai, M. M., Adigun, J. O. and Yekini, N. A. (2012). A Biometric Model for Examination Screening and Attendance Monitoring in Yaba College of Technology. World of Computer Science and Information Technology Journal (WCSIT). ISSN: 2221-0741, 2(4), pp. 120-124.
Saheed Y.K., Aliyu Jubril, Hambali Moshood A. & Aderbibgbe LO (2015). A Framework for Examination Clearance Using Biometrics System. Multidisciplinary Innovations & Technology Transfer iSTEAMS (MINTT) Conference – UNIBEN 2015. Book of Proceedings. Series8, pp. 107 – 116.
Saile Prabhakar , Sharath Pankanti and Anil K. Jain (2003). Biometric Recognition: “Security and Privacy Concerns” IEEE Security & Privacy March/April, 2003.
Shoewe, O., Olaniyi, O.M. and Lawson, A. (2011). Embedded Computer-Based Lecture Attendance Management System. African Journal of Computing & ICT, 4 (3), pp 27- 36.