Journal of Scientific Research & Reports
12(6): 1-10, 2016; Article no.JSRR.29179
ISSN: 2320-0227

SCIENCEDOMAIN *international*
www.sciencedomain.org

Fingerprint-Based Authorization Platform for Electronic-Based Examination

G. B. Iwasokun[1*], O. K. Akinyokun[1], R. O. Akinyede[1] and S. S. Udoh[2]

[1]Department of Computer Science, Federal University of Technology, Akure, Nigeria.
[2]Department of Computer Science, University of Uyo, Nigeria.

Authors' contributions

Author GBI conducted the literature review in collaboration with author OKA and also designed the proposed system. All the authors participated in the implementation and evaluation of the system. Author GBI wrote the manuscript and it was proofread and approved by other authors.

Article Information

DOI: 10.9734/JSRR/2016/29179
Editor(s):
(1) Martin J. Bohner, Missouri University of Science and Technology, Rolla, Missouri, USA.
Reviewers:
(1) Giuseppe Schirripa Spagnolo, Roma Tre University, Italy.
(2) Lin Tian, University of Electronic Science and Technology of China, China.
Complete Peer review History: http://www.sciencedomain.org/review-history/17464

Original Research Article

Received 26th August 2016
Accepted 27th September 2016
Published 7th January 2017

ABSTRACT

The advent of technology has revolutionized systemic approach to issues and methodology in different areas of life. Technological apparatus has stepped up human performance and efficiency in transportation, agriculture, entertainment, resource management, training, assessment and other areas of man's endeavour. Specifically, educational assessment has witnessed a shift in paradigm. Since the traditional approaches to examination suffer in areas of security and standard, they are now being replaced in several places with electronic-based methods which have helped human factors in efficient service delivery. Existing electronic-based examination use PIN, password or token for authorization and they are susceptible to different forms of irregularities ranging from impersonation to other related practices. The research reported in this paper focused on the development of a platform that uses fingerprint-based technology for authenticating electronic-based examination takers with a view to improve on security and control. The platform uses suitable mathematical models for fingerprint database, enhancement, feature extraction and pattern matching. A prototype of the platform was subjected to evaluation using fingerprints from different scanners and 500 research subjects. Analysis of results on error rates and matching speed revealed the suitability of the proposed platform.

**Corresponding author: E-mail: gbiwasokun@futa.edu.ng;*

Keywords: E-Test; authentication; fingerprint; CBE; examination.

1. INTRODUCTION

Examination is defined as observation, evaluation or short written or spoken activity that is based on a series of questions or exercises for establishing the quality, performance or reliability of an individual, especially before it is taken into use. In the education line, examination is used for measuring the skill, knowledge, intelligence, capacities or aptitudes of an individual or group. A standardized examination requires all takers to answer the same questions from common bank of questions in the same way and return scores in a standard or consistent manner, which guarantees comparative analysis on relative or individual performance basis. Some of the existing examination techniques include in-class activities, quizzes, class deliverables, examinations, papers, projects, presentations and portfolios. Examinations based on these conventional methods are time-consuming, lack sufficient level of availability and do not measure real-world skills effectively. Electronic-based examination (e-exam) system relies on the use of information technology for any examination-related activity and is conducted using a personal computer or any other electronic platform or device, in which the delivery, responses and assessment are controlled electronically. An e-exam system is conceptualized in Fig. 1 [1].

Two major modes for e-exam delivery are offline and online. With the offline mode, a computer based assessment is delivered without the use of Internet and is strictly operated on machine software and authentication information on single Personal Computer (PC). The online mode involves the usage of an internal network (or the Internet) and its distributed authentication servers to locally provide access to the question banks through server-client interactions among computers in the network [2-3]. E-exam is noted for its timeliness, on-line real-time capabilities and flexibility of scoring, location and timing, diversity in question type or format and lower long-term cost. It is also known for its reliability, impartiality, storage efficiency, enhanced question styles and safety of scripts [4].

The conventional techniques for access rights and privileges for e-exam include knowledge and object-based authentication methods. While the

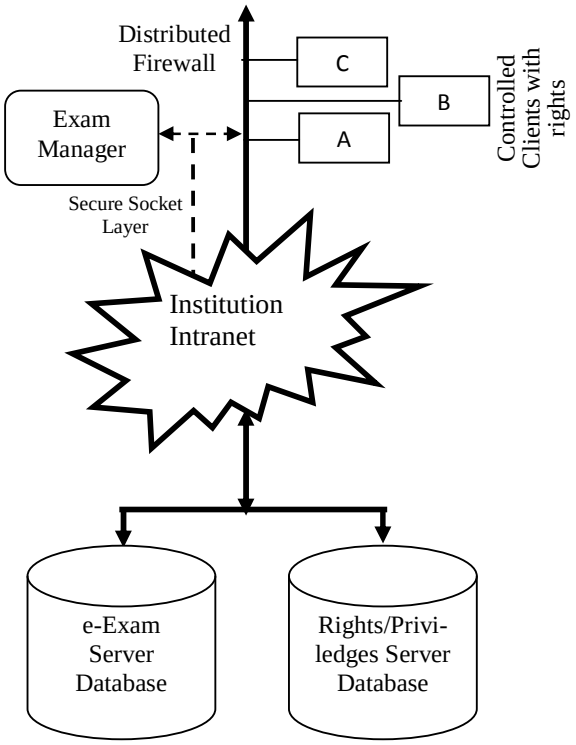

Fig. 1. Electronic-based e-exam system

knowledge-based approach verifies users on the basis of their knowledge of very popular scheme such as username and password, the object-based approach authenticates individuals through the use of identity objects or physical devices such as magnetic, electronic and Integrated Circuit (IC) cards [5]. A conventional authentication system for electronic-based examination is presented in Fig. 2.

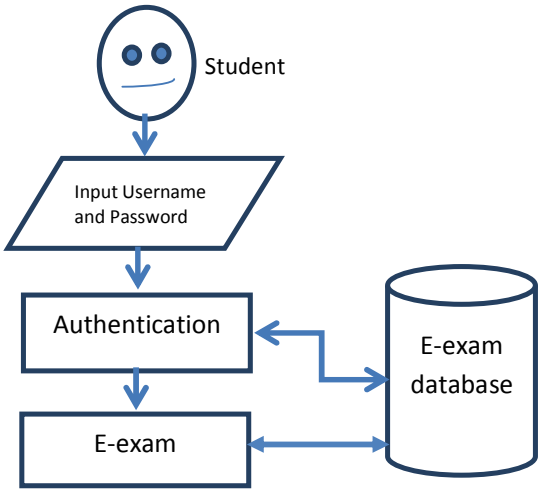

Fig. 2. A conventional e-test authentication system

The conventional techniques are susceptible to share and transfer which pose as major threats and challenges to institutions and administrators administering electronic examination [6].

2. BIOMETRICS-BASED AUTHENTICATION IN E-EXAMINATION

In several human activities requiring controlled access and monitoring, the burden of insecurity has been relieved through the use of biometrics authentication strategies. Biometrics Authentication (BA) refers to the identification of humans by their physiological characteristics (such as fingerprint, face, DNA and hand print) and behavioral characteristics (such as signature, gait, voice and typing rhythm) [7]. With this approach, an individual is freed from memorizing username and passwords as well as carrying cards. Other advantages include accuracy, uniqueness, non-repudiation, universality and simplicity of enrolment. Fingerprint is one of the most commonly used biometrics authentication features simply because it offers a unique global identifier. It is highly considered to be unique, with no two fingers having exact dermal ridge characteristics. In addition, fingerprint enjoys high universality, collection rate, performance, permanence and distinctiveness. The dominance of fingerprint has been established by the continuous emergence of series of Automated Fingerprint Identification Systems (AFIS), which conduct activities ranging from fingerprint enrolment, creation of profile database, minutiae detection and extraction, pattern recognition and matching, error fixing and decision making [8-9].

AFIS is currently used for guaranteeing transparency, safety and security during voting, operation of bank accounts among others. They are also used for controlling access to highly secured places like offices, equipment control rooms and centers and so on [10]. The recent employment and eventual widespread acceptance of electronic examination has also extended the application of fingerprint for human identity management. Challenging currently confronting e-examination include connived impersonation (an invigilator collude with fraudulent students to participate), transfer of security information (by genuine student to a fraudulent one) and login transfer (genuine candidate login and allow a fraudulent one to continue the examination on his behalf).

The need to formulate counter measures against these foul practices had motivated several research works. The author in [11] presented a model for remote and electronic examination and invigilation of students during formal assessment by utilizing transparent authentication for a non-intrusive and continuous verification of candidates' identity during an examination timeframe. Though, technology evaluation demonstrates the feasibility of the model, further validation under stress is required as well as end-user survey of impact and overall usability. The authors in [1] developed a platform comprising of distributed firewall system for monitoring candidates' actions during examination as well as a fingerprint biometrics solution for identity management of electronic examinations takers. The platform strengthens e-examing security but its identification and network security policy specification remain under the control of the network/examination administrator. In [12-13], platforms that use web-camera surveillance and fingerprint-based authentication for e-examination and attendance monitoring were proposed. The platform serve well in ridding impersonation and countering intrusion but any interruption (or failure) on the

part of the server may lead to authentication or monitoring error. The author in [14] proposed a fingerprint-based authentication framework for e-examinations. The framework acts as a firewall against impersonations and unauthorized data upload as well as access to examination questions. The authors in [15] presented a theoretical model for live video monitoring and a bi-modal biometrics authentication for guaranteeing cheating-free summative e-assessment in distance learning. The model offers real-time monitoring and significant reduction of foul play, but requires complex image and video processing to function. A multi-modal biometrics and knowledge based authentication framework for student authentication in online examinations is proposed in [16]. Though the framework has potential for promoting security of online examination system, its usability, security, privacy and reliability aspect of the biometrics authentication in online examination have not been investigated.

3. PROPOSED FINGERPRINT E-EXAMINATION AUTHENTICATION SYSTEM

The choice of fingerprint for the research is based on the fact that fingerprints stands out as the most popular biometrics mode for its uniqueness (no two people with identical print) and consistency (it may change in scale but not in relative appearance). It also enjoys high availability (it is naturally fixed on all individuals) and universality (possessed by every individual irrespective of gender, age or race) [17-20]. In addition, fingerprint is not forge-able, stole-able, misplace-able or forget-able and in cases of damages, it reproduces in short interval of time [21-22]. These strengths give an overridden view over some perceived limitations of fingerprint which include intrusiveness, susceptible to non-condonable error rates (especially in cases of dryness or dirt on the finger skin) and demand for large memory. The proposed fingerprint authenticated framework for Computer-Based Examination (CBE) is conceptualized in Fig. 3 with user interface, registration, verification, e-examination and system database modules. The interface module facilitates visual interaction with the system while the registration module serves as the backbone for pre-registration of examination takers.

3.1 Verification Module

The verification module is conceptualized in Fig. 4 and its flowchart is shown in Fig. 5. This module, handles the investigation of a candidate's validity and legitimacy for the examination. The first phase of the investigation involves verification of the candidate's fingerprint based on sequence of activities including enrolment, pre-processing, minutiae extraction and matching. Stages involved in pre-processing of live scan fingerprint image include smoothening and noise removal processes of ridge segmentation, normalization, orientation and frequency estimations, binirization and thinning [23].

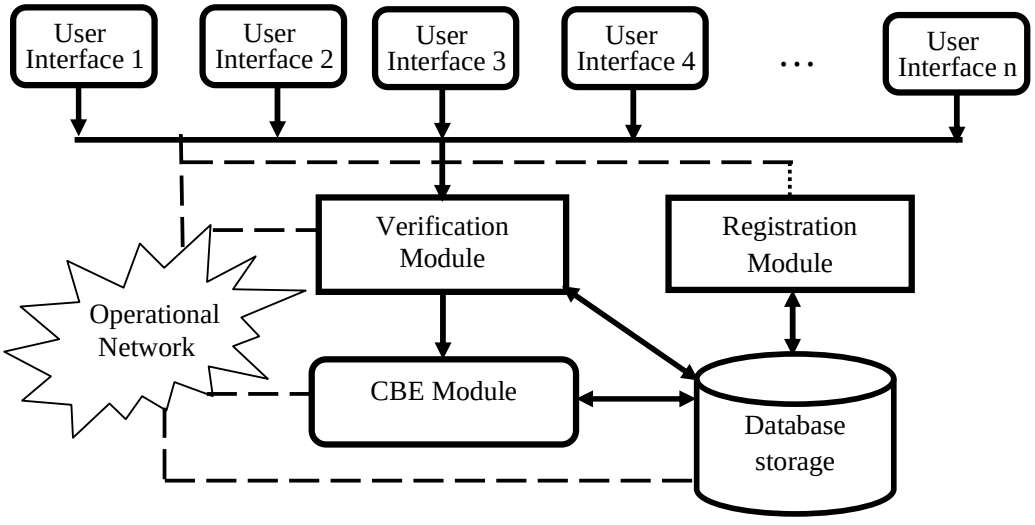

Fig. 3. Proposed fingerprint authenticated CBE framework

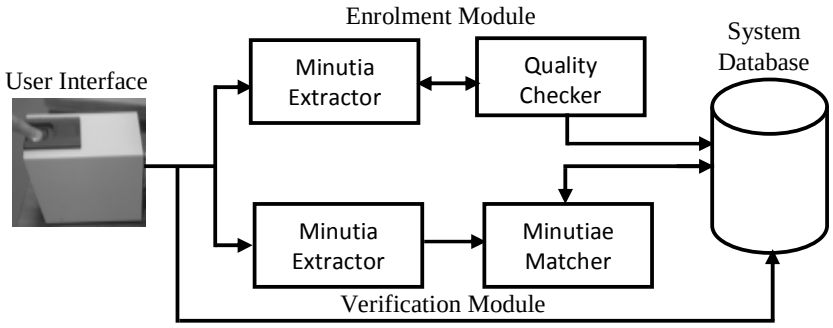

Fig. 4. System fingerprint verification module

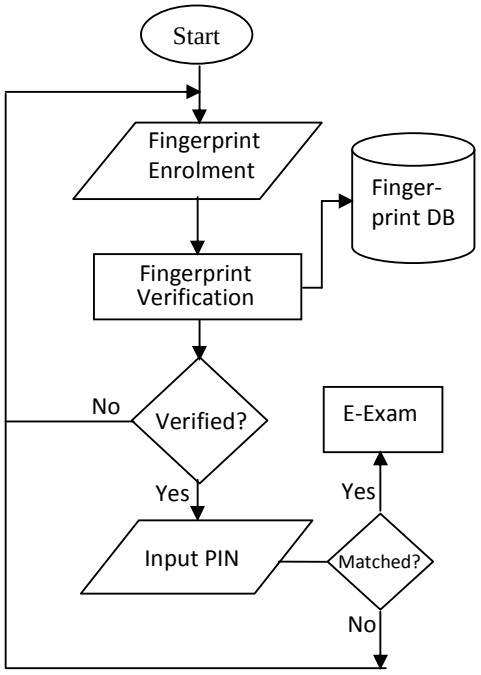

Fig. 5. Flowchart of fingerprint and PIN-based investigation

The feature extraction module extracts all the candidate minutiae points from the enrolled fingerprints (based on the formula presented in Equation 1) to obtain a template set.

$$CN = \sum_{k=1}^{7} |M_{k+2} - M_{k+1}|, \;\; M_9 = M_1 \qquad (1)$$

M_k is the grey level value for the kth minutia in the 8-neighbourhood of the candidate minutia point. A template set is a bit strings-based synthesis of all the extracted minutiae from a fingerprint. Based on the algorithm proposed in [24], the matching sub-module matches the bit string template set with the pre-extracted sets in the template database. The matching score, M_s for K and L fingerprint images is obtained from the formula:

$$M_s = \sum_{i=1}^{n} (|G(i) - H(i)|) * \{G(i)\}^{-1} \qquad (2)$$

G(i) and H(i) represent the distance between the i^{th} minutia point and the core points in K and L minutiae sets respectively. If the size of the feature set for K is lesser than or equal to the size of feature set for L, then s is the size of the feature set for K otherwise s is the size of the feature set for L.

The second part of the investigation focuses on further authentication of examination takers using PIN-based technology.

3.2 Examination Module

This module provides the platform for examining successfully authenticated candidates.

3.3 Database Storage

This layer serves as the backend for hidden and background operations. Apart from its querying capability, it houses candidates' biodata and fingerprints as well as examination questions with expected and returned scores.

4. EXPERIMENTAL STUDY

An experimental study of the proposed platform was carried out in an environment characterized by Window 10 operating system on Intel dual Core T6400 processor with 2G RAM and 40GB hard disk. For simplicity, easiness and high speed, the system's database was implemented

with Microsoft SQL server while a frontend comprising of C# on Microsoft.NET framework was used for robustness, easy programming and excellent database connectivity. Biometric based authentications were conducted for 500 selected students who participated in a presumed Computer Based Examination (CBE) of the Federal University of Technology, Akure, Nigeria (FUTA). Prior to authentication, 100 fingerprint impressions (consisting of 10 impressions each from 10 different scanners shown in Fig. 6) and other relevant data were collected from selected students, processed and stored in a designated database, whose extract is shown in Fig. 7.

False Acceptance Rate (FAR) and False Rejection Rate (FRR) performances metrics were generated and used to evaluate the suitability of the proposed system. FAR represents the degree or frequency of which information from the fingerprint of one person inadvertently match those from fingerprint of another person. It basically describes the rate at which an impostor is validated, authenticated or accepted. For every subject, each of the 10 fingerprints enrolled via each of the scanners, is matched with the other 4990 fingerprints of the same scanner to obtain the FAR. FRR basically describes the rejection of a genuine individual

Fig. 6. Selected scanners used for fingerprint enrolments

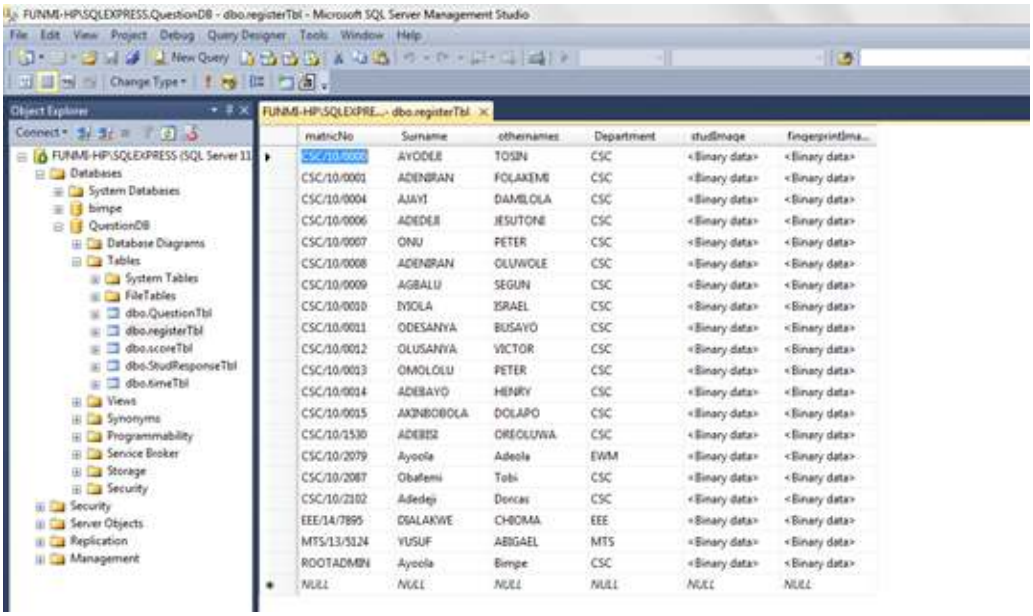

Fig. 7. Extract of database of selected students

and it is a measure of the matching failure frequency for fingerprints of the same finger. It is obtained by matching for all selected subjects, each of the 10 fingerprints with 9 other impressions of the same finger and scanner. The FAR and FRR values recorded for fingerprints from each of the 10 different scanners are presented in Table 1. An instance of FAR of 0.00001 implies that not more than 1 out of 100000 impostors or fake candidates is likely to be authenticated while 0.00000 implies no impostor or fake candidate is likely to be authenticated. Similarly, the FRR value of 0.00018 and 0.00021 means a maximum of 18 and 21 rejections or authentication failures will be recorded for 100000 genuine candidates for SecuGen PC Hamster Pro 20 and Dou/CL scanners respectively. The FAR recorded for matching each of the 100 fingerprints of the same finger (enrolled using ten scanners) with 49900 images of other fingers is 0.0000101 while the FRR for matching each of the 100 fingerprints with 99 other impressions of the same finger is 0.000231. The FAR value of 0.00000101 shows that matching images obtained from different and same scanners does not lead to significant difference in FAR. The FRR value of 0.000231 implies a maximum of 23 rejections or authentication failures will be recorded for 100000 genuine candidates.

Table 2 presents the Acceptance (A) and Rejection (R) results for 10 authentication trials for the 500 selected subjects. The results show zero rejections in most cases and some few non-zero rejections. The non-zero rejections are attributed to poor enrolment results, which makes feature extraction difficult and ultimately resulted in matching failure.

To verify the efficiency of the system, a formative evaluation was conducted in line with some related indices. The view and responses of the five hundred selected subjects were investigated with the aid of a questionnaire on speed of operation, matching accuracy, ease of use, usefulness for authentication, anti fraud support and support for human experts. The indices were rated on a scale of 5, 4, 3, 2 and 1 for 'Excellent', 'Very Good', 'Good', 'Average' and 'Poor' respectively. Table 3 presents the average index ratings for the 500 subjects while Fig. 8 presents the percentage equivalence (ratings).

Table 1. FAR and FRR values for different sensors

Sensor	FAR	FRR
SecuGen PC Hamster Pro 20	0.00001	0.00018
SecuGen PC Hamster Pro Duo/CL	0.00001	0.00021
SecuGen PC Hamster Pro IV	0.00001	0.00018
SecuGen Hamster Plus	0.00000	0.00011
Finkey Hamster II	0.00001	0.00010
UareU4000	0.00002	0.00019
USB HF6000	0.00001	0.00012
Verifi P5100	0.00000	0.00011
FS800	0.00001	0.00009
Digital Persona URU4000B	0.00000	0.00017

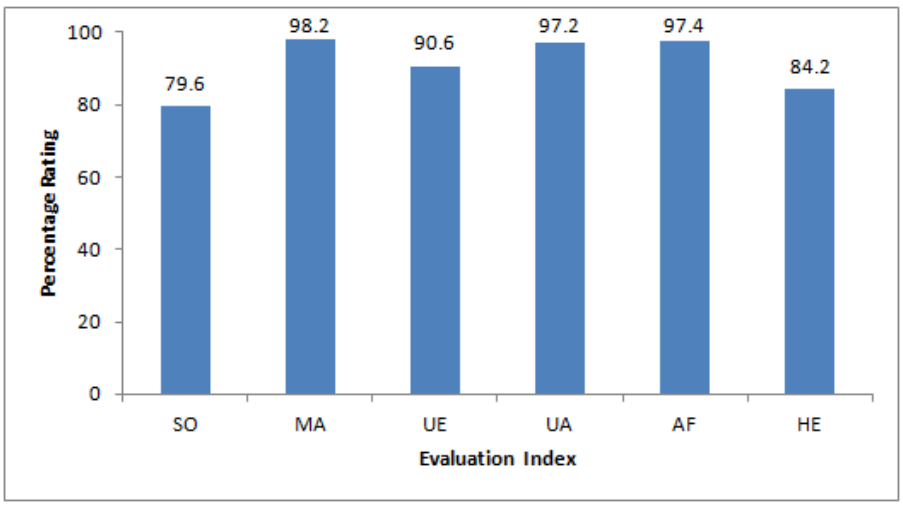

Fig. 8. Selected subjects' index-based percentage ratings

Table 2. Acceptance and rejections results for authentication trials for selected subjects

Sensors	Trials																			
	1		2		3		4		5		6		7		8		9		10	
	A	R	A	R	A	R	A	R	A	R	A	R	A	R	A	R	A	R	A	R
SecuGen PC Hamster Pro 20	500	0	500	0	500	0	500	0	500	0	499	1	500	0	500	0	500	0	500	0
SecuGen PC Hamster Pro Duo/CL	499	1	500	0	500	0	500	0	500	0	500	0	500	0	499	1	499	1	499	1
SecuGen PC Hamster Pro IV	500	0	500	1	500	1	500	0	498	2	500	0	500	0	500	0	500	0	500	0
SecuGen Hamster Plus	499	1	492	8	499	1	498	2	500	0	500	0	499	1	499	1	500	0	500	0
Finkey Hamster II	500	0	491	9	497	3	500	0	497	3	499	1	500	0	500	0	500	0	499	1
UareU4000	500	0	500	0	500	0	500	0	500	0	500	0	500	0	500	0	500	0	500	0
USB HF6000	500	0	497	3	495	5	500	0	499	1	499	1	498	2	500	0	500	0	499	1
Verifi P5100	500	0	500	0	499	1	499	1	500	0	500	0	500	0	499	1	499	1	500	0
FS800	500	0	500	0	500	0	500	0	499	1	499	1	500	0	498	2	499	1	499	1
Digital Persona URU4000B	500	0	500	0	499	1	500	0	500	0	499	1	499	1	500	0	498	2	499	1

Table 3. Average index ratings

Index	Rating
Speed of operation (SO)	3.98
Matching accuracy (MA)	4.91
Ease of use (EU)	4.53
Usefulness for authentication (UA)	4.86
Anti fraud support (AF)	4.87
Support for human experts (HE)	4.21

Fig. 8 reveals that all the indices enjoyed significant ratings with 'Matching accuracy' emerging as the most rated index of 98.2% followed by 'Anti-fraud support' and 'Usefulness for authentication' with percentage ratings of 97.4% and 97.2% respectively. The implication of these values is that the subjects expressed their confidence in the system and excellently approve that it be used for the authentication of candidates for electronic-based examinations. The very high scores recorded for 'Matching accuracy', 'Anti-fraud support', 'Usefulness for authentication' and 'Usefulness for authentication' are all attributed to the system efficiency, friendliness, simplicity and consistency. The lower scores recorded for 'Speed of operation' and 'Support for human experts' are consequences of some occasional delays (due to multiple trials in cases of initial matching failures) experienced by the subjects.

5. CONCLUSION

The paper presented a fingerprint and PIN-based authentication framework for investigating the validity of an e-exam taker. The framework relies on suitable models for processing and matching of fingerprints. Experimental results show the functionality of the framework for different scanners as well as its capacity to deliver at very minimal error rates. Trials directed at surveying users' acceptability established high performances in terms of speed, accuracy, ease of use, usefulness as well as security and support for human experts. Future research focuses on adopting a multi-modal approach (combining fingerprint with other biometrics such as face) for e-exam takers validity investigation with a view to securing higher reliability index and further lowering of the error rates.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Onyeizu MN, Ejiofor VE. Distributed architecture for post-UTME assessment, (Unpublished Masters theses). Nnamdi Azikiwe University, Awka, Nigeria; 2013.
2. Mohammad AS, Mohammed I. Challenges of online exam, performances and problems for online university exam. International Journal of Computer Science Issues. 2013;10(1):439-443.
3. Peat M, Franklin S. Use of online and offline formative and summative assessment opportunities: Have they had any impact on student learning? Proceeding of ASCILITE; 2002. Available:www.ascilite.org/conferences/auckland02/proceedings/papers/019.pdf
4. Abi TA. Design and implementation of online entrance examination (A case study of Caritas University Enugu); 2013. Available:2Fpubs.caritasuni.edu.ng%2Fdownload.php%3Ffile%3Dprojects%2F2012-2013%2520Projects%2FCOMPUTER%2520SCIENCE%2FDESIGN_AND_IMPLEMENTATION_OF_ONLINE_ENTRANCE_EXAMINATION.pdf
5. Singh S, Rylander DH, Mims TC. Efficiency of online vs. offline learning: A comparison of inputs and outcomes. International Journal of Business, Humanities and Technology. 2012;2(1).
6. Onyesolu MO, Ejiofor VE, Onyeizu MN, Ugoh D. Enhancing security in a distributed examination using biometrics and distributed firewall system. International Journal of Emerging Technology and Advanced Engineering. 2013;3(9):65-70.
7. Anil KJ, Arun R, Pankanti S. Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security. 2006;1(2).
8. Angaye OC, Akinyokun OC, Iwasokun GB. Experimental study of minutiae based algorithm for fingerprint matching. Proceedings of the International Conference on Computer Science, Engineering and Applications, New- Delhi, India. 2013;2013:33-46. Available:airccj.org/CSCP/vol3/csit3504.pdf
9. Iwasokun GB, Akinyokun OC, Angaye CO. Spatial relation approach to fingerprint matching, Book Chapter, Intelligent

Systems for Science and Information Studies in Computational Intelligence. 2014;5:87-110.
Available:www.link.springer.com/chapter10

10. Iwasokun GB, Akinyokun OC, Olabode O. A mathematical modeling approach to fingerprint ridge segmentation and normalization. International Journal of Computer Science and Information Technology & Security, Singapore. 2012; 2(2):263-267.
11. Clarke NL. E-invigilator: A biometric-based supervision system for e-assessments. Centre for Security, Communication. & Network Res. (CSCAN), Plymouth Univ., Plymouth, UK; 2013.
12. Levy Y, Ramin MM. A theoretical approach for biometrics authentication of e-exams; 2007.
Available:http://telem pub.openu.ac.il/users /chais/2007/mor ning_1/M1_6.pdf
(Accessed 15/04/2015)
13. Penteado BE, Marana AN. A video-based biometric authentication for e-learning web applications. Lecture Notes in Business Information Processing. 2009;24: 770-779.
14. Alotaibi S. Using biometrics authentication via fingerprint recognition in e-exams. Proceedings of the 4th Saudi International Conference, University of Manchester; 2010.
15. Sabbah Y, Imane S, Amira K. Synchronous authentication with bimodal biometrics for e-assessment: A theoretical model. Proceedings of the 6th International Conference in Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), Sousse. 2012;139–145.
16. Ramu T, Arivoli T. A framework of secure biometric based online exam authentication: An alternative to traditional exam. International Journal of Scientific & Engineering Research. 2013;4(11).
17. Roberts C. Biometrics; 2009.
Available:http://www.ccip.govt.nz/newsroo m/informoation-notes/2005/biometrics.pdf
(16 July 2013)
18. Michael C, Imwinkelried E. A cautionary note about fingerprint analysis and reliance on digital technology. Public Defence Backup Center Report. 2006;21(3):7-9
19. Palmiotto MJ. Criminal investigation. Chicago: Nelson Hall; 1994.
Available:https://www.ncjrs.gov/App/public ations/ abstract.aspx?ID=166681
(Accessed 25/06/2014)
20. Salter D. Thumbprint – an emerging technology', engineering technology. New Mexico State University; 1996.
21. Iwasokun GB. Development of a hybrid platform for the pattern recognition and matching of thumbprints, PhD Thesis, Department of Computer Science, Federal University of Technology, Akure, Nigeria; 2012.
22. Yang Y, Mi J. ATM terminal design is based on fingerprint recognition, Proceedings of 2nd International Conference of Computer Engineering and Technology (ICCET-2010), Chengdu; 2010.
23. Iwasokun GB, Akinyokun OC, Alese BK, Olabode O. Fingerprint image enhancement: Segmentation to thinning. International Journal of Advanced Computer Science and Applications (IJACSA), Indian. 2012;3(1):15-24.
24. Iwasokun GB, Akinyokun OC, Angaye CO. Spatial relation approach to fingerprint matching, Book Chapter, Intelligent Systems for Science and Information Studies in Computational Intelligence, 2014;5:87-110.
Available:www.link.springer.com/chapter10

Peer-review history:
The peer review history for this paper can be accessed here:
http://sciencedomain.org/review-history/17464