Applied Computer Science, vol. 15, no.3, pp. 56–64
doi:10.23743/acs-2019-21

Submitted: 2019-07-12
Revised: 2019-08-03
Accepted: 2019-09-12

distance education, online examination, authentication, assessment, Biometric system

Hamid JAN[0000-0003-2065-8515]*, *Beena HAMID*[**]

THE APPLICATION OF FINGERPRINTS AUTHENTICATION IN DISTANCE EDUCATION

Abstract

Currently the distance education has obtained a wider ever acceptance. One of the main tasks of distance education is the process of checking student's knowledge by online examination. To conduct a fair examination and prevent unauthorized users to appear in the examination, different biometric technologies are used; we in this paper implement a fingerprint biometric system for distance education students and found by survey that the students are comfortable with fingerprint biometric system.

1. INTRODUCTION

The invention of computer technology has changed our lives and found new directions. The ways of communication and getting information through Web is another change for people. Distance education through web technology or online education is the new way of getting education emerged from World Wide Web (Alavi & Leidner, 2016; Takahashi, Abiko & Negishi, 2006). These technologies are very attracting and interesting but also face various threats, especially when tests are conducted online. (King, Guyette & Piotrowski, 2009) studied and come to the conclusion that 73.6% of the students think that cheating is easy in the online exam as compared to conventional exam. These were the students selected for the sample.

[*] Sarhad university of Science & Information Technology, Landi Akhund Ahmad, Ring Road, Peshawar 25000,Pakistan, hod.csit@suit.edu.pk
[**] Jalya Khan Institute of Modern Sciences, Ghani Khan Road, Shaheedan Salarabad, Charsadda 25000, Pakistan, beenhamidjan@gmail.com

Distance learning is a modern form of education and is the interaction of the teacher and students with each other at a distance or on internet (King, Guyette & Piotrowski, 2009). It provides the learning process different from the conventional form of education. The problems of distance learning can be divided into two groups: pedagogical problems and technical problems. In this paper, we considered only technical problems, in particular, the problem of identifying the true user during Examination.

The place of the student and the teacher is different in online examination, because communication is done through the Internet. As the distances increases between teacher and student, the chances of committing negligence increases, and revealing the wrong actions of the students is quite difficult. To avoid such unfair means, the actions of the students must be continuously supervised during the examination. In supervising the first move may be the use of an authentication method, that is, the identification of the student, which is the right person who is eligible for the exam occasionally a student who has been registered in the exam is different from the student who wrote the exam. Therefore, authentication plays a role in determining the correct user.

A new method to authenticate people based on their biometrics has become known for many years (Green & Romney, 2005; Frischholz & Dieckmann, 2005). William (2002), for example, explains that biometric data are unique physical characteristics of a person, such as fingerprints, iris, face, fingerprints, etc. Biometric fingerprint systems are very common and are known for their accuracy, ease and proven record (Aggarwaltt, Rathat, Jeat & Bollet, 2008; Ali, Ali, Shahzad & Malik, 2006; Ratha, Connell & Bolle, 2001).

However, like any other biometric system, fingerprints also represent several threats and risks to the authentication process (Maltoni, Maio, Jain & Prabhakar, 2003). Education should not be thought as distance or conventional, unless it is associated with assessments and exams. Student assessment is an important part of the education and training system. First, it is important to know that how much knowledge is required for a student and secondly the students themselves need to know about their knowledge. The most tried assessment procedure due to its clarity is the use of MCQs type exam.

The interactions of students with online materials and the collection of all information for examination from such material are very helpful. It is also handy to support the examiner in his work.

2. RELATED WORK

Althaff et al. (2009) offers a unimodal approach that ensures the security of online exams by using facial recognition techniques. They use the methods of discrete casino transformation (DCT) and Karhunen-Loeve transformation (KLT) to capture the facial image functions, and then compare these results with facial recognition. This method can be further extended by comparing faces with a protected image.

Agulla et al. (2008) provides uniform protection technologies using biometric authenticity of the Internet. This method uses biochecker software, which is handy for verification of images on user side. Visualize user images and handy for user behavior monitoring. The drawback of this method is that you need powerful servers to run this software.

Hsieh & Leu (2011) provides unimodal technique for implementing a unique authentication method based on passwords. This method supply independent passwords based on location and time of a mobile user. By using this password only, the application on mobile device can be accessed, such as Internet banking. This helps in reduction the risk of intrusion. This method can be used during the student authentication process.

Taiwo Ayodele et al. (2011) offered an automatic learning method that prevents theft, impersonation of exams online. This method shows the student's behavior during the exam, thus avoiding negligence.

Apampa et al. (2010) Proposes a multiple-step approach to the model, presenting authentication methods to initiate a student session and follow-up student monitoring while the examination is in progress. To authenticate, the student has three options, i.e by face recognition, by passwords or by tokens. After authentication the student is continuously check through the webcam. If some unfair means or risks are identified, the student will be asked to authenticate again.

Nasser Modiri et al. (2011) offered a multimode technique, in which the system is designed to conduct distance examinations in secure domain. To do this, the student provides user-id and passwords at the time of registration and then the student supervision is done through the webcam. It assists to monitor students' behavior during the examination.

3. METHODOLOGY OF FINGERPRINT AUTHENTICATION

The working diagram of scanner that was used in fingerprint Authentication (Maltoni, Maio, Jain & Prabhakar, 2003) is shown in figure 1.

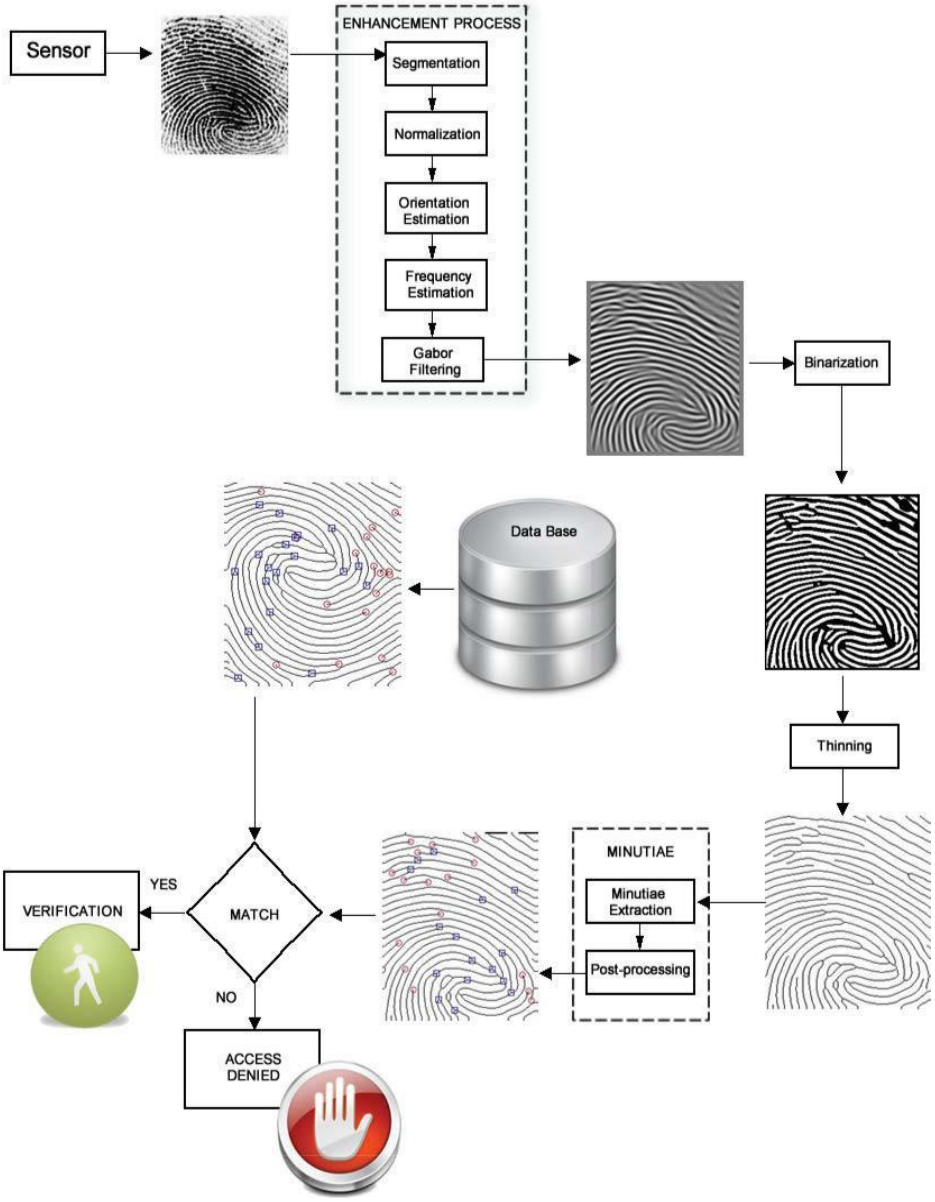

Fig. 1. Fingerprint authentication system

The fingerprint consists of the following two types of features:

1. The Global Features: They are core and delta. The core is the inner most point and delta is the location where three ridges meet.
2. The Local Features: The lines on fingerprint are called Ridges and the spaces between them are called valleys. These ridges form different patterns and are called minutiae points. The most common minutiae points are ridge bifurcation and ridge ending**.**

With the help of local and global features of fingerprint, we can differentiate users. The global and local features of finger prints are shown in figure 2.

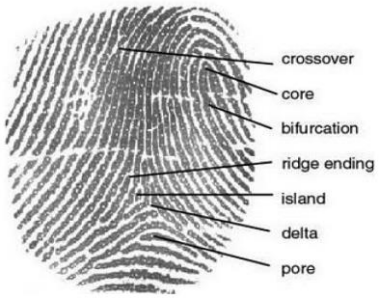

Fig. 2. Local and Global features of fingerprints

Students will be able to appear in exam online. Each student will be given access to a computer in the classroom, connected to the server. The internet connection will not be available during exam. The student will authenticated first through biometric system by matching his fingerprints. Once the student is recognized by the system, the system allows him to complete the exam. The test of the student is send for checking to the teacher electronically and the system also send the copy of test to the printer for student.

Once the student is recognized by the system, his identity will be known and now the student can be punished, if found using unfair means in the examination. There are many advantages and disadvantages of conducting exam online. The ability to track the actions of a student identified by system, allows us to constantly evaluate him and giving student the best experience. Any online activity can be vulnerable, so a reliable security policy will be required. Fingerprint Biometrics appears again as a way of reducing the likelihood of threats.

4. RESULT AND DISCUSSION

During the examination, 100 students were verified on fingerprint biometric system. The detail of these student were presented in figures 3,4 and 5. Most of them are in the range from 17 to 30 years old, Students of Computer Science at Comwave College Islamabad, a Distance Learning Centre of SUIT. Students in Computer science Department mostly come after completing twelve years of schooling. Almost all (91.3%) are men. All of them were enrolled in the different subjects.

The purpose of the experiment was to analyze the attitude of students towards a new tool for controlling access to e-learning. 80% of students think that fingerprint registration is a very easy or easy way to use online courses. Those who welcome the use of fingerprint biometric system said they look more secure, it's simple and faster than other access tools. Those who oppose fingerprint biometric system consider that the password is sufficient. The data in Table 1 clearly supports the choice of a fingerprint biometric technology.

Tab. 1. The choice of best Biometric System

Biometric Choice	Frequency	%age	Cum.%
Fingerprint	80	80.0	80.0
Face	5	5.0	85.0
Iris	13	13.0	97.0
Voice	2	2.0	100.0
Total	100	100.0	

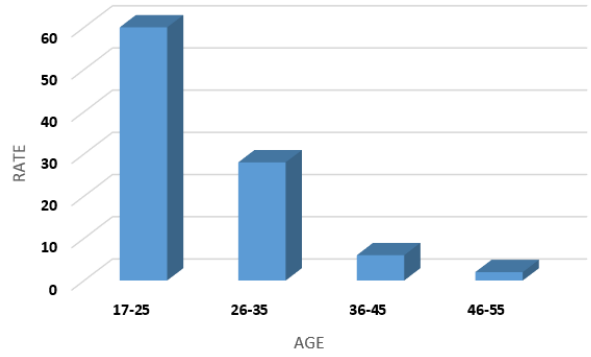

Fig. 3. The Age of Students

To find about the ease of use of a new fingerprint interface, students find it very easy or easy to use (80.0%) (see Table 2).

Tab. 2. The opinion poll of students

Opinion	Frequency	%age	Cum.%
Very Easy	45	45.0	45.0
Easy	35	35.0	80.0
Difficult	17	17.0	97.0
Useless	3	3.0	100.0
Total	100	100	

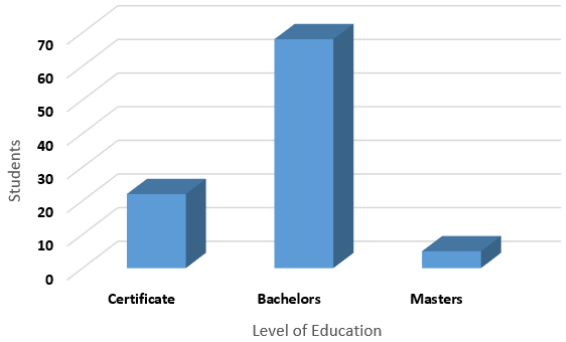

Fig. 4. The Level of Education

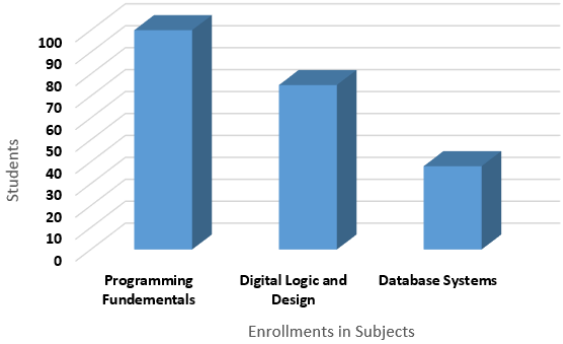

Fig. 5. Total enrollment of Students in Each Subject

Students were analyzed for their level of knowledge about biometric system and to what extent they have used it. Many students were new to these methods and hardly have used biometric systems (see Table 3).

The main challenge of survey was whether the students think the fingerprint biometric system verification appropriate for accessing online courses. The students were divided into two groups. The group one contains those who accept the fingerprint verification and the group two includes those who did not accept it. Two-dimensional analysis of tree segmentation to assess which category is supported by many students is applied.

Tab. 3. Knowledge of Students about Biometric System

Knowledge	Frequency	%age	Cum.%
Expert Level	1	1.0	1.0
Intermediate Level	11	11.0	11.0
Elementary Level	15	15.0	26.0
no Knowledge	74	74.00	100.00
(Total)	100	100.00	

Two questions were asked from the students. Question no. 1 was: "What do you think about the verification via fingerprint to access online courses?". 77% students think that verification via fingerprint is very easy while 23% students think that verification by such method is very difficult. Question no. 2 was: "Which one of the biometric technologies would you select?". The total students in favor of biometric technology were seventy seven (77). Seventy (70) students selected Fingerprint Biometric technology while the other seven (7) students selected the other technology.

5. CONCLUSION

A fingerprint matching technique based on local features of fingerprints was used for verification and registration. The technique performed well when tested for online examination. The students were keen to use the biometric system for online learning. The students think that it is a faster and easy way to verify and register for online courses. Most of the students have never used the biometric system and have very little knowledge about biometric systems. Eventually the fingerprint biometric system was implemented in the distance education online examination and introduce a new way of conducting examination in distance.

REFERENCES

Aggarwaltt, G., Rathat, N. K., Jeat, T. Y., & Bollet, R. M. (2008). Gradient based Textural Characterization of Fingerprints. In *2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems* (pp. 1–5). Arlington, VA. doi:10.1109/BTAS.2008.4699383

Agulla, E. G., Rifón, L. A., Castro, J. L. A., & Mateo, C. G. (2008). Is my student at the other side? Applying Biome tric Web Authentication to E-Learning Environments. In *2008 Eighth IEEE International Conference on Advanced Learning Technologies* (pp. 551–553). Santander, Cantabria. doi:10.1109/ICALT.2008.184

Alavi, M., & Leidner, D. (2016). Research commentary: Technology mediated learning-a call for greater depth and breadth of research. *Information Systems Research*, *12*(1), 1–10. doi:10.1287/isre.12.1.1.9720

Ali, I., Ali, U., Shahzad, M. I., & Malik, A. W. (2006). Face and fingerprint biometrics integration model for person identification using gabor filter. In *IEEE International Conference on Computer Systems and Applications* (pp. 140–143). Dubai, UAE. doi:10.1109/AICCSA.2006.205081

Althaff, I., Syusaku, N., Karim, O., &Yoshimi, F. (2009). Face-based Access Control and Invigilation Tool for e-Learning Systems. In *2009 International Conference on Biometrics and Kansei Engineering* (pp. 40–44). Cieszyn. doi:10.1109/ICBAKE.2009.43

Apampa, K. M., Wills, G., & Argles, D. (2010). An approach to presence verification in summative e-assessment security. In *2010 International Conference on Information Society* (pp. 647–651). London.

Ayodele, T., Shoniregun, C. A., & Akmayeva, G. (2011). Toward e-learning security: A machine learning approach. In *International Conference on Information Society (i-Society 2011)* (pp. 490–492). London.

Frischholz, R. W., & Dieckmann, U. (2000). Bioid: A Multimodal Biometric Identification System. *Computer*, *33*(2), 64–68.

Green, N., & Romney, G. W. (2005). Establishing Public Confidence in the Security of Fingerprint Biometrics. In *005 6th International Conference on Information Technology Based Higher Education and Training* (pp. S3C/15-S3C/18). Santo Domingo. doi:10.1109/ITHET.2005.1560332

Hsieh, W., & Leu, J. (2011). Design of a time and location based One-Time Password authentication scheme. In *2011 7th International Wireless Communications and Mobile Computing Conference* (pp. 201–206). Istanbul. doi:10.1109/IWCMC.2011.5982418

King, C. G., Guyette, R. W., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students 'views'. *The Journal of Educators Online*, *6*(1), 1–11.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition*. London: Springer.

Modiri, N., Farahi, A., & Ketabi, S. (2011). Providing security framework for holding electronic examination in virtual universities. In *The 7th International Conference on Networked Computing and Advanced Information Management* (pp. 73–79). Gyeongju.

Ratha, N. K., Connell, J. H., & Bolle, R. (2001). An analysis of minutiae matching strength. In: J.Bigun & F. Smeraldi (Eds.), *Audio- and Video-Based Biometric Person Authentication. AVBPA 2001*. *Lecture Notes in Computer Science* (vol. 2091). Berlin, Heidelberg: Springer. doi:10.1007/3-540-45344-X_32

Takahashi, Y., Abiko, T., & Negishi, E. (2006). An Ontology-based System for Network Security. In *19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers)* (pp. 197–202 vol.1). Taipei, Taiwan. doi:10.1109/AINA.2005.116

Williams, J. W. (2002). Biometrics or ... biohazards? In *Proceedings of the 2002 Workshop on New Security Paradigms NSPW '02* (pp. 97–107). doi:10.1145/844118.844120