A proposed Iris Recognition Model for Authentication in Mobile Exams

https://doi.org/10.3991/ijet.v15i12.13741

Aayat Shdaifat (✉), Randa Obeidallah, Ghadeer Ghazal, Alaa Abu Srhan
Hashemite University, Zarqa, Jordan
aayat@hu.edu.jo

Nesreen Rabah Abu Spetan
Jordan Ministry of Education, Amman, Jordan

Abstract—Mobile learning is an extended version of e-learning. The revolution of handheld devises had encouraged to design courses to be compatible with different mobiles versions, brands and platforms. Mobile exams need more attention to strengthen mobile learning certificates. A major issue with mobile exam is student authentication and identification before and during exam session. With no presence of proctor, more techniques are available to ensure student identification. In this paper, we proposed a model that uses a tradition user name and password in addition to the biometric iris recognition technique to verify student identity before and during mobile exam.

Keyword—Biometric; Mobile exam; Mobile learning; iris recognition; Authentication; Cheating; Identification; Learning.

1 Introduction

Wireless technology refers to a global communication without cables nor wires. Handheld devices such as phone mobiles and tablets… are depending on Wireless technology to connect, transmit, and share files and documents. The increased use of handheld devices, tablet computer notebook and digital reader in learning had encouraged the use of a new learning phenomenon called mobile learning. Mobile learning gives students the ability to study anywhere and anytime [14] [11]. Mobile learning is an attractive way in learning [5].

One of the most important phases in learning is assessment or exam. According to [32] the most important point in teaching is exam; it is the phase that evaluate what student learn during a certain course [9].

Today, computer based exam known as online exam and e-exam is the process of achieving the exam or test through a personal computer or a laptop. Meanwhile, Mobile exam or m-exam is the process of achieving the exam through mobile devices or hand held devices [22]. The biggest issue with online exam or mobile exam is security and increased cheating levels [39]. [34] Showed that cheating in e-exam had increased compared with the traditional exam since a student achieves the exam without the presence of a proctor. The most important challenge in mobile exam is impersonation [37]. The risk of authentication before and during exam is a problem with online exam [3].

Many methods and techniques are used to reduce and prevent cheating levels in e-exams and m-exams. Such traditional methods are the use of username/password, and/or the use of a card or badges. Other techniques depend upon biometric features which depend on unique features or characteristics owned by individual and differ them from the other, like finger print, face recognitions, DNA, Palm hand…etc., these features are distinctive and measurable [6] [23].

In this paper, we will consider Iris recognition as a biometric technology to help identify students while using handheld devices. Iris is a flexible and colored tissue that controls the pupil [40].Iris recognition is the process of capturing iris image and save the extracted data, and then compare data with previous saved data to verify the student identity. Mathematical analysis is performed to distinguish between peoples [40].

This research proposed a model that use biometric iris recognition method alongside with traditional method to login to mobile exam in mobile learning. The proposed model is applied during exam by capturing iris image randomly during exam, which help to increase authentication of student who conduct the exam. The proposed framework aims to prevent the impersonation of students and cheating in mobile exams.

This paper is structured as follows: A review of mobile learning is introduced in section 2. A preview of related work is in section 3. Section 4 represent the iris recognition technique. The proposed model and discussion are introduced in section 5 and section 6 respectively. And finally, conclusion and future work in section 7.

2 Mobile Learning

Mobile learning is being deployed in many higher education institutions as a result of the evolution of wireless technology and handheld devises [8]. The success of mobile learning is determined by the availability of technology and support for students and instructor. This support is divided into: software, hardware and training. As well as the Integration and ownership of the technology [27].

[11] Encouraged the use of mobile learning since mobiles are always available with young people, affordable prices, and ease of use. However, they also mentioned the drawback of the small size of screen, limited storage, battery problem and the problem of using 3G and 4G when moving graphic elements.

A successful mobile learning program requires the availability of many features and requirements. [14] Defined important features that must be within mobile learning which are: flexibility, timely, virtual and trans-time-space, popularization and personalization, interactivity and universality. Technical characteristics like accessibility and portability, and pedagogical characteristics are important to maintain the use of such learning [18].

The quality of mobile learning outcomes depends on the assessment phase. Assessment is important to ensure student completed successfully all of course objectives and he/she deserve the certificate. In order to accept mobile learning, the exam must be accomplished with strong authentication method before and during exam. This is important to accept the given certificate or degree [36].

In mobile learning, security and authentication are one of the most important challenges that need to be highlighted. Other challenges include: security and privacy, copy right, protect data stored in mobile and content filtering [17].

3 Related Work

In online exam, cheating is incredibly increased compared to traditional classroom. A study conducted by [24] showed that teachers believes that number of students cheating in online exam are greater than in paper exam, because of no presence of proctor.

Many threats and dishonest behaviors were found in online exams that are similar in traditional exam. [28] Reviewed several cheating behaviors that appear during exams. The most important threat is student authentication before and during the exam. Authentication is one of most important goals in security [3]. The authentication process is usually happened before conducting the exam, though, the exam is not supervised by proctor. Therefore, the mobile device could be given to someone else during the exam. Another threats may occur that user name and password are given to others to answer the exam, or after logging in someone else answer the exam.

Authentication and verification methods are divided into two types: traditional authentication and biometric authentication. Traditional authentication is either a knowledge-based techniques or object based. The knowledge based that are frequently used is the use of username and password while object-based authentication is the use of what you have like cards, keys, Badges ...etc. Using traditional authentication method user name and password only in online exam increase attack and security problem [30].

Biometric authentication uses a human physical or behavioral feature to authenticate and verify use. A unique feature is different from one person to another; no one can have except you, this feature is considered as a vector [2] [30]. Physical features include: face recognition, iris recognition, finger print recognition, hand vascular, palm print, hand or ear geometry recognition. Behavioral features include gait recognition, voice recognition, keystroke or signature.

The use of some biometric authentication requires special hardware and software. Therefore, not all these biometric techniques are applicable for mobiles [10]. Behavioral type of biometric is more difficult and need accurate logging records of user behavior [2]. [31] Proposed a model for online exam to enhance security, which facilitate the effective online exam by decreasing security risk and cheating.

Many researchers worked with biometric techniques to improve security in online exams and mobile exams. [21] Proposed an approach that prevents unethical access to e-learning environment using finger print feature. While [20] proposed the use of QR reader to increase security in mobile exam as well as a good distribution random question. [3] proposed a model for online exam security and authentication risk. They suggested the use of multi biometric authentication. The model was updated by [34] by supplement it with cryptography within the electronic monitoring system. [36] Proposed a model applied in mobile and online exam with two biometric methods first apply face recognition then keystroke dynamic in addition to the traditional authentication method. While [26] used keystroke behavioral biometrics method to accept student login in online exam. [30] Supposed two layers to authenticate student to login and track student during online exam. They used biometric authentication and knowledge based authentication. [28] Proposed two biometric techniques for student authentication in handheld devices before exam login by first using fingerprint and during the exam by image similarity.

A proposed model for mobile exam which is integrated with Moodle learning management system is proposed by [15]. The proposed model enhanced security through several points. They suggested to provide random questions distributions, stop "unattended exam", use biometric authentication to prevent impersonation, prevent student change their device during exam, help to facilitate exam security in online or offline

Mobile Exam System (MES) application is designed by [25]. MES is supported by IOS and Android, students reacted positively with this system. Another mobile exam system was designed by [38] called Mobi-exam. A friendly, efficient, and easy to use system.

In this paper, we will use Iris recognition in mobile exam authentication and tracking. Iris is a flexible and colored tissue that controls the pupil [40]. Iris recognition is a way to control student impersonation another in online exam [4]. [19] Used Iris recognition method for mobile phone to prevent unauthorized access to mobile phone by using mobile camera for recognition. [13] applied iris recognition in mobile phone using adaptive Gabor filter. While [16] applied multi-unit iris authentication method using support vector machine algorithms, it is used to prevent unauthorized mobile user.

4 Iris Recognition

One of the most reliable and accurate physical biometric features is the human eye's iris [12].Iris is located behind the cornea and in front of the lens. A small colored tissue that is unique for every person [29] [33]. It is different between identical twins, as well as the left and right eye for the same person are different also [35]. This is a reason why iris recognition is a reliable biometric technique to be used in authentication. It can be used for blind people as well.

As every biometric system, Iris recognition includes four phases as the following:

1. Image acquisition: This phase deal with capturing iris image. The quality of iris image is important in developing matrices of iris image [7]. Factors that affect the image quality image acquisition include: illumination, location and camera, the

occlusion, and lighting [35]. In mobile exam, the process of image acquisition is happened through the mobile camera.

2. Preprocessing phase: Preprocessing include many steps like segmentation and normalization. In iris recognition; many technique are used to locate iris and pupil like Hough transformation, integrodifferential operator and gradient based edge detection [35] [7]. After that iris unwrapping process is used to calculate the variation of pupil size with illumination change to transform from iris texture to polar coordinate [33]. This process make iris matching more easer [33].
3. Feature extraction and encoding: In this phase the distinguish feature are extracted for used in classification like: x-y coordinates, radius, shape and size of the pupil, intensity values, orientation of the pupil ellipse and ratio between average intensity of two pupils [35]. Gabor wavelets are commonly used as encoding mechanism. Firstly, extracted local phasor from iris texture and represent the phasor response in two bits of data [33].
4. Matcher phase, compare the new capture feature with data that decision if authorizes or not.

5 Proposed Model

Biometric is a good choice to authenticate and verify users. Iris verification technology is a better choice for the following reasons: fast, reliable, secure and not changeable with age like face recognition. It has a static feature that cannot change as happened in finger print recognition where the pattern size change with age. Iris recognition can be used for all, even for blind people [37] [1].

The proposed model (see figure 3) is applied for mobile learning, which all students from different locations are connected with course by mobile or tablet. Students register online and get their user name and password. The registry is completed in the course once the student provides his/her iris image through the mobile camera. The iris recognition process is applied and features calculated and saved in server database for future use in exam sessions. When student register and capture his/her iris, the student must make sure not wearing any lenses, and in good light for best iris image capture.

The proposed model has three phases: registration to course, login and during exam. Explanation of each phase are examined below:

5.1 Registration phase

The student in this phase register and enroll to online course and get a user name and password to login to course material. During the process of registry, student is supposed to provide an iris image. Iris recognition data are acquired and saved in server database to be used later in mobile exam authentication. The image is captured using mobile camera and a built-in application that direct the student to center the eye within a certain area in the screen. It is important to mention that mobile cameras are enhanced to provide a reliable high resolution image to be used for identification.

During this phase, iris recognition is conducted using four steps.

- Capture image: using mobile camera to get an iris image or can get a lot of frame using mobile video camera.
- Segmentation: this step responsible to extract the basic element of eye like sclera, pupil, eyelids and eyelashes [33].
- Normalization step: the iris image represented in 2D and the noise in image is removed using mask filter [2].
- Encoding and feature extracted: using feature extraction to represent the iris feature in vector, feature filter using classifier Laplacian of Gaussian filter to be represented in a vector.

The results after these steps are saved in database server. See Figure1 that shows the process of iris recognition steps.

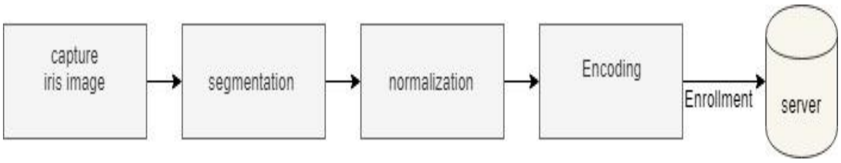

Fig. 1. Iris recognition steps

5.2 Login phase

In our proposed model, the process of login to the mobile exam requires two steps. The first step: A traditional authentication is applied where student (Si) provides a user name (Ui) and a password (Pi) to login to the mobile exam. The user name and password are the same as the one used to enter the course content. In addition to Ui and Pi, the second step direct the student to provide the iris image through mobile camera. The captured image is then processed through iris recognition steps explained in phase 1 and vector result is verified with data stored in database. See figure 2 that shows the verification of iris recognition results. The results of matcher are represented as a vector send with Ui to server to verify student Si. If the student is verified then go to the exam session to start exam, otherwise the login is canceled.

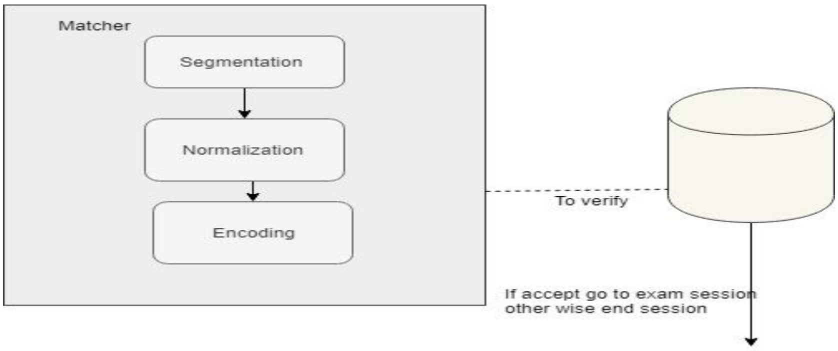

Fig. 2. Login phase step 2

6 During Exam Phase

During exam session, capturing iris image is taken randomly for student to ensure that the same person who login is the same person who is conducting the exam. The Instructor can determine the period of randomly ask the student for the image. This is occurred to prevent student to give his/her mobile phone to another to answer the exam.

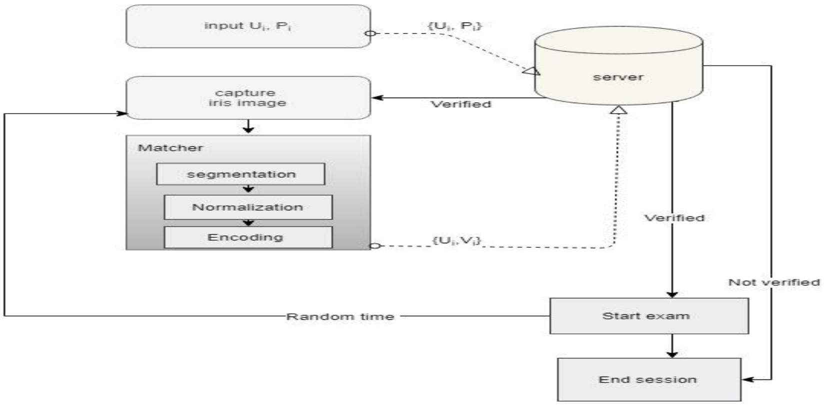

Fig. 3. The proposed framework

7 Model’s Discussion

The proposed model offers an ease to use, effective, quick and less cost authentication system to login to exam. It provides a way to support online exam with less students cheating in identification. The proposed model aims to help both instructors and students in the assessment phase. Student can take exam through their mobile or tablets devices anywhere at any time, while instructor need a secure and fast model to achieve assessment.

The proposed model is used with mobile learning system with no physical connect between student and instructor. The registration, payment, discussion, using course material and exam all do online.

The assessment through mobile exam in mobile learning is an open book exam; the student can use material to answer the questions. However, with mobile exam the ability to cheat between students increase since students can get mobile to another to answer the questions. The proposed model focus to this point. Also, the proposed model prevents the use of any other application during exam.

The proposed model starts with registration phase, where student can get their account with user name and password after that the iris recognition, in this phase the iris recognition is done through several steps as discussed before. The result of this step is a vector that is saved with user name and password in server database.

The next phase is login to exam the student login by providing their user name and password. An encrypted message that include Ui and Pi are sent to database server, if the decrypted message is verified with data saved on server, the iris image is requested. In this step the student captures an iris image using mobile camera, during capturing iris the student must remove any lenses or eyeglasses. Through the process the iris image recognition includes the same steps done in registration phase, the result after this step are presented as vector Vi, that contain Ui, Pi, and iris extracted features. Vi is sent as encrypted message to server. The decrypted message on server side is compared with data store in database. If verified then student can start exam session, otherwise the login is canceled.

The last phase in the proposed model focus on preventing cheating during exam. Through mobile exam there is no monitoring over student during exam time. Student can give the mobile to someone else to solve the questions. In order to prevent this type of cheating; the proposed system capture an iris image during exam in random time. This can help to avoid students of cheating and forgery, when student give their mobile to someone else to answer the questions.

8 Conclusion and Future Work

Mobile learning has generated a new challenge in security and authentication especially within the assessment phase. The reliability and trustworthiness of mobile learning course outcome is measured using exam, the results determine the power of mobile learning certificate. In this research, a new model is proposed to authenticate students using two type of authentication. Student uses traditional login method user name and password, in addition to the biometric authentication using iris recognition to verify the student. In addition, the proposed framework checks for student randomly during exam to prevent impersonality.

The proposed model requires no additional hardware, nevertheless we need to determine the minimum requirements for mobile camera resolution to capture a high-quality image. For future purposes, we will study the impact of using such system to determine the needed time required in capturing iris image during the exam and how it will affect the grades of students.

9 References

[1] Al-Raisi, A. N., & Al-Khouri, A. M. (2008). Iris recognition and the challenge of homeland and border control security in UAE. Telematics and Informatics, 25(2), 117-132. https://doi.org/10.1016/j.tele.2006.06.005

[2] Amin, R., Gaber, T., ElTaweel, G., &Hassanien, A. E. (2014). Biometric and traditional mobile authentication techniques: Overviews and open issues. In Bio-inspiring cyber security and cloud services: trends and innovations (pp. 423-446). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-43616-5_16

[3] Apampa, K. M., Wills, G., &Argles, D. (2010). User security issues in summative e-assessment security. International Journal of Digital Society (IJDS), 1(2), 1-13. https://doi.org/10.20533/ijds.2040.2570.2010.0018

[4] Bal, A., & Acharya, A. (2011, December). Biometric authentication and tracking system for online examination system. In 2011 International Conference on Recent Trends in Information Systems (pp. 209-213). IEEE. https://doi.org/10.1109/retis.2011.6146869

[5] Baran, E. (2014). A review of research on mobile learning in teacher education. Journal of Educational Technology & Society, 17(4), 17-32.

[6] Bhandwalkar, K. T., & Hanwate, P. S. (2014). Continuous User Authentication Using Soft Biometric Traits for E-Learning. International Journal of Innovative Research in Science, Engineering and Technology, 3.

[7] Bowyer, K. W., Hollingsworth, K., & Flynn, P. J. (2008). Image understanding for iris biometrics: A survey. Computer vision and image understanding, 110(2), 281-307. https://doi.org/10.1016/j.cviu.2007.08.005

[8] El-Hussein, M. O. M., & Cronje, J. C. (2010). Defining mobile learning in the higher education landscape. Journal of Educational Technology & Society, 13(3), 12-21.

[9] Gikandi J.W., Morrow D., DavisN.E.(2011), "Online formative assessment in higher education: A review of the literature", Computers & Education, vol.57, pp 2333–2351. https://doi.org/10.1016/j.compedu.2011.06.004

[10] Hanul, S., Niklas, K., Sebastian, M.: Poster: User preferences for biometric au-

[11] thentication methods and graded security on mobile phones. In: Symposium on Usability, Privacy, and Security (SOUPS). (2010).

[12] Hashemi, M., Azizinezhad, M., Najafi, V., & Nesari, A. J. (2011). What is mobile learning? Challenges and capabilities. Procedia-Social and Behavioral Sciences, 30, 2477-2481. https://doi.org/10.1016/j.sbspro.2011.10.483

[13] Jain, A.K. and Kumar, A. (2010) Biometrics of Next Generation: An Overview to Appear in Second Generation Biometrics, Springer.

[14] Jeong, D. S., Park, H. A., Park, K. R., & Kim, J. (2006, January). Iris recognition in mobile phone based on adaptive gabor filter. In International Conference on Biometrics (pp. 457-463). Springer, Berlin, Heidelberg. https://doi.org/10.1007/11608288_61

[15] Jiugen, Y., & Ruonan, X. (2016, August). Mobile terminal based mobile learning system design. In 2016 11th International Conference on Computer Science & Education (ICCSE) (pp. 699-703). IEEE. https://doi.org/10.1109/iccse.2016.7581664

[16] Kaiiali, M., Ozkaya, A., Altun, H., Haddad, H., &Alier, M. (2016). Designing a secure exam management system (SEMS) for M-learning environments. IEEE Transactions on Learning Technologies, 9(3), 258-271. https://doi.org/10.1109/tlt.2016.2524570

[17] Kang, B. J., & Park, K. R. (2010). A new multi-unit iris authentication based on quality assessment and score level fusion for mobile phones. Machine Vision and Applications, 21(4), 541-553. https://doi.org/10.1007/s00138-009-0184-0

[18] Kambourakis, G. (2013). Security and Privacy in m-learning and beyond: Challenges and state of the art. International Journal of u-and e-Service, Science and Technology, 6(3), 67-84.

[19] Kljunić, J., & Vukovac, D. P. (2015, January). A survey on usage of mobile devices for learning among tertiary students in Croatia. In Central European Conference on Information and Intelligent Systems (26; 2015).

[20] Kurkovsky, S., Carpenter, T., & MacDonald, C. (2010, April). Experiments with simple iris recognition for mobile phones. In 2010 Seventh International Conference on Information Technology: New Generations (pp. 1293-1294). IEEE. https://doi.org/10.1109/itng.2010.75

[21] Lalitha, V., &Periasamy, J. K. (2018). Mobile based secured student online exam system.

[22] Levy, Y., & Ramim, M. (2007). A theoretical approach for biometrics authentication of e-exams. Nova Southeastern University, USA, 93-101.

[23] Lu, J., Sundaram, A., Meng, Z., Priya, A., Lu, G., & Stav, J. B. (2012). Mobile Exam System–MES: Architecture for Database Management System. In Learning with Mobile Technologies, Handheld Devices, and Smart Phones: Innovative Methods (pp. 1-20). IGI Global. https://doi.org/10.4018/978-1-4666-0936-5.ch001

[24] Masek, L. (2003). Recognition of human iris patterns for biometric identification (Doctoral dissertation, Master's thesis, University of Western Australia).

[25] Mellar, H., Peytcheva-Forsyth, R., Kocdar, S., Karadeniz, A., &Yovkova, B. (2018). Addressing cheating in e-assessment using student authentication and authorship checking systems: teachers' perspectives. International Journal for Educational Integrity, 14(1), 2. https://doi.org/10.1007/s40979-018-0025-x

[26] Meng, Z., & Lu, J. (2011). Implementing the emerging mobile technologies in facilitating mobile exam system. IACSIT Press.

[27] Monaco, J. V., Stewart, J. C., Cha, S. H., & Tappert, C. C. (2013, September). Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works. In 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS) (pp. 1-8). IEEE. https://doi.org/10.1109/btas.2013.6712743

[28] Naismith, L., & Corlett, D. (2006). Reflections on success: a retrospective of the mLearn conference series 2002-2005. mLearn 2006–Across generations and cultures. Banff, Canada.

[29] Obeidallah, R., Al Ahmad, A., Farouq, F. and Awad, S. (2015) 'Students authentication in e-assessment sessions: a theoretical biometric model for smartphone devices', Int. J. Business Information Systems, Vol. 19, No. 4, pp.450–464. https://doi.org/10.1504/ijbis.2015.070204

[30] Raina, V. K. (2011). Integration of biometric authentication procedure in customer oriented payment system in trusted mobile devices. International Journal of Information Technology Convergence and Services, 1(6), 15. https://doi.org/10.5121/ijitcs.2011.1602

[31] Ramu, T., & Arivoli, T. (2013). A framework of secure biometric based online exam authentication: an alternative to traditional exam. Int J Sci Eng Res, 4(11), 52-60.

[32] Rao, N. S. S., Harshita, P., Dedeepya, S., & Ushashree, P. (2011). Cryptography–analysis of enhanced approach for secure online exam process plan. International Journal of Computer Science and Telecommunications, 2(8), 52-57.

[33] Richard N. (2015), "The Form of Examination to be used for effective assessment In Institutions of Higher Learning: Views of lecturers from Four Universities in Zimbabwe", Am. J. Soc. Mgmt. Sci, vol.6, No.1, pp 18-23.

[34] Ross, A. (2010). Iris recognition: The path forward. Computer, 43(2), 30-35.

[35] Sabbah, Y. W., Saroit, I. A., &Kotb, A. M. (2012). A Smart Approach for Bimodal Biometric Authentication in Home-Exams (SABBAH Model). Biometrics and Bioinformatics, 4, 32-45. https://doi.org/10.1109/setit.2012.6481902

[36] Sheela, S. V., & Vijaya, P. A. (2010). Iris recognition methods-survey. International Journal of Computer Applications, 3(5), 19-25.

[37] Sungkur, R. K., Beekoo, I., & Bhookhun, D. L. (2013, September). An enhanced mechanism for the authentication of students taking online exams. In 2013 Africon (pp. 1-5). IEEE." https://doi.org/10.1109/afrcon.2013.6757790

[38] Trabelsi, Z., & Shuaib, K. (2011). Implementation of an Effective and Secure Biometrics-Based Student Attendance System. International Journal of Computers and Applications, 33(2), 144-153. https://doi.org/10.2316/journal.202.2011.2.202-2928

[39] Tufekci, A., Ekinci, H., & Kose, U. (2013). Development of an internet-based exam system for mobile environments and evaluation of its usability. Mevlana International Journal of Education, 3(4), 57-74. https://doi.org/10.13054/mije.13.59.3.4

[40] Miguel Moneo, J. An information security model based on trustworthiness for enhancing security in on-line collaborative learning.

[41] Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2014). Surveying the development of biometric user authentication on mobile phones. IEEE Communications Surveys & Tutorials, 17(3), 1268-1293. https://doi.org/10.1109/comst.2014.2386915

10 Authors

Aayat Shdaifat works as a Tutor in Basic Science Department in The Hashemite University. She obtained her Masters in Computer Information System from Jordan University in 2010. Her Research interests are involved In Information Retrieval, and Information systems. aayat@hu.edu,jo

Randa Obeidallah works as a Tutor in Computer Information System Department in The Hashemite University. She obtained her Masters in Computer Information System from Jordan University in 2009. Her Research interests are involved In Information Retrieval, e-learning Systems, and Information systems. randa.ali@hu.edu.jo

Ghadeer Ghazal works as a Tutor in Basic Science Department in The Hashemite University. She obtained her Masters in Computer Information System from Jordan University in 2010. Her research interests are involved in Services Composition and e-learning. ghadeeri@hu.edu.jo

Alaa A. Abu Srhan, is a full-time lecturer at the Hashemite University, she holds a Master degree from faculty of science and information technology, Zarqa University. She holds a bachelor degree from Al Balqa University. Her research interest includes optimization, machine learning deep learning, and image processing. alaaa@hu.edu.jo

Nesreen Rabah Abu Spetan is a computer teacher at ministry of education (MOE), she has been working in this profession since 2004 , have a master's Degree in Computer information System ,from Jordan university since 2010 .Nasreen wrote thesis about Digital Elevation Model Using Numerical Simulation Model , as a part of my master's course, she is interested in studies in E-learning and image processing. nesreen__a_spetan@hotmail.com

Article submitted 2020-02-13. Resubmitted 2020-03-17. Final acceptance 2020-03-22. Final version published as submitted by the authors.