Date of publication DEC-31, 2021, date of current version JAN-17, 2021.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.20.4.2441

A Robust User Authentication Technique in Online Examination

NADER ABDEL KARIM, HASAN KANAKER, SHADI ALMASADEH, JAMAL ZARQOU
Isra University, Amman, Jordan, (nader.salameh@iu.edu.jo, hasan.kanaker@iu.edu.jo, shadi.almasadeh@iu.edu.jo, jamal_sam@iu.edu.jo)

Corresponding author: Nader Abdel Karim (e-mail: nader.salameh@iu.edu.jo).

ABSTRACT User authentication in the online environment is promoting a hugely challenging issue. This has contributed to the realization of a user authentication where the exams can be performed over the Internet at any time and from any place and by using any digital device. Consequently, further investigations are required to focus on improving user authentication methods to enhance online security mechanisms, especially in the field of e-exams. This research proposes a new user authentication technique based on the user interface (UI). The novel idea is created based on the design preferences of candidates who are taking the e-exams. Several design features are used to design a special user interface for e-exams, for example, the font attributes, back colour, number of questions per page, group categories for questions based on difficulties, and timer setting. The introduced technique can be used to support the user authentication process in the e-exams environment. Furthermore, the proposed technique provides the ability to login to the e-exam without the need to remember the login information, but to select what the student prefers according to his/her personal information. Based on the literature review, a primary evaluation claiming that the students have differences in their preferences and that each user has stable design preferences within different sessions is revealed. In regard to these facts, they become the resource and essence of this research. The security performance of the proposed method is evaluated. The results of the experiments show a false positive (FP) rate of 0.416% and a false negative (FN) rate of 0%.

KEYWORDS online exams interface design; user preferences; online authentication; authentication methods; e-exam.

I. INTRODUCTION

DUE to the simultaneous growth of using the Internet; the learning style becomes able to be transformed from an old-style such as school rooms, classes, and institutes into a more valuable resource available at any time and at any place like e-learning systems. This is beyond physical limitations which is available remotely from dispersed geographic locations. As witnessed or seen in this era, humanity is advancing in different areas of science and technology which also leads to a significant improvement of E-learning within the education processes in the future. In a recent report by Global Industrial Analyst, (2010), 107.3 billion dollars was expected to be reached in the E-learning market by 2015. Various disciplines such as colleges, universities, and educational institutes are likely to accept E-learning due to its ability to be accessible, updatable, available, usable, resource-efficient, and economical. The examination performed in e-learning combines both the teaching and learning components. There will not be any physical contact between the teachers, students, and administration within an e-learning environment. The user authentication procedure tends to be crucial for the e-learning environment. But the e-learning environment also tends to be at risk of different security threats. E-exams might fall victim to imitation or impersonation by the use of stake tools together with applications because it is considered a crucial part of the e-learning environment. User authentication is a main important issue within the online environments making it one of the major aims of student authentication which is to make sure that an authentic user is one interacting with the e-exam.

The remaining sections are as follows: section 2 covers related works, section 3 shows the mechanisms of e-exams authentication methods, section 4 discusses the interface designs; Section 5 presents the association of user characteristics with his/her UI preferences, section 6 explores the proposed evaluation method, and section 7 concludes the contributions of this research and presents the future works.

II. RELATED WORKS

Many researchers are trying to solve the problem of user authentication in e-exam sessions. A variety of solutions with different authentication methods were introduced, for example, in [1], a remote biometrics authentication method for e-exams was proposed. They used regular commercial webcams as a sensor for immediate facial recognition while preceding a continuous facial recognition process based on requesting fingerprint checking to get a dependable identification. In [2] authors tried to investigate the accuracy of face recognition that was captured online using a webcam for user authentication in the online examination. Authors in [3] suggested a novel authentication system that integrates username and password with a palm print, forming a biometric authentication. Moreover, a video recording system was also compound into their proposed authentication system. A new approach called PBAF (Profile-Based Authentication Framework) was proposed in [32]. The security questions were used to identify users attending the e-exams. In [4], the authors proposed an authentication system with multi-biometrics levels such as fingerprints and mouse movements to support various e-learning services.

In [5], the authors proposed an examination system that depends on a single zip disk. This system requires only a simple separate computer to take an exam, which also offers a secure and efficient examination platform. The system provides security by making use of the encryption of all data and users' registration files. It also checks the unique network card address of the PC on which the test is being run.

III. E-EXAMS AUTHENTICATION METHODS

In general, most computerized systems are secured by integrating with a user authentication process [6]. The authentication identity requires the user to provide extra information to guarantee his/her identity. Overall, user authentication methods can be classified into three main categories:

A. KNOWLEDGE-BASED AUTHENTICATION (NBA)

Private information about the user is required to identify the owner of the account such as user-id, password, security questions, etc. NBA is a well-known user identification method since passwords are memorable, easy to use, low cost, and user-friendly [4, 7]. However, because of the nature of e-exams, students can pass their login details to another person to obtain more grades [4].

B. POSSESSION-BASED AUTHENTICATION (PBA)

This kind of authentication stands on the private details of a user based on using his/her tokens and tickets. A token means a hardware device in which a user can keep or carry. On the other hand, it does not prove enough verification of ownership of a token because it can be stolen or copied by others [7-9]. Smart card tokens, memory cards, dongles, and keys are common tools used in PBA [7].

C. BIOMETRICS-BASED AUTHENTICATION (BBA):

For this procedure, user identification is carried out based on the physiological and behavioral characteristics of the individual. Physiological biometrics utilizes the user's physical characteristics (e.g., face, fingerprints, iris, etc.), on the other side behavioral biometrics is associated with measuring and focusing on uniquely identifying and measuring the patterns in human activities (e.g., gait, voice, keystroke dynamic, etc.) [6-8, 10-14] BBA provides the best effective and accurate identification method because biometrics cannot be easily impersonated or shared with others. However, BBA is known to be a complex and expensive method because of the special kinds of hardware and software required to run it [7, 10]. Furthermore, BBA is not usually the preferred choice by users since it is seen as an intruding tool and also a violation of user privacy [7]. Moreover, several methods of user authentication can help in the authentication process such as IP address, location, and timestamp as it was presented in [15].

IV. USER INTERFACE DESIGN

The simultaneous growth in the production of computer technology and information including the usage of the internet has globally drawn attention to the significance of UI [16-20]. New technologies are being developed to serve the users easily and confidently. Hence, user interfaces are becoming one of the most important parts of products [16]. In [21], UI was defined as software or hardware or both that enable the user to interact with and perform some operations on a system, device, or program.

The UI design is considered a significant element of any computer application by enabling the end-users to learn, accept, and proficiently interact with the whole system [22]. Whatever the kind of essential technology used, the users will operate the system by using UI design [23, 24]. For example, a student taking an e-exams interacts with the UI that is a combination of many elements that are normally used to display the questions of a given exam conveniently. UI offers also the ability to assist the student to attend the examination easily and efficiently [18, 25, 26].

V. USER CHARACTERISTICS AND INTERFACE PREFERENCES

User characteristics tend to cause a direct effect on the interface design [18, 27, 28]. As a result, the UI design of the e-exam should take into account the capability and character of an individual. According to the researches in [27-29], and [30], the user features that might affect the UI design can be

categorized into physical, cognitive, psychomotor, demographics, or experiences.

UI preferences are optional to be used in the UI elements which creates the whole UI. Based on the literature [31-33] it can be concluded that there is a connection preference between the characteristics and the interface of a user. For example, Mills and Michael agree that a relationship exists between users' characteristics and the type of font they prefer [31]. Personality reasons lead to changes in user interface design preferences [32]. However, Evers et al., [33] showed that design preferences have to affect interface acceptance. Therefore, the users' characteristics might eventually affect their interface preferences while each user has his/her characteristics for diverse interface designs.

It is worth knowing the type of choices that can be offered to users to improve the efficiency as well as the convenience of examinees when attending e-exams, besides using these factors as an indication of the user's identity. On reviewing the literature relating to the design of online examinations [34-39], it can be concluded that e-exams contain nine main design features, namely font style, font size, font type, font colour, background colour, sound alert, questions group, number of questions per page, and counters. Each of these design features has potential values that can be explored for an optimal UI design, which tries to give both the effectiveness and convenience of e-exam takers.

VI. PREFERENCES-BASED AUTHENTICATION (PrBA)

In current times, numerous human-computer interaction (HCI) studies are concentrating on developing an adaptive UI with the intention to enhance the usability of the systems and to improve the user's convenience [30, 40] aiming to launch appropriate UI depending on the personal characteristics of the users [30] as shown in Fig. 1.

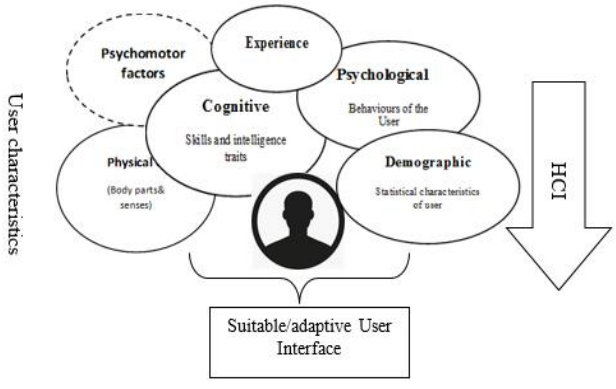

Figure 1. The relationship between UI design and user characteristics [9]

This was prepared in reverse concerning the suggested technique by demanding to distinguish the individuals based on their favourite preferences. The novel technique provides users with the decision to make their own choices for preferable UI design with their characteristics. Consequently, the UI preferences can be used as an indication of the user's identity as the work introduced in [4] by using security questions. The contributions of this research are based on discovering the fact that the security questions are not proficient enough [41]. The added step in the e-exam promotes a challenging user-unfriendly interface to the individuals. In the meantime, the proposed method offers the interface of e-exams with several preferences of the students which later allows them to have a suitable design based on their choice retrieved from their characteristics. This process intends to make it more convenient, and also would be able to identify the examinees of the e-exams. The introduced user authentication technique to identify a user in relation to his/her preferences is shown in Fig. 2.

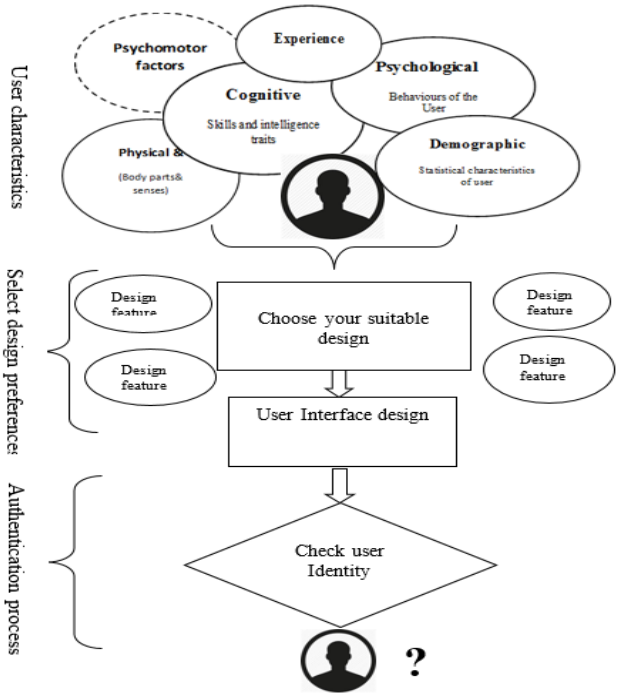

Figure 2. The Framework of the Proposed Preferences-Based Authentication Method

The proposed authentication method allows the online user to choose the interface design preferences based on his/her characteristics, and hence, the user can be identified based on the chosen interface that reflects the characteristics of that user. Furthermore, we try to encounter a classical problem involving the trade-off between security and usability in user authentication [43].

As shown in Fig. 2, the user chooses his/her interface design preferences, which are built from several design features, and each design feature comprises at least two values (later will be used for authentication). Having chosen the UI preferences, the perceived UI design appears; thus, user identity can be identified based on the UI preferences retrieved from UI design.

The proposed system will double-check the user identity before the user can gain access to the online examination session. The authentication process will involve the following phases:

Login Phase: getting access can be done by using a user id and password. If a user passes the former step then the UI of e-exam preferences will be taken into account.

E-exam UI Preferences Phase: The extracted preferences from the web page provide the individual with the capability to decide his /her own favorite design of UI exam based on his personal characteristics. Different e-exam design features are to be presented on this page (see Figure 3), such as number of questions/page, font type, font size, font style, font colour, background colour, time counter (digital counter(descending/ascending), old-style clock), sound alert, number of questions/page.

In this stage, the user will be asked to choose the preferences for UI design based on his/her own characteristics. Thus, the system will match the user interface preferences with the previously stored user's preferences template, and then the system will decide to either accept or reject the user.

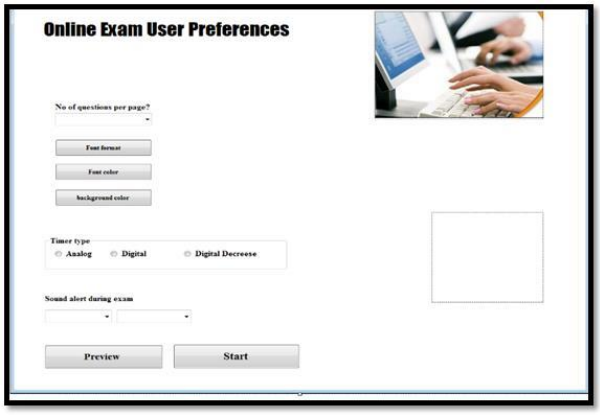

Figure 3. E-exams design preferences webpage

Answers Confirmation Phase: The authentication can be achieved by considering face recognition. Hence, before submitting the answers, a comparison between the target image and the face of the authorized user is performed to confirm the authority.

In the proposed work, each answer will not be considered until confirming the user identity. This can be applied by saving the face image for each user in a common database which later can be used to conduct the comparison. When the system tends to save the answer; the camera is then used to capture the face of the user and compare it with its synonym. Based on the luminance, the measurements of the similarity between the two images can be calculated as shown in Equation 1. The face of the user is detected based on the work presented in [42], also the target images that contain the faces of the users are saved based on this work as well. Consequently, the confirmation phase is conducted based on applying the SSIM between the target image and the incoming image of the user.

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)}, \quad (1)$$

where σ_x, σ_y, μ_x, μ_y, and σ_{xy} are standard deviations and the means for images of x and y.

Based on the conducted experiments, it was found that the SSIM value of greater than 0.5 returns the best results of matching. SSIM works better with enough source of light that focuses on the face and vice versa.

The steps of recognizing identities are explored in Figure 4. The maximal and minimal of SSIM images synthesized with the MSE in several images are illustrated in Figure 5. The images have been assigned with the same MSE values concerning the reference image, but with different perceptual quality. The algorithm of face detection that was used in [42] is employed to achieve the first step of this research work. 200 frames are used to test the performance of this algorithm. The results revealed that 91% of corrected matches were achieved, where 9% of incorrect matches was occurred by rejecting the matches. The strength of this work is originating from no any of the correct matches was occurred for the false matches. Also, it was noted that decreasing the source of light decreases the performance of the proposed algorithm. Another note that should be taken into account, that the reference image should be updated consequently to provide a better match than depending on an old version.

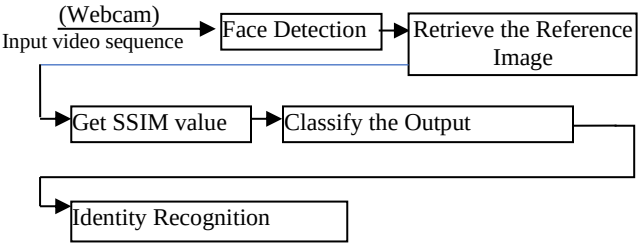

Figure 4. The sequence steps of recognizing identities.

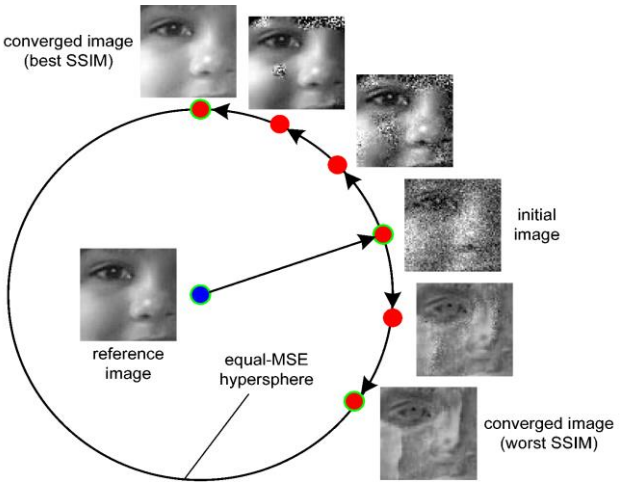

Figure 5. Several converged images for a reference image.

Figure 6 shows the process model for the proposed environment of the e-exam authentication process. The presented idea explores the e-exam authentication system by possesses two-steps of authentication login and a preference. The following stages describe how the authentication system takes place which starts with obtaining the user's information and finishes with the user identification.

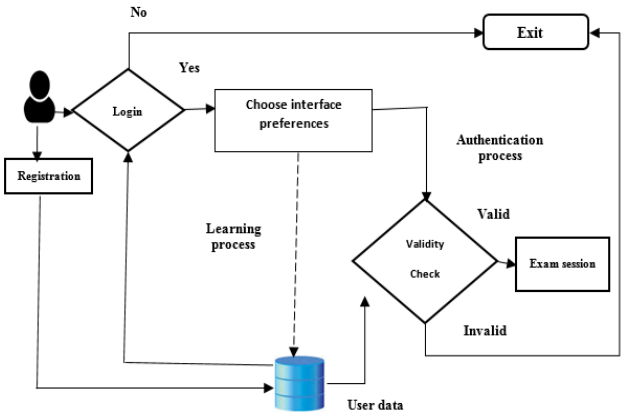

Figure 6. The flow control of the proposed model

Stage 1: For this part, two steps should be carried out before starting the actual e-exam.

a. Registration: As shown in Figure 6, the procedure begins after the completion of the registration to obtain the login information. The members are to come up with their accounts to finish the online registration. This process consists of choosing the user id, password, date of birth, email, gender, and educational level.

b. Learning process: Following the previous step, the student will be guided to an exam preference page to select his/her own "exam UI preferences" for exercise and training purposes. After completing the practice session, the system requires to save the UI preferences which the individual has picked and entered. The data then will be saved in a database which later will be used to conduct some experiments and evaluate the results.

Stage 2: Both authentications of login and preferences will be carried out.

a. Login authentication: The login procedure allows a maximum of three times to access the e-exam by entering the user id and password. Passing the former then it will be linked to the "e-exam UI design preferences" webpage. Otherwise, the user will not be able to log in.

b. Preferences Authentication: During the verification process; if the set of extracted interface preferences matches any of the saved user preferences; then the student will be able to access the e-exam session. Otherwise, the student will not be able to have access. If a denial logging has occurred then it will be reported to the system administrator.

VII. EXPERIMENTAL RESULTS

To evaluate the proposed method, the preferences can be used as evidence on user identity, several experiments were conducted on 30 undergraduate students. The main goal of the experiments was to check the existence of variations in the online-exam interface design that uses preferences and count the consistency in the preferences of each login to the e-exam. Seven design features were chosen in the e-exam preferences page to check the student's identity as shown in Figure 3. The features that were used are font (face, style, and size), number of questions/page, time counter, and sound alert, in addition to the biometric confirmation identity (based on face recognition).

A training set from the e-exam preferences web page was created, the students selected their e-exam design preferences 4 times in different sessions within 2 weeks. In each session, after the login, each student picked his preferences (7 choices in each session), so that in total, each student picked up 28 choices in 4 sessions.

The primary results have revealed that there are no two or more students that can have the exact preferences. Ten students selected the same preferences during 4 sessions with an accuracy rate of 100%, three students made one change with an accuracy rate of 96.4%, four students selected 2 different choices in comparison to the first trial with an accuracy rate of 92.6%, eleven students selected 3 different preferences based on the first trial with an accuracy rate of 88.7%, and two students selected four different preferences based on the first trial with an accuracy rate of 84.6%. The average total accuracy of all the students was 93% as shown in Table 1.

Table 1. Students' choices, accuracy, and total changes in 4 sessions

No. of Students	No. of preferences have changed (4 Trials)	Choice Accuracy /student %
10	0	100.00
3	1	96.47
4	2	92.60
11	3	88.70
2	4	84.60
30 Students	27 Total changes	93% accuracy for 30 students

Note: each student tried this experiment 4 times, so the total number of choices for each one would be (7*4=28). **Choice Accuracy /student** =((1- (No. of user changes "4 attempts")/(4 "attempts" * 7"possible changes"))*100)%

Two experiments were conducted to evaluate the performance of applying the proposed method as a user authentication approach. To evaluate the performance of any authentication method, two important measures are used, namely, FP and FN (i.e., falsely rejecting a legitimate user or falsely accepting an impostor). In the first experiment, FN rates were measured, 91 students were recruited from local universities. FN means: authorized (legitimate) users cannot pass the authentication phase to start his/her exam. A total of 83 participants finished all of the phases of the experiment. Based on the results, 13 legitimate users failed the preference authentication in three attempts given the zero thresholds (i.e., 0 mistakes), and hence, the FN rate was 15.6%. Moreover, three users failed to access the system for the threshold of 1 mistake, resulting in an FN rate of 3.6%. Finally, all participants accessed their accounts when the threshold was 2 or more mistakes, which indicates a 0% FN rate. See Table 2. Users needed an average time of around 36 s to pass the preference authentication. Results seemed reasonable compared with the method proposed by (Markus Jakobsson & Siadati, 2013), which required around 100 s for registration and around 40 s for authentication.

Table 2. False Negative Rates for Legitimate Users with Three Attempts

Threshold	0 mistake	1 mistake	2 mistakes	3 mistakes
No. of users	13	3	0	0
FN rate	15.6%	3.6 %	0%	0%

FN: authorized users cannot access the system

In the second experiment, FP rates were measured, 6 adversaries were recruited to overcome the proposed authentication method, four of them with security backgrounds (i.e., Hk1 to Hk6). The experiment is focused on the most dangerous case of adversary attack (Markus Jakobsson et al., 2008)—those by informed adversaries—to obtain reliable and accurate results. Experiment results and the relationship between the obtained FP rates and the threshold values are shown in Table 3. When the threshold value was 0, the FP rate for the attack was 0%. When thresholds were up to 2 mistakes only, the FP rate was 0.41%. Finally, when the threshold included 3 mistakes, the FP rate was (0.83%).

Table 3. FP Rates for Adversaries with 240 Hacking Attempts

Threshold	0 mistake	1 mistake	2 mistakes	3 mistakes
FP rate	0%	0.41%	0.41%	0.83%

According to (M Jakobsson & Siadati, n.d.; Reeder & Schechter, 2011), the ideal setting when testing the performance of authentication methods is 1 since it keeps both FN and FP rates below 1%. In the current work, the requirement of 1% was satisfied by the threshold for 2 mistakes.

The face recognition was tested by allowing ten students to try to submit the answers to the authorized users, the result was fine with recognizing them as unauthorized but 3 over 30 were unable to send their answers because of the failure of SSIM recognition. This can be justified that the source light was not enough on the face of that user causing the failure of matching.

VIII. CONCLUSION & FUTURE WORK

The user authentication procedure might be KBA, PBA, or BBA. Each one of these authentication techniques comes with both advantages and drawbacks. BBA is known to be the best precise and common authentication method utilised in e-exams. The suggestion in this article is related to the e-exam authentication method. The technique is made up of three stages for the authentication process. The first stage consists of login authentication focuses on entering the user name or ID and password. The second stage consists of the PrBA that is developed for the e-exam based on UI design which can be chosen by the user. The PrBA normally relies on a particular structure which stresses that the users' characteristics normally affect the interface design, and each user or individual possesses his/ her own way of doing things known as characteristics. Finally, identity confirmation was achieved based on face recognition to authorize user identity before submitting the final answers. Also, the e-exam UI design that is picked by the candidate before starting the exam session can provide evidence of the user's identity. Prominent results were achieved based on several experiments that involved 30 students to check up the consistency of their preferences and the variation in their e-exam interface design (preferences), and biometric identity recognition. Based on the conducted experiments, the security performance of the proposed method shows a false positive (FP) rate of 0.416% and a false negative (FN) rate of 0%. However, larger sample size needs to be recruited to confirm these results.

Future research can be carried out to investigate the performance using a wider sample of students.

References

[1] A. Moini and A. M. Madni, "Leveraging biometrics for user authentication in online learning: A systems perspective," *IEEE Syst. J.*, vol. 3, no. 4, pp. 469–476, 2009. https://doi.org/10.1109/JSYST.2009.2038957.

[2] B. Penteado and A. Marana, "A video-based biometric authentication for e-learning web applications," *Enterp. Inf. Syst.*, 2009. https://doi.org/10.1007/978-3-642-01347-8_64.

[3] S. M. Al-Saleem and H. Ullah, "Security considerations and recommendations in computer-based testing," *Scientific World Journal*, vol. 2014, p. 562787, 2014. https://doi.org/10.1155/2014/562787.

[4] A. Ullah, H. Xiao, M. Lilley, and T. Barker, "Using challenge questions for student authentication in online examination," *Int. J. Infonomics*, vol. 5, no. 3, pp. 631–639, 2012. https://doi.org/10.20533/iji.1742.4712.2012.0072.

[5] S. Asha and C. Chellappan, "Authentication of e-learners using multimodal biometric technology," *Proceedings of the 2008 Int. Symp. Biometrics Secur. Technol.*, pp. 1–6, 2008. https://doi.org/10.1109/ISBAST.2008.4547640.

[6] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, "Continuous user authentication using multi-modal biometrics," vol. 53, issue C, pp. 234–246, 2015. https://doi.org/10.1016/j.cose.2015.06.001.

[7] M. Zviran, "Identification and authentication : Technology and implementation issues," *Commun. Assoc. Inf. Syst.*, vol. 17, no. 1, pp. 2–30, 2006. https://doi.org/10.17705/1CAIS.01704.

[8] T. Peltier and J. Peltier, *Complete Guide to CISM Certification*, Netw. Secur., 2007, 476 p.

[9] N. A. Karim and Z. Shukur, "Using preferences as user identification in the online examination," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 6, no. 6, pp. 1026-1032, 2016. https://doi.org/10.18517/ijaseit.6.6.1412.

[10] N. A. Karim, Z. Shukur, and A. E. M. AL-banna, "UIPA: User authentication method based on user interface preferences for account recovery process," J. Inf. Secur. Appl., vol. 52, 102466, 2020. https://doi.org/10.1016/j.jisa.2020.102466.

[11] O. Ogbanufe and D. J. Kim, "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment," *Decis. Support Syst.*, vol. 106, pp. 1–14, 2018. https://doi.org/10.1016/j.dss.2017.11.003.

[12] A. Alzubaidi and J. Kalita, "Authentication of smartphone users using behavioral biometrics," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 1998–2026, 2016. https://doi.org/10.1109/COMST.2016.2537748.

[13] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, 2015. https://doi.org/10.1109/MSP.2015.2434151.

[14] I. Velásquez, A. Caro, A. Caro, and A. Rodríguez, "Authentication Schemes and Methods: a Systematic Literature Review," *Information and Sowtware Technology*, vol. 94, pp. 30-37, 2018. https://doi.org/10.1016/j.infsof.2017.09.012.

[15] Z. Abdel Karim, Nader, Shukur, "Review of user authentication methods in online examination," *Asian J. Inf. Technol.*, vol. 14, no. 5,

pp. 166–175, 2015.
[16] K. S. Park and C. Hwan Lim, "A structured methodology for comparative evaluation of user interface designs using usability criteria and measures," *Int. J. Ind. Ergon.*, vol. 23, no. 5–6, pp. 379–389, 1999. https://doi.org/10.1016/S0169-8141(97)00059-0.
[17] G. Calvary, J. Coutaz, D. Thevenin, Q. Limbourg, L. Bouillon, and J. Vanderdonckt, "A unifying reference framework for multi-target user interfaces," *Interact. Comput.*, vol. 15, pp. 289–308, 2003. https://doi.org/10.1016/S0953-5438(03)00010-9.
[18] P.-L. P. Rau, Y.-Y. Choong, and G. Salvendy, "A cross cultural study on knowledge representation and structure in human computer interfaces," *Int. J. Ind. Ergon.*, vol. 34, no. 2, pp. 117–129, 2004. https://doi.org/10.1016/j.ergon.2004.03.006.
[19] D. Lam and D. Swayne, "Issues of EIS software design: Some lessons learned in the past decade," *Environ. Model. Softw.*, vol. 16, no. 5, pp. 419–425, 2001. https://doi.org/10.1016/S1364-8152(01)00011-1.
[20] W. O. Galitz, *The Essential Guide to User Interface Design: An Introduction to GUI Design Principles and Techniques*, Wiley, 2007.
[21] G. McDaniel, *IBM Dictionary of Computing*, 1994, 758 p.
[22] A. R. Puerta, "Supporting User-Centered Design of Adaptive User Interfaces Via Interface Models," *Time Intell. User Interfaces Decis. Support*, 1998.
[23] P. A. Chalmers, "The role of cognitive theory in human-computer interface," *Comput. Human Behav.*, vol. 19, no. 5, pp. 593–607, 2003. https://doi.org/10.1016/S0747-5632(02)00086-9.
[24] A. Agah and K. Tanie, "Intelligent graphical user interface design utilizing multiple fuzzy agents," *Interact. Comput.*, vol. 12, no. 5, pp. 529–542, 2000. https://doi.org/10.1016/S0953-5438(99)00022-3.
[25] K. S. Kim, "Information-seeking on the Web: Effects of user and task variables," *Libr. Inf. Sci. Res.*, vol. 23, no. 3, pp. 233–255, 2001. https://doi.org/10.1016/S0740-8188(01)00081-0.
[26] M. Zajicek, "Successful and available: Interface design exemplars for older users," *Interact. Comput.*, vol. 16, no. 3, pp. 411–430, 2004. https://doi.org/10.1016/j.intcom.2004.04.003.
[27] A. M. Figueroa, R. Juárez-Ramírez, S. Inzunza, and R. Valenzuela, "Implementing adaptive interfaces: A user model for the development of usability in interactive systems," *Comput. Syst. Sci. Eng.*, vol. 29, no. 1, pp. 95–104, 2014.
[28] P. Zhang, "Integrating human-computer interaction development into SDLC: A methodology," Proceedings of the Americas Conference on Information Systems *AMCIS 2004*, August 2004, pp. 1–7.
[29] D. Stone, C. Jarrett, M. Woodroffe, and S. Minocha, User Interface Design and Evaluation, Published by Morgan Kaufmann, Los Altos, CA, 2005, xxviii + 669 p.
[30] E. Zudilova-Seinstra, "On the role of individual human abilities in the design of adaptive user interfaces for scientific problem solving environments," *Knowl. Inf. Syst.*, vol. 13, no. 2, pp. 243–270, 2007. https://doi.org/10.1007/s10115-006-0061-3.
[31] M. Bernard, C. H. Liao, and M. Mills, "The effects of fonttype and size on the legibility and reading time of online text by older adults," *CHI'01 Ext. Abstr. Hum. Factors Comput. Syst.*, pp. 175–176, 2001. https://doi.org/10.1145/634067.634173.
[32] A. Karsvall, "Personality preferences in graphical interface design," *Proceedings of the Second Nord. Conference on Human-Computer Interaction, ACM*, 2002, pp. 217–218. https://doi.org/10.1145/572020.572049.
[33] V. Evers and D. Day, "The role of culture in interface acceptance," *Proceedings of the Hum. Comput. Interact. Interact'97*, no. 1993, pp. 260–267, 1997. https://doi.org/10.1007/978-0-387-35175-9_44.
[34] Z. Islam, M. Rahman, and K. Islam, "Online examination system in bangladesh context," *Sci. Environ. Technol.*, vol. 2, no. 3, pp. 351–359, 2013.
[35] L. Rello, G. Kanvinde, and R. Baeza-Yates, "Layout guidelines for web text and a web service to improve accessibility for dyslexics," *Proceedings of the Int. Cross-Disciplinary Conf. Web Access W4A'12*, 2012, p. 1. https://doi.org/10.1145/2207016.2207048.
[36] R. H. Hall and P. Hanna, "The impact of web page text-background colour combinations on readability, retention, aesthetics and behavioural intention," *Behav. Inf. Technol.*, vol. 23, no. 3, pp. 183–195, 2004. https://doi.org/10.1080/01449290410001669932.
[37] "Exam Layouts – What's Best? – Etudes." [Online]. Available at: http://etudes.org/exam-layout/.
[38] N. A. Karim, Z. Shukur, and M. Ghazal, "Proposed features of online examination interface design," *Asian J. Inf. Technol.*, vol. 15, no. 16, pp. 2733-2736, 2016.
[39] N. Abdel Karim and Z. Shukur, "Proposed features of an online examination interface design and its optimal values," *Comput. Human Behav.*, vol. 64, pp. 414–422, 2016. https://doi.org/10.1016/j.chb.2016.07.013.
[40] V. López-Jaquero, F. Montero, J. P. Molina, P. González, and A. Fernández-Caballero, "A seamless development process of adaptive user interfaces explicitly based on usability properties," *Lect. Notes Comput. Sci.*, vol. 3425, pp. 289–291, 2005. https://doi.org/10.1007/11431879_19.
[41] M. Just and D. Aspinall, "Personal choice and challenge questions: a security and usability assessment," *Proceedings of the 5th Symp. Usable Priv. Secur SOUPS'09*, 2009, pp. 1–11. https://doi.org/10.1145/1572532.1572543.
[42] J. Zraqou, W. Alkhadour, and A. Al-Nu'Aimi, "An efficient approach for recognizing and tracking spontaneous facial expressions," *Proceedings of the 2013 2nd Int. Conf. E-Learning E-Technologies Educ. ICEEE 2013*, pp. 304–307, 2013. https://doi.org/10.1109/ICeLeTE.2013.6644393.

Dr. NADER SALAMEH was awarded his Ph.D. in 2017 from the National University of Malaysia (UKM), Malaysia. His Ph.D. thesis investigated a new User authentication method based on user interface preferences for the account recovery process (UIPA). He has very good experience in the field of user authentication, cyber-security, Human-Computer Interaction (HCI), and E-learning. Also, he has had been engaged in several research works such as Preferences based authentication, virtual privacy technique.

Dr. HASAN MAHMOUD KANAKER received a Bachelor degree in Computer Information System (CIS) from Al Zaytoonah University of Jordan and a Master degree in *computer science (CS) from Al Balqa'* Applied University. Dr.Kanaker got his Ph.D. in information security from Islamic Science UniversityofMalaysia (USIM), 2018. Currently, he is an assistant professor in the Cybersecurity department at Isra University, Jordan. His research interest includes information Security, Malware and Malware Detection, Cloud Computing Security, Data Mining and Machine learning, and Network Security.

Dr. SHADI R. MASADEH received a BSc degree in Computer Science and Computer Information System in 2000 and an MSc degree in Information Technology in 2003. with a Thesis titled *"A Mathematical Approach for Ciphering and Deciphering Techniques"* After that, he received Ph.D. from the department of Computer Information System/ Information and Network Security in 2009 with a Thesis

titled *"A New Embedded Method for Encryption/Decryption Technique Using Self Approach"*. His research interests include E-learning Management, Encryption, and Decryption Systems. Networking and Wireless security. Currently, I'm working at Isra University in Computer Information System and Cybersecurity ashead of the Department. He has submitted several conference papers and journals.

Dr. JAMAL ZRAQOU was awarded his Ph.D. in 2011 from Bradford University, United Kingdom. His Ph.D. thesis investigated the development of new technologies for processing information contained in multiple and overlapping images of the same scene to produce images of improved quality. He has very good experience in the field of image processing such as super-resolution, objects detection and tracking, facial expression tracking and recognition, object character recognition, and 3D image reconstruction from un-calibrated stereo pair of images. Also, he had been engaged in multiple research works such as: building smart cities, tracking systems based on GPS service, and information security.