Advances in Internet of Things, 2014, 4, 5-12
Published Online April 2014 in SciRes. http://www.scirp.org/journal/ait
http://dx.doi.org/10.4236/ait.2014.42002

Scientific Research

Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems

Ayham Fayyoumi[1], Anis Zarrad[2]

[1]Department of Information Systems, Al Imam Mohammad IBN Saud Islamic University (IMSIU), Riyadh, Saudi Arabia
[2]Department of Computer Science and Information Systems, Prince Sultan University (PSU), Riyadh, Saudi Arabia
Email: a.fayyoumi@ccis.imamu.edu.sa, azarrad@psu.edu.sa

Received 10 April 2014; revised 21 April 2014; accepted 28 April 2014

Abstract

The main objective of this research is to provide a solution for online exam systems by using face recognition to authenticate learners for attending an online exam. More importantly, the system continuously (with short time intervals), checks for learner identity during the whole exam period to ensure that the learner who started the exam is the same one who continued until the end and prevent the possibility of cheating by looking at adjacent PC or reading from an external paper. The system will issue an early warning to the learners if suspicious behavior has been noticed by the system. The proposed system has been presented to eight e-learning instructors and experts in addition to 32 students to gather feedback and to study the impact and the benefit of such system in e-learning environment.

Keywords

Online Exam, Face Recognition, Authentication, Exam Cheating

1. Introduction

Nowadays, e-learning systems have become vital components in the education and training domains. Several countries are attempting to overcome the Knowledge Divide. Through education and training, countries are able to develop the skills of their citizens, consequently bridging the Knowledge Divide within the country and with more developed ones. Success in the Knowledge Economy relies heavily on a qualified and skilled population,

How to cite this paper: Fayyoumi, A. and Zarrad, A. (2014) Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems. *Advances in Internet of Things*, **4**, 5-12.
http://dx.doi.org/10.4236/ait.2014.42002

thus effective education and training systems are required.

Simultaneously, Information and Communication Technologies (ICTs) continue to grow at a rapid pace and have changed the way people live, work, and learn. The integration of ICT tools in education and training has created new ways of delivering, accessing, and processing useful knowledge, as well as has provided support to knowledge sharing between different actors and to lifelong learning [1]. In addition, technological development and the growth of the Internet have resulted in the emergence of e-learning as an important learning approach. E-learning provides innovative methods for educating people. Moreover, the e-learning market is expanding because of its many advantages over traditional education. E-learning is also highly flexible, scalable, employs a rapid learning method, less expensive, and proven to be effective compared with traditional education. In particular, the following are the three main drivers for the increasing global importance of e-learning:

- Movement toward a knowledge-based economy;
- Paradigm shift in education delivery;
- Technological developments and Internet growth.

The development of e-learning and online assessment systems is increasing rapidly, both globally and locally, with many universities and corporations investing significant capital in e-learning programs and initiatives. This growth is also reflected in the report by Ambient Insight, which was published in 2010, indicating that the e-learning market has reached US$ 27.1 billion in 2009 and will surpass $49.6 billion by 2014 [2]. The growth of the e-learning industry requires new services to ensure reliability and effectiveness of its systems, especially during the examinations process, by addressing the issue of cheating in online examinations and identity theft.

E-learning is prospering on global and local levels. In Saudi Arabia, the government is focusing to the education sector in general and to e-learning in particular in responding to the increasing number of male and female students enrolled in educational institutions. Many universities in Saudi Arabia have already implemented e-learning systems and are offering distance learning courses and degrees. Thus, ensuring the reliability of e-learning systems, especially during examinations, is highly critical. Online examination cheating and identity theft should be considered, while the privacy of learners' data and more importantly, their images is guaranteed.

2. E-Learning Systems

The Web is easy to use, easy to update, and is available worldwide. The Web is the driver of the knowledge economy and is therefore a natural vehicle for learning [3]. Hall and Snider defined e-learning as synonymous to all computer-related applications, tools, and processes of learning and teaching [4].

E-learning offers flexible learning anytime and anywhere. The increasing speed of the Internet, the growth of the World Wide Web, and the emergence of high-speed computers contribute to the availability of e-learning 24/7 and worldwide. Moreover, e-learners can access materials at any time and place convenient for them. E-learning has other advantages for learners, teachers, and instructional developers. Learners, for example, will benefit from their interaction with other students and with their instructors, and they can study at their preferred pace. Learners can also select the material they want or be directed to the content that meets their level of knowledge, interest, and needs. Furthermore, learners become responsible for their learning. Meanwhile, teachers can develop materials using online resources, and then publish them in many different ways such as text, images, video, audio, simulations, and games. Teachers will subsequently gain satisfaction through quality student participation. Finally, developers can develop detailed and standardized courses. E-learning allows developers to design the course and use it for multiple times by using learning objects.

E-learning provides much enrichment to the many models, markets, interest groups, and different degrees of satisfaction in the educational process. E-learning technologies offer a potential for high-quality formative assessment. Online assessment provides dynamic visuals, sound, user interactivity, adaptation to individual learners, and almost real-time score reporting, thus expanding examination options beyond the limitations of traditional tests [5].

Learner assessments are undoubtedly essential in the educational process. Examination scores inform the instructor on whether a student's progress is satisfactory or not. Online assessment systems provide instructors with many advantages, such as the creation of online examinations within a short time, administration of the examination through the computer, easy monitoring of answers during the examination, fast access to examination results without spending time on evaluation and correction, and easy calculation of the trends of the examination results. In addition, online examinations benefit learners by allowing them to not be physically present at

a given location to take an examination, and the results can be made available to them immediately.

In online examinations, learners should register their names and passwords. The examination items will then be generated by the test bank according to the parameters set by the instructor. The items in online assessments are usually true/false and multiple choice questions, as well as involves reordering/rearrangement (matching, categorization, ranking, and others), completion, concept maps, and essays. Examination questions will appear on the screen, and then each learner will start answering them through his/her computer. At the end of the time limit, the examination will stop and the score will appear. The learner will then obtain the test results immediately.

3. Online Assessment Reliability

Security issues of e-learning systems have been discussed by many researchers [6]. Online examination is a challenge for e-learning security [7]. Currently, online assessments are mostly conducted at specific examination centers and require supervision mainly because, if administered in unsupervised locations, learners may acquire assistance from others to improve their examination results or have another individual take the examination for them. In such cases, instructors will become uncertain on who answered the examination questions, which conflicts the flexibility advantage of online education. Therefore, despite the expansion of the e-learning market locally and globally, a problem remains, especially with off-site examinations. Failure to verify the learners attending an examination is a major challenge in online learning environments.

Very little attention has been given in solving the problem of learners' unethical conduct. Moreover, many researchers criticized current e-learning systems for not focusing on the authentication of learners, particularly those who engage in online quizzes and examinations [8]. McGinity noted that biometrics has replaced the conventional password systems [9]. Another study highlighted the importance of detection mechanisms beyond the initial access to the e-learning system [10]. Therefore, a system must be developed to ensure that the person taking an examination is the student enrolled in the course. Yang and Verbauwhede suggested that biometrics systems provide better security than password systems [11]. Moreover, Hugl highlighted many technologies related to security that have not been used in e-learning [12]. These technologies include biometrics technologies that are increasingly becoming essential in a number of applications. Biometric authentication is the automatic recognition and identification of learners by using their physiological characteristics such as voice, hand geometry, fingerprints, and facial images. Generally, biometric authentication requires comparison of the stored data against the captured data.

No perfect biometric system that fits all needs has so far been created. All known systems have their advantages and disadvantages. A few studies had focused on improving e-learning security using biometric systems, but a limited number of them addressed the issue of continuous user authentication. In a recent study, Flior and Kowalski discussed a method for providing continuous biometric user authentication in online examinations via keystroke dynamics [13]. However, keystroke biometrics has its disadvantages, such as the major differences that can occur over time as a result of changes in typing pattern, tiredness of the hands after a period of typing, and improvement of skills.

In line with the previously mentioned concept, researchers are presently looking for the best biometric authentication method that will help validate the identification of the learner attending the examination and that will ensure that he/she is the same person as the one registered in the course without compromising his/her privacy. Face recognition systems are human-friendly because they require no contact and no additional hardware (given that most PCs and laptops come with a camera). More importantly, face recognition systems can be used for the continuous authentication of the learner during the entire examination period.

4. Prototype Development: The Proposed Solution

Face recognition technologies operate by scanning the person's face and matching it with the stored image. The face recognition biometric system is a system that records distinguished facial features and stores the template in a server. In scanning the face, the camera identifies facial features and transmits the signal to the server where the scanned features are processed for matching (See **Figure 1**). Facial recognition identifies key features from the facial image. The system detects the face and captures image(s) of facial features that do not change over time, while avoiding those that change, such as facial expressions or hair. The first step in face recognition is the detection of the face in the image. Yang and his colleagues evaluated the main methods used for face detection,

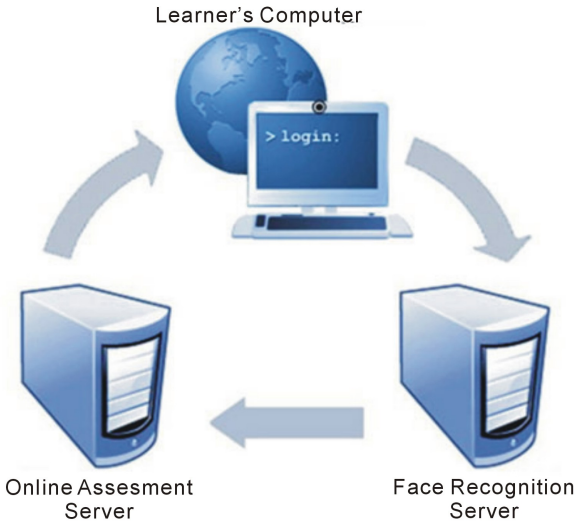

Figure 1. Proposed system solution.

namely, knowledge-based method, appearance-based approach, feature invariant method, and template-matching method. The second step is the conduct of several approaches to model and recognize the facial image, such as direct correlation, elastic graph matching, neural networks, principal component analysis (PCA), and multi-resolution analysis [14].

The proposed examination system includes the development of a test bank on a specific field. The test bank contains a variety of question items (e.g., matching, ranking, essay, categorization, multiple-choice items, and true/false questions). These questions are classified into three difficulty levels: easy, moderate, and difficult. In designing the test, the instructor can specify the number of test questions, types of questions, and the difficulty associated to each question. The system will then automatically generate a random set of questions based on the criteria specified by the instructor. Therefore, each learner will receive a different set of questions but with the same difficulty level. The instructor is also allowed to design a new question and specify its difficulty. The newly formulated questions will be stored in the database and then added into the test bank. At the end of the examination time or after completing the test, the score and time spent by each learner during the examination will appear. The database will also save other data related to the registered users or learners, including profiles and images.

The face recognition system is integrated in the online assessment tool to identify and verify the learners allowed to access the exam and to continuously validate the learner's identity until the end of the examination. Specifically, during registration in the course (when used as part of an e-learning system) or for an examination, images of learners, in addition to other required data, are captured and stored in the database. Captured images are encrypted to protect learners' privacy. During examination time, the learner's identity is verified for attendance in the examination and is monitored by comparing the captured images with the one stored in the database. **Figure 2** shows an overview of the proposed system architecture.

In addition, to address the issue of cheating in online examination systems, continuous checking is implemented, as shown in **Figure 3**. In the said figure, the learner is captured looking at the screen (left), reading (middle), and looking at an adjacent learner's PC (right). In the two-second video taken during the examination period, the images in the video are compared with each other to verify if the learner was looking somewhere else other than his/her screen. If, for all images within the two seconds, the learner was not looking at the screen and therefore was not focused in solving the examination questions, he/she will be warned by a change in background color, as shown in **Figure 4**. Failed authentication will also be made visible to the learners by the change in background color.

If the authentication failure continues for more than a few seconds, the system will stop and perform collaborative verification. In this stage, the system will ask the user to put his/her face in an appropriate position to capture a new image. If the error is repeatedly encountered, the examination will not be administered for suspected cheating.

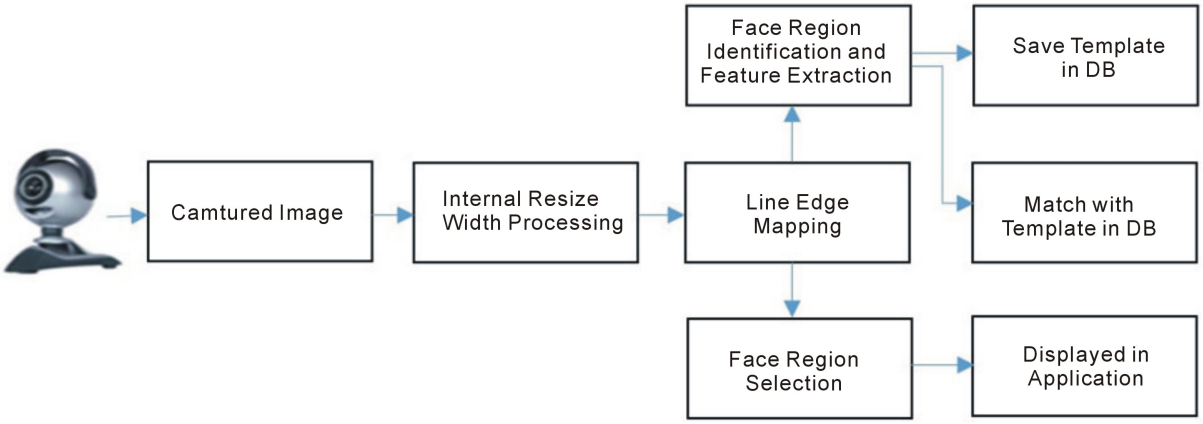

Figure 2. Face recognition system architecture.

Figure 3. Images of learner at different positions.

In practice, for learners not to be disturbed and to minimize matching failures, a two-second video of the learner is recorded and the best image in terms of facial expressions, lighting, and resolution will be selected by an application previously installed on the client's side of the system. This image is sent to the server and will be compared with the stored image.

5. Survey Results

Two surveys were conducted. The first survey targeted online instructors, and the second targeted potential users/students. The first investigation was conducted to identify the rate of image capture and the number of times the suspicious behavior is accepted without affecting learners' concentration during the examination. Moreover, e-learning instructors and experts (n = 8) were provided with the description of the proposed solution and were asked to rate the following statements using a five-point Likert scale (5—Strongly Agree to 1—Strongly Disagree): 1) the system will provide reliable results that reflect learners' achievements, 2) the system will effectively validate the learners' identity, 3) the probability of cheating during examinations will be minimized, 4) I will recommend this system to other instructors, and 5) the students will study harder. In addition, the instructors and experts were asked to specify the following information: 6) the capture rate of images for presence checks and 7) the acceptable number of times of suspicious behavior (warnings) during the examination. **Figure 5** shows the results of the survey involving e-learning instructors and experts.

Table 1 presents the suggested rate of image capture and the suggested acceptable number of warnings.

Meanwhile, learners were engaged in an online quiz in a Blackboard environment and were provided with an explanation of the proposed system. The learners (n = 32) were asked to rate the following statements: 1) the probability of cheating during exams will be minimized, 2) the system's operation is easy to understand, 3) the system will benefit the student (e.g., encourage more focus in answering the examination), and 4) the system will encourage students to study harder. **Figure 6** shows the results of this survey involving learners.

6. Conclusions

Results show that almost all e-learning instructors agree with the given statements. However, some instructors

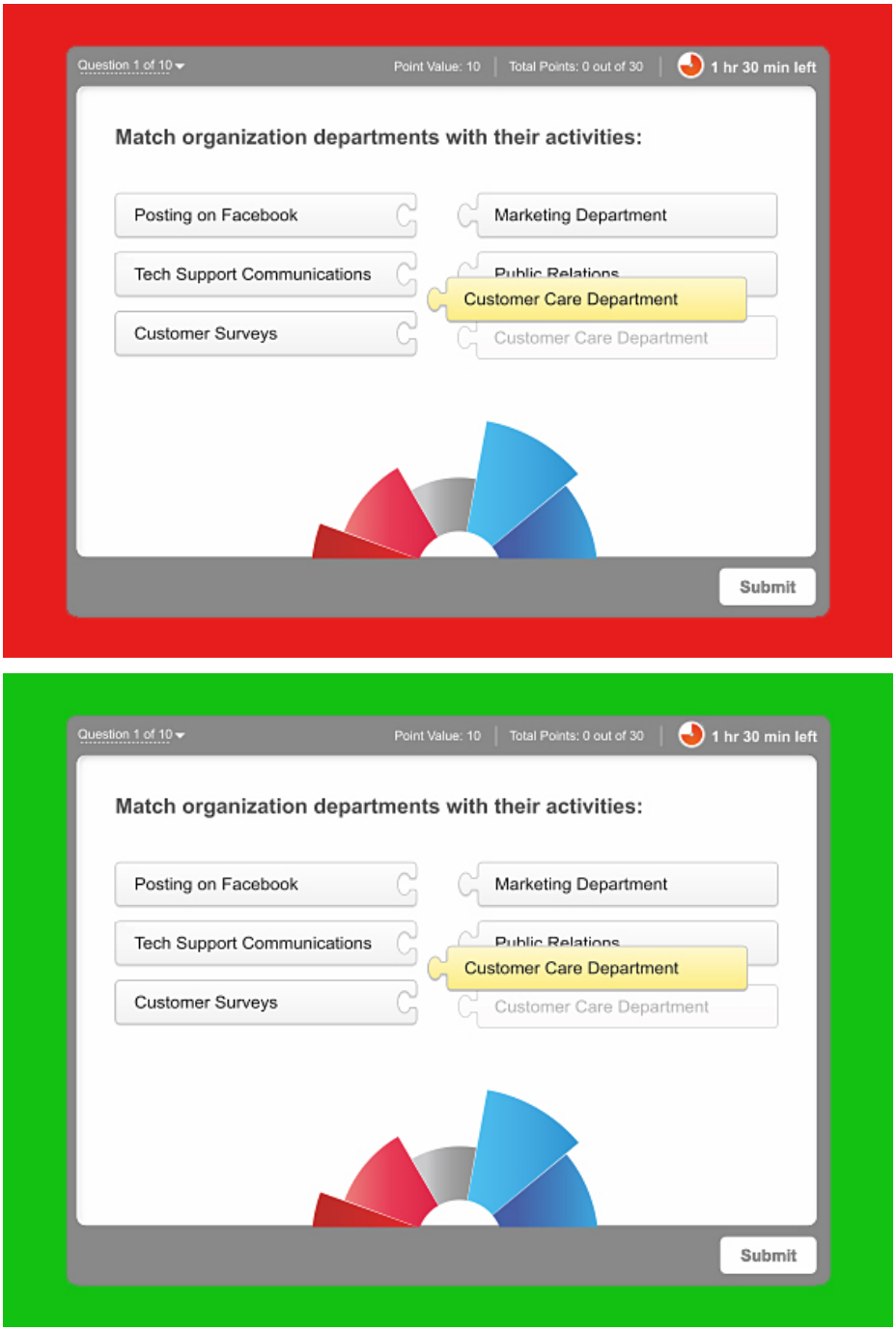

Figure 4. Red color as warning for learner with suspicious behavior.

Table 1. Suggested values from e-learning instructors/experts.

	Every 10 sec	Every 30 sec	Ever 1 min	Every 5 min	Every 10 min
The rate of images captured for presence checks	1	3	3	1	0
	1 time	2 times	3 times	4 times	5 or more
The number of times suspicious behavior is accepted during the exam	1	4	2	1	0

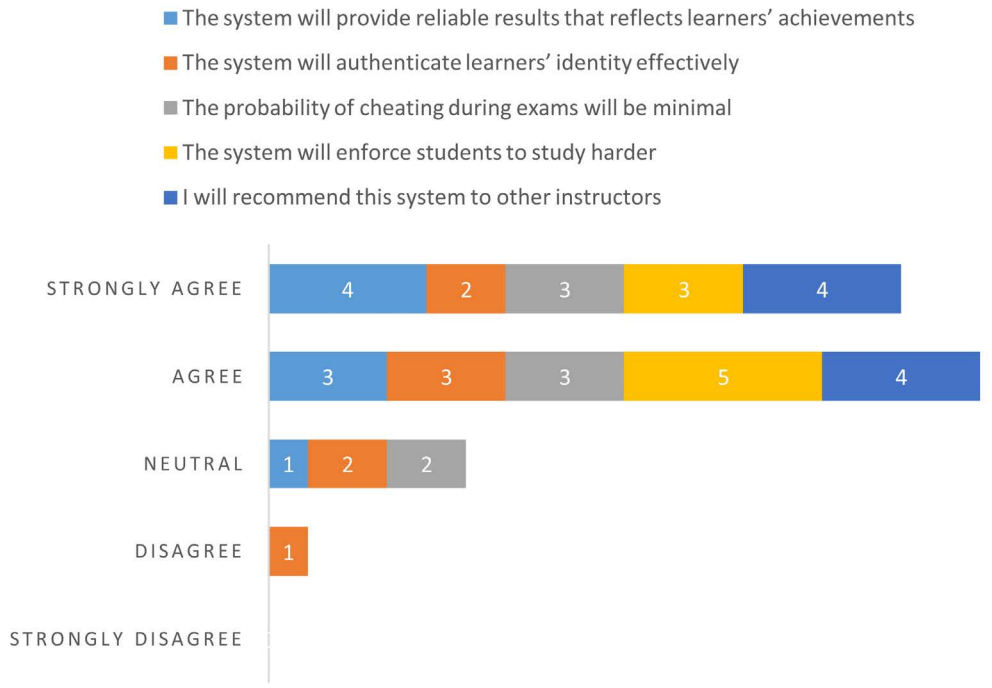

Figure 5. Results of e-learning instructors/experts survey.

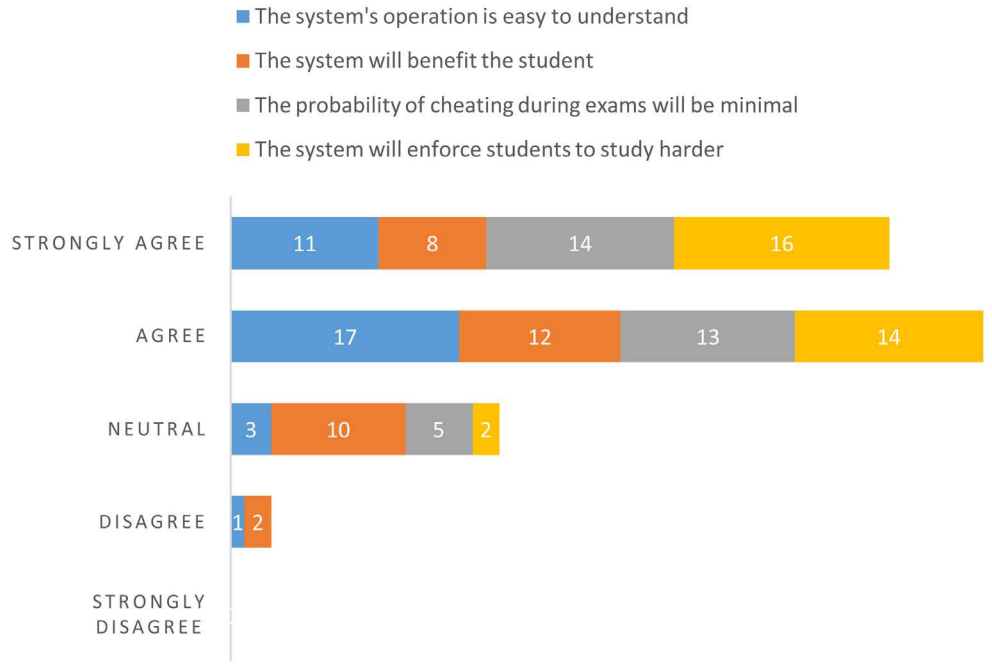

Figure 6. Results of e-learners survey.

expressed doubts regarding the effective authentication of learners and the reduced probability of cheating during examinations. Meanwhile, the students' survey showed a high percentage of neutral cases, mainly regarding the benefits that the system will provide to students.

Two questions were asked to both e-learning instructors and students. These questions were whether the probability of cheating will decrease and whether the system will encourage students to study harder. Both parties believed that cheating will be reduced with the implementation of the facial recognition system and will mo-

tivate students to study harder. The facial recognition system should consider the image capture rate of 30 seconds for presence checks. This balanced value is appropriate to lessen the load on the system and to guarantee the level of reliability. Moreover, the learner with suspicious behavior should be warned twice.

Other applications of the facial recognition system include monitoring the attendance in virtual classrooms. In measuring the attendance rate, if the result of the student's verification is positive, the system will register an attendance mark for him/her. Otherwise, he/she will be marked absent.

References

[1] Assaf, W., Elia, G., Fayyoumi, A. and Taurino, C. (2007) Prospect of e-Learning: The Case of Jordan. *e-Society* 2007 *—IADIS Multi Conference on Computer Science and Information Systems*, Lisbon, 3-8 July 2007.

[2] Ambient Insight (2010) The Worldwide Market for Self-Paced eLearning Products and Services: 2009-2014 Forecast and Analysis Report.

[3] Rosenberg, M.J. (2001) E-Learning: Strategies for Delivering Knowledge in the Digital Age. McGraw-Hill, New York.

[4] Hall, B. and Snider, A. (2000) Glossary: The Hottest Buzz Words in the Industry.

[5] Scalise, K. and Gifford, B. (2006). Computer-Based Assessment in E-Learning: A Framework for Constructing "Intermediate Constraint" Questions and Tasks for Technology Platforms. *Journal of Technology, Learning, and Assessment*, **4**.

[6] Levy, Y. and Ramim, M. (2007) A Theoretical Approach for Biometrics Authentication of e-Exams. Nova Southeastern University, 93-101.

[7] Huszti, A. and Petho, A. (2008) A Secure Electronic Exam System. *Informatikafelsőoktatásban*, 1-7.

[8] Huang, W., Yen, D. C., Lin, Z.X. and Huang, J.H. (2004) How to Compete in a Global Education Market Effectively: A Conceptual Framework for Designing a Next Generation eEducation System. *Journal of Global Information Management*, **12**, 84-107. http://dx.doi.org/10.4018/jgim.2004040105

[9] McGinity, M. (2005) Staying Connected: Let Your Fingers Do the Talking. *Communications of the ACM*, **48**, 21-23. http://dx.doi.org/10.1145/1039539.1039558

[10] Pillsbury, C. (2004) Reflections on Academic Misconduct: An Investigating Officer's Experiences and Ethics Supplements. *Journal of American Academy of Business*, **5**, 446-454.

[11] Yang, S. and Verbauwhede, I. (2003). A Secure Fingerprint Matching Technique. *Proceedings of the* 2003 *ACM SIGMM workshop on Biometrics Methods and Applications*, California, 89-94. http://dx.doi.org/10.1145/982507.982524

[12] Hugl, U. (2005) Tech-Developments and Possible Influences on Learning Processes and Functioning in the Future. *Journal of American Academy of Business*, **6**, 250-256.

[13] Flior, E. and Kowalski, K. (2010) Continuous Biometric User Authentication in Online Examinations. *Seventh International Conference on Information Technology IEEE Computer Society*, Las Vegas, 12-14 April 2010, 488-492.

[14] Yang, M., Kriegman, D. and Ahuja, N. (2002) Detecting Faces in Images: A Survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **24**, 34-58.