Journal of Al-Azhar University Engineering Sector

Vol. 18, No. 68, January 2023, 129 - 151 6, Jan

A SYSTEMATIC SURVEY ON EXAMINEES IDENTITY AUTHENTICATION IN ONLINE DISTANT EXAMS

Gehan Saleh [1]*, Gamal Tharwat [2], Shehab Gamalel-Din [3]

Systems and Computers Department, University of Al-Azhar, Faculty of Engineering, Cairo, Egypt

Correspondence: gehan.khlefa@gmail.com

Received: 22 June 2022 Accepted: 17 Oct. 2022

Abstract

The COVID-19 pandemic has changed the lifestyle in global education systems in favor of more reliance on e-learning, which is believed to be a change that will continue. Exams are no exception as they are also moving towards online remote exams where examinees can take their exams at their remote locations. However, it is worth noting that it is still difficult to ensure that the full discipline of the exam session is administered remotely, as is the case for traditional exams that are conducted in the classroom and in the presence of proctors. However, there are many attempts at the commercial and research levels to overcome many of the challenges facing this problem from different angles.

Therefore, this survey article attempts to review some of those attempts at both the solutions and technology levels. The article also made some comparisons and evaluations of the techniques and algorithms reviewed as an attempt to assess their weaknesses and strengths in counteracting persistent attempts to circumvent the discipline of the exam system.

Hence, this article aims to pave the way for system designers who wish to implement remote exam session management systems by reviewing both commercially available and under-researched technologies. It also aims to introduce researchers to the findings of scientific research so far, while shedding light on open gaps and problems that have not yet been researched.

KEYWORDS: **Online exams, Distant exams, Exam auto proctoring, Continuous Authentication, Authentication spoofing.**

مسح منهجي حول المصادقة على هوية الممتحن في جلسات الامتحانات عن بعد عبر الإنترنت

جيهان صالح، جمال ثروت، وشهاب جمال الدين

قسم هندسة النظم والحاسبات، كلية الهندسة، جامعة الازهر، القاهرة، مصر

البريد الإليكتروني: gehan.khlefa@gmail.com

الملخص العربي:

غيّرت جائحة كورونا (COVID-19) نمط الحياة في أنظمة التعليم العالمية لصالح المزيد من الاعتماد على التعلم الإلكتروني، والذي يُعتقد أنه تغيير سيستمر. الامتحانات ليست استثناء حيث إنها تتجه أيضًا نحو الاختبارات عن بعد عبر الإنترنت حيث يمكن للممتحنين إجراء امتحاناتهم في مواقعهم البعيدة. ولكن يجدر ذكر انه لا يزال من الصعب ضمان إدارة الانضباط الكامل لجلسة الامتحان عن بعد كما هو الحال بالنسبة للامتحانات التقليدية التي تتم في الفصول وبحضور المراقبين. إلا انه يوجد العديد من المحاولات على المستويين التجاري والبحثي للتغلب على الكثير من التحديات التي تواجه هذه المشكلة من زوايا متفرقة. لذلك، تحاول مقالة الاستطلاع هذه مراجعة

بعض تلك المحاولات على مستويي الحلول والتقنيات. وقد قام المقال أيضًا بإجراء بعض المقارنات والتقييمات للتقنيات والخوارزميات التي تمت مراجعتها كمحاولة لتقييم نقاط ضعفها وقوتها في التصدي للمحاولات المستمرة للتحايل على انضباط نظام الامتحان.
ومن ثم فان هذه المقالة تهدف إلى تمهيد الطريق لمصممي الأنظمة الذين يرغبون في تنفيذ أنظمة إدارة جلسات الامتحان عن بُعد وذلك من خلال مراجعة التقنيات المتاحة تجاريًا والأخرى التي لا مازالت قيد البحث. كما يهدف إلى تعريف الباحثين بما توصل إليه البحث العلمي حتى الآن مع إلقاء الضوء على الفجوات المفتوحة والمشاكل التي لم يتم بحثها بعد.

الكلمات المفتاحية: الامتحانات عبر الإنترنت، الامتحانات عن بعد، المراقبة التلقائية للاختبارات، المصادقة المستمرة، انتحال المصادقة.

1. INTRODUCTION

COVID-19 pandemic has changed people's lifestyles globally, with most activities being forced to move online, including education. E-Learning took its position quickly in the educational system proving its effectiveness; however, the fair remote assessment of students remains a challenging problem, especially for certification and formal education systems. Standard exams used to have expensive but robust settings to prevent cheating of all types. As an example, exam halls are arranged in such a way to guarantee appropriate spacing between students and human proctors check students' identities (identity authentication) and continuously monitor the exam hall to prevent cheating. As the pandemic made it challenging to arrange such physical exams for all students, exams have been in dire need of being conducted online. This article reviews the different approaches, researches, and commercial solutions used to maintain the discipline and integrity of online distant exams.

Distant online exams take the management of the exam sessions onto several far new dimensions that are completely different from those of in-class sessions. For instance, along the dimension of identity authentication, the examinee identity does not change all over the exam session with the attendance of a proctor, which is not guaranteed in unattended remote sessions; a new person can later easily replace the originally authenticated person at exam enrollment time or at least can sit beside to help. In addition, there are several cheating methods that are newly innovated during the exam session, while several other evolutions to the traditional in-class methods to make advantage of the nature of the online setups.

The focus of this article is on the first dimension of the exam session management, namely authentication, while the second dimension, namely proctoring against cheating, will be handled in another article to follow immediately.

This review article aims to give both researchers and system integrators a broad map of the problems and challenges involved and the suggested solutions. It highlights a variety of suitable technologies that fit the implementation. Comparisons and evaluations were also presented to spot the pros and cons of each technology.

The criteria that is followed in selecting the reviewed articles is summarized as follows:

- Recent articles within the last five years, with very exceptional historical cases.
- Articles published in high-impact factors journals and international conferences.
- When several articles handle the same established technology, the oldest are selected and/or those having a new novel approach.

Section 2 of this article presents the three-phased students identity authentication model that represents the structure of this article's presentation, i.e., this article reviews the different solutions and techniques categorized as per this three-phased model of D-exam identity authentication. Whereas Section 3, Section 4, and Section 5 review the different technologies and techniques that are used by the researchers and/or the system integrators for each of the three phases of the mode.

2. The Review Strategy followed in this Survey

We classify exam setups into three types: traditional, online, and distant exams (D-exams). As it is well known, traditional exam setups mandate the setup of exam halls, where both the students and the human proctors coexist. The human proctor is responsible for authenticating students before the exam begins, and to detect any cheating attempts during the exam session. Online exam setups are like those of the traditional setups except for the use of technology, e.g., replacing paper & pencil with computing devices (e.g., laptops or tablets). The Human proctor can either perform his role like in the traditional setup or use surveillance cameras.

On the other hand, D-exams assume students are placed freely anywhere, hence it is totally impossible to employ human proctors. D-exams raise a new set of cheating-prevention challenges. Table 1 sheds lights on some of these challenges.

Generally, D-exam session management operates in two phases, namely authentication and proctoring. This article, however, focuses only on the authentication in D-exams, while proctoring will be discussed later in a separate article.

The model that was followed in our survey process follows.

2.1. Authentication

Authentication, in general, is the process of verifying a user`s identity to ensure they are those who claim to be [1].

TABLE 1. New Cheating-Prevention Challenges raised by D-exams.

	Type of Cheating	Classical setup	Online setup	D-exam setup
1	Looking at another student's answer sheet.	✔		
2	Answers are communicated through sign language or a code.	✔	✔	
3	Writing on desks.	✔	✔	✔
4	Using Prewritten cheating sheets hidden in books or under files beneath the desk.	✔	✔	✔
5	Faculty rules allow students to go to the bathroom, allowing students to review notes hidden in the trashcan in the bathroom.	✔	✔	✔
6	Using electronic devices (e.g., cell phones) to communicate an answer by text messaging.	✔	✔	✔
7	Using any text-based memory calculator to keep track of all equations, notes, theorems, proofs, and so on.	✔	✔	✔
8	Listening to an iPod, Earphone cables can be concealed underneath long hair.	✔	✔	✔
9	More than one face per session detects during the exam.			✔
10	Someone views an exam from an open door or window using powerful binoculars, providing answers.			✔
11	Two students took the exam side by side in the same house, assisting each other.			✔
12	Leave the camera’s frame.			✔
13	Turn left or right more than time.	✔	✔	✔
14	Request verbal assistance from another person in the same room or over the phone.			✔
15	Having family or friends stationed in the same room but away from the webcam or behind the screen. They write the answers on a placard.			✔
16	Students frequently copy-paste correct answers from documents or notepads kept ready on a separate window before the test.		✔	✔
17	Use auto coding software in online programming tests.		✔	✔
18	Browse the internet, visit unauthorized websites during the test, copy the questions and paste them into the URL, and find the best solution.		✔	✔
19	Stop the camera for a look at a book or other and then run again			✔
20	Take a screenshot of the exam to send it to another student.		✔	✔
21	Copy and paste the exam to a word processing program for another student.		✔	✔
22	Print the quiz or exam for another student.			✔
23	Use external hard drives, USBs, Micro SDs, and other smart devices that are easy to conceal and difficult to detect.			✔
24	Using screen sharing, use multiple monitors with friends to simultaneously access the exam questions and provide answers on a different screen.			✔
25	The student has a net-connected tablet/laptop next to the actual system's monitor.			✔
26	Looking into the computer monitor, which is placed slightly away from the user.			✔
27	Using the keyboard, mouse, or laptop mouse pad by somebody else.			✔
28	Fixing the camera and the eye tracker in front of the exam taker and moving the computer to another individual to give unauthorized help.			✔
29	Students were entering the domain from various IP addresses and taking the exam for their classmates.			✔
30	Taking an exam for another student.	✔	✔	✔

Human proctors do the job in traditional and online exams, while automated proctors are the genuine substitute in D-exams. In D-exam systems, this process begins early enough at the time of student registration to the system, and continues till the end of the exam session, since the student should be authenticated before being enrolled to a D-exam and will go through a non-intervening complex continuous authentication process all over the exam session [2, 3].

Our followed authentication model operates in three phases as shown in **Fig.1.** The continuous authentication phase is mainly added to the model to guarantee that the examinee is unchanged all over the exam session; this is to substitute for the absence of a human proctor. In the following sections, we will go over the authentication requirements for each phase.

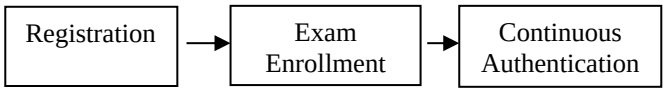

Fig. 1: A model for exam authentication

2.2. Exam Registration (phase 1)

This phase occurs at the time of the student's registration into the examination system. During this process, student data is collected and saved in a database for later use. Among the collected data are the necessary biometrics needed by the authentication mechanism, e.g., facial features, fingerprints, keystroke dynamics, palm prints, etc. As discussed in Section III, most of these biometric techniques are considered in this article's survey.

2.3. Exam Enrollment (phase 2)

This is the stage before allowing students to enroll in the exam session. There are two types of authentications here: static authentication and continuous authentication. Static authentication refers to the authentication that takes place directly before enrollment into the exam. Meanwhile, continuous authentication refers to the authentication that continues all over the exam session to make sure that the examinee is not replaced.

Noteworthy, some biometrics especially for the face features may change from the time of registration. Examples of such changes are beards, cosmetics such as eye shadow, lipstick, and liquid foundation on the face, which changes the facials, and contact lenses that change the color of the eyes. It is also possible to wear a veil or remove it to change the shape of the face of women. Therefore, the exam-session enrollment phase should update the stored biometrics to reflect the timely status. In addition, it should capture a few temporal information that should not change during the short-period session, such as the ornaments, dress color, beard, scarfs, and mustache, which will aid in the continuous authentication process [4].

The system should track the face and the body separately to extract registered modalities for matching or storing histograms of both the face and body [5, 6]. For instance, the system registers face biometric data every time a user logs in to mitigate the illumination difference between registration and identification time during login [5]. A set of frontal-view images of the test taker is captured; a 160-dim HSV color histogram of the clothing is also extracted to be used for continuous authentication [7].
Furthermore, spoofing is another common threat to biometric authentication systems [8]. It may occur at the enrollment stage when a person tries to masquerade as another student, e.g., by using face photographs, and thereby gains legitimate access to the exam session. Photo attacks, one of the cheapest and easiest spoofing approaches, and photographic masks are examples of such attacks [9]. Photographic Masks are made by getting a high-resolution photograph of a student's face, cutting out the eyes and the mouth, and looking through it like a mask. Another used spoofing approach is artificial fingers that are used in systems that authenticate based on fingerprints [10].

2.4. Continuous Authentication (phase 3)

To understand the role of the exam enrollment stage and its procedures, we need to discuss the meaning and requirements of the continuous authentication stage (stage 3) since stage 2 is made to serve stage 3.

As a one-time static authentication, static authentication is not sufficient in D-exams as there is no guarantee that the examinee will not be replaced during the exam session. After entering the exam, a continuous authentication for the student is necessary to verify the examinee throughout the session. Continuous authentication is, therefore, sometimes called dynamic authentication as opposed to static authentication.
In general, researchers define continuous authentication as providing continuous verification of identity when the user uses the system or accesses protected resources [4,6,11,12,13,14,15,16,17,18].

However, researchers define continuous authentication as providing an extra security measure next to the initial authentication. It applies after starting an exam session and ongoing checks during the exam period that the current student is the same as the one who started the exam [1,7,19, 20, 21, 22, 23, 24].

3. The Registration Phase.

Three types of biometric data can be collected in the online exam registration process: physiological biometric data such as (face, fingerprint, iris, retina, palm-print), behavioral biometric data (keystroke dynamics, mouse dynamics, voice), and multi-modal biometric data (combining information from two or more biometrics).

3.1. Face features

Some researchers enroll facial feature points such as the eyes, brows, nose, mouth, chin, and ears. Some features do not change over time, but some change such as facial expressions or hair [5, 6,19, 20]. These features must be avoided during authentication process. Other researchers are storing various poses of the user to use in cheating detection during the exam. Storing various poses like turning head down, turning head to the right, turning head to left, stretching the arms, quitting, and leaning back in the chair because the user may make movements during exam [4,15]. Take photos of students` faces and record them in a database for future comparison in the authentication process as in [7,24,25,26,27,28,29,30,31,32,33,34, C1, C2, C3].

3.2. Fingerprint

Nobody has the same fingerprint as Even twins with identical D.N.A have different fingerprints; some research records users` fingerprints to be later used for authentication purposes [10,35, 36, 37, 38, 39, 40,41, 42, 43, 44].

3.3. Iris

Two irises are unalike in their mathematical details; each eye's iris is unique, even between identical twins or between the left and right eyes. Shdaifat, et.al. [45] extracted the iris pattern from the student eye image to generate and store the code used to identify students in online exams. Mock, et.al. [46] extracted iris-like x-y coordinates, pupil radius, shape, and size, intensity values, pupil ellipse orientation, and ratio of average intensity of two to be used later in mobile exam authentication. The authors scanned a student's iris and saved its pattern in a database for future matching during login [47,48, 49].

3.4. Retina

The retina is a secure and reliable source of person recognition as it lies behind the eye and is unforgivable. Mushtaq, Rashi [50] extracted the feature vector of all the captured retinal images for persons and stored them in a database. Ghada, Moustafa and Essam [51] captured snapshots of the eye using an ordinary camera. They Converted this image into the base64, which will return the code of the image in the form of a string. Retrieved the retina from this converted image and stored it in the database for future student verification.

3.5. Palm print

Ahmed and Traore extracted the desired features from the region of interest of a student`s palm print images and stored them in a database for the verification process [52].

3.6. Keystroke Dynamics

Keystroke biometric systems measure typing characteristics are believed to be unique to an individual and difficult to duplicate [53]. There are two basic types of keystroke dynamics: fixed-text and free-text. The fixed-text keystroke dynamics approach is based on a predefined text that the system has already trained on and that the user must give at the login time. On the other hand, the free-text keystroke approach is easier for the user because it does not need memorization. After all, the text used for enrollment and login does not have to be the same [54,55,56]. Free-text keystroke dynamics also improve security by providing ongoing and non-intrusive authentication [54,56,57]. To create a template of the users` keystroke dynamics for future authentication, we use some pre-determined text (fixed text) such as username and password [58,59,60], some digits [61] and fixed string as in [59,62,63] or some random text (free text) as in [6,18,65,66,67,68,69,70,146]. The user's features are captured, and a reference template is created. This reference is used to authenticate the user at the time of login.

3.7. Mouse Dynamics

Mouse dynamics refers to a person's behavior with a computer-based pointing device, such as a mouse or a touchpad. The mouse biometrics traits for each user extract and stored in a database to be used in the verification process [71,72,73,74].

3.8. Voice

A voice biometric is a numerical representation of a person's voice tone, pattern, and rhythm [75]. A voice biometric, also known as a "voiceprint," is as unique as a fingerprint or palm print. As a result, speech recognition can authenticate students in online exams. The proposed approach creates speech templates by registering the user for the first time, and it also authenticates the user by recognizing the voice template made [76,77].

3.9. Multi-factors

Many researchers have indicated that utilizing a single biometric element is insufficient for a safe authentication technique [78, 79] compared to employing several authentication methods [80, 81]. For example, Fenu, Marras and Boratto building a template containing features of the following five modalities, face images, voice data, touch data, mouse data, and keystroke dynamics [82]. The student's face will be captured and stored in addition to the student's dynamic keystrokes [14,83,84]. Alternatively, Shen, et.al. building the template of the students` face images, skin color, and keystrokes is dynamic [17]. Schiavone, et.al. registered images of a face, fingerprint, and keystroke dynamic [22], while Jagadamba, et.al. captured the student`s typing pattern and his face image [85]. Bal, Acharya used the examiner's fingerprint image as a cover image to hide the Personal Authentication Number (P.A. N) [41]. The authors in [86,87] Recorded the facial image and an image of the fingerprint. Rudrapal, et.al. asking the examine to apply his fingerprint using a fingerprint mouse scanner, a still photo taken with a high-resolution camera, and some challenging questions asked to extract the examinee's keystroke dynamics feature [88]. Ullah, et.al. created a multi-factor knowledge-based authentication scheme that employs a login-identifier, password, and challenge questions [89]. Hayes, Ringwood suggested storing a combination of username/password and features of student's palm-print [90]. Alshehri, Coenen and Bollegala Stored pin code and image for both smart card and face of user [24]. Recording a person's fingerprint and iris as in [91, 92]. Morales, et.al. Stored keyboard and mouse features [93]. Kumar, et.al.[94] used hand images of every user to automatically extract the palm print and hand geometry features for personal authentication The results obtained are significant because the two biometric traits are derived from the same image, as opposed to other bimodal biometric systems that require two different sensors/images. In [95,96], the authors described a study that built a combination of a student's Keystroke and stylometry template. Bal, Acharya suggested using a mix of steganography and students` fingerprints [41]. This template was

previously used in other domains, such as online voting [97] and online buying [98]. While Bimpe, Ayoola stored face images, fingerprints, and challenge questions to build a template for student's authentication in E-learning [99]. However, Canales, et.al.[100] stored face images, voice, and challenge questions. Parkavi, Babu, and Kumar [101] stored faces and gestures of users extracted from videos. Jorgensen, Yu [102] stored a mix of fingerprint and mouse dynamics. Durcheva, Rozeva Stored facial images and voices of students [103]. Teh, et.al.[104] stored face images, voice, and Keystroke dynamics. Rudrapal, et.al. [88] stored students' passwords, tokens, fingerprints, and keystroke dynamics. Almalki, Chatterjee and Roy [105] used data gathered from a mouse and student`s eyes to build a student template. Hossain, et.al. [106] stored different student events, such as mouse dynamics, clicks, mouse wheel, and keyboard use. In [C5], the template is based on a student's face, ID, and knuckle scan. They were storing the only image for the student and his ID as in [C4]. The system in [C6, C8] stores the test taker's institution-approved ID card (contains face image + student ID) in a database, while in [C7], the authors storing student ID, challenge questions, Keystroke. Instead of student ID in [C7], the authors in [C9] store students' faces.

4. Exam Enrollment Authentication (Static Authentication)

All exams begin by verifying students' identities, a process known as authentication. User authentication's primary goal is to determine whether or not the person interacting with the online examination system is a legitimate user. Several studies have been conducted proposing user authentication in an online examination system [107, 108,109]. Authentication methods are divided into traditional authentication methods and biometric authentication methods (advanced authentication methods). Traditional authentication is either a knowledge-based technique or possession-based. The knowledge-based, frequently used username and password, while possession-based authentication uses what students have like cards, keys, Badges, etc. Using traditional authentication methods username and password only in online exams increases attacks and security problems. So, all the previous advanced authentication methods used in the registration process will identify a person's identity static authentication.

4.1. Spoofing Detection

Spoofing attack is still a threat for biometric authentication systems [8]. In biometrics, liveness detection refers to a system's capacity to determine if a fingerprint or face (or other biometric) is genuine (taken from a live individual present at the time of capture) or not (from a spoof artifact or lifeless body part). So, we need to find a solution to spoofing problems during authenticating students before the online exam.

4.2. Liveness detection of fingerprint

In the fields of fingerprint recognition, liveness detection, which uses the recognition of human physiological activity as an aliveness indication to resist spoofing attacks, is becoming increasingly popular [8, 110, 111, 112]. Spoofing is when someone uses a falsified biometric device (such as a plastic finger) to access a secure system. This prosthetic finger behaves exactly like the original natural finger when it comes to recognizing the user. This difficulty can be solved by using liveness detection. Intruders frequently use prosthetic fingers to try to achieve authentication. Different approaches for detecting Liveness can divide into two categories: Ways that require additional hardware; use temperature, pulse, blood pressure, electric resistance, and so on; and methods that use information already in the system; use skin deformation, pores, perspiration, and so on. Before matching the captured fingerprint with the stored one in E-exams, an intelligent agent will perform live detection tests. Alotaibi ensured that no fake fingers are being used to impersonate another student based on perspiration from the fingers, which is considered a sign of life and is not present in the case of fake fingers [37]. Derakhshani, et.al. developed a new

methodology for detecting vitality using sensitive scanners and fingerprint examination [113]. This method is based on detecting the sweating pattern from two successive fingerprints taken for 5 seconds. A back-propagation neural network trained on example fingerprints is used to classify the data. It calculates the perspiration pattern and ultimately concludes the fingerprint's liveliness. Ackley, Hinton and Sejnowski [114] developed an approach for detecting fraudulent fingerprints in authentication-based systems, in which they adopt several features called deep features retrieved from images, such as the Deep Boltzmann Machine (DBM) proposed by Pan,et.al. [115]. DMB's key advantage is the layered design aids for the investigation of complicated correlations between characteristics and allows for deep learning of very detailed data characteristics. The results of the experiment show that the Deep Learning model is resistant to spoof forgeries such as wood glue, gelatin, and Play-Doh.

Putte, Keuning said that The epidermis has a temperature of around 26-30 C. When a thin silicone artificial fingerprint is used, the temperature transfer to the sensor is reduced by a maximum of 2 C. Without a doubt, keeping the temperature of the artificial fingerprint within the sensor's working tolerances will not be difficult. Outdoor sensors often have a larger working margin, providing the intruder with even better conditions [116]. Chugh, Cao and Jain proposed a new method that uses the wavelet transform on the ridge signal taken from fingerprint images to detect Liveness [117]. The results reveal that the capacitive DC and optical scanners can detect vitality by utilizing a single fingerprint and a perspiration pattern exclusive to live fingers. This liveness detection technology is entirely software-based, and it can defend fingerprint scanners from spoof attacks. Pan, et.al. [118] used fingerprint domain knowledge to train MobileNet-v1 CNN models by extracting local patches centered and aligned using minutiae in the input fingerprint image. The local patch-based technique provides valuable clues for distinguishing between fake and live fingerprints.

4.3. Liveness detection of Face

The most popular method of spoofing the face recognition system is to utilize a valid user's facial photograph, which is easily available to the public, for example, obtained off the web and taken unintentionally by the camera. One of the simplest and cheapest spoofing methods is photo assault. There are three sorts of methodologies for spoofing detection: techniques based on Liveness, methods based on Texture, and methods based on 3D geometry.

4.3.1. Methods based on Liveness

Asthana, et.al. said that any dynamic physiological indicator of life, such as eye blinking, lip movement, facial expression changes, and pulse beat, can solve the spoofing problem. Anti-spoofing protection in facial recognition systems relies on detecting eye blinks [119]. The system works only using a web camera, and no other sensors like depth sensors or infrared light beam are used. With Blink Detection, recognizing a printed photo is much easier, in which they successfully identify blinks on a live camera feed [33]. So, face recognition is triggered only after a successful blink detection occurs. Researchers use eye blinking in [119, 120] to discriminate between a face and a facial snapshot. Blinking the eyes is a physiological process that occurs 15 to 30 times each minute [121]. As a result, GCD cameras with a frame rate of at least 15 frames per second can catch two or more frames each blink [119]. Soukupov and Cech [122] suggested a real-time system for detecting eye blinks in video sequences captured with a conventional camera. The proposed method can tell the difference between open and closed eyes. It calculates landmark positions [123, 124] and calculates the eye aspect ratio (EAR), which describes the eye-opening size in each frame. Because there are no eye movements in the photographs, Alshehri, Coenen and Bollegala used Eye Tracker to detect a genuine exam taker in front of the camera [125]. Because there is no depth or head movement information in this 2D image, it can also detect using a photograph as a mask with eye holes to overcome the eye tracker protection. Some studies have used the

lips of a person's Face to detect spoofing. Uliyan, Sadeghi and Jalab [126] proposed a method for detecting photo attacks by scanning the lips of the presented Face while the user is required to pronounce a randomly selected sequence of numerals. Saied, Elshenawy and Ezz [127] proposed a method that may be used with any authentication system with a camera, such as a mobile phone, tablet, laptop, access control device, etc. The suggested method takes an authorized person's image and locates the eye region, using CNN to classify open and closed eyes, before capturing face dynamics using a challenge-response authentication mechanism that uses eye blinking. The challenge will be launched by authenticated devices, which will ask the user to blink their left or right eyes in a specified order, and the user must then follow this order to be authenticated. Each time the user logs in, the authenticated device will issue a new challenge, protecting the system from spoofing facial video. Tan, et.al. [128] suggested that a robust feature representation that incorporates deep texture characteristics and eye-blink cues to defend against presentation attacks on pictures and replays (spoofing problem). Both aligned face photos and full frames are used to learn texture properties in a generic-to-specific manner, resulting in fantastic complementarity. An eye-blink detection technique based on picture difference is developed to aid in texture cues with low computing cost.

4.3.2. Methods based on Texture

In these methods, the textural attributes of the object supplied to the system are investigated as genuine Face or fake. Wang, et.al. [129] used physical models to model the respective reflectivity of genuine faces and face-printed photos. The idea behind this method is that a face-painted photo image is more distorted than a real face image because it has been captured twice and printed once in the interim, whereas real faces are only captured once [130]. Brocardo, et.al. [131] estimated the noise of a specific spoof face image in order to detect photo attacks. The spoof picture was calculated as the sum of the original image and picture-dependent noise (e.g., blurring, reflection) introduced during the spoof picture generation process because the noise in an actual image was supposed to be zero.

4.3.3. Methods based on 3D geometric

This method uses 3D geometric features to distinguish between a genuine face with a 3D structure and a faked face with a 2D structure. The most commonly used 3D geometric cues are the 3D shape reconstructed from the 2D image acquired by the RGB camera and the face depth map (the distance between the camera and each pixel in the facial region). Saragih, Lucey and Cohn [132] proposed a method for detecting photo attacks in which the 3D facial structure reconstructed from 2D facial landmarks [133] that was detected using various viewpoints [134]. A genuine face and a planar photo have different reconstructed 3D structures. The reconstructed 3D geometric structure from the real facial profile retains its 3D geometric structure. On the other hand, a fake photo's reconstructed structure is just a line indicating the photo's boundary, while suggesting an approach that takes advantage of the fact that the depth map of a live face has variable height values, whereas depth maps for photo attacks are constant [135,125].

5. Continuous authentication (dynamic authentication)

Throughout time exam, continuous random authentication is essential in online examinations to verify that the examinee is the correct student [37,136, 137, 138, 139]. Continuous user authentication can be divide into three categories: physiological biometrics (iris scanning, fingerprint scanning, facial recognition, hand geometry, etc.), behavioral biometrics (mouse movements, keystroke dynamics, speech recognition, etc.), and multi-modal biometrics (uses information from two or more biometrics).

5.1. Continuous authentication based on physiological biometrics

5.1.1. Face Recognition

Face recognition is desirable because the system should not require active participation from users to authenticate them. Face recognition continuously collects images for the student`s Face from the camera at random time intervals and compares them to the base image stored in the database for ensuring that the learner who started the exam is the same one who continued until the end [1, 15, 20, 24,31,140,141]. The system continuously authenticates the user using the soft Face and clothing enrollment templates registered in the enrollment process [4, 5, 6, 7]. Aisyah, Bandung and Subekti proposed a system that tracks the Face and the body separately based on the histograms registered in the initial login process as his frontal facial view is not available to the webcam, the template registered at the beginning and the second frame of the video are subjected to the matching process [21]. Authenticate students who use Android mobile devices in online exams continuously by taking pictures during an exam at random intervals and match them with the base image. When taking the exam, the proctor will be constantly monitoring the student by video for continuous authentication, and the entire session will be recorded [C4, C5].

5.1.2. Fingerprint

Fingerprints are among the most reliable human characteristics that can be used for student authentication in online exams due to their distinctiveness and persistence. Levy, Ramin proposed solution that ask the student randomly to apply his fingerprint during the exam for authentication. Assumed that the student is focused during the exam and is not disturbed by anything, this solution is inappropriate during electronic exams because it causes inconvenience to the student during the exam period [142]. Alotaibi proposed an intelligent agent that will extract the fingerprint from the fingerprint mouse and keyboard (which can scan the user's fingerprint while working) every second without extra effort to get his fingerprint scanned [37]. This solution will be appropriate in electronic exams conducted in halls equipped with the keyboard and mouse mentioned in the research. It is also suitable in the case of exams that contain essay questions and multiple-choice questions, where the keyboard captures the fingerprint in the case of essay questions or by the mouse in the case of multiple-choice questions. Asha, Chellappan proposed a continuous presence verification system that can deploy reliably to ensure a high level of examination integrity. They demonstrated that it is possible to lessen and eventually eliminate the reliance on the remote proctor by capturing test-taker fingerprints at random intervals and confirming them via the national Aadhaar service [43]. Their system is made of commercially available components.

5.1.3. Iris Recognition

Shdaifat, et.al. proposed a system that automatically captures the student's image without informing him/her and applies the proposed code generation process to compare it with the stored one in a database for controlling the student's authentication during the online examination [45]. However, during the real-time picture acquisition, the user is writing on the screen, he stares at it in a specific position. As a result, the eyelid covers a majority of the iris, causing issues with feature extraction. The user interfaces are well-designed to force users to look at the top of the screen while installing the camera. Mock, et.al. suggested that capturing iris images randomly for a student during the exam session, to ensure that the same person who logged in is the same person conducting the exam on mobile by comparing iris extracted features with features in the database [46]. The proposed model provides an easy-to-use, effective, and fast authentication system that does not require additional hardware devices, but it annoys the student during the test because he/she directs to focus his/her eye within a specific area of the screen to take a picture of his eye at each interval of time. A commercial eye tracker can be used for continuous user authentication

via iris recognition in [48], because eye trackers have a relatively wide field of view, allowing continued tracking even when the user moves his/her head.

5.2. Continuous authentication based on behavioral biometrics

5.2.1. Keystroke Dynamics

Al-Saleem, Ullah said that the online learning website Coursera applies keystroke features to verify the identity of students [143]. Lu, et.al. Detecting a user's keystroke habits as they enter text can be used to continuously verify the user's identity without affecting user input. When users type free text, the proposed method authenticates them through their keystrokes; the user keystroke data is divided into a fixed-length keystroke sequence, which is converted into a keystroke vector sequence based on the time feature Keystroke [64]. A CNN-RNN model is used to learn a sequence of individual keystroke vectors in order to obtain individual keystroke features for identity authentication. A trained model easily combines with continuous authentication mechanisms. A method for reducing the dimensionality of the features a vector describing a session. Then, features vector is extracted from each input stream of keystrokes to form a model representing the user typing patterns; this can later be used for the continuous verification process. Shimshon, et.al. [144] proposed a method for providing continuous biometric user authentication in online examinations via keystroke dynamics. The system records the exam question answer and generates a signature every 50 keystrokes that is compared to the ten signatures stored in the system [136]. As a result, the problem of requiring a fixed text for authentication via keystroke dynamics can be overcome by generating multiple signatures from a single set of text and using the average cosine correlation value. Variations from one signature to the next are reduced in this manner, resulting in a more accurate correlation between the trial and recorded signatures.

Ceker, Upadhyaya proposed a new methodology for continuous authentication of users by processing the long text and extracting features for keystroke dynamics for long-term continuous authentication the key-logger uses to collect the character, key's press, and release time. This method requires the analysis of only certain digraphs efficiently without additional modalities [145]. Mushtaq, Rashi proposed a survey on the use of keystroke dynamics to continuously authenticate a user using the system, focusing on free-text Keystroke [50], described a way for continuous authentication by monitoring the user's typing behavior to detect anomalies [1]. They adopted the distance function, and we came up with a penalty and reward function. This penalty and reward function will keep track of the user's behavior over time and will decide on locking out a user or not. Discuss how keystroke dynamics can be used for a true continuous authentication system using the "Trust Model" [146]. In this model, the current user's behavior is compared to the template of the genuine user; trust in the user's genuineness is adjusted based on each single action performed by the user. If the trust falls below a predefined level, the system locks itself and requires static authentication of the user to continue working. Continuous data collection was carried out in an uncontrolled environment to simulate the users' typical computer usage behavior, with no instructions or specific tasks given to the user.

A mechanism represents typing patterns in free text for iterative Keystroke continuous authentication (KCA). The idea is to use sequences of keystroke dynamics in the form of time series, to monitor such time series, as a continuous data stream we periodically extract subsequences from these time series and authenticate the subsequences [65]. Zamfiroiu, et.al. proposed a method for Keystroke continuous authentication (KCA) using time series analysis to recognize typing patterns from free text in a manner suitable for the continuous authentication required for digital learning [67]. Simultaneously, the proposed method operates using the keystroke timing features associated with all keystrokes, not just specific n-grams. The proposed approach operates by considering typing behavior terms of Multivariate Keystroke Time Series (M-KTS) subsequences A novel feature extraction method for free-text keystroke dynamics

in continuous authentication that is based on n-graphs and extends, with N-graphs representing the latency between n consecutive events and extended-n-graphs being an improved version of the commonly used n-graphs. Instead of extracting the same features for each n-graph, they propose calculating the extended list of features on each N-gram [57].

Antal, Norbert suggested a method for verifying a student's identity in virtual tests based on statistical modeling of KD using GMMs. The system was tested in two modes: (1) intrusive mode (text-dependent) and (2) non-intrusive mode (text-independent). (In other words, the user is unaware that his/her identification being checked), because the user's identity may be constantly checked without disrupting the activity, the non-intrusive mode can be used during assessment activities. Although the model has a greater CUA, verification can be done on any text typed by the user, even those written during the examination [72]. So, Keystroke systems based on free-text keystrokes can be used in electronic exams to ensure students' identity for the exam duration because they do not cause the student any inconvenience during the exam. It is appropriate for tests with essay questions, but it cannot be used for multiple choice questions because the keyboard is not used in the answer.

5.2.2. Mouse Dynamics

Factors related to how each individual uses the mouse can be used to identify them because each person's use of the mouse while utilizing the system is different. Khanam, Ahsan used mouse movement dynamics to implement continuous behavior-metric user authentication in electronics examination. The mouse movement software runs in the background throughout the examinee's examination, comparing data from the mouse movement to data already saved in the database for ensuring that the authorized examinee is the one taking the examination [74]. The validity of employing mouse biometric as a primary or supplemental security measure for ongoing verification of an individual during an online multiple-choice examination was discussed. The results are that mouse biometrics may not be entirely reliable for authentication because the amount of data required to analyze mouse clicks and movements accurately is sometimes large. The resources required to regularly assess this information are limited. It would be incredibly difficult to tell if a user is genuine during a quiz if the person's data profile was not broad enough to reveal any patterns [147].

Mogus, Djurdjevic and Suvak Demonstrated a novel approach to developing a continuous authentication system in which the system determines the user's genuineness in every occurrence. They tested this theory using six different machine learning methods and a publicly available mouse dynamics dataset [71]. Mooad, Rasmi and Hassan Presented a continuous user authentication model based on the analysis of mouse clickstream data. Three machine-learning classifiers are used to perform verification and authentication processes. They employed 39 mouse actions, including mouse motion, point and click, and drag and drop. With reasonable accuracy, the classifiers distinguished a legitimate user from an impostor. Because they do not cause any inconvenience to the student throughout the exam, mouse dynamics-based systems can be employed in electronic exams to confirm the identity of students for the duration of the exam. It is best for tests with multiple-choice questions because they prefer to solve problems with the mouse rather than the keyboard [148].

5.2.3. Stylometry

The "statistical analysis of writing style" is defined as stylometry (also known as authorship analysis). Kaur, et.al. suggested a novel framework for carrying out CA based on stylometric analysis, which uses n-gram analysis and features merging to create new stylometric characteristics. The framework also employs a deep machine learning methodology for the first time to classify stylometric profiles. They also looked into the three key issues that any CA system faces: short authentication delays, authentication

accuracy, and forgery resistance [149]. Stewart, et.al. proposed a new framework for continuous authentication is based on stylometry analysis; their feature-set comprises existing lexical, syntactic, and application-specific features in the first place. They also used n-gram analysis to come up with 16 new features. They compute and analyze the information gain to select the best features to represent each user profile. As a result, they can reduce their feature set from 349 to 50 on average [150].

5.2.4. Typing Behavior

Mungai, Huang Suggested a novel biometric modality that allows real-time continuous user identification while typing, based on the hypothesis that each computer user has a unique and consistent habitual pattern of hand movements, independent of the text, while typing on a keyboard (TB). They create real-time computer vision algorithms to automatically extract hand movement patterns from video streams using a webcam pointing toward a keyboard. Unlike common continuous biometrics like keystroke dynamics (KD), TB provides reliable authentication with a short delay and avoids explicit key-logging [151].

5.3. Continuous authentication based on multimodal biometrics

Aside from using a single biometric trait for the continuous authentication process, several methods combine more than one biometric. There is a study on the fusion of fingerprint, face recognition, and soft biometrics. While operating a personal computer through the mouse, a fingerprint image is captured, and matching is carried out. If no match is found, authentication is done through face recognition at the specific time interval based on webcam images of the person. If the face is not recognized, the process is switched to soft biometrics, where skin and cloth color recognition is done. If the cloth color does not match, the system logs off. This process is repeated until the user shutdowns the system [11].

Wiklund, et.al. proposed a novel continuous authentication technique combining touch behavior and face recognition; The system will automatically take an image of the user during login and capture an image for each question-answer to be stored in the database. Then compare all the recorded images of the user with images already captured during the login and compare the behavior of all the captured images for user authorization during an online exam [152]. Chao, et.al. proposed an approach that continuously verifies the presence of a logged-in user in a non-intrusive and continuous way by combining three biometric modalities Keystroke, Face, and skin color. By fusing these three biometrics, the continuous authentication system combines both temporal and modality intonation holistically and can keep verifying who is using the computing system without troubling users' activities [17].

Schiavone, et.al. proposed a continuous authentication mechanism for desktop applications designed by integrating face recognition, fingerprint, and Keystroke. At the verification step, features extracted from the new traits are compared with the stored templates to generate a matching score [22]. Fenu, Marras and Boratto designed a multi-biometric system that integrates with an e-learning platform to continuously authenticate students on desktop and mobile devices. The system will be supporting the most common types of interaction, by performing a score-level fusion of different biometric responses (Face, voice, touch, mouse, and Keystroke). The global authentication response is computed by adding the matching scores from all the subsystems, weighted with their reliability measures [82].

Issa, et.al. proposed a continuous authentication service that continuously validates the test taker's identity throughout the exam using a multi-modal biometric framework, which integrates the following three biometric modalities: mouse dynamics, keystroke dynamics, and facial scans. These modalities can be collected without the active cooperation of the student. Face biometric scans can be collected using standard video cameras and collecting mouse dynamics keystroke dynamics using standard computing devices (mouse and keyboard) throughout a session without any user knowledge [12]. Sim, et.al. described a system that continuously verifies the presence of a logged-in user by combining temporal and modality information holistically rather than sequentially, allowing their system to output the probability

that the user is still present even when no observations are made [153]. The verification uses two types of observations: fingerprint and Face images. Fingerprint images captured by the SecureGenTM mouse incorporate a fingerprint scanner ergonomically, where the thumb would normally be placed. Monaco, et.al. suggested the combination of keystroke dynamics and stylometry (writing style) for verifying the identity of students in online examination environments. The system can collect raw keystroke data over the Internet as well as from a key logger on an individual machine; it focuses on free-text input where sufficient keystroke data are available. Keystroke measurements include keypress duration (dwell) times, transition (latency) times, and the identity of the keys pressed, while the stylometry system employs a set of 228 linguistic features, including 49 character-based, 13 word-based, and 166 syntax-based features [154]. Ryu, et.al. proposed a continuous multi-biometric authentication system to identify the person during an online exam using two modalities; face recognition and keystroke dynamics. Both will be verified continuously. Each modality is processed independently to generate matching scores, and the fusion method is applied at the score level to improve accuracy. During the exam session, facial image and typing behavior will be repeatedly captured at set times to ensure the continuous authentication of the user [14]. Srivastava, Sudhish proposed a multi-biometric system, which uses facial recognition and keystroke dynamics, which can both easily be captured on modern computing devices for continuous authentication [155].

Jagadamba, et.al. proposed system which is an adaptive multi-factor authentication system for e-learning applications designed to work with keystroke dynamics and face recognition authentication. The information on the typing behavior includes dwell time, the interval between the following keystrokes, and the typing error rate, flying time, etc. The Face features are the distance between two eyes, eye slant, nose shape, and distance between eye and cheek. When the user accesses the Application, his Face and Keystroke are continuously captured and compared with the stored data [85]. Rudrapal, et.al proposed continuous authentication that is done as follows, during answering the MCQ or match questions, the examinee's fingerprint is captured and compared, while in the case of answering essay questions, or complete questions, the examinee's keystroke dynamics are extracted and compared [88]. Jackn, Kevin developed an initial method for a continuous authentication system using Face, voice, and fingerprint as individual biometric modes for simulating channels with different temporal characteristics [156]. Ketab, Clarke and Dowland proposed a novel e-invigilation system design incorporated a range of behavioral and physiological biometrics, including face recognition, keystroke analysis, mouse dynamics, linguistic analysis, and iris recognition for continuous student identification in differing examination scenarios (e.g., essay writing, multiple-choice test) [157].

Liu, Jiang and Devenere proposed two models for secure e-examinations propose; the Interactive and Secure e-Examination Unit (ISEEU) is the first model, and it has two ways. One uses a webcam (ISEEU-WC), while the other uses video calls (i.e., ISEEU-VC). Smart Approach for Bimodal Biometrics Authentication in Home-exams is the name of the second model (SABBAH). Continuous Authentication uses video matching, fingerprints, and keystroke dynamics [158]. Maas, Heather and Do looked at how well a continuous user authentication and identification system for a PC performed using various analytical approaches. For the analysis, they used a novel identification methodology known as Pairwise User Coupling (PUC); this dataset is made up of data on keystrokes and mouse movements [159]. Tong, et.al. a biometric authentication based on mouse dynamic and Keystroke has been disclosed; They gathered data on mouse movement and keystrokes from 53 people using software; They developed a robust, trusted algorithm to function on a continuous authentication system. Several new mouse movement features; divided mouse events into four categories: single click, double click, move, and drag-and-drop; They compared their findings to those of other studies and discovered that their proposed methodology produces better results [160].

6. Conclusions

D-exams are of special nature that makes managing the exam session is completely different than all other exam types, namely, in-class and online exams. D-exams differ in both main management tasks, namely, examinee identity authentication and detection and prevention of cheating. This article focusses on the identity authentication for d-exams, while cheating in d-exams if left to another article that will follow shortly. This article presents an intensive survey for the authentication process that is viewed by this article as a three-staged process: registration, session enrollment, and continuous authentication during session. Solutions, techniques, and algorithms are reviewed in this survey for each of the three stages. The survey covers available commercial systems and under research ideas and contributions. This review article aims to give both researchers and system integrators a broad map of the problems and challenges involved and their suggested solutions. It highlights a variety of suitable technologies that fit the implementation. Comparisons and evaluations were also presented to spot the pros and cons of each technology.

References

[1] Bours, Patrick; Mondal, Soumik. , "Continuous Authentication with Keystroke Dynamics." , 2015 Gate to Computer Science and Research, Recent Advances in User Authentication Using Keystroke Dynamics Biometrics.doi:10.15579/gcsr.vol2.ch3.

[2] Ullah, Abrar; Xiao, Hannan; Lilley, Mariana; Barker, Trevor, "Using Challenge Questions for Student Authentication in Online Examination ", International Journal for Infonomics, Volume 5 (3/4): 631-639 – Sep 1, 2012. DOI:10.20533/IJI.1742.4712.2012.0072.

[3] A. Ullah, H. Xiao and M. Lilley, "Profile based student authentication in online examination", International Conference on Information Society (i-Society 2012), 2012, pp. 109-113.

[4] Prakash, Krishnaveni,et al "Soft Biometrics Traits for Continuous Authentication in Online Exam Using ICA Based Facial Recognition", International Journal of Network Security, Vol.20, No.3, PP.423-432, May 2018.

[5] Niinuma, Koichiro, and Anil K. Jain. "Continuous user authentication using temporal information." Proceedings of SPIE, Volume 7667 (1) – Apr 5, 2010, doi: 10.1117/12.847886

[6] Kalyani, P.S.Hanwate," Continuous User Authentication Using Soft Biometric Traits for E-Learning", International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 4, April 2014.

[7] Atoum, Yousef; Chen, Liping; Liu, Alex X.; Hsu, Stephen D. H.; Liu, Xiaoming, "Automated Online Exam Proctoring", IEEE Transactions on Multimedia, Volume 19 (7): 1609-1624 – Jul 1, 2017. doi:10.1109/tmm.2017.2656064

[8] Bigun, J., Fronthaler, H., & Kollreider, K. (n.d.)," Assuring liveness in biometric identity authentication by real-time face tracking",Proceedings of the 2004 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, 2004. CIHSPS 2004. doi:10.1109/cihsps.2004.1360218

[9] Patel, Keyurkumar; Han, Hu; Jain, Anil K," Cross-Database Face Antispoofing with Robust Feature Representation", Biometric Recognition, Lecture Notes in Computer Science: 611-619 – Jan 1, 2016. doi:10.1007/978-3-319-46654-5_67

[10] Choi, Hyunsoek; Park, Hyeyoung," A Multimodal User Authentication System Using Faces and Gestures", BioMed Research International, Volume 2015 – Jul 13, 2015. doi:10.1155/2015/343475

[11] B.Kokila, S.Pravinthraja, et al ," CONTINUOUS AUTHENTICATION SYSTEM USING MULTIPLE MODALITIES", International Journal of Pure and Applied Mathematics Volume 117 No. 15 2017, 1129-1142.

[12] Issa Traoré, Youssef,et al," Information Security Practices: Ensuring Online Exam Integrity Through Continuous Biometric Authentication",Springer Journals — Jan 3,2017,doi:10.1007/978-3-319-48947-6_6.

[13] Brocardo, Marcelo Luiz; Traore, Issa; Woungang, IsaacBiometric-Based Physical and Cybersecurity Systems: Continuous Authentication Using Writing Style", Springer Journals — Oct 25, 2018, doi:10.1007/978-3-319-98734-7_8

[14] Ryu, Riseul; Yeom, Soonja; and Kim, Soo Hyung, "Continuous multibiometric authentication for online exam with machine learning", Australasian Conference on Information Systems 2020, Wellington

[15] Asep, Hadian S. G.; Bandung, Yoanes , "A Design of Continuous User Verification for Online Exam Proctoring on M-Learning" , International Conference on Electrical Engineering and Informatics (ICEEI) – Jul 1, 2019,

doi:10.1109/iceei47359.2019.8988786

[16] Arwa Alsultan and Kevin Warwick, “Keystroke Dynamics Authentication: A Survey of Free-text Methods”, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013.

[17] Chao Shen; He Zhang; Zhenyu Yang; Xiaohong Guan, “Modeling Multimodal Biometric Modalities for Continuous User Authentication”, IEEE International Conference on Systems, Man, and Cybernetics (SMC) – Oct 1, 2016. doi:10.1109/smc.2016.7844515

[18] Pragati, Pournima, et al, " Person Authentication using Iris Recognition", International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 04 | Apr -2017

[19] Lj Arnautovski,” Face recognition technology in the exam identity authentication system - implementation concept”, 2-nd International Scientific Conference MILCON'19, Skopje, November 12th, 2019.

[20] Ayham, Anis,” Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems”, Advances in Internet of Things, Volume 04 (02): 5-12 – Jan 1, 2014, doi:10.4236/ait.2014.42002

[21] Aisyah, Siti; Bandung, Yoanes; Subekti, Luki B.,” Development of Continuous Authentication System on Android-Based Online Exam Application”, International Conference on Information Technology Systems and Innovation (ICITSI) – Oct 1, 2018. doi:10.1109/icitsi.2018.8695954

[22] Schiavone, Enrico; Ceccarelli, Andrea; Bondavalli, Andrea; Carvalho, Ariadne M.B.R,“Usability Assessment in a Multi-Biometric Continuous Authentication System”, Seventh Latin-American Symposium on Dependable Computing (LADC) – Oct 1, 2016. doi:10.1109/ladc.2016.17

[23] Ayeswarya, S.; Norman, Jasmine.,” A survey on different continuous authentication systems”, International Journal of Biometrics, Volume 11 (1): 33 – Jan 1, 2019. doi:10.1504/ijbm.2019.096574

[24] Alshehri, Abdullah; Coenen, Frans; Bollegala, Danushka.,” Iterative Keystroke Continuous Authentication: A Time Series Based Approach.”, KI - Künstliche Intelligenz, Volume 32 (4) – Jan 18, 2018. doi:10.1007/s13218-018-0526-z

[25] Penteado, Bruno Elias; Marana, Aparecido Nilceu “A Video-Based Biometric Authentication for e-Learning Web Applications”, Enterprise Information Systems, Lecture Notes in Business Information Processing : 770-779 – Jan 1, 2009, doi:10.1007/978-3-642-01347-8_64

[26] Mallik, Sharthak; Halder, Shovan; Saha, Pranay; Mukherjee, Saswati, " Proceedings of International Conference on Frontiers in Computing and Systems: Multi-factor Authentication-Based E-Exam Management System (EEMS)”, Springer Journals — Nov 24, 2020. doi:10.1007/978-981-15-7834-2_66

[27] Al-Waisy, A. S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., & Nagem, T. A. M. (2017). A multi-biometric iris recognition system based on a deep learning approach. Pattern Analysis and Applications, 21(3), 783–802. doi:10.1007/s10044-017-0656-1

[28] Sucianna Ghadati Rabiha;Hendro;Sasmoko;Noerlina;Hanry Ham.,” Image processing model based E-Learning for students authentication”, International Conference on Information Management and Technology (ICIMTech), 15-17 Nov. 2017. doi:10.1109/icimtech.2017.8273535

[29] Guillén-Gámez, Francisco D. “Biometrics and education: a review about facial authentication software for the identification and verification of students who use virtual learning platform (LMS).” (2017). Advances in Educational Technology and Psychology (2017) 1: 1-8 Clausius Scientific Press, Canada.

[30] Meshach Baba and Victor Legbo Yisa, “Novel Solution for Addressing Identity Theft and Cheating in Electronic Examinations using Mouse Dynamics”, 2015 INTERNATIONAL CONFERENCE ON CYBERSPACE GOVERNANCE - CYBERABUJA2015 NOVEMBER 4 - 7, 2015

[31] Dubey, Prakash; Patidar, Rinku; Mishra, Vikas; Norman, Jasmine; Mangayarkarasi, R, “Novel continuous authentication using biometrics”, IOP Conference Series: Materials Science and Engineering, Volume 263 (4): 6 – Nov 1, 2017. doi:10.1088/1757-899X/263/4/042041.

[32] Adetoba, B.T, Awodele, O, et al,“An Improved Authentication and Monitoring System for E-Learning Examination Using Supervised Machine Learning Algorithms", International Journal of Scientific & Engineering Research Volume 11, Issue 3, March-2020 ,ISSN 2229-5518

[33] Mondal, Soumik; Bours, Patrick,” Person Identification by Keystroke Dynamics Using Pairwise User Coupling.”, IEEE Transactions on Information Forensics and Security, Volume 12 (6): 1319-1329 – Jun 1, 2017. doi:10.1109/tifs.2017.2658539

[34] Alshbtat, Abdullah; Zanoon, Nabeel; Alfraheed, Mohammad,” A Novel Secure Fingerprint-based Authentication System for Student’s Examination System”, International Journal of Advanced Computer Science and Applications, Volume 10 (9) – Jan 1, 2019. doi:10.14569/ijacsa.2019.0100968

[35] Wei, L., Cong, Z., & Zhiwei, Y. (2010)” Fingerprint Based Identity Authentication for Online Examination System”,

Second International Workshop on Education Technology and Computer Science – Jan 1, 2010, doi:10.1109/etcs.2010.409

[36] Babatunde, Abubakar, et al," Design of a Fingerprint Biometric Authentication Technique for Electronic Examination", International Journal of Computer Science and Telecommunications,Volume 8, Issue 2, March 2017

[37] S. Alotaibi, "Using Biometrics Authentication via Fingerprint Recognition in E-exams in E-Learning Environment". The 4th Saudi International Conference, University of Manchester, United Kingdom, 2010.

[38] Madhu Babu Anumolu, N.Bharadwaj, "An Online Examination System Using Wireless Security Application", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 9- Sep 2013

[39] Liu, Lili; Cao, Tianjie," The Research and Design of an Efficient Verification System Based on Biometrics. ",2012 International Conference on Computer Science and Electronics Engineering – Mar 1, 2012. doi:10.1109/iccsee.2012.435

[40] Mohamed, Farid," Biometrics: Effectiveness and Applications within the Blended Learning Environment", Computer Engineering and Intelligent Systems, Vol.5, No.5, 2014

[41] Bal, Aditi; Acharya, Arunasish," Biometric authentication and tracking system for online examination system", International Conference on Recent Trends in Information Systems – Dec 1, 2011. doi:10.1109/retis.2011.6146869

[42] Zahedi, Ali; Sadjedi, Hamed; Behrad, Alireza," A new retinal image processing method for human identification using radon transform 6th Iranian Conference on Machine Vision and Image Processing – Oct 1, 2010. doi:10.1109/iranianmvip.2010.5941139

[43] Asha, S.; Chellappan, C.," Authentication of e-learners using multimodal biometric technology", International Symposium on Biometrics and Security Technologies – Apr 1, 2008. doi:10.1109/isbast.2008.4547640

[44] Alsultan, Arwa; Warwick, Kevin, "User-Friendly Free-text Keystroke Dynamics Authentication for Practical Applications", IEEE International Conference on Systems, Man, and Cybernetics – Oct 1, 2013. DOI: 10.1109/SMC.2013.793

[45] Shdaifat, Aayat Mahmoud; Obeidallah, Randa A; Ghazal, Ghadeer; Abu Sarhan, Alaa; Abu Spetan, Nesreen Rabah, "A proposed Iris Recognition Model for Authentication in Mobile Exams", International Journal of Emerging Technologies in Learning (iJET), Volume 15 (12): 205 – Jun 26, 2020. DOI:10.3991/ijet.v15i12.13741

[46] Mock, Kenrick; Hoanca, Bogdan; Weaver, Justin; Milton, Mikal," Real-time continuous iris recognition for authentication using an eye tracker", Association for Computing Machinery — Oct 16, 2012. doi:10.1145/2382196.2382307

[47] Hasan Alkhateeb, Jawad," A Novel Framework for Ensuring Online Exam Authentication at Taibah University", International Journal of Software Engineering and Computer Systems , Volume 6 (1): 1-7 – May 31, 2020, doi:10.15282/ijsecs.6.1.2020.1.0064

[48] Sheela, Vanitha, et al, "DETECTION OF IMPERSONATION IN ONLINE EXAMINATION", JOURNAL OF CRITICAL REVIEWS-ISSN- 2394-5125 VOL 7, ISSUE 10, 2020

[49] Ogherohwo, Ezeoba, "Design and Construction of a Biometric Examination Authentication Device", International Journal of Advanced Research in Physical Science (IJARPS), Volume 3, Issue 5, 2016, PP 29-39

[50] Mushtaq, Rashi, "DEVELOPMENT OF RETINA BASED BIOMETRIC AUTHENTICATION TOOL FOR UNIVERSITY SECURITY SYSTEM", International Journal of Advance Research in Science and Engineering,Volume No.07, Special Issue No.04, March 2018.

[51] Ghada, Moustafa, Essam "A New Remote Authentication Model forOnline Examination Systems" European Journal of Scientific Research,ISSN 1450-216X / 1450-202X Vol. 125 No 1 September, 2014, pp.115-127

[52] Ahmed, Ahmed A; Traore, Issa, "Biometric Recognition Based on Free-Text Keystroke Dynamics", IEEE transactions on cybernetics, Volume 44 (4): 15 – Mar 30, 2015. doi:10.1109/TCYB.2013.2257745

[53] Alsultan, Arwa; Warwick, Kevin; Wei, Hong, "Non-conventional keystroke dynamics for user authentication", Pattern Recognition Letters, Volume 89: 53-59 – Apr 1, 2017. doi: 10.1016/j.patrec.2017.02.010

[54] Lohit Jain, John V. Monaco, Michael J. Coakley, and Charles C. Tappert," Passcode Keystroke Biometric Performance on Smartphone Touchscreens is Superior to that on Hardware Keyboards", International Journal of Research in Computer Applications & Information Technology Volume 2, Issue 4, July-August, 2014, pp. 29-33.

[55] Banerjee, Salil Partha; Woodard, Damon, "Biometric Authentication and Identification Using Keystroke Dynamics: A Survey ", Journal of Pattern Recognition Research, Volume 7 (1): 116-139 – Jan 1, 2012. doi:10.13176/11.427

[56] Banerjee, Salil Partha; Woodard, Damon, "Biometric Authentication and Identification Using Keystroke Dynamics: A Survey ", Journal of Pattern Recognition Research, Volume 7 (1): 116-139 – Jan 1, 2012. doi:10.13176/11.427

[57] Samson Idemudia, Mohd Foad, et al, "A Smart Approach of E-Exam Assessment Method Using Face Recognition to Address Identity Theft and Cheating", International Journal of Computer Science and Information Security

(IJCSIS), Vol. 14, No. 10, October 2016.

[58] Md Liakat, Kutub, et al," Keystroke Biometric User Verification Using Hidden Markov Model", 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing.

[59] C.J Tsai, T.Y. Chang, Y.J. Yang, M.S Wu and Y.C Li, "An Approach for User Authentication on non-keyboard devices using mouse click characteristics and statistical based classification", International Journal of Innovative Computing, Information and Control, Vol 8, Number II, November 2012

[60] Young, Jay R.; Davies, Randall S.; Jenkins, Jeffrey L.; Pfleger, Isaac," Keystroke Dynamics: Establishing Keyprints to Verify Users in Online Courses", Computers in the Schools, Volume 36 (1): 48-68 – Jan 2, 2019. doi:10.1080/07380569.2019.1565905

[61] Yadav, Jatin, et al. "Keystroke dynamics based authentication using fuzzy logic." 2017 Tenth International Conference on Contemporary Computing (IC3). IEEE, 2017.

[62] Alshanketi, Faisal, et al. "Improving performance and usability in mobile keystroke dynamic biometric authentication." 2016 IEEE Security and Privacy Workshops (SPW). IEEE, 2016.

[63] D'Lima, N., & Mittal, J. (2015). Password authentication using Keystroke Biometrics. 2015 International Conference on Communication, Information & Computing Technology (ICCICT). doi:10.1109/iccict.2015.7045681

[64] Lu, Xiaofeng; Zhang, Shengfei; Hui, Pan; Lio, Pietro,"Continuous authentication by free-text keystroke based on CNN and RNN.",Computers & Security , Volume 96: 101861 – Sep 1, 2020, doi:10.1016/j.cose.2020.101861.

[65] Mondal, Soumik; Bours, Patrick.," Combining keystroke and mouse dynamics for continuous user authentication and identification.", IEEE International Conference on Identity, Security and Behavior Analysis (ISBA) – Feb 1, 2016. doi:10.1109/isba.2016.7477228

[66] Mondal, Soumik and Patrick A. H. Bours. "Continuous authentication using mouse dynamics." 2013 International Conference of the BIOSIG Special Interest Group (BIOSIG) (2013): 1-12.

[67] Zamfiroiu, Alin; Constantinescu, Diana; Zurini, Mădălina; Toma, Cristian,"Secure Learning Management System Based on User Behavior", Applied Sciences , Volume 10 (21) – Oct 31, 2020 . doi:10.3390/app10217730

[68] Kamble, Kiran P.; Ghorpade, Vijay R., "Video Interpretation for Cost-Effective Remote Proctoring to Prevent Cheating.", Proceeding of First Doctoral Symposium on Natural Computing Research, Volume 169 – Oct 21, 2020. doi:10.1007/978-981-33-4073-2_25

[69] Abadi, Eden; Hazan, Itay," Improved Feature Engineering for Free-Text Keystroke Dynamics" Security and Trust Management, Lecture Notes in Computer Science : 93-105 – Jan 1, 20. doi.org/10.1007/978-3-030-59817-4_6

[70] Javier Hernandez, Roberto Daza, "edBB:Biometrics and Behavior for Assessing Remote Education", Association for the Advancement of Artificial Intelligence (www.aaai.org). Dec 2019

[71] Mogus, Ana M; Djurdjevic, Ivana; Suvak, Nenad, "The impact of student activity in a virtual learning environment on their final mark ", Active Learning in Higher Education, Volume 13 (3): 13 – Nov 1, 2012. doi:10.1177/1469787412452985

[72] Antal, M. and Norbert Fejér. "Mouse dynamics based user recognition using deep learning." Acta Universitatis Sapientiae, Informatica 12 (2020): 39 - 50.

[73] Anam Khan, Suhail Javed, et al," Mouse Dynamics as Continuous User Authentication Tool,International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277 3878, Volume-8 Issue-4, November 2019.

[74] Khanam, Zeba; Ahsan, Mohammed Najeeb, "Implementation of pHash algorithm for face recognition in secured remote online examination system", International Journal of Advances in Scientific Research and Engineering, Volume 4 (11): 01-05 – Jan 1, 2018. doi:10.31695/ijasre.2018.32917

[75] Kim, Chanwoo; Stern, Richard M., "Feature extraction for robust speech recognition based on maximizing the sharpness of the power distribution and on power flooring,", IEEE International Conference on Acoustics, Speech and Signal Processing – Jan 1, 2010. doi:10.1109/icassp.2010.5495570

[76] Kawamata, Taisuke; Ishii, Takatoshi; Fujimori, Susumu; Akakura, Takako, "Student authentication by updated facial information with weighting coefficient in e-Learning", IEEE Region 10 Conference (TENCON) – Nov 1, 2016. doi.org/10.1109/tencon.2016.7848061

[77] Escobar Grisales, Daniel; Vásquez-Correa, Juan. C.; Vargas-Bonilla, Jesús F.; Orozco-Arroyave, Juan Rafael, "Identity verification in virtual education using biometric analysis based on keystroke dynamics", TecnoLógicas, Volume 23 (47): 197-211 – Jan 30, 2020. doi:10.22430/22565337.1475

[78] Feng Hao; Anderson, R.; Daugman, J. ,"Combining crypto with biometrics effectively," IEEE Transactions on Computers , Volume 55 (9): 1081-1088 – Sep 1, 2006, doi:10.1109/tc.2006.138

[79] Sandhya, Mulagala; Prasad, Munaga V.N.K, "A hybrid biometric cryptosystem for securing fingerprint minutiae templates", International Journal of Trust Management in Computing and Communications , Volume 3 (4) – Jan 1,

2016, doi:10.1504/IJTMCC.2016.084560

[80] Ailisto, Heikki; Vildjiounaite, Elena; Lindholm, Mikko; Mäkelä, Satu-Marja; Peltola, Johannes, "Soft biometrics—combining body weight and fat measurements with fingerprint biometrics," Pattern Recognition Letters , Volume 27 (5): 325-334 – Apr 1, 2006, doi:10.1016/j.patrec.2005.08.018

[81] Bouchaffra, Djamel; Amira, Abbes , "Structural hidden Markov models for biometrics: Fusion of face and fingerprint",Pattern Recognition,Volume41(3):852-867–Mar1,2008, doi:10.1016/j.patcog.2007.06.033

[82] Fenu, Gianni; Marras, Mirko; Boratto, Ludovico," A multi-biometric system for continuous student authentication in e-learning platforms ", Pattern Recognition Letters, Volume 113: 83-92 – Oct 1, 2018. doi: 10.1016/j.patrec.2017.03.027.

[83] Gupta, A., Khanna, A., Jagetia, A., Sharma, D., Alekh, S., and Choudhary, V. 2015. "Combining Keystroke Dynamics and Face Recognition for User Verification ", IEEE 18th International Conference on Computational Science and Engineering – Oct 1, 2015, doi:10.1109/cse.2015.37

[84] Giot, Romain; Hemery, Baptiste; Rosenberger, Christophe, "Low Cost and Usable Multimodal Biometric System Based on Keystroke Dynamics and 2d Face Recognition,", 20th International Conference on Pattern Recognition – Aug 1, 2010, doi:10.1109/icpr.2010.282

[85] Jagadamba, G; Sheeba, R; Brinda, K N; Rohini, K C; Pratik, S K.,"Adaptive E-Learning Authentication and Monitoring.", 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) – Mar 1, 2020. doi:10.1109/icimia48430.2020.9074955

[86] Fayaz, Fayaz Ahmad; Mohi-Ud-Din, Shakir; Batool, Irtiza; Kaur, Satinder; Rashid, Mamoon," Novel Face Recognition Based Examinee Authentication System using Python D-Lib", Fifth International Conference on Image Information Processing (ICIIP) – Nov 1, 2019. doi:10.1109/iciip47207.2019.8985983

[87] Naveen, M Ganesh, et al," MULTI-FACTOR AUTHENTICATION SCHEME FOR ONLINE EXAMINATION", International Journal of Pure and Applied Mathematics, Volume 119 No. 15 2018, 1705-1712

[88] Rudrapal, Dwijen; Das, Smita; Debbarma, S.; Kar, N.; Debbarma, N.," Voice Recogniton and authentication as a proficient biometric tool and its application in online exam for P.H people", International Journal of Computer Applications, Volume 39 (12): 6-12 – Feb 29, 2012. DOI:10.5120/4870-7297

[89] Ullah, Abrar; Xiao, Hannan; Barker, Trevor; Lilley, Mariana ," Evaluating security and usability of profile based challengequestions authentication in online examinations", Journal of Internet Services and Applications , Volume 5 (1) – Mar 4, 2014, doi:10.1186/1869-0238-5-2

[90] Hayes, B.; Ringwood, J.V., "Student Authentication for Oral Assessment in DistancE-learningPrograms", IEEE Transactions on Learning Technologies, Volume 1 (3): 165-175 – Jul 1, 2008. DOI:10.1109/TLT.2009.2

[91] Buckley, F., Barnes, V., Corum, T., Gelardi, S., Rainsford,K., Dressner, P., & Monaco, J.V. "Design of the Data Input Structure for a Mouse Movement Biometric System to Authenticate the Identity of Online Test Takers", Proc.Research Day, CSIS, Pace University, May 2015,http://csis.pace.edu/~ctappert/srd2015/2015PDF/b6.pdf, accessed February 2016.

[92] S. S. Ketab, N. L. Clarke, and P. S. Dowland, "E-invigilation of e-assessments," Proceedings of INTED2015 Conference 2nd-4th March 2015, Madrid, Spain

[93] Aythami, Julian, et al "BIOMETRIC TECHNOLOGIES FOR ONLINE STUDENT AUTHENTICATION", Proceedings of EDULEARN15 Conference 6th-8th July 2015, Barcelona, Spain

[94] Kumar, Ajay; Wong, David C. M.; Shen, Helen C.; Jain, Anil K., "Personal Verification using Palmprint and Hand Geometry Biometric", Lecture Notes in Computer Science, Audio- and Video-Based Biometric Person Authentication : 668-678 – Jan 1, 2003, doi:10.1007/3-540-44887-x_78

[95] Brocardo, Marcelo Luiz; Traore, Issa; Woungang, Isaac, "Toward a framework for continuous authentication using stylometry", IEEE 28th International Conference on Advanced Information Networking and Applications – May 1, 2014. DOI:10.1109/AINA.2014.18

[96] Zhong, Yu; Deng, Yunbin; Jain, Anil K.," Keystroke dynamics for user authentication", IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops – Jun 1, 2012. doi:10.1109/cvprw.2012.6239225

[97] Anitha Devi, M.D; ShivaKumar, K B, « A Novel Image Steganography Technique for Secured Online Transaction Using DWT and Visual Cryptography", IOP Conference Series : Materials Science and Engineering, Volume 225 (1) : 8 – Aug 1, 2017. doi:10.1088/1757-899X/225/1/012070

[98] Tan, Bozhao and S. Schuckers. "Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing." 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06) (2006): 26-26. DOI:10.1109/CVPRW.2006.120

[99] Bimpe C. Ayoola " Fingerprint Authentication framework for E-Testing (A case study of CSC 101 students)",

[100] Canales O, Monaco V, Murphy T, et al. A stylometry system for authenticating students taking online tests.", Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 6th, 2011

[101] Parkavi, R.; Chandeesh Babu, K.R.; Kumar, J.Ajeeth," Multimodal Biometrics for user authentication", 11th International Conference on Intelligent Systems and Control (ISCO) – Jan 1, 2017. doi:10.1109/isco.2017.7856044

[102] Jorgensen, Z., & Yu, T. (2011). On mouse dynamics as a behavioral biometric for authentication. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security - ASIACCS '11. doi:10.1145/1966913.1966983

[103] Durcheva, Mariana; Rozeva, Anna,"Authentication with TeSLA system instruments supporting eAssessment models in engineering courses", PROCEEDINGS OF THE 45TH INTERNATIONAL CONFERENCE ON APPLICATION OF MATHEMATICS IN ENGINEERING AND ECONOMICS (AMEE'19) – Jan 1, 2019. doi:10.1063/1.5133513

[104] Teh, Pin Shen; Teoh, Andrew Beng Jin; Tee, Connie; Ong, Thian Song, "Keystroke dynamics in password authentication enhancement," Expert Systems with Applications, Volume 37 (12): 8618-8627 – Dec 1, 2010. DOI:10.1016/J.ESWA.2010.06.097

[105] Almalki, Sultan; Chatterjee, Prosenjit; Roy, Kaushik, "Continuous Authentication Using Mouse Clickstream Data Analysis.", Security, Privacy, and Anonymity in Computation, Communication, and Storage, Lecture Notes in Computer Science: 76-85 – Jan 1, 2019. DOI:10.1007/978-3-030-24900-7_6

[106] Hossain, Md Shafaeat; Haberfeld, Carl; Yuan, Kate; Chen, Jundong; Rahman, Khandaker Abir; Hussain, Ishtiaque, "Continuous Authentication Using Creative Writing", International Symposium on Networks, Computers and Communications (ISNCC) – Oct 20, 2020. doi: 10.1109/ISNCC49221.2020.9297312.

[107] Labayen, M., Vea, R., Flórez, J., Guillén-Gámez, F.D., García-Magariño, I.," Smowl: a tool for continuous student validation based on face recognition for online learning", Edulearn14 Proceedings, pp. 5354–5359. IATED (2014)

[108] Y. m. Cheung and Q. Peng, "Eye Gaze Tracking with a Web Camera in a Desktop Environment", IEEE Transactions on HumanMachine Systems, Vol.45, Issue.4, pp.419-430,2015.

[109] Guo, Yanhui; Yin, Xijie; Zhao, Xuechen; Yang, Dongxin; Bai, Yu," Hyperspectral image classification with SVM and guided filter", EURASIP Journal on Wireless Communications and Networking, Volume 2019 (1) – Mar 8, 2019. doi:10.1186/s13638-019-1346-z

[110] Parthasaradhi, S.T.V.; Derakhshani, R.; Hornak, L.A.; Schuckers, S.A.C.," Time-series detection of perspiration as a liveness test in fingerprint devices", IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews), Volume 35 (3): 335-343 – Aug 1, 2005. DOI:10.1109/TSMCC.2005.848192

[111] Antonelli, A.; Cappelli, R.; Maio, D.; Maltoni, D, "Fake finger detection by skin distortion analysis", IEEE Transactions on Information Forensics and Security, Volume 1 (3): 360-373 – Sep 1, 2006. DOI: 10.1109/TIFS.2006.879289

[112] Kobojek, P., & Saeed, K.," Application of recurrent neural networks for user verification based on keystroke dynamics", Journal of telecommunications and information technology, (3), 80-90,2016

[113] Derakhshani, Reza; Schuckers, Stephanie A.C.; Hornak, Larry A.; O'Gorman, Lawrence ,"Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners ",Pattern Recognition , Volume 36 (2): 383-396 – Feb 1, 2003, doi:10.1016/s0031-3203(02)00038-9.

[114] Ackley, David H.; Hinton, Geoffrey E.; Sejnowski, Terrence J, "A learning algorithm for Boltzmann machines", Cognitive Science - A Multidisciplinary Journal, Volume 9 (1) – Jan 1, 1985. doi:10.1207/s15516709cog0901_7

[115] Pan, G., Sun, L., Wu, Z., & Lao, S. (2007). Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera. 2007 IEEE 11th International Conference on Computer Vision. doi:10.1109/iccv.2007.4409068

[116] Putte, Ton; Keuning, Jeroen," Biometrical fingerprint recognition: don't get your fingers burned", Smart Card Research and Advanced Applications : 289-303 – Jan 1, 2000, doi:10.1007/978-0-387-35528-3_17.

[117] Chugh, Tarang; Cao, Kai; Jain, Anil K.,"Fingerprint Spoof Buster." IEEE Transactions on Information Forensics and Security, Volume 13 (9): 2190-2202 – Sep 1, 2018. doi:10.1109/tifs.2018.2812193

[118] Pan, Gang; Sun, Lin; Wu, Zhaohui; Lao, Shihong.," Eyeblink-based anti-spoofing in face recognition from a generic webcamera", 2007 IEEE 11th International Conference on Computer Vision – Jan 1, 2007. DOI:10.1109/ICCV.2007.4409068

[119] Asthana, Akshay; Zafeiriou, Stefanos; Cheng, Shiyang; Pantic, Maja," Incremental Face Alignment in the Wild", IEEE Conference on Computer Vision and Pattern Recognition – Jun 1, 2014. doi:10.1109/cvpr.2014.240

[120] KARSON, CRAIG N," Spontaneous eye-blink rates and dopaminergic systems", Brain, Volume 106 (3) – Sep 1, 1983. DOI:10.1093/BRAIN/106.3.643

[121] Kollreider, Klaus; Fronthaler, Hartwig; Faraj, Maycel Isaac; Bigun, Josef," Real-Time Face Detection and Motion Analysis with Application in "Liveness" Assessment ", IEEE Transactions on Information Forensics and Security, Volume 2 (3): 548-558 – Sep 1, 2007. doi:10.1109/tifs.2007.902037

[122] Pan, Gang; Sun, Lin; Wu, Zhaohui; Lao, Shihong," Eyeblink-based anti-spoofing in face recognition from a generic webcamera", IEEE 11th International Conference on Computer Vision – Jan 1, 2007. DOI: 10.1109/ICCV.2007.4409068

[123] Xiong, Xuehan ; De la Torre, Fernando, « Supervised descent methods and its applications to face alignment ", IEEE Conference on Computer Vision and Pattern Recognition – Jun 1, 2013. DOI: 10.1109/CVPR.2013.75

[124] Schuckers, Stephanie A.C, "Spoofing and Anti-Spoofing Measures", Information Security Technical Report, Volume 7 (4): 56-62 – Dec 1, 2002. DOI:10.1016/S1363-4127(02)00407-7

[125] Alshehri, Abdullah; Coenen, Frans; Bollegala, Danushka,"Spectral analysis of keystroke streams: Towards effective real-time continuous user authentication", Proceedings of the 4th International Conference on Information Systems Security and Privacy – Jan 1, 2018. doi:10.5220/0006606100620073

[126] Uliyan, Diaa M.; Sadeghi, Somayeh; Jalab, Hamid A,"Anti-spoofing method for fingerprint recognition using patch based deep learning machine", Engineering Science and Technology, an International Journal , Volume 23 (2): 264-273 – Apr 1, 2020. doi:10.1016/j.jestch.2019.06.005

[127] Saied, Marwa; Elshenawy, Ayman; Ezz, Mohamed M, "A Novel Approach for Improving Dynamic Biometric Authentication and Verification of Human Using Eye Blinking Movement ",Wireless Personal Communications , Volume 115 (1) – Nov 23, 2020, doi:10.1007/s11277-020-07601-x.

[128] Tan, Xiaoyang; Li, Yi; Liu, Jun; Jiang, Lin, « Face liveness detection from a single image with sparse low rank bilinear discriminative model", Computer Vision – ECCV 2010, Lecture Notes in Computer Science: 504-517 – Jan 1, 2010. DOI:10.1007/978-3-642-15567-3_37

[129] Wang, Tao; Yang, Jianwei; Lei, Zhen; Liao, Shengcai; Li, Stan Z," Face liveness detection using 3d structure recovered from a single camera", 2013 International Conference on Biometrics (ICB) – Jun 1, 2013. DOI:10.1109/ICB.2013.6612957

[130] Oren, Michael; Nayar, Shree K," Generalization of the lambertian model and implications for machine vision", International Journal of Computer Vision, Volume 14 (3): 25 – Apr 1, 1995. doi:10.1007/BF01679684

[131] Brocardo, Marcelo Luiz; Traore, Issa; Woungang, Isaac; Obaidat, Mohammad S.," Authorship verification using deep belief network systems", International Journal of Communication Systems, Volume 30 (12) – Aug 1, 2017. doi:10.1002/dac.3259

[132] Saragih, Jason; Lucey, Simon; Cohn, Jeffrey," Deformable model fitting by regularized landmark mean-shift", International Journal of Computer Vision, Volume 91 (2) – Sep 25, 2010. doi:10.1007/s11263-010-0380-4

[133] Bai, Jiamin; Ng, Tian-Tsong ; Gao, Xinting ; Shi, Yun-Qing, » Is physics-based liveness detection truly possible with a single image ?", Proceedings of 2010 IEEE International Symposium on Circuits and Systems – May 1, 2010. DOI:10.1109/ISCAS.2010.5537866

[134] Atoum, Yousef; Liu, Yaojie ; Jourabloo, Amin ; Liu, Xiaoming, » Face anti-spoofing using patch and depth-based cnns", 2017 IEEE International Joint Conference on Biometrics (IJCB) – Oct 1, 2017. DOI:10.1109/BTAS.2017.8272713.

[135] Jourabloo, Amin; Liu, Yaojie; Liu, Xiaoming," Face de-spoofing: Anti-spoofing via noise modeling", Computer Vision – ECCV 2018, Lecture Notes in Computer Science: 297-315 – Jan 1, 2018. DOI:10.1007/978-3-030-01261-8_18

[136] Flior, Eric; Kowalski, Kazimierz," Continuous Biometric User Authentication in Online Examinations". 2010 Seventh International Conference on Information Technology: New Generations, Jan 1, 2010, doi:10.1109/itng.2010.250

[137] Hsu, Sam; Sharda, Nalin; Marques, Oge, "Internet-Based Distance Learning", Handbook of Internet Computing, Internet and Communications – Jun 27, 2000, doi:10.1201/9781420049121.ch20

[138] Kikelomo Apampa, Gary Wills, David Argles, "User Security Issues in Summative e-Assessment Security", International Journal of Digital Society (IJDS), Volume 1, Issue 2, June 2010.

[139] A. Marcus, J. Raul, R. Ramirez-Velarde and J. Nolazco-Flores, "Addressing Secure Assessments for Internet-Based Distance Learning Still an Irresolvable Issue", Proceedings of the 9 Latin-American Congress of Educational Computing, Caracas, Venezuela, March 2008.

[140] Sukmandhani, Arief Agus; Sutedja, Indrajani," Face Recognition Method for Online Exams", International Conference on Information Management and Technology (ICIMTech) – Aug 1, 2019. doi:10.1109/icimtech.2019.8843831

[141] Subramanian, N. Sethu; Narayanan, Sankaran; Soumya, M. D.; Jayakumar, Nitheeswar; Bijlani, Kamal, "Using Aadhaar for Continuous Test-Taker Presence Verification in Online Exams", Springer Journals — Apr 14, 2018. doi.org/10.1007/978-981-10-7563-6_2

[142] Y. Levy, and M. M. Ramin, "A Theoretical Approach for Biometrics Authentication of e-Exams", February 20, 2007

[143] Al-Saleem, Saleh M.; Ullah, Hanif., "Security Considerations and Recommendations in Computer-Based Testing.", The Scientific World Journal, Volume 2014 – Sep 1, 2014. doi:10.1155/2014/562787

[144] Shimshon, Tomer; Moskovitch, Robert; Rokach, Lior; Elovici, Yuval,"Continuous verification using keystroke dynamics.", International Conference on Computational Intelligence and Security – Dec 1, 2010. doi:10.1109/cis.2010.95

[145] Ceker, Hayreddin; Upadhyaya, Shambhu , "User Authentication with Keystroke Dynamics in Long-Text Data" ,IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS) – Sep 1, 2016, doi:10.1109/btas.2016.7791182

[146] Ghizlane, Moukhliss; Hicham, Belhadaoui; Reda, Filali Hilali," A New Model of Automatic and Continuous Online Exam Monitoring", International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBIoTS) – Dec 1, 2019. doi:10.1109/syscobiots48768.2019.9028027

[147] Musambo, Lubasi Kakwete and J. Phiri. "Student Facial Authentication Model based on OpenCV's Object Detection Method and QR Code for Zambian Higher Institutions of Learning." (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 5, 2018

[148] Mooad, Rasmi, A.Hassan," Evaluation of E-exam during Covid-19", PSYCHOLOGY AND EDUCATION (2021) 58(1): 4604-4612, ISSN: 00333077

[149] Kaur, Navjot; Prasad, P. W. C.; Alsadoon, Abeer; Pham, L.; Elchouemi, A.," An enhanced model of Biometric Authentication in E-Learning Using a combination of Biometric features to access E-Learning environments", 2016 International Conference on Advances in Electrical, Electronic and Systems Engineering (ICAEES) – Nov 1, 2016. DOI:10.1109/ICAEES.2016.7888025

[150] Stewart, John C.; Monaco, John V.; Cha, Sung-Hyuk; Tappert, Charles C.," An investigation of keystroke and stylometry traits for authenticating online test takers", International Joint Conference on Biometrics (IJCB) – Oct 1, 2011. doi:10.1109/ijcb.2011.6117480

[151] Mungai, Peter Kimani; Huang, Runhe, » Using keystroke dynamics in à multi-level architecture to protect online examinations from impersonation", IEEE 2nd International Conference on Big Data Analysis (ICBDA) (– Mar 1, 2017. doi:10.1109/icbda.2017.8078710

[152] Mats Wiklund, Peter Mozelius, et al, "Biometric Belt and Braces for Authentication in Distance Education", Conference: ECEL 2016At: Prague, Czeck Republic, October 2016

[153] Sim, Terence; Zhang, Sheng; Janakiraman, Rajkumar; Kumar, Sandeep, "Continuous verification using multimodal biometrics", IEEE transactions on pattern analysis and machine intelligence, Volume 29 (4): 14 – Apr 24, 2007.

[154] Monaco JV, Stewart JC, Cha SH, Tappert CC ," Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works.", 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS) – Sep 1, 2013, doi:10.1109/btas.2013.6712743

[155] Srivastava, Stuti; Sudhish, Prem Sewak, "Continuous Multibiometric User Authentication Fusion of Face Recognition and Keystoke Dynamics", IEEE Region 10 Humanitarian Technology Conference (R10-HTC) – Dec 1, 2016 , doi:10.1109/r10-htc.2016.7906823

[156] Curran, Jack; Curran, Kevin," Biometric Authentication in Online Learning Environments", Biometric Authentication in Online Learning Environments, Advances in Educational Technologies and Instructional Design: 266-278 – Jan 1, 2019. doi:10.4018/978-1-5225-7724-9.ch011

[157] S. S. Ketab, N. L. Clarke, and P. S. Dowland," A Robust e-Invigilation System Employing Multimodal Biometric Authentication", International Journal of Information and Education Technology, Volume 7 (11): 796-802 – Jan 1, 2017. doi:10.18178/ijiet.2017.7.11.975

[158] Liu, Yudong; Jiang, Yusheng; Devenere, John," Using Deep Learning for Fusion of Eye and Mouse Movement based User Authentication", IEEE International Joint Conference on Biometrics (IJCB) – Sep 28, 2020. doi:10.1109/ijcb48548.2020.9304926

[159] Maas, Andrew; Heather, Chris; Do, Chuong (Tom); Brandman, Relly; Koller, Daphne; Ng, Andrew. "Offering Verified Credentials in Massive Open Online Courses: MOOCs and technology to advance learning and learning research (Ubiquity symposium).", Ubiquity, Volume 2014 (May) – May 1, 2014. doi:10.1145/2591684

[160] Tong Wu, Kangfeng Zheng, et al "User Identification Using Real Environmental Human Computer Interaction Behavior", KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 13, NO. 6, Jun. 2019. DOI:10.3837/tiis.2019.06.016

COMMERCIAL SYSTEMS

[C1] Examsoft.com

[C2] Talview.com

[C3] Mettl.com

[C4] PSI

[C5] Proctor track

[C6] proctorio.com

[C7] Proctoru.com

[C8] Examity.com

[C9] Kryterion Webassessor