2017-11-01

A Robust e-Invigilation System Employing Multimodal Biometric Authentication

SS Ketab

NL Clarke *School of Engineering, Computing and Mathematics*

PS Dowland

A Robust e-Invigilation System Employing Multimodal Biometric Authentication

Salam S. Ketab, Nathan L. Clarke, and Paul S. Dowland

***Abstract*—The significant growth in users of e-learning technologies and their use in courses has given rise to a major concern over protecting them from misuse; a significant concern is that of the potential for cheating or illicit assistance during online examinations. This paper presents the development of robust, flexible, transparent and continuous authentication mechanism for e-assessments. To monitor the exam taker and ensure that only the legitimate student is taking the exam, the system offers a continuous user identification employing multimodal biometrics; a security layer using an eye tracker to record the student's eye movement; and, speech recognition to detect inappropriate communication. The focus of this paper in particular is the development and evaluation of 3D facial authentication. An experiment has been conducted to investigate the ability of the proposed platform to detect any cheating attempts. During the experiment, participants' biometric data, eye movement, and head movements have been collected using custom software. The 3D camera also captured the session using a built-in microphone and the system recognized speech (employing a speech recognition algorithm). 51 participants participated in this experiment. The FRR of all legitimate participants was 0 and 0.0063 in 2D and 3D facial recognition modes respectively. Furthermore, three participants were tasked with a series of eight scenarios that map to typical misuse. The results of the FAR and FRR of five of these threat scenarios in both 2D and 3D mode were 0 with two cases exhibiting an FAR of 0.11 and 0.076 in the 2D mode.**

***Index Terms*—Biometric, e-assessment, e-invigilation, e-learning, facial recognition.**

I. Introduction

The past ten years have seen increasingly rapid advances in distance-based learning, and became an essential and positive factor in the education progress. An enormous number of e-learning providers utilize platforms to deploy various scientific, educational, training, and teaching courses to reduce the burden from teachers. E-learning has offered flexibility and remote-based learning, but some of the course delivery aspects still depend on the traditional approaches, the most critical of these is the assessment process. Though much effort has been spent on the establishment and distribution of a primary open-source Virtual Learning Environment, less attention has been given to the linked problem of providing controlled electronic monitoring. In order to maintain the integrity of the assessment process, exams and tests are often undertaken under controlled circumstances within defined classrooms with physical invigilators. A significant obstacle in providing remote assessment is the ability to prove the legitimacy of the student, and to do so in a manner that is highly secure and convenient for all system users (academics and learners). A system needs to be resistant against possible cheating and unauthorized participation or assistance.

This work builds upon a previous publication by the authors [1] by exploring the viability of the previously proposed framework. Therefore, this phase of the work is dedicated to experimentally testing, evaluating, and validating the architecture. The system will monitor the exam taker and ensure that only the allowed/legitimate student is taking the exam, it will offer a continuous user identification process employing 2D and 3D facial recognition and an eye tracker to follow/record the student's eye movement. In addition to capturing facial images, a microphone monitors the users' session which is subsequently analyzed and saved as text.

The rest of this paper is organized as follows: an analysis of the current state of the art in the use of biometrics in e-assessment, which goes on to describe the domain of active authentication is presented in Section II. Section III presents the proposed approach system requirements and architecture, with Section IV describing the prototype of the system. Section V reflects on the experimental methodology and the results before Section VI presents a discussion. Finally, the concluding remarks and outline areas for future work are presented in Section VII.

II. Related Work

The literature shows that there is growing interest in online assessment and particularly in the security of such systems to perform e-invigilation. Most of the studies rely on computers in the classroom or another controlled physical environment – rather than allowing a student to remotely take an assessment. Biometric approaches are currently being adopted in this area with many researchers suggesting unimodal biometric solutions (e.g. iris recognition [2], or keystroke recognition [3]). However, studies including Asha & Chellappan [4] and Ross & Jain [5] claim that multimodal biometrics would be a more suitable and robust alternative. A camera supporting head geometry capture and fingerprint scanners could offer solutions for secure user identification for login in addition to continuous authentication [6]. But, this study considers students' acceptance of multimodal

Manuscript received June 24, 2016; revised January 2, 2017.

Salam S. Ketab and Paul S. Dowland are with the Centre for Security, Communications and Network Research, Plymouth University, United Kingdom (e-mail: salam.ketab@plymouth.ac.uk, paul.dowland@plymouth.ac.uk).

Nathan L. Clarke is with the Centre for Security, Communications and Network Research, Plymouth University, United Kingdom. He is also with Security Research Institute, Edith Cowan University, Perth, Western Australia, Australia (e-mail: nathan.clarke@plymouth.ac.uk).

doi: 10.18178/ijiet.2017.7.11.975

biometrics systems for verification throughout an online test, rather than focusing on the practicality, security, applicability and performance of the suggested strategy. Asha & Chellappan [4] recommend merging behavioral and physiological biometrics by using a physical fingerprint recognition combined with mouse dynamics (both biometrics authentication achieved using a mouse with an inbuilt fingerprint scanner). Many practical studies argue that the time required for data collection of mouse dynamics is very long [7]; this would open the door for suspicious student activities. Additionally, the system ignores the other potential problems including the secure environment around the student (e.g. orally discussing questions with someone nearby). Sabbah [8] offered a multimodal approach combining keystroke analysis and fingerprint recognition along with video monitoring. Whilst the idea has merit, his research neither clearly dissected how the approaches overcame the issue of cheating, nor the biometric performance being experienced in practice. Hernández et al. [9] proposed a prototype using fingerprint recognition to deal with the problem of student identification at the beginning of the e-assessment, together with a synchronized and continuous surveillance employing a web camera until the end of the online examination. Despite the fact this study is well evaluated, it did not explain the continuous video monitoring during the exam time (e.g., how it could be used in practice – would an examiner need to watch the individual video feeds of all participants?). Moreover, the use of a fingerprint offers only limited protection against cheating – with the examinee likely being complicit in the cheating.

III. EIEA Solution

The sections that follow present and discuss the requirement and complete core architecture for the proposed E-Invigilation of E-Assessments (EIEA) system. It has been designed to capture, process, and monitor students in a flexible, continuous, multimodal, secure and convenient fashion.

A. System Requirements

The prior literature has proven that the idea of a system that takes the role of physical proctor can face lots of requirements in order to reach a satisfactory level that enables this system to be an appropriate replacement. An analysis of the problem results in the following requirements being derived [1]:

- The system should have the ability to monitor students using the most robust biometric measures. A key difference in the method taken in this research is that the biometrics are not used to provide or deny access, but simply as a tool for the inspector/academic to be able to check the students behavior and facilitate the detection of misuse.
- The system must be usable. For examinees, it has to be lightweight and transparent. For the examiner, the output must provide a useable interface to identify and investigate cases of cheating.
- The system needs to be hardened against attack from both internal and external threats. Given the nature of the data being held (i.e. biometric-based), user's privacy and data security should also be maintained.
- The system should be scalable to manage the storage, retrieval and processing of biometric samples from large populations of users.
- A system should not be limited to present sensing technologies and biometric backend systems, so that it can adapt to new modalities and classification algorithms.
- System administrators should have the ability to add/remove security modules to/from the system (providing a user-centric approach to the design). This will help ensure both inspectors and students are provided with a system that is naturally intuitive and requires minimal learning.

B. General System Architecture

The EIEA system has been proposed to be a modular framework to include multimodal biometric authentication, including a variety of applicable, feasible and robust behavioral and physiological biometrics, for instance: face recognition, keystroke analysis, mouse dynamics, linguistic analysis, iris recognition, head and eye movement. Thus, the more transparent and robust biometrics that are employed; the more convenient and secure e-assessment are achieved.

A complete architecture of the suggested EIEA system [1] is shown in Fig. 1. Continuous biometric-based monitoring of the user and system-level proctoring to prevent cheating are the operational objectives of this architecture. In addition to a range of management-level functionality that provides the basis for creating and managing exams. This can be identified within the architectural diagram as the Biometric Acquisition & Processing, System-Level Monitoring, and Assessment Manager respectively. Furthermore, to reduce the volume of data to be transmitted and provide an increased level of privacy, the suggested system allows for client-side biometric sample preprocessing.

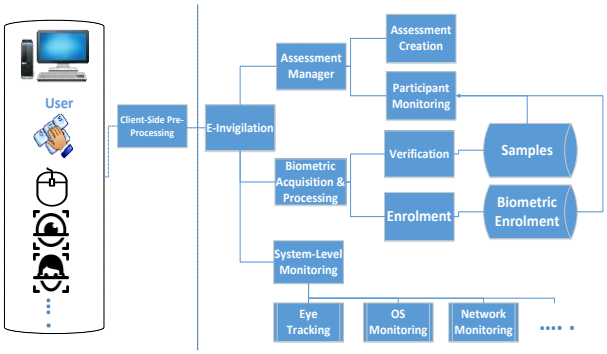

Fig. 1. The proposed EIEA architecture.

IV. Prototype

When implementing the previous architecture, a number of practical decisions had to be made such as which biometric modalities to use given what is practically available. It wasn't the purpose of the research to develop biometric techniques themselves. Hence, for implementation purposes and to prove the novelty, usability, and feasibility of a more robust biometric authentication, the research decided to focus upon the use of 2D and 3D facial recognition as the underpinning continuous and transparent biometrics.

The 2D facial recognition is the main (user-friendly and widely implemented) authentication approach that has already been used in the prototype e-invigilation system. However, for more robust facial recognition, this phase of the work has focused upon the development and evaluation of novel continuous and transparent authentication utilizing depth information (distance and head movement) for adding a further dimension to facial authentication using a 3D camera. The suggested algorithm utilizes the depth information provided by an infrared camera as the main factor to enhance recognition.

C. Requirements

The system offers facial recognition using a front-facing Creative 3D camera to recognize a student's face and to record sounds during the exam via the microphone. Moreover, the system implements eye tracking (using an Eye Tribe Tracker) to follow and record the student's eye movement.

D. Security

The EIEA system offers many layers of security including:

- System Log In: In order to log in the system, the participants will provide their username and student number and/or password.
- 2D and 3D facial recognition (verification).
- Continuous eye tracking: Using the eye tracking technology (Eye Tribe) to follow and record the participants' eye movements or locations (x,y) to check whether they were focusing on the computer screen. The eye tracking is linked to the camera to take a picture whenever the student moves his/her eyes away from the screen for a period of time.
- Speech recognition and recording: in addition to capturing/recording the whole session, the 3D camera that used in this experiment has a built-in microphone with noise-cancelation is used to get a clear voice recording of any sounds during the exam time (continuously). For privacy, avoiding/filtering unnecessary sounds recording, and using the available storage effectively, the system captures any dialogue and saves it as text (reducing storage and processing requirements). This has been achieved utilizing the textual representation of grammars for use in speech recognition (Java Speech Grammar Format (JSGF)).
- Utilizing the 3D camera, the system can continuously recognize, capture and record all times and durations of any other or different face(s), more than one face, no face at all, and face movements (turn right, turn left, up, and down).

Fig. 2 provides an example of system parameters.

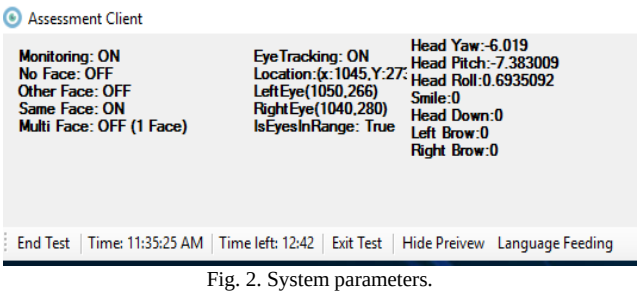

Fig. 2. System parameters.

These parameters provide real time Boolean and numerical information about:

- continuous Monitoring Statuses (in case of no, other, same, and multiple face(s)),
- continuous Eye Tracking (location, left eye, right eye, and is-eye-in-range),
- continuous Head Movements (yaw, pitch, and roll),
- and Face Expressions (including smile, head down, and eyebrow movement).

E. E-invigilation Algorithm

In this work, the algorithm achieves: user registration, biometric verification, continuous user identification, and continuous system security; as described in the following steps and shown in Table I.

- Registration: in this step, patterns of the student's biometrics are collected. For instance samples of his/her face are received and stored in the Realsense databases for later 2D and 3D facial recognition.
- Biometric verification: in each log in, the verification process is done by multibiometric recognition sub algorithms respectively.
- Continuous user identification via the multibiometric recognition sub algorithms (e.g. 2D and 3D facial recognition).

The security subsystems are continuously running, such as: eye tracking (in 2D and 3D modes), session sounds recording (in 2D and 3D modes), and head movements (in 3D mode only).

TABLE I: SYSTEM AUTHENTICATION AND SECURITY

System Actions	Authentication/Security		
	Log In Verification	Continuous Authentication	Continuous Misuse Tracking
2D Facial Recognition	Yes (Once)	Yes, For 5 Minutes	No
3D Facial Recognition	Yes (Once)	Yes, For 10 Minutes	No
Eye Tracking	No	No	Yes, For 15 Minutes
Head Movements	No	No	Yes, , For 10 Minutes
Speech Recognition	No	No	Yes, For 15 Minutes

The main system processes have been depicted in the following diagram, Fig. 3.

F. Implementation

In system implementation, in order to register or access the system, the participants work through a process of registrations where the system will collect their face images template data, and calibrate the basic eye movement around the screen (optional) as shown in Fig. 4. In this process, only a legitimate user should be involved, so the academic needs to perform a check using the university enrollment data. A continuous user identification using 2D facial recognition sub algorithm will be continually enabled during the first 5 minutes, and their facial features will be compared with the information in the Realsense database. The samples will be taken and saved every 4 seconds. With every successful

matching the system stores the taken sample to measure the 2D FRR. With every matching failure the system stores the taken sample to measure the 2D FAR.

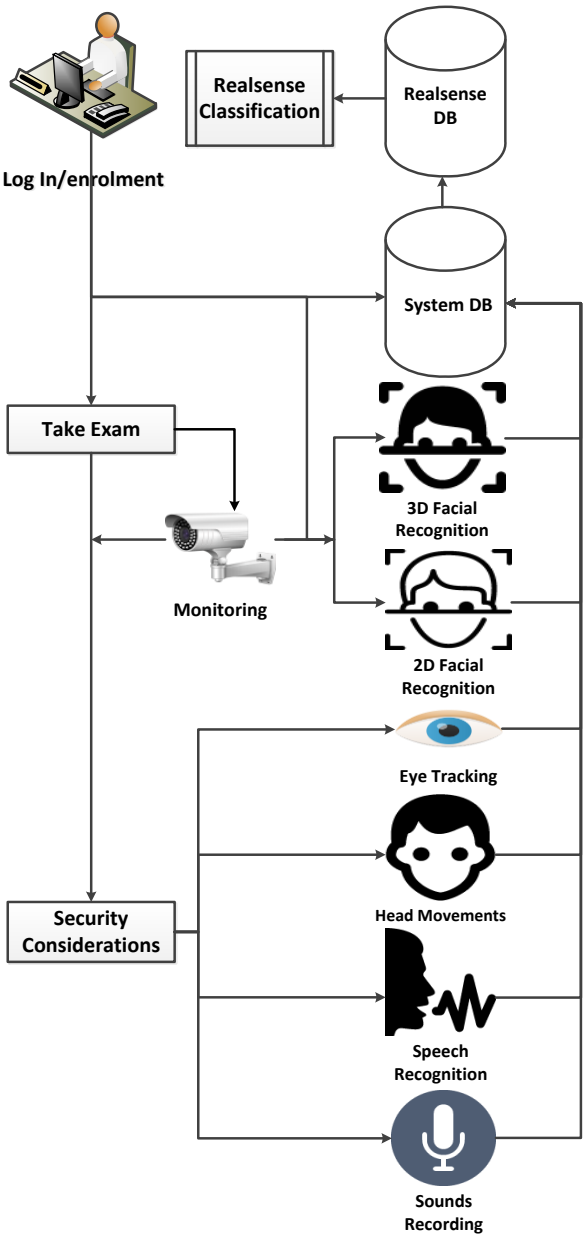

Fig. 3. System process diagram.

Due to the fact that the camera can only operate in either 2D or 3D mode in a specific time, after the first 5 minutes of the online assessment; the system will change the mode to continuous 3D face identification for the remaining 10 minutes of the test. All facial features will be compared with the information in the Realsense database. The samples will be taken and stored every 4 seconds. With every successful match the system stores the sample to measure the 3D FRR. With every match failure the system stores the sample to measure the FAR. The eye tracking security subsystem is continuously running during both 2D and 3D modes. The tracking results (the captured photos and all left, right eye movements and center locations), about 30 samples every second, will be stored in a text file (for later analysis). The continuous audio recording subsystem, and the textual representation of grammars for use in speech recognition (JSGF) will be run during both 2D and 3D modes, and the recognition results, times, and durations will be saved in the system database. The head movements (Roll, Yaw, and Pitch) will be measured continuously during 3D mode only, and the measurement values (about 3×25 samples every second) will be saved in a text file.

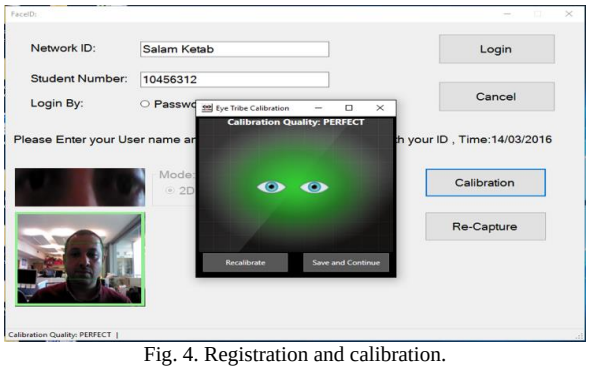

Fig. 4. Registration and calibration.

V. Experiment

A. Methodology

The experiment has been conducted to explore the feasibility of monitoring students while taking university online assessments. it has been achieved by involving:

- Participants were asked to take a controlled/monitored online assessment for a maximum duration of 15 minutes.
- The experiment has been conducted at Plymouth University on a dedicated computer equipped with the required technologies to achieve the experiment objectives.
- The capturing devices have been attached to a computer in front of the participant (the front-facing peripheral F200 3D camera and The Eye Tribe eye tracker).
- Participants sat a virtual assessment (online IQ test) that contained 30 simple multiple-choice questions.
- During the experiment, custom software collected the participants' biometrics/data (2D, depth, and infrared images), in addition to left and right eye images, face distances, and head movements via a 3D web camera; and eye movements using an Eye Tracker sensor.
- All of the information was treated confidentially and data was anonymous during the collection.

B. Results

51 participants participated in this experiment with an FRR of 0 in 2D facial recognition mode and 0.0063 in 3D facial recognition mode. The results are shown in Table II (some consequence participants' results, particularly in 3D facial recognition mode, contain 1 to 14 of 146 rejected samples; this would be due to some hardware/connections failure during the experiment).

TABLE II: FRR Results of the 51 Legitimate Participants

Mode	FRR of The 51 Legitimate Participants	
	Per user	All Users
2D Facial Recognition Results	0/73 = 0	0/3723= 0
3D Facial Recognition Results	0/146 = 0	47/7446= 0.0063

In order to evaluate the robustness of the approach against targeted misuse three participants were tasked with a series of eight scenarios that map to typical misuse. The eight predefined threat scenarios are:

1) Leaving the location or the chair (no one in front of the camera).
2) Using the keyboard, mouse, or the laptop mouse pad by somebody else.
3) Providing unauthorized help by answering the questions by another individual orally.
4) Fixing the camera and the eye tracker in front of the exam taker and moving the computer to another individual to give unauthorized help (e.g. answering the questions for the rest of the test).
5) Turning the head to the left, right, up, or down (looking for unauthorized help from somebody else).
6) Using a photo of a legitimate/genuine exam taker in front of the camera by another individual (e.g. full color 2D photo from tablet device).
7) Using a photograph as mask with eye holes by an intruder to bypass the eye tracker security.
8) Another individual pretending to be a genuine exam taker.

In the 2D mode, when participants left the location or chair, the camera captures no face in front of it; in addition, the eye tracker lost the eye movement information. While in 3D mode, the camera captured: no face, no head movements, no depth information, and no face expiration information; in addition, the eye tracker lost the eye movement information. In the case of using the keyboard, mouse, or the laptop mouse pad by somebody else, that should be close enough from the legitimate user to do this, the camera captured more than one face in both 2D and 3D modes. If another individual answered the questions orally, the JSGF algorithm captured every spoken sentence in both modes relying on an English dictionary of the most used 10,000 words.

Fixing the camera and the eye tracker in front of the exam taker and moving the computer to another individual was the fourth threat scenario, the result has shown that it was extremely difficult to hold and handle both the camera and the eye tracker or mimic original locations. Therefore, the system captured too many illegitimate photos via both eye tracker and 3D camera security subsystems.

In the case of turning the head to the left, right, up, or down (e.g. looking for unauthorized help from somebody else or reading a book or a text in mobile phone), they have completely been captured by Eye Tracker in the 2D mode, and by Eye Tracker in addition to the 3D camera relying on the head movements parameters that are running in the 3D mode only. When participants have been asked to put a photo of a genuine exam taker in front of the camera (e.g. A full color 2D photo from tablet device), the recognition succeeded for the majority of the samples which have been captured by the 2D facial recognition sub algorithm, however, they have been captured by Eye Tracker anyhow because there is no eye movements in the photos. In the 3D mode, the photos have been captured by Eye Tracker, in addition to the 3D camera via 3D facial recognition sub algorithm, because there are no depth and head movements information in this 2D image. The same can be said for the seventh scenario, which was asking the participant to behave as intruder by using a photograph of the legitimate user as mask with eye holes to bypass the eye tracker challenge, the experiment results have shown that the holes should be much more bigger than the original eyes in order to enable the eye tracker to reach the intruder eyes, nevertheless, this scenario has completely failed in the 3D mode because there are no depth and head movements information. In the last threat scenario a participant has been asked to set on behalf of the legitimate user, in both 2D and 3D modes the system easily highlighted there was an intruder in front of the camera. All results of the previous scenarios are saved in the database and images folders. The following Table III summarizes those results.

TABLE III: RESULTS OF THE 8 THREAT SCENARIOS REPEATED WITH 3 PARTICIPANTS IN 2 MODES

Threat	2D and 3D Facial Recognition (FR) Authentication (Auth.) and Security Capture				
	2D FR Mode Auth.	3D FR Mode Auth.	Head Movement Security	Eye Tracking Security	Speech Recognition Security
1	✓	✓	✓	✓	–
2	✓	✓	✓	✘	–
3	–	–	–	–	✓
4	Most	Most	Most	Most	–
5	Some	Some	✓	✓	–
6	Most	✓	✓	✓	–
7	Most	✓	✓	Most	–
8	✓	✓	–	✘	–

Table IV presents the results of the FAR and FRR of the 1st, 2nd, 6th, 7th, and 8th threats scenarios which are repeated with 3 participants in both modes. The results were zeros for all cases except the FAR of the 6th and 7th scenarios were 0.11 and 0.076 respectively in the 2D facial recognition mode.

TABLE IV: THE FAR AND FRR RESULTS OF ALL PARTICIPANTS IN 5 OF THE THREAT SCENARIOS

Threat	FAR Results for All Users		FRR Results for All Users	
	2D Facial Recognition Auth.	3D Facial Recognition Auth.	2D Facial Recognition Auth.	3D Facial Recognition Auth.
1	0	0	0	0
2	0	0	0	0
6	2/(4+6+8) = 0.11	0	0	0
7	2/(8+9+9) = 0.076	0	0	0
8	0	0	0	0

In addition to the 8 threat scenarios, in the beginning of the experiment, each of those three participants has been asked to log in the exam as intruder by implementing three predefined log in thread scenarios:

1) Log in using another participant's credentials. In this case, the system automatically prevents the intruder from

writing the information in the log in fields; this due to the face recognition procedure which decided that an unauthorized user is trying to log in.

2) Using a full color photo of a legitimate participant to log in. None of the three participants succeeded in this attempt in either 2D or 3D mode.
3) A legitimate participant accompanied with illegitimate participant trying to log in together at the same time to pass the face recognition barrier. The system prevented this threat by recognizing more than one face in front of the camera.

VI. Discussion

Due to its transparency and reliability, Realsense face recognition has been chosen to be the main authentication approach in this e-invigilation system. Beyond the former modality, many of the other proposed biometric modalities can be utilised to enhance the performance. For instance, the low-cost mouse movements and keystroke recognition, which could provide high level of transparency and usability; in addition to their encouraging implementation especially in the case of combining them with other biometric techniques, such as linguistic analysis. However, more work is required on those modalities to get them to the point of being reliable and implementable within this system.

Both eye tracking (left eye, right eye, and the center point of 30 sample every second), and head movement information (Roll, Yaw, and Pitch of 3x25 samples every second) are continuously measured and recorded during the exam time. This could give the opportunity to explore the possibility of proposing these collected data to be used to produce a novel and new behavioral biometric modalities, thereby can be utilized as additional non-intrusive and feasible biometric modalities to improve the authentication performance.

During the experiment, participants' left and right eye images are collected by the custom software, this occurs in the registration stage using the 3D camera, which opens the door for utilizing these images for iris recognition as an additional biometric. Iris recognition offers an interesting opportunity as it is generally considered to be a highly reliable modality with robust performance. However, research has not thoroughly investigated to what extent a partial iris image is useful in providing identity verification and to what degree of performance.

The use of an eye tracker in the experiment was interesting as it is an effective and reliable technique. However, current implementations require a sensitive near infrared camera/sensor. In the current system, both the 3D camera and the Eye Tracker sensor can be utilized for that purpose, which increases our alternatives. Furthermore, the manufacturers have recently released a version of the 3D camera to be built into laptop computers; this offers more usability, reliability, applicability, cost effectiveness, and security. This is very feasible especially with the fourth experimental threat scenario, which prevents the possibility of moving the camera from the computer screen.

In both 2D and 3D modes, the JSGF algorithm captures every spoken sentence relying on an English dictionary. A subroutine called Language Feeding has been developed (as depicted in Fig. 2), which enables the system users to easily change the size/type of dictionary according to their need. Since the recognition algorithm can be applied on any language, the dictionary language is not restricted to English, the system users can choose any language they would like (e.g. Arabic dictionary, Chinese dictionary, or etc.). As long as it captures the speech start and end, then the duration for each spoken sentence can be calculated. Hence, in case of any suspicious action would happen in future, this will give the academic a chance to listen to those short periods rather than the whole session. Furthermore, these captured sentences, can be used to facilitate utilizing transplant linguistic analysis in the final EIEA architecture.

In terms of the operational aspects, the required space on the disk was very satisfactory. The database size including all photos and Realsense DB was 978.1 MB which whilst not a small volume of data is operationally within limits and demonstrates the ability to be scalable (into the order of hundreds (rather than thousands) of simultaneous assessments). Detailed data sizes are shown in Table V, knowing that the size of each exam is 19.1 MB.

TABLE V: Complete Data Sizes

Categorizations	Participants	
	Per User	51 Users
2D Samples	1 Every 4 Seconds (about 73), 2 MB	3723 Samples, 102 MB
3D Samples	1 Every 4 Seconds (about 146), 4 MB	7446 Samples, 204 MB
Audio Recording	12 MB	612 MB
Eye Tracking	0.6 MB	30.6 MB
Head Movements	0.5 MB	25.5 MB
Total Size	19.1 MB	974.1 MB + 4 MB For DB

VII. Conclusion and Future Work

This paper has focused on the development of a more secure, transparent and continuous authentication mechanism for e-assessments. Employing face recognition as the most transparent multimodal (2D and 3D) biometric, and novel security features through eye tracking, head movements, and speech recognition to enable a robust and flexible e-invigilation approach. A multiple scenario experiment involving 51 participants has proven to be very successful in terms of identifying misuse and operationally in terms of the volume of data that is generated and needs processing. In order to evaluate the robustness of the approach to target misuse three participants conducted a series of different scenarios (e.g. another individual pretending to be a genuine exam taker) that map to those misuse cases. The results of the FAR and FRR of the 1st, 2nd, 6th, 7th, and 8th threats scenarios in both 2D and 3D facial recognition modes were 0 for all cases except the FAR of the 6th and 7th scenarios were 0.11 and 0.076 respectively in the 2D facial recognition mode. The next stage of the research will focus upon the development of a complete e-invigilation system, utilizing the results of the current experiment to feed into the academic

subsystem interfaces – to allow academics to quickly identify and judge cases of misuse.

REFERENCES

[1] S. S. Ketab, N. L. Clarke, and P. S. Dowland, "E-invigilation of e-assessments," in *Proc. INTED2015 Conference*, 2015, pp. 1582–1591.

[2] A. Bal and A. Acharya, "Biometric authentication and tracking system for online examination system," in *Proc. 2011 International Conference on Recent Trends in Information Systems*, 2011, pp. 209–213.

[3] E. Flior and K. Kowalski, "Continuous biometric user authentication in online examinations," in *Proc. 2010 Seventh International Conference on Information Technology: New Generations*, 2010, pp. 488–492.

[4] S. Asha and C. Chellappan, "Authentication of e-learners using multimodal biometric technology," in *Proc. 2008 International Symposium on Biometrics and Security Technologies*, 2008, pp. 1–6.

[5] A. Ross and A. Jain, "Information fusion in biometrics," *Pattern Recognit. Lett.*, vol. 24, no. 13, pp. 2115–2125, Sep. 2003.

[6] Y. Levy and M. Ramim, "Initial development of a learners' ratified acceptance of multibiometrics intentions model (RAMIM)," *Interdiscip. J. E-learning Learn. Objects*, vol. 5, p. 19, 2009.

[7] Z. Jorgensen and T. Yu, "On mouse dynamics as a behavioral biometric for authentication," in *Proc. 6th ACM Symp. Information, Comput. Commun. Secur. - ASIACCS '11*, p. 476, 2011.

[8] Y. W. S. Sabbah, "Proposed models for secure e-examination system," Cairo Uiveristy, 2012.

[9] J. A. Hernández, A. O. Ortiz, J. Andaverde, and G. Burlak, "Biometrics in online assessments: A study case in high school students," in *Proc. 18th International Conference on Electronics, Communications and Computers (conielecomp 2008)*, 2008, pp. 111–116.

Salam S. Ketab received a bachelor's degree with very good in computer science from Baghdad University, Iraq, in 2001. He was awarded his MSc with distinction in computer science from Baghdad University, Iraq, in 2005. He is currently a PhD candidate in the Centre for Security, Communications and Network Research at Plymouth University, United Kingdom. His research interests reside in the area of information security, biometrics, and e-learning.

Nathan L. Clarke is a professor in cyber security and digital forensics at Plymouth University. His research interests reside in the area of information security, biometrics, forensics and cloud security. Prof Clarke has over 140 outputs consisting of journal papers, conference papers, books, edited books, book chapters and patents. He is the Chair of the IFIP TC11.12 Working Group on the Human Aspects of Information Security & Assurance. Prof Clarke is a chartered engineer, a fellow of the British Computing Society (BCS) and a senior member of the IEEE. He is the author of Transparent Authentication: Biometrics, RFID and Behavioural Profiling published by Springer.

Paul S. Dowland is a member of the Centre for Security, Communications & Network Research and is the associate head (Computing) at Plymouth University. His interests include network and system security, teaching and learning technologies, and security education. Dr. Dowland is the secretary to the International Federation for Information Processing (IFIP) working group 11.1 (Information Security Management), a Fellow of the Higher Education Authority, a Senior Member of the IEEE, an Honorary Fellow of the Sir Alister Hardy Foundation for Ocean Science and a Fellow of the BCS. He is the author of over 60 papers in refereed international journals and conference proceedings, edited 28 books and co-authored "E-Mail Security: A Pocket Guide" (2010). Further details can be found at the CSCAN website (www.cscan.org/pdowland). Paul can also be followed on Twitter (@pdowland).