Information Sciences Letters

Volume 12
Issue 6 *Jun. 2023*

Article 34

2023

Enhancing Authentication in Online Distant Exams: A Proposed Method Utilizing Face and Voice Recognition

Ahmed T. Resha
Information System Department, Faculty of Computers and Information System, Fayoum University, Fayoum, Egypt\\ Higher Institute of Marketing, Commerce & Information Systems, New Cairo, Egypt, at1380@fayoum.edu.eg

Mohammed A. Azize A. Razek
Faculty of Science, Computer Science Department, Al-Azhar University, Cairo, Egypt, at1380@fayoum.edu.eg

Eslam E. El maghraby
Information System Department, Faculty of Computers and Information System, Fayoum University, Fayoum, Egypt, at1380@fayoum.edu.eg

Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/120634

Enhancing Authentication in Online Distant Exams: A Proposed Method Utilizing Face and Voice Recognition

Ahmed T. Resha[1,2,], Mohammed A. Azize A. Razek[3] and Eslam E. El maghraby[1]*

[1]Information System Department, Faculty of Computers and Information System, Fayoum University, Fayoum, Egypt
[2]Higher Institute of Marketing, Commerce & Information Systems, New Cairo, Egypt
[3]Faculty of Science, Computer Science Department, Al-Azhar University, Cairo, Egypt

Received: 2 Mar. 2023, Revised: 27 May 2023, Accepted: 28 May 2023.
Published online: 1 Jun. 2023.

Abstract: Due to COVID-19 pandemic, face-to-face teaching has been replaced by online education to reduce the risks of spreading the Coronavirus. Online examination is an important asset in the context of online learning to assess students, but observing students during testing and ensuring that they do not engage in misbehavior remains a major issue. Human observation is one of the most common methods when conducting an exam to ensure that students do not perform any unexpected behaviors, by entering the student in a laboratory or hall at the university and observing him throughout the exam period visually and soundly. However, this method is costly and labor-intensive. In this paper, a system is created that monitors students during an online test automatically based on face recognition and voice recognition using a machine learning algorithm. The camera on the student's computer will be used to track the student's facial movements, pupils, and lip movements, monitoring the student's behavior throughout the test, and stopping any unexpected behavior. In this system, there are two parts: facial recognition and unexpected behavior detection. The face was recognized with an accuracy of 98.3%, and unexpected behavior was detected with an accuracy of 97.6%. There is also an opportunity to increase accuracy by improving the quality of the images in the dataset.

Keywords: Face recognition, speech recognition, online exam, machine learning, automatic proctoring, cheating.

1 Introduction

Face-to-face teaching has been substituted by online teaching to reduce the risk of spreading the Coronavirus. This led to the emergence of e-books and open-source training courses through the Internet [1]. The use of the Internet and television in the learning process has become one of the advantages of the technological renaissance, as each of them has an effective role in the distance learning process [2]. Due to the spread of distance education, there must be a means of evaluation for that online test. It must be more effective to be more transparent. Recently, human monitoring has been adopted to be a safe means for monitoring students [3]. Students can be asked to come to the university or school and use the equipped laboratories to monitor the students visually and soundly during the test, and this is the way to ensure transparency and authentication in the test. However, these methods are labor-intensive and costly [4]. Exams can be classified into three types: traditional exams, online exams, and distance exams (D-exams) [5]. In the traditional exam, a set of questions are presented to the students in the classroom, where these questions are fixed for all students, and the test has a fixed start and end time for all students. Online exams, sometimes called e-examination and defined as internet-based questions, created randomly from a set of questions for each student to complete the exam within a certain time limit. In this type of exam, students should attend a classroom to perform the exam. D exams are ways to ask questions of students who are not in a traditional setting such as a classroom. They are randomly generated from a series of questions for each student, with a specific time limit. Additionally, they save or reduce the time required for paper testing, and in addition to saving paper and printing, this type of testing also protects the environment. The D-exam presents new challenges for professors on how to prevent students from cheating. Therefore, designing an online monitoring system using artificial intelligence can automatically detect and minimize malicious student behavior during exams.

There are many types of cheating, some new to the online testing environment and some observed in live testing. These include but are not limited to: Interact with other students via the Internet to obtain answers, or switching between the student who started the test and another person to complete the test instead of him [6]. This study focuses on how to prevent cheating using face recognition to achieve the maximum possible authentication in online exams so that universities and schools can test students without worrying about cheating. Machine learning has been used to monitor students to prevent them from engaging in abnormal behavior (cheating) and to improve the level of distance learning,

*Corresponding author e-mail: at1380@fayoum.edu.eg

so that maximum fairness is reached among the students [7]. There are many methods used to recognize faces and monitor students using machine learning, the most famous of which are CNN, and RNN, but there are also many algorithms that are based on observing students using face recognition such as Support Vector Machine, Eigenface, Dlib's face keypoint detector, Yolov3 altho. There are also ready-made libraries in Python that are used for face recognition, such as OpenCV, MTCNN, and Dlib.

The remains of the study are arranged as follows: Section 2, describes previous work, algorithms used, and researcher results. The motives and goals of the system will be discussed in Section 3. The proposed methodology for creating the system and the explanation of the system will be in Section 4. The main system and how it works and the algorithm that will be used to create the system will be in Section 5. validation and evaluation of the proposed model in section 6, The results are described in section 7. Finally, we summarize the work and its contributions in Section 8.

2 Literature Review

In this section, related works using different machine learning algorithms with different datasets that are used to recognize faces in online tests will be presented.

Akshat [8] used the eye to identify if the user is looking right, left, down, up, or looking at another person in the same room or a note by Dlib's facial keypoint detector to identify the points of the face and used OpenCV For more image processing, also used YOLOv3 trained on the COCO dataset to detect people and mobile phones in the webcam feed. The researcher also used artificial intelligence to integrate four indicators to work together, which are tracking the users' eyes, tracking the mouth if it is closed or open, knowing the number of people in the room, and knowing the location of the mobile phone. The researcher used Dlib and OpenCV to track the pupil of the eye and the movement of the lips, as the distance between the lips is limited to speech, and if the distance between them increases, this indicates that the user is talking to another person. The following cases are detected and reported to the supervisor) If the user is looking to the right, left, up, or down + If the user opens and closes his mouth a lot (talking to another person) + Number of people in the room + Detect impersonation if the user is a person other than the one who started the exam). The researcher explained that in the laptop's quick test of Face detection, the normal version gave 17.5 frames per second while the quantitative version gave 19.5 frames per second. Where he measured the speed and did not measure the accuracy.

Senbo [9] built a system that uses a webcam to monitor the behavior of the examinee and puts the head and mouth condition under the supervision of a set of rules that exist in a logical system to identify and detect cheating. The system starts by taking a picture of the examinee through video and then recognizes the face and mouth. For the face, it is entered into the system to estimate the position of the face based on the CNN to obtain the head angle and then use the registration information to make a judgment if there is abnormal behavior. Face detection is completed using the Adaboost + haar algorithm, AdaBoost is an iterative algorithm. The researcher divided the examinee's face into three XYZ axes so that the nose is the origin of the three axes, as shown in Fig.1. The characteristic points of the face are detected and then the face of the head is compared to the model prepared previously using CNN. DLib is also used to define facial features and to identify characteristic points of the mouth. Since there was no data set, a set of videos was used to implement the system. The natural angle of the examinee's head is 0, and if the angle of the examinee's head is more than 15 degrees, it is considered an attempt to cheat, as the position of the head is from (0, 90) degrees. After testing the system, 90% accuracy was obtained in detecting cheating cases.

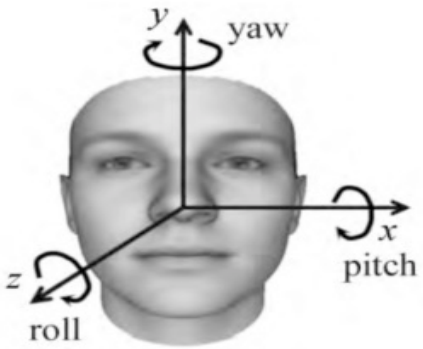

Fig. 1: Human Head Rotation Gesture in the Coordinate System. See [2].

Garg [10] built a system that uses a student's webcam to track his face and behavior during an exam to stop any malicious behavior. This system tracks, marks, and recognizes the student's face using machine language and applies the rules that reference cheating. Viola jones was used to detect the student's face and CNN was used to recognize the

student's face and identify malicious behaviors, using the two makes the system fast and efficient. To monitor the student and his behavior is done in three steps:

1- face detection.

2- Facial recognition.

3- Observing the face, evaluating and interpreting the actions and activities of the student.

The upper left part of the face was used when using the Viola-Jones algorithm, making the system inexpensive and fast. The accuracy of face detection was obtained by 93%, and the researcher stated that it was possible to obtain higher accuracy, but the system achieved the main goal of detecting cheating.

Ganidisastra [11] used four different facial recognition algorithms (LBP- HAAR CASCADE - MTCNN - YOLOFACE) and an additional training process for facial recognition was proposed to save time and cost. The data set was collected by observing students during online lectures to be used to recognize the examinee's personality during exams. The work is divided into five stages, the first three stages are during the online lecture, and the last two stages were during the exam User Registration - Dataset Collecting - Dataset Training - Face Detection - Face Verification. In the first stage, User Registration, the student's face is taken from all directions, as shown in Fig. 2

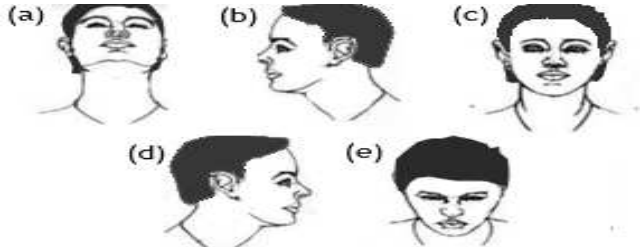

Fig. 2: Initial Face Poses (a) Half Lookup View; (b) Left View; (c) Frontal View; (d) Right View; (e). Half-Bow View. See [4].

The stage of face detection and face embedding takes place in the Facenet model. The face detection, face verification, and training process are developed by using Python and Tensorflow environments. The OpenCV library is used to support image processing and face detection using HaarCascaded and LBP. It was concluded that the deep learning method (MTCNN and YOLO-face) gives better performance than the traditional method (Viola-Jones and LBP). After training and testing the model, an accuracy of 98% was obtained in the training phase. In the testing phase, the accuracy of some images appeared to be 99%, and the researcher did not mention the final result of the accuracy of the model in the testing phase.

Geetha [12] designed the system based on two models (Eigenface- SVM). Eigenface recognizes a face by extracting its features. SVM trains datasets to improve the accuracy of face detection. The system was implemented to perform three main steps (Extracting embeddings from the images - Training the SVM model - Recognizing faces from static images and video frames). The data set was compiled by students studying in students studying at Kongu College of Engineering and the system was implemented in the same college. After testing the system (SVM-based face recognition system) achieves a matching accuracy of about 61% with 50 real-time images in the dataset. The researcher mentioned that the accuracy of the match can be increased if the dataset is increased.

Sukmandhani [13] divided the work into two parts, training, and testing. In the training process, training sets (data sets) are extracted by taking pictures of the user's face through the webcam of the examiner's computer and then performing facial recognition using EIGENFACE. IN Implementation The researcher divided the system into two parts, Backand, in which the administrator can enter the student's data and the faces he uses in the database, and frontend, in which the student's face is matched with his face data that will be used during the test. The researcher created this system to be used on the desktop only, using Python language and the EMGU CV library. He also used the SQL Lite database system as a server to store data in the application. The researcher mentioned that the minimum limit for the user's computer or laptop must be Inter (R) Core (TM) i5-825OU CPU @ 1.60GHz, the Windows 10 64-bit operating system, the screen size is 1366 x 768 pixels, and 8.00 GB RAM.

Yongcun [14] created a system to monitor students during exams This system aims to improve the security of online exams. When the examinee takes the test, at first the examinee in using the username and password, then the system identifies the examinee's face and applies the rules that prevent cheating, which as follows. (When multiple faces are detected on the interface when it is recognized that the examinee does not match the person's face(not the same person), there may be an alternative test situation, during the test, if multiple faces appear, the test will be suspended and send a warning or inform the test administrator). The system identifies five main points in the face, through which the status of

the examinee's face is known and in which direction he is looking. The position of the examinee's head is calculated by using a method based on geometric features because it is simple and convenient, and there is no computational complexity too much, and through which the head position can be known in real-time, and the position of the main feature points of the face is determined precisely according to the MTCNN algorithm. The data set used to test the system was collected from the local faces database from the preschool. The test was also taken at the same school. The system achieved what the researcher wanted to stop the cheating behaviors of the students.

Baseer [15] built a system that authenticates the student during the login and monitors him throughout the exam period by recognizing his face. The system takes a picture of the examinee during login and compares this image with the examinee during the exam. The system also prevents the user from doing multiple logins during the exam. The system also performs some functions are:

Authentication through Image Verification.

Continuous Monitoring.

Window event detection.

Prevention of Copy Paste.

Prevention of Screenshots.

The system works as follows: At first, the student and the professor create an account with their data and photos that are stored in the database to be verified later during the test, and then the image is verified using the unit called Deep Face. It captures eye movements, and these movements are recorded to know the student's position. YOLOv3 was also used to find out the number of people and discover the mobile phone and all the steps are done using the convolutional neural network (CNN).

Masud [16] built a system that works as follows, at first, the system identifies the examinee through the user authentication system. After confirmation and authentication, the system detects the face and then stores it to use the face to verify the user throughout the exam period at regular intervals. The video is recorded throughout the exam period and used in four main axes:

1. Tracking the movement of the eye by following the pupil of the eye, where the student can point with his eye or the student can blink in a certain way that indicates the request for cheating, and all this without moving the head

2. Tracking the head movement, where the student can move his head to try to cheat, as the system determines the angle of the head, and if the student changes the angle of the head, it is considered cheating.

3. Tracking the movement of the mouth, where the student can talk to someone who is not in the range of the camera and try to cheat by calculating the angle of opening the mouth throughout the exam

4. Tracking the student's identity where another person can be present in the camera frame and indicates the existence of a case of outright cheating. The researcher used CNN, a special type of RNN called long-term memory (LSTM), and BiGRU. The researcher collected the data through the volunteers, where he recorded a video and instructed them that cheating can be attempted during the exam and how cheating can be done, then he used these videos in the training phase. With each of the steps of the system (the four mentioned above), the accuracy varies from one to the other, and the highest accuracy is single when tracking the eye movement, and the accuracy is 89.8%, then comes the head movement tracking with 82%, but in the case of combining them, the accuracy is 92.2%. If you combine the four, the accuracy is 97.7%.

Patil [17] built a system that helps female professors put an exam for students online and monitor students throughout the exam period through the following steps:

1- Taking a picture of the student through his webcam and verifying his identity by comparing it with his photos in the database.

2 - Taking records of students' photos every period.

3 - Make recording of sound frequencies every 5 seconds for students.

4- Detection of more than one person in the examination

5- Gaze Estimation: Estimating the student's body position and eye movements

6- The function of cutting, copying, pasting, and taking screenshots is disabled

Gopalakrishnan [18] created a framework that monitors the students during the exam. This framework is based on three

main steps, continuous face detection and recognition, mouth opening and closing, and gaze tracking. Face recognition was done using Open cv. For mouth opening and closing, and pupil tracking he used Dlib. At the end of the test, it will be indicated whether the examinee's behavior is normal or not.

Jia [19] built a system based on machine learning using an online intelligent monitoring system (IOPS), which was based on Python and C languages. The system works as follows. First, use the user's password and username to enter the system. After verifying the password and the username, it takes a picture of the examinee and compares it with his pictures in database then stores the captured image in the database and then the user enters the test page (the main page).

Sridhar [20] built a system through which the student takes the test, and the student is monitored throughout the test period through the following steps:

1- Register the student on the platform using the contact information and a face photo.

2. Provide the latest face photo for each test registration, a database will use the stored photo for verification.

3. When the student starts the test, the monitoring system starts the test.

4. Every period a photo of the student is taken and compared to the photo before the exam. If the pictures do not match, they will also be recorded.

5. Also, the recognition of multiple faces and the absence of any face on the screen are to be documented.

6. if more than one sound is heard It will also be recorded

Kasinathan [21] built a system that monitors students through a webcam and detects any suspicious activity through artificial intelligence algorithms. The system detects the face to detect the presence of more than one person or when the user moves away from the computer using the webcam. It also performs eye tracking to detect when the user is looking away from the screen. It also estimates head position to detect when the user is facing away from the screen. Finally, the system monitors browser activity to detect when a user switches a tab or splits the screen.

3 Motivation and Objectives

Motivation: After the Covid-19 pandemic spread, and it became dangerous to mix with people to avoid the spread of the disease, it became necessary to change the way students are taught, as students are taught remotely through online teaching platforms. [22]. By changing the contents of training courses and the method of online teaching, the way online exams are evaluated must change. There is an important thing about online exams, which is to monitor students permanently because monitoring students and stopping unexpected behavior is an important part of the evaluation so that the educational process is done well [23]. Therefore, there is a need to enhance the way of detecting cheating in online assessments.

Objectives: The general objective of this study is to make online exams more reliable and transparent so that there is equality in exams among different students and test results are more reliable. This is done by establishing a system that monitors the student during the exam by recognizing the face and monitoring his behavior to stop any mischievous practices that the student may perform during the online exam.

4 Proposed Method

This study focuses on enhancing authentication in the online distant exam using face recognition and speech recognition.

Phase 1: The registration phase

Students register for the exam, and the system takes the features of the student's face and stores them.

In phase 2: The authentication phase

Before the exam start, the system detects the face of the student. If the face matches the stored student face in the database, the exam will begin.

In phase 3: Continuous authentication: Each period the system authenticates the face and checks for any cheating. Explanation of the system operation in Fig. 3 and Fig. 4

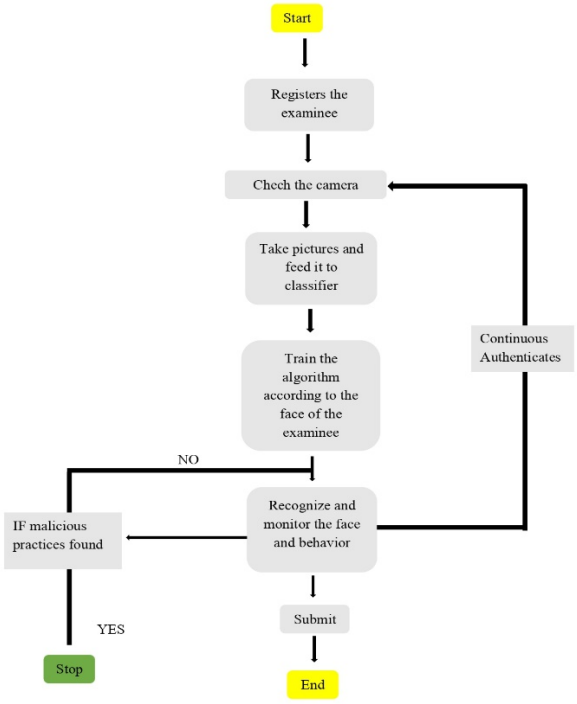

Fig. 3: Flow Chart of the System Working Algorithm

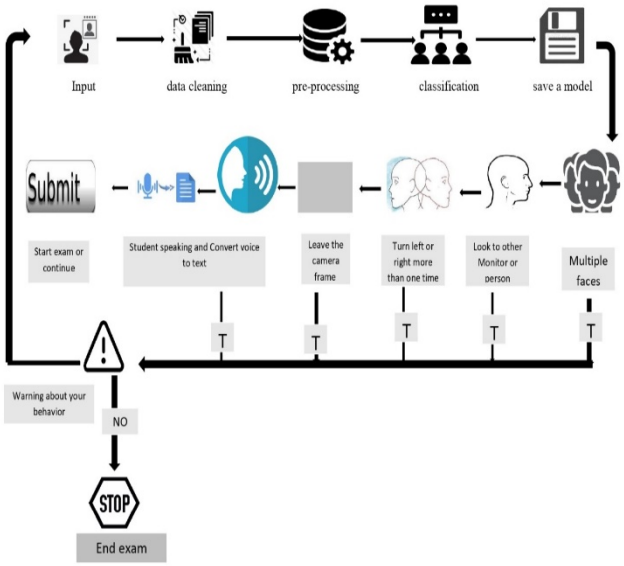

Fig. 4: Block Diagram for Training the Algorithm According to the Face of the Examinee

5 Main System and Testing

System description: The main idea of this system is to use the student's camera and microphone to monitor him throughout the exam and prevent any abnormal behaviors by using machine learning through some steps as follows:

The first step: Recording the data set of students on the system by taking five pictures from five different angles of the student's face, while entering the system. Then store these images in the database so that each student's data is used in their exam.

The second step: The system takes a picture of each student after entering his username and password at the beginning of each exam. Afterward, compares it with the original one from the first step to verify the student's face using an open cv. If the image matches the student's face, the test starts.

The third step: When the test is started, the system will impose the conditions that, if met, unexpected behavior: More than one face (multiple face detection) is detected for each session during the test, leave the camera frame, turn left or right more than once, looking on the monitor computer or other person placed away and speaking during the test. Open cv and Dlib will also be used. If unexpected behavior is detected, the system warns the student and tells him to modify \ behavior and then perform the previous steps again. If the system detects unexpected behavior for the second time in a row, it terminates the test, but if it does not find unexpected behavior, the test will continue. The system repeats this step throughout the test and ensures that the test rules are not violated until the student has finished the test.

In the third step, the work of the system was divided into five basic stages that are carried out continuously throughout the testing period in parallel.

The first stage is to recognize the student's face, where a picture is taken through the student's webcam, then an encoded face is created and compared to the student's face in the dataset to ensure that the student is the one who solves the test. In this stage, the face recognition library was used to recognize the face, and an open cv was used to create the encoded face.

In the second stage, two of the aforementioned conditions are applied, namely, More than one face (multiple face detection) is detected for each session during the test and leave the camera frame. this is done through open cv to detect the location of the face in the camera frame and using DLIB to detect the number of faces in the camera frame. if the number of faces is less than one, this means that the student left the camera frame, and if the number of faces is more than one, this means multiple face detection.

In the third stage, two conditions are met, namely, turning left or right more than once, looking at the monitor computer or other person placed away, tracking the pupil of the eye, and knowing if the student is looking outside the camera frame. This is done by using DLIB to track the pupil of the eye and determine The exact location of them and using Open cv to locate the face.

In the fourth stage, the last condition is met, which is speaking during the test, and this is done by tracking the movement of the lips, and if the lips are open or closed by knowing the distance between the lips. open cv was used to detect the location of the face and lips and determine the distance between the lips.

In the fifth stage, if the student speaks, whether there is cheating or not, it is confirmed by using the student's microphone, converting the voice into text, and comparing the text with the text in the test, using the speech recognition library.

System Testing: the system was tested with the help of students the Higher Institute of Marketing, Commerce and Information Systems in the First Settlement in Cairo, Egypt, by collecting approximately 1,000 photos from the institute's students and graduates to be Dataset, then testing the system on 600 students enrolled in the institute, and this was done throughout December 2022. The system has proven its effectiveness, and this will be illustrated by the following results.

6 Validation and Evaluation of the Proposed Method

Validation and evaluation of a data classification model are one of the most important steps to building model steps. The purpose of validation is to estimate the level of performance that may be expected from models generated by the modeling process.

The main objective of building the classification rule is to classify the largest possible number of future units. There are several criteria available to evaluate a set of classification rules. simplest and the most frequently used criterion is confusion matrix [24]. The confusion matrix is N×N, where N is the number of target values (classes). The performance of such models is commonly evaluated using the data in the matrix. The following table displays a 2×2.

Table 1: Confusion Matrix for Two Classes (Positive and Negative)

Confusion Matrix		**Target**	
		Positive	**Negative**
Model	**Positive**	TP	FN
	Negative	FP	TN

As can be seen in Table 1, True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN),

are the four different possible outcomes of classification prediction for a two-class case with classes “1” (“yes”) and “0” (“no”). A False Positive is when the outcome is incorrectly classified as “yes” (or “positive”), when it is in fact “no” (or “negative”). A false negative is when a result is positive while it is incorrectly classified as negative. True Positives and True Negatives are obviously correct classifications. Below formulae were used to calculate accuracy, sensitivity (Recall), precision and F1 score.

Accuracy, which is the proportion of true results (both true positives and true negatives) in the population, can be obtained by the following formula:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Sensitivity or Recall (equivalent to the true positive rate) It is the percentage that the test detects well when the cases are positive. In other words, when tested on positive individuals, sensitivity measures how effective the system is. When sensitivity is 1, the test is ideal for positive individuals, equivalent to a random draw when sensitivity is 0.5. The test reverses performance if sensitivity is less than 0.5, in which case the rule is reversed to maximize so that sensitivity is higher than 0.5(provided that this does not affect the specificity). The mathematical definition is given by:

$$\text{Recall} = \frac{TP}{TP \times FN}$$

Precision is the ratio of correctly predicted positive observations to the total predicted positive observation. High precision relates to the low false positive rate [25].

$$\text{Precision} = \frac{TP}{TP \times FP}$$

The F1 Score is the weighted average of Precision and Recall. Therefore, this score takes both false positives and false negatives into account. Intuitively it is not as easy to understand as accuracy, but F1 is usually more useful than classification accuracy, especially if we have an uneven class distribution. If the cost of false positives and false negatives are very different, it is better to look at both Precision and Recall.

$$\text{F1 Score} = \frac{2 \times \text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}}$$

7 Result

The proposed method was conducted for 600 students and divided into two parts: recognizing the student’s face and discovering unexpected behavior.

In the first part, which is recognizing the student's face, the students were divided into two groups. We have previous pictures of their faces, numbering 480 students, and for the other 120 students, we did not have pictures of their faces. In the first group, 473 students whose faces were recognized by the system the first time, and 7 students were not recognized. After reviewing the stored photos of the seven students, it was found that the quality of the stored photos was poor. After adding the photos of these seven students, the system recognized their faces.

In the second group, most of the faces were not recognized, and they numbered 117 students. As for the three students who were identified, it was found that the recognized pictures are of poor quality and are similar. Therefore, it is best to review all students' photos before taking the test. Table 2 shows the true positive, true negative, false positive, and false negative.

Table 2: Face Recognition Ratios

Sub elements	**face recognized**	**Not recognized**
Face exists	TP 473	FN 7
not exist	FP 3	TN 117

Recall = 94.6%

Precision = 99.36%

Accuracy = 98.33%

F-measure = 96.92 %

The second part is discovering unexpected behavior. The students were also divided into two groups the first group, 480 students, where the students try to behave in unexpected behavior and implement the five conditions, as we mentioned earlier, and the second group 120 students, and they do not perform any unexpected behavior, and the results are as shown in Table 3.

Table 3: Unexpected Behavior Ratios

Sub elements	**Recognized Unexpected behavior**	**Unexpected behavior Not recognized**
Unexpected behavior exist	TP 1404	FN 36
Unexpected behavior does not exist	FP 7	TN 353

Recall = 97.5%

Precision = 99.5%

Accuracy = 97.6%

F-measure = 98.4%

8 Conclusion

There are three types of exams: traditional, online, and distance exams. The online distance exam is the main concern of this study, as it plays an important role in the E-learning system, to detect cheating to achieve equality in the evaluation. The professor must devise some control procedure to assure the validity of the purported identity of a student who completes and submits online exams and other assignments. Therefore, this research, a system was created to perform remote electronic tests using the Python language using DLIB, Open CV, Face Recognition Library, and Speech Recognition Library. The system relied on basic steps, namely: 1) Recognizing the faces of students to verify the identity of the examining student, whether before the start of the exam or throughout the exam period. Its effectiveness has been proven with an accuracy of 98.66%. 2) count the number of students in front of the camera; this part is 100% accurate, 3) track the pupil of the eye to determine the student's point of focus during the test; accuracy was 98.16%, 4) the student's lips are moved to indicate whether or not they are speaking, and this part's accuracy was 99.1%, and 5) with a 98.66% accuracy rate, text conversion from any speech using voice recognition.

Conflict of interest

The authors declare that there is no conflict regarding the publication of this paper.

References

[1] Abdelrahman, A., Soliman, T. H. A., Taloba, A. I., & Farghally, M. F. A Predictive Model for Student Performance in Classrooms Using Student Interactions With an eTextbook. *arXiv preprint arXiv:2203.03713*, (2022).

[2] Azza Mostafa, Recent Trends in the Research of Television Role in Teaching and Learning (2010-2020), VPROCTOR. ISPRS Annals of Photogrammetry, Remote Sensing & Spatial Information Sciences (2022).

[3] Guney, C., Akinci, O., & Çamoğlu, K. ARTIFICIAL LEARNING-BASED PROCTORING SOLUTION FOR REMOTE ONLINE ASSESSMENTS:" VPROCTOR". ISPRS Annals of Photogrammetry, Remote Sensing & Spatial Information Sciences, (2021).

[4] Li, H., Xu, M., Wang, Y., Wei, H., & Qu, H. A visual analytics approach to facilitate the proctoring of online exams. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems , 1-17, (2021).

[5] Bawarith, R., Basuhail, A., Fattouh, A., & Gamalel-Din, S. E-exam cheating detection system. International Journal of Advanced Computer Science and Applications, 8(4), (2017).

[6] Ebaid, I. E. S, Cheating among accounting students in online exams during Covid-19 pandemic: exploratory evidence from Saudi Arabia. Asian Journal of Economics, Finance and Management, 9-19, (2021).

[7] Aldahiri, A., Alrashed, B., & Hussain, W, Trends in using IoT with machine learning in health prediction system. Forecasting, 3(1), 181-206, (2021).

[8] Akshat Shrivastava, Ashray Parmar, Anurag Sen, Ayush Soun, Suresh Kapare, Face Recognition Classification in Proctored Exam. in 2020 INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT), (2020).

[9] Hu, S., Jia, X., & Fu, Y, Research on abnormal behavior detection of online examination based on image information. In 2018 10th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC) **Vol**. 2, 88-91, (2018).

[10] IEEE. Garg, Kavish, et al. "Convolutional neural network-based virtual exam controller." 4th International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, (2020).

[11] Ganidisastra, A. H. S., & Bandung, Y, An incremental training on deep learning face recognition for m-learning online exam proctoring. In 2021 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob) 213-219, (2021).

[12] Geetha, M., Latha, R. S., Nivetha, S. K., Hariprasath, S., Gowtham, S., & Deepak, C. S, Design of face detection and recognition system to monitor students during online examinations using Machine Learning algorithms. In 2021 international conference on computer communication and informatics (ICCCI) . 1-4. IEEE, (2021).

[13] Sukmandhani, A. A., & Sutedja, I, Face recognition method for online exams. In 2019 International Conference on Information Management and Technology (ICIMTech) , **Vol**. 1, 175-179, (2019).

[14] Yongcun, W., & Jianqiu, D. Online Examination Behavior Detection System for Preschool Education Professional Skills Competition Based on MTCNN. In 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE) , 999-1005, (2021).

[15] K. K. Baseer, M. Jahir Pasha, A. V. Rama Krishna Reddy, Kamarthi Rekha, M. Shaheda Begum, Sandhya E, Smart Online Examination Monitoring System.. in 2022 JOURNAL OF ALGEBRAIC STATISTICS 13.3, (2022).

[16] Masud, M. M., Hayawi, K., Mathew, S. S., Michael, T., & El Barachi, M, Smart online exam proctoring assists for cheating detection. In Advanced Data Mining and Applications: 17th International Conference, ADMA 2021, Sydney, NSW, Australia, February 2–4, 2022, Proceedings, Part I, 118-132, (2022).

[17] Prayag Ashok Patil, Abhimanyu Dilip Jha, Rishi Sunil Maheshwari, Mrityunjay Pandey, Online Exam System with Secured Approach. in 2021. International Journal of Research in Engineering, Science and Management 4.12 87-89, (2021)

[18] Gopalakrishnan, K., Dhiyaneshwaran, N., & Yugesh, P. Online proctoring system using image processing and machine learning, (2022).

[19] Jia, J., & He, Y, The design, implementation and pilot application of an intelligent online proctoring system for online exams. Interactive Technology and Smart Education, 19(1), 112-120, (2022).

[20] Sridhar, A., & Rajshekhar, J. S, AI-integrated Proctoring system for online exams. Journal of Artificial Intelligence and Capsule Networks, 4(2), 139-148, (2022).

[21] Kasinathan, V., Yan, C. E., Mustapha, A., Hameed, V. A., Ching, T. H., & Thiruchelvam, V, ProctorEx: An Automated Online Exam Proctoring System. Mathematical Statistician and Engineering Applications, 71(3s2), 876-889, (2022).

[22] Ewing, L. A., & Cooper, H. B, Technology-enabled remote learning during COVID-19: perspectives of Australian teachers, students and parents. Technology, pedagogy and education, 30(1), 41-57, (2021).

[23] Jena, P. K, Online learning during lockdown period for covid-19 in India. International Journal of Multidisciplinary Educational Research (IJMER), 9, (2020).

[24] Fawzy, H., Rady, E. H. A., & Fattah, A. M. A., Forecasting time series using a hybrid ARIMA-ANN methodology. J. Appl. Probab. Stat, 16, 95-106, (2021).

[25] Alrweili, H., & Fawzy, HForecasting crude oil prices using an ARIMA-ANN hybrid model. J Stat Appl Probab, 11(3), 845-855, (2022).