ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 8, August 2024

Monitoring Student Actions during Online Testing Using Machine Learning

[1] M. Serik, [2] D.Tleumagambetova, [3] A. Kintonova, [4] N. Duissegaliyeva

[1] [2] [3] [4] L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
Corresponding Author Email: [1] serik_meruerts@mail.ru, [2] danara1310@gmail.com, [3] aliya_kint@mail.ru, [4] nasipzhan@mail.ru

Abstract*— As a result of the widespread spread of education and assessment in the internet system, ensuring the integrity of online testing has become a major problem for educational institutions. Traditional proctoring methods may not be possible or scalable in an online environment, requiring the use of automated approaches. Machine learning offers promising opportunities to track students ' actions during online testing, allowing them to identify suspicious behavior that indicates academic dishonesty. This article provides a comprehensive overview of the process of monitoring the actions of students during online testing using machine learning methods. The process includes several basic steps: data collection, feature acquisition, data preprocessing, sample selection, training, evaluation, deployment, and feedback loop. Data collection involves various aspects of student interaction during online tests, including timestamps, mouse movement, keystrokes, and browser interaction. The research work was considered by students of the educational programs "6B01511-Informatics", "7M01511-Informatics", "7M01525-STEM education", "8D01511-Informatics" of the Eurasian National University named after L. N. Gumilyov. As a result, using machine learning to monitor students ' actions during online testing is a promising way to improve the integrity and security of online assessments while reducing the burden on teachers and administrators.

***Index Terms*—machine learning, education, online learning, detection, recognition.**

I. INTRODUCTION

In recent years, online education has become an integral part of the educational process, especially in the context of global events such as the COVID-19 pandemic. Online testing is an important tool for assessing students' knowledge, but at the same time, new challenges arise related to ensuring the honesty and reliability of the results. To overcome these issues, a consideration-checking framework has been created that can give data about understudy engagement levels amid online classes. These frameworks utilize cutting-edge apparatuses such as video conferencing, computer vision, artificial intelligence, machine learning, and information analytics. Most of them utilized two or more components among facial highlights and expressions, head developments, eye looks, discourse, and voice, as well as information on learner intelligence and exercises inside an internet learning stage to survey learner consideration levels. Numerous cutting-edge observing frameworks have critical confinements that require advanced investigation and advancement. Essentially, these frameworks depend on facial expressions, eye developments, and head introduction to survey students' considerations, raising concerns almost exactly. In our research work, not only human face recognition but also additional sounds and telephone usage possibilities are considered to create academic reality during online learning.

The purpose of this research is to develop a system that can automatically detect suspicious behavior of students during online testing to prevent cheating and ensure the integrity of the assessment.

To achieve this goal, it is necessary to solve the following tasks:

- Collect and preprocess data on student actions during online testing.
- Analyze the data and identify the signs that are most informative for detecting fraudulent activities.
- Develop and train a machine learning model to automatically detect suspicious student activities.
- Evaluate the performance of the developed system on real data and compare it with existing methods.

II. LITERATURE REVIEW

In recent years, monitoring student performance during online testing using machine learning methods has attracted significant research attention. In this review, we will look at several key studies on this issue.

H. Ali's research paper, "Cheating Detection in online exams using machine learning" proposes a machine learning-based method for detecting student cheating behavior during online testing. The authors analyzed various features, such as mouse movement patterns, time intervals between answers, and the number of attempts to answer one question. The developed model demonstrates high accuracy and reliability of fraud detection [1].

In the article "Using Machine Learning Techniques to Detect Cheating in Online Exams" by N. Patel, the authors present a system based on machine learning techniques to automatically detect cheating during online testing. The focus is on analyzing keystroke and mouse movement patterns and using neural networks to identify abnormal behavioral patterns among students [2].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 8, August 2024

G. Kasliwal's research paper "Cheating detection in online examinations" proposes an improved method for detecting cheating in online tests using machine learning algorithms. The authors propose a hybrid approach that combines different types of features, such as data on student performance during testing and characteristics of the test itself, to improve the accuracy and reliability of cheating detection [3].

In the article " A systematic review on machine learning models for online learning and examination systems " by S. Kaddoura, the authors present a method for monitoring student activity during online testing based on machine learning methods. Particular attention is paid to the analysis of patterns of time intervals between student actions and the use of classification models to identify abnormal behavioral patterns [4].

In general, the presented studies indicate the widespread use of machine learning methods in the field of monitoring student actions during online testing. They demonstrate the effectiveness and reliability of various approaches to detecting cheating and monitoring student activity to improve the integrity and validity of testing in online education.

III. METHODOLOGY

During online testing using machine learning, theoretical and empirical research methods are used to control students' actions.

Records of student actions during online testing, such as mouse movements, keystrokes, response times, and other metrics, are used as input data. Data is collected in a developed online educational platform. Next, we clean the data from noise, fill in missing values, and scale the features to ensure that each contributes equally to the model. The data identifies signs that may indicate fraudulent activity, such as unusual mouse movement patterns, an excessive number of answer attempts, or response times that do not match the difficulty of the question. Various machine-learning models are used to detect suspicious student activities. Models are trained on labeled data, then their performance is assessed using quality metrics such as precision, recall, and F1-measure [5]. To improve the generalization ability of the model, cross-validation and hyperparameter tuning methods are used. The developed system is integrated into an online testing platform and tested on real data. System performance is monitored in real-time and adapted to changing conditions.

IV. RESULTS AND DISCUSSION

The first step was to implement a real-time facial recognition system using a Python script. Face recognition mainly consists of four stages: face detection, normalization, feature extraction, and finally the face is recognized for identification. Face recognition was implemented using a convolutional neural network (CNN), which involves passing a filter over an image multiple times and determining where parts of the image correspond to specific patterns. During the experiment, when comparing face recognition methods EigenFaces, Fisherfaces, and LBPH, it was revealed that the Fisherfaces algorithm has a better success rate, LBPH has a slightly lower success rate than Fisherfaces, while at the same time, they both maintain a constant level of accuracy. LBPH had a lower probability of success with a small data set, however when the data set was increased, the probability of success increased [6]. The EigenFaces method had a nearly constant success rate, even though the dataset size was very small or very large. For this work and for implementing a proctoring system with appropriate sets, the Fisherfaces method performed much better than other methods. In this regard, for the further creation of the pipeline, the Haar OpenCV detector and the Fisherfaces method will be used for recognition. Modern system is necessity and the use of such systems for continuous monitoring of digital exams, including pre-employment exams, will soon become the norm [7].

The next step was to develop an anti-spoofing system to implement academic integrity. The implementation of an anti-spoofing system in facial recognition aims to detect deception attempts when an attacker uses fake facial images, such as photographs or videos, to bypass the facial recognition system. To implement the anti-spoofing system, a dataset was created containing genuine facial images and fake images such as photographs, pictures, and videos, and the data was divided into training and testing sets. Training an anti-spoofing model requires both genuine and fake images and their class labels. The neural network method was chosen to detect fake images. The dataset collected approximately 300-350 photographs per user. Subsequently, further work was carried out to prevent organized attacks during the system's authentication process (Figure 1).

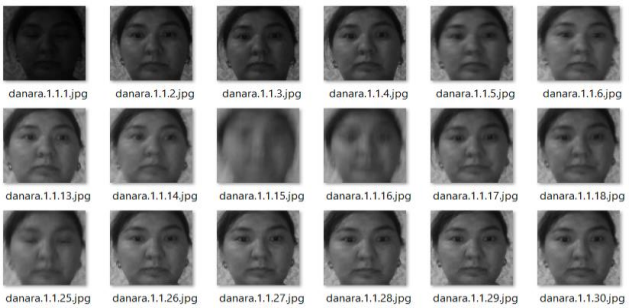

Fig. 1. Database

As a next step, the detection of eye movements was considered. Within the first portion, we are going examine the eye angle proportion and how it can be utilized to decide in case an individual is blinking or not in a given video outline. From there, we are going to compose Python, OpenCV, and dlib code to perform facial point of interest discovery and identify flickers in video streams. In terms of blink detection, we are only interested in two sets of facial structures - the eyes.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 8, August 2024

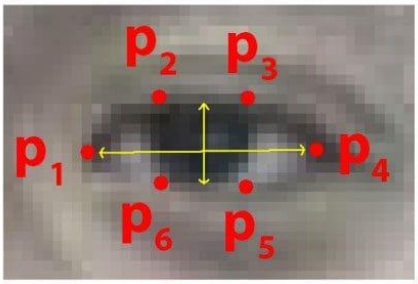

Fig.2. The facial landmarks associated with the eye

Each eye is represented by 6 (x, y)-coordinates, starting at the left corner of the eye. Where p1, …, p6 are 2D facial landmark locations. The numerator of this equation computes the distance between the vertical eye landmarks while the denominator computes the distance between horizontal eye landmarks, weighting the denominator appropriately since there is only one set of horizontal points but two sets of vertical points [8].

And eventually we'll look at object recognition. Object recognition refers to the identification of objects from digital images. Object classification can be divided into three tasks: object localization, image classification, and object detection. Object segmentation is the final task of object recognition. R-CNN, YOLO, SSD, RetinaNet, and ImageNet are popular deep learning-based object recognition models. We chose the YOLO object recognition model. The YOLO algorithm takes an image as input and then uses a simple deep convolutional neural network to detect objects in the image [9]. The first 20 convolution layers of the model are pre-trained using ImageNet by plugging in a temporary average pooling and fully connected layer. Then, this pre-trained model is converted to perform detection since previous research showcased that adding convolution and connected layers to a pre-trained network improves performance. YOLO's final fully connected layer predicts both class probabilities and bounding box coordinates. YOLO divides an input image into an S × S grid [10]. If the center of an object falls into a grid cell, that grid cell is responsible for detecting that object. Each grid cell predicts B bounding boxes and confidence scores for those boxes. These confidence scores reflect how confident the model is that the box contains an object and how accurate it thinks the predicted box is. The YOLOv3 model was employed in our suggested approach. This model was trained on pictures from the COCO dataset with different sizes and includes 80 labels such as laptop, mobile phone, and book.

To implement our proposed system, we use OpenCV for image processing, and the dlib package for machine learning. We continuously proctor the exam system and concurrently implement each of the methods. Several experiments have been carried out to determine its efficiency, and the results are presented below. We used the confusion matrix, which is a technique for summarizing the performance of a classification algorithm.

Table 1. Data identification

	Predicted No	Predicted Yes
Actual No	TN=635	FP=81
Actual Yes	FN=78	TP=245

Where TP-True Positive, the sample is correctly identified.

TN-True Negative, the sample is not identified.

FP-False Positive, the sample, which is not in the database is identified.

FN-False Negative, an error where the sample in the database is not detected.

$$Accuracy = \frac{TN + TP}{Total\_number\_of\_instances} = 84.69 \quad (1)$$

Therefore, the performance of the model under consideration is 84.69%.

V. CONCLUSION

This article presented a technique for monitoring student actions during online testing using machine learning. The developed system is capable of automatically detecting suspicious actions by students, which improves the fairness and reliability of testing results. Further research can be aimed at improving system performance and expanding its functionality.

Research works were considered by students of the educational programs "6B01511-Informatics", "7M01511-Informatics", "7M01525-STEM education", "8D01511-Informatics" of the Eurasian National University named after L.N. Gumilyov. The informational education portal includes only test tasks on the subject of machine learning. It is planned to introduce other subjects in the future. In addition, in the future, looking out the window, communicating with people, paying attention to other directions, moving, etc. It is planned to introduce activities that determine different human behavior. We only use the yolov3 model because it has fast object detection algorithms, although there are several other ways to detect objects. In the following study, we will focus on such approaches and compare them with the current proposed system.

VI. ACKNOWLEDGMENT

This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP19677348 "Development educational portal on machine learning as an artificial intelligence's direction to improve the Informatic teacher's training in education globalization").

REFERENCES

[1] K.K. Rehab and Z.H. Ali, "Cheating Detection in online exams using machine learning," Journal Of AL-Turath University College, vol. 2, iss.2, pp. 35-41, 2023.

[2] N.A. Patel and R. Patel, "A survey on fake review detection using machine learning techniques," 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, pp.1-6, 2018.
[3] G. Kasliwal, "Cheating detection in online examinations," 2015.
[4] S. Kaddoura, D.E. Popescu and D. Jude, "A systematic review on machine learning models for online learning and examination systems," PeerJ Computer Science, 8, 2022.
[5] S.K.Agrawal, "Metrics to Evaluate your Classification Model to take the right decisions", 2024. [Online]. Available: https://www.analyticsvidhya.com/blog/2021/07/metrics-to-evaluate-your-classification-model-to-take-the-right-decisions/
[6] N. Delbiaggio, A comparison of facial recognition's algorithms, 2017. [Online]. Available: https://core.ac.uk/download/pdf/84801048.pdf
[7] M. Anggo and L. Arapu, "Face recognition using fisherface method," Journal of Physics: Conference Series, Vol. 1028, No. 1, p. 012119, 2018.
[8] I. Ahmad, I., F. AlQurashi, E. Abozinadah and R. Mehmood," A novel deep learning-based online proctoring system using face recognition, eye blinking, and object detection techniques," International Journal of Advanced Computer Science and Applications, vol. 12(10), 2021.
[9] P. Jiang, D. Ergu, F. Liu, Y. Cai and B. Ma, "A Review of Yolo algorithm developments," Procedia Computer Science, 199, pp. 1066-1073, 2022.
[10] C. Liu, Y. Tao, J. Liang, K. Li and Y. Chen, "Object detection based on YOLO network," In 2018 IEEE 4th information technology and mechatronics engineering conference (ITOEC), pp. 799-803, December 2018.