Seetha Lakshmi R, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

VIGILFY Real Time Exam Surveillance Tool

[1]Seetha Lakshmi R, [2]Vijaya harshitha R, [3]Saranya P
Computer Science and Engineering,
Francis Xavier Engineering College, Tirunelveli – Tamil Nadu – India

Abstract- In this project, it has been proposed the use of AI and ML for the purposes of real-time surveillance and detection of malpractices in an online examination system. As there could be many ways that a student may try to commit unfair practices, such as utilizing external aid, multiple candidates, or any other suspicious browsing activity; therefore, the current methodologies do not guarantee the absolute correctness and integrity of an examination. Video analysis using AI and monitoring browser activity have been combined to analyze continuous flows of information in order to detect anomalies like non-attendance, multiple people being in view, and distracted attention. The identified violations are marked and saved, and then the corresponding clips are selected to create reports that help the educators review the candidate's actions during the test. It will help minimize the necessity for manual control and will ensure higher precision and consistency. The purpose of the project is to enable real-time detection and analysis of any exam activities by means of monitoring with intelligence.

Keywords:AI, Machine learning, Online Examination Security , AI Proctoring and Computer Vision , Real-Time Monitoring , Behavioral Analysis , Browser Tracking , Anomaly Detection , Automated Surveillance , Video Processing , Pattern Recognition.

I. INTRODUCTION

Due to increase of online tests owing to increase in distance education, there has been a loss of direct human vigilance and therefore fairness and integrity of the examinations face risks. One possible method for academic dishonesty by students is use of tab-switching, unauthorized material and even external invigilation which can't be identified using traditional methods. Such actions are masked in normal activities and hence traditional invigilation is not very effective. Students can easily use internet enabled device and therefore face further risk of misconduct. This demands for an intelligent invigilation system that secures the tests. AI surveillance can perform detection of malicious actions by using real-time surveillance of web and webcam which provides higher accuracy.

Monitoring Difficulty: The conventional methods used for monitoring online examinations fail as a result of the perpetual aspect involved in taking online tests without any form of physical monitoring. These types of acts, camouflaged amidst other student actions, can be challenging to identify because they occur during the examination period.
Global Impact of Online Examination Systems Due to the ease of internet connectivity through internet-capable gadgets and other internet-based platforms, students have access to numerous forms of external help and materials. This means there is an increased risk of misconduct in online examinations.

Scale of Content on Online Examinations: Monitoring Scale for Online Examinations: It gives a small peek at how many students are taking part in online examinations at one time, making it impossible to detect any violation of rules without resorting to any automation since the numbers are too high. Real-time monitoring is necessary since

cheating should not be tolerated under any circumstances.

Online Exam Environment: There are many exam activities that occur in digital spaces in which students have access to different sources of information in their exams, making it hard to monitor any malpractice or regulate it.

Increased Accuracy: The use of AI eliminates human error in detecting any suspicious activities since it uses uniformity and impartiality in its evaluation, hence enhancing the precision of monitoring.

Efficiency : The deployment of AI makes the process of detection automated, which increases efficiency in monitoring, as it allows for constant surveillance throughout the day.

Real-Time Detection: Artificial Intelligence-enabled software facilitates the detection of suspicious activity during online tests in real time, allowing for alerts to be generated immediately for any violations like abnormal behavior or any suspicious activity. This enables one to take immediate action in case malpractice occurs.

Adaptability: Since students could always try something new in order to cheat, the software is continuously improved by AI algorithms to adapt to any changes in patterns, thereby increasing effectiveness against any form of cheating.

Coverage: The software enabled by AI technology is capable of detecting suspicious activity among several students at once. This is due to the fact that an exam conducted online might include several candidates sitting from different locations and using different types of gadgets.

II. LITERATURE REVIEW

Historically, when it comes to online assessment proctoring, methods like manual invigilation and recording video were the primary ways to monitor student behaviour. The previous versions of these systems provided no real-time capabilities and required a large amount of human work. The introduction of webcam-based monitoring proved ineffective at reliably identifying deceptive behaviour, and browser monitoring methods did not provide complete validation without the presence of visual evidence.

- Video/audio recording and manual supervision offer no real-time detection; they need to be reviewed by a person.
- Webcam-based monitoring was ineffective at accurately identifying dubious activities.
- Browser monitoring does not ensure the integrity of an exam without visual confirmation.

Advancement in computer vision technology has created substantial enhancements in increasing monitoring of students at online examinations. The use of real-time video processing provides immediate detection of questionable behaviours while producing a greater amount of accurate information about monitored individuals thanks to continuous frame analysis.

- Computer vision can report behaviours such as not having a face in the frame, having multiple faces in front of the camera, or being distracted from their task and will provide real-time video processing capability for monitoring students throughout the exam process.
- Continuous monitoring allows for an uninterrupted examination using video monitoring systems.
- Lightweight frameworks like OpenCV make the development and use of computer vision technologies easy.

Machine-learning solutions have added greater value to automated proctoring. Through supervised or rule-based classification of student behaviour, these systems can differentiate between acceptable and unacceptable activity. The integration of browser tracking with video monitoring represents a comprehensive approach to increasing security against cheating.

- Supervised and rule-based methods classify student behavior effectively.

- Detection models improve accuracy in identifying suspicious activities.
- Integrated systems combine video and browser monitoring for better exam security.

III. PROPOSED METHODOLOGY

The implementation of the VIGILFY system is done using a systematic procedure beginning with user verification, setting up the examination, and real-time examination monitoring. During the period of the examination, data will be collected from both the webcam and the activity from the browser.

- User verification and scheduling of the examination constitute the main inputs for the VIGILFY system.
- The data collection process in this case involves capturing webcam frames and browser activities.
- Data pre-processing makes sure that the frames are extracted and the examination process initiated correctly.

Suspicious behavior of the candidate during the examination will be identified using image processing methods. The video stream from the webcam can be analyzed in real time and it would be detected if there is no presence of a face, presence of multiple faces, and unusual movements. Image processing on the frames will allow for monitoring of the candidate throughout the entire examination.

- Object detection models locate and classify items associated with drug sales.
- Image segmentation basically aids in the extraction of main regions of interest within images for further scrutiny.
- Some of the feature extraction techniques used are SIFT and these refer to Scale-Invariant Feature Transform. It improves object recognition.

Machine learning models, in particular deep learning architectures such as ResNet and VGGNet, become a big aspect of the visual data analysis. These models are trained with large amounts of labeled datasets and can be finely tuned for specific detection tasks[5]. Additionally, support vector machines (SVMs) and random forest classifiers handle text-based classification tasks.

- Deep learning models excel in processing complex visual patterns.
- SVMs and decision trees classify text data for identifying language patterns.
- Hybrid models leverage both image and text data for a holistic analysis.

Image recognition models can analyze visual aspects from different kinds of data, to determine malicious items. Social media feeds are accessed via API, then the analyzed contents are fed to models that use image recognition to determine the presence of any malicious items, and the outcome is logged into the database. In case of a malicious finding, an alert is immediately triggered and authorities are notified, providing them with means for immediate action.

- Social media data: the system uses a robust ingestion system to handle high volume traffic of data from multiple sources.
- Image recognition models: analyze visual features from various data types to recognize malicious items.
- Results are stored for further analysis and alerts notify relevant authorities.

IV. IMPLEMENTATION

During the implementation phase, the system is monitored and validated using real-time data. To make webcam input more reliable, OpenCV-based computer vision techniques like frame processing and threshold-based detection are used. To make sure that monitoring works well, system performance is measured by how accurate the detection is, how quickly the response time is, and how many alerts are sent out.

Using big labeled datasets to train models makes them more accurate.

- Continuous frame analysis makes it easier to find things.

- Detection based on thresholds helps cut down on false alarms and makes sure everything is the same.
- The effectiveness of real-time monitoring can be measured by its accuracy and response time.

There are a few steps in video analysis, starting with capturing frames and preprocessing. Then, the algorithms for face detection and tracking are used to find behaviors that seem suspicious, like being absent, having more than one face, or being distracted during the test. The results are written down and kept for later use

- Video frames are taken, resized, and processed so that they can be looked at
- Behaviors that are found are put into groups and given violation tags.
- The results of detection are saved with timestamps for later review.

The system's success depends on how well it can detect things. Using metrics like the detection rate and the false alert rate to check reliability is part of evaluating system performance. We test real-time performance by running the system during live exam sessions to make sure it can monitor and send out alerts on time.

UUBetter monitoring accuracy means higher detection rates.

- Better monitoring accuracy means higher detection rates.
- Constant tuning makes the system work better and makes fewer mistakes.

V. CHALLENGES AND LIMITATIONS

AI-powered exam surveillance systems such as VIGILFY also have issues such as: issues in terms of privacy of user data and the overall reliability of the system. Continual webcam monitoring would give rise to worries about data security and the ethical use of information, and information collected would have to be secured.

- Data privacy regulations necessitate secure storage and controlled access to recorded images.
- Issues concerning ethics as to constant video surveillance of the user.
- There must be an approval and a guarantee given to the system user.

Third, hardware and environment variability: Hardware quality of webcam and lighting environment may affect the detection precision of examinations, such as the variance of the system detection precision due to unstable network. Varying users may produce different detection outcomes on various platform..

- Instagram's model is image-based.
- Twitter's model emphasizes on text and interaction.
- Constantly evolving due to the updates of platform policy and algorithm.

Another limitations are false positives and model bias during training. Mistaking some legal material as drug-related can result in bad user reputation and consequences for users.

- Mistaking some innocent users.
- Models would not be accurate for a wider variety of user groups.
- Model human-in-the-loop review can avoid false positives.

VI. CASE STUDIES AND ANALYSIS

The application of VIGILFY Real-Time Exam Surveillance Tool through AI surveillance systems demonstrates its potential to improve online examination security. The computer vision and activity tracking combination from AI monitoring solutions operates successful at detecting suspicious activities.

- The system identified suspicious actions which included face absence and multiple candidates.
- The system delivered immediate alerts which enabled fast response.

- The research showed that precise model training enables better detection outcomes.

The following case study examines the functions of browser activity monitoring tools that track user activities during online examination periods. The investigation of tab-switching patterns and navigation patterns enabled institutions to identify cheating activities.

- The study documented tab switching behavior and focus loss behavior during exams.
- The system prevented access to websites which it categorized as unauthorized.
    - The study demonstrated that effective browser system control requires visual monitoring tools as its essential component.

The AI system VIGILFY demonstrates better performance than traditional invigilation methods because it achieves higher efficiency and scalability. Human intervention remains necessary to verify findings and handle exceptional situations.

- The AI system monitors multiple students at the same time in real-time.
- The system uses automated detection to reduce manual tasks while increasing accuracy.
- The combination of AI and human review creates a system which produces reliable decisions.

VII. FUTURE DIRECTIONS

The future of *VIGILFY – Real-Time Exam Surveillance Tool* depends on two main developments which are better AI technology and more monitoring intelligence which will strengthen online exam security and accuracy.

- The proctoring model can be used in different settings through transfer learning which requires only a few extra data points to achieve its goals

- Self-supervised learning enables model training without needing extensive labeled datasets

The combination of smart alert systems with institutional control systems establishes stronger protection for real-time exam monitoring and emergency response processes. The automated alert system provides exam administrators with immediate notification capabilities about detected suspicious activities.

- Real-time alerts enable immediate intervention during exams
- The system connects to admin dashboards which enables fast response to rule breaches
- The collection of data-based knowledge enables better exam monitoring methods

The upcoming systems will use cloud-based infrastructure for conducting online exams which require ongoing monitoring and data storage throughout the entire exam process. The system will achieve better performance and scalability through this change which allows institutions to manage a higher volume of students.

- The cloud-based deployment system provides academic institutions with an expandable and adaptable framework for monitoring their test-takers
- The system needs less local machine processing power because it uses automated processing functions
- The system establishes continuous monitoring that operates in real time which helps uphold exam integrity throughout the entire testing process

VIII. CONCLUSION

This project has successfully demonstrated that an AI-based exam surveillance system such as VIGILFY is capable of detecting suspicious activities during an online exam by using computer vision and monitoring techniques. In order to prevent any illegal acts during exams, computer vision is combined with webcam observation and browsing control, allowing both the detection of a visual violation or a behavioral one.

- It integrates video monitoring with automatic analysis.
- It has the capacity to be used as a scalable system that allows monitoring examinations on a real time basis.

An AI-based examination surveillance system will contribute to make on-line examinations more fair and truthful to students and also institutionally reliable. The advantage would be:

- Builds a relationship of trust between students and the institutions where they learn.
- Creates more secure examinations and reduces the chances for cheating.
- Provides a process of evaluation that is both honest and reliable.

REFERENCES

1. Caetano et al., "Enhancing Weakly-Supervised Video Anomaly Detection With Temporal Constraints," IEEE Access, 2025.
2. Muzaffar et al., "A Systematic Review of Online Exams Solutions in E-Learning," IEEE Access, 2021.
3. Yeni Dwi Rahayu et al., "Advancements and Challenges in Video-Based Deception Detection," IEEE Access, 2025.
4. Abdelsalam et al., "Improving Reliability of Online Exam Results Using Blockchain," IEEE Access, 2023.
5. Duong et al., "Deep Learning-Based Anomaly Detection in Video Surveillance," Sensors (MDPI), 2023.
6. Lee & Fangyu, "Online Exam Proctoring Technologies: Innovation or Deterioration?," BJET, 2022.X. Sun, Y. Wang, "AI Techniques for Crime
7. Zhang et al., "Online Video Anomaly Detection," Sensors, 2023.
8. Muhammad Ramzan et al., "Effectiveness of Pre-Trained CNN Networks for Detecting Abnormal Activities in Online Exams," IEEE Access, 2022.
9. Adeyemi J. O et al., "Real-Time Detection of Examination Malpractices Using CNN and Video Surveillance: A Systematic Review with Meta Analysis," British Journal of Computer, Networking and Information Technology, 2025.
10. Dilky Felsinger et al., "Video-Based Action Detection for Online Exam Proctoring in Resource-Constrained Settings," Education and Information Technologies (Springer), 2024.