© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716853

Unauthorized Activity Detection During Online Exams

MASTAN VALI[1], VANGALA DIVYA[2], SHEGANTI PANKTHI[3], J. ANKITHA[4]
[1]*Assistant Professor, Sreenidhi Institute of Science and Technology Hyderabad-Telangana, India*
[2,3,4]*Computer Science and Engineering Sreenidhi Institute of Science and Technology Hyderabad-Telangana, India*

Abstract - The rapid growth of online education has increased the demand for secure and reliable examination systems. However, traditional online exams are highly vulnerable to impersonation and cheating activities. This paper presents an AI-based smart exam monitoring system that integrates face recognition, object detection, and audio analysis to ensure secure and fair examination processes. The proposed system uses facial recognition techniques to authenticate users during registration and login, preventing unauthorized access and duplicate identities. A face encoding mechanism is employed to uniquely identify each user and eliminate duplicate registrations. During the examination, real-time monitoring is performed using a deep learning-based object detection model (YOLO) to identify suspicious objects such as mobile phones, laptops, and the presence of multiple individuals. Additionally, head and eye movement tracking is implemented using Haar Cascade classifiers to detect inattentive or suspicious behavior. The system also incorporates audio monitoring to detect abnormal sound levels, indicating potential malpractice. Whenever suspicious activity is detected, the system generates alerts, captures screenshots as evidence, and records the entire session for further review. An automated decision mechanism is implemented to terminate the exam if abnormal behavior persists beyond a defined threshold duration. The integration of multiple monitoring techniques enhances the overall accuracy and robustness of the system. This solution provides a scalable and efficient approach to maintaining academic integrity in online examinations.

Key Words: Face Recognition, Online Exam Monitoring, YOLO, Object Detection, Audio Analysis, Proctoring System, Deep Learning, Computer Vision, Authentication, Security System

I. INTRODUCTION

The rapid advancement of digital technologies has significantly transformed the education sector, leading to the widespread adoption of online learning and examination systems. However, ensuring the integrity and security of online examinations remains a major challenge due to the increasing risks of impersonation, cheating, and unauthorized assistance. Traditional authentication mechanisms such as usernames and passwords are insufficient to guarantee user authenticity, necessitating the use of more secure and intelligent systems [18].

Face recognition has emerged as a reliable biometric technique for user authentication due to its non-intrusive nature and high accuracy. It utilizes unique facial features to identify individuals, making it suitable for applications requiring secure access control [19]. Early approaches to face detection, such as the Viola-Jones algorithm, provided real-time detection capabilities using Haar-like features and boosted classifiers [1]. With the evolution of deep learning, convolutional neural networks (CNNs) have significantly improved the accuracy and robustness of image recognition tasks [2], [14].

In addition to authentication, monitoring user behavior during online examinations is equally important. Object detection techniques such as YOLO (You Only Look Once) enable real- time identification of suspicious objects like mobile phones and laptops, which may be used for malpractice [3], [4]. Similarly, facial behavior analysis tools and tracking methods can detect head and eye movements, providing insights into user attentiveness [10], [13]. These computer vision techniques are further supported by libraries such as OpenCV and Dlib, which facilitate efficient image processing and machine learning implementations [5], [7].

Recent research has focused on integrating multiple modalities, including audio analysis, to enhance the detection of abnormal activities during exams [18]. Deep learning-based systems combining facial recognition, object detection, and behavioral analysis offer a comprehensive solution for secure online proctoring. Despite these advancements, challenges such as varying lighting conditions, pose variations, and system performance remain

areas of ongoing research.

This paper proposes an AI-based smart exam monitoring system that integrates face recognition, object detection, and audio monitoring to ensure secure and fair examination environments. The system aims to prevent impersonation, detect suspicious activities in real time, and provide recorded evidence for further analysis.

II. PROPOSED SYSTEM

The proposed system is an AI-based smart exam monitoring solution designed to ensure secure and fair online examinations. It integrates face recognition, object detection, behavioral analysis, and audio monitoring to prevent impersonation and detect suspicious activities in real time. The system architecture combines computer vision and deep learning techniques to provide a multi-layered security mechanism.

2.1 Face Registration and Authentication

The system begins with a secure registration process where users provide personal details along with their facial data captured through a webcam. The captured image is processed using face recognition algorithms to extract unique facial encodings. These encodings are stored in the database and used for future authentication. During login, the system captures the user's face again and compares it with stored encodings using a predefined threshold. This ensures that only authorized users can access the system and prevents duplicate registrations and impersonation attempts.

2.2 Real-Time Face Monitoring and Behavior Analysis

During the examination, continuous face monitoring is performed to ensure the presence of only one individual. The system detects facial features and tracks head and eye movements using Haar Cascade classifiers. Any abnormal behavior such as looking away from the screen, absence of the face, or multiple faces in the frame is flagged as suspicious. This real-time behavioral analysis helps in maintaining user attentiveness and prevents unfair practices during the exam.

2.3 Object Detection Using Deep Learning

To detect unauthorized objects, the system employs a deep learning-based object detection model (YOLO). The model identifies objects such as mobile phones, laptops, and additional persons within the camera frame. If any prohibited object is detected, the system marks it as abnormal activity. The integration of YOLO enables fast and accurate detection, ensuring that candidates do not use external devices for cheating.

2.4 Audio Monitoring and Automated Decision System

In addition to visual monitoring, the system incorporates audio analysis to detect abnormal sound levels during the examination. High noise levels may indicate communication with others or external assistance. When suspicious activities are detected through visual or audio inputs, the system triggers alerts, captures screenshots, and records video evidence. If abnormal behavior persists beyond a specified time threshold, the system automatically terminates the exam. This automated decision- making mechanism ensures strict enforcement of examination rules.

2.5 System Architecture

The above diagram illustrates the overall architecture of the proposed AI-based smart exam monitoring system, which is composed of client-side, server-side, and administrative components. The system ensures secure and continuous monitoring of candidates during online examinations by integrating multiple modules.

At the student device level, hardware components such as the webcam and microphone are used to capture real-time video and audio data. The webcam captures facial images for authentication and monitoring, while the microphone records ambient sound to detect abnormal noise levels.

The client-side application, running in a web browser, consists of the monitoring user interface and face capture module. The monitoring UI provides an interactive platform for students during the examination, while the face capture module collects facial data and sends it to the server for processing.

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716853

On the server-side (Django application), the core functionalities are implemented. The face recognition engine processes captured images and verifies user identity using stored facial encodings. The proctoring logic continuously analyzes video and audio streams to detect suspicious activities such as multiple faces, unauthorized objects, or unusual behavior. The media handler module manages the storage of screenshots and recorded videos as evidence. Additionally, the user management module handles registration, authentication, and user data operations. All relevant information, including user details and activity logs, is stored in the database.

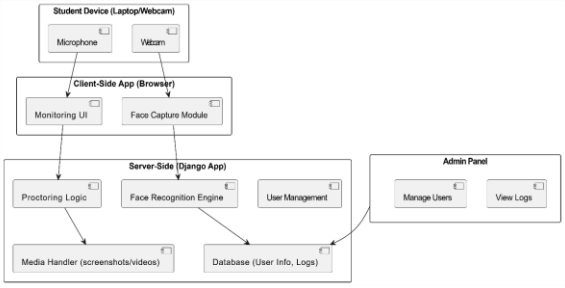

Fig-1 System Architecture

III. IMPLEMENTATION DETAILS

The proposed system is implemented using a combination of web technologies, computer vision techniques, and deep learning models to ensure efficient and secure online exam monitoring. The backend is developed using the Django framework, while the frontend utilizes HTML, CSS (Tailwind), and JavaScript for user interaction and webcam integration.

3.1 System Development Environment

The system is developed in Python due to its extensive support for machine learning and image processing libraries. The face_recognition library is used for facial feature extraction and encoding, while OpenCV is utilized for image processing and real-time video handling. The YOLOv8 model is integrated for object detection tasks. Additionally, NumPy and PIL are used for image manipulation, and sounddevice is used for audio monitoring.

Table 1: Technologies and Tools Used

Component	Technology/Tool Used
Backend	Django (Python)
Frontend	HTML, Tailwind CSS, JS
Face Recognition	face_recognition, Dlib
Object Detection	YOLOv8
Image Processing	OpenCV, PIL
Audio Monitoring	sounddevice
Database	SQLite

3.2 Face Recognition Implementation

The face recognition module plays a critical role in authentication. During registration, facial images are captured and converted into numerical encodings using the face_recognition library. These encodings are serialized using pickle and stored in the database. During login and exam verification, the system compares newly captured face encodings with stored encodings using a distance-based metric. A threshold value is defined to determine whether the faces match. This approach ensures accurate identification while minimizing false positives.

3.3 Real-Time Monitoring Implementation

The system continuously captures video frames using the webcam and processes them in real time. Face detection is performed using Haar Cascade classifiers to ensure only one person is present. The YOLOv8 model detects objects such as mobile phones, laptops, and additional persons. Eye and head movement tracking is implemented to analyze user attentiveness. Additionally, the system monitors audio input and calculates sound intensity to detect abnormal noise levels.

Table 2: Detection Modules and Their Functions

Module	Functionality
Face Detection	Detects presence of user in frame
Face Recognition	Authenticates user identity
Object Detection	Detects mobile, laptop, multiple persons
Eye/Head Tracking	Monitors user attention
Audio Monitoring	Detects abnormal sound levels
Media Capture	Stores screenshots and video recordings

3.4 Data Storage and Processing

All user data, including personal details and facial

encodings, are stored in the database. Screenshots of suspicious activities and recorded exam sessions are stored in designated directories within the system. The media handler module ensures proper organization and retrieval of these files. The system also maintains logs of user activities for administrative review.

3.5 Automated Decision Mechanism

An automated decision-making system is implemented to handle abnormal activities. If suspicious behavior such as multiple faces, prohibited objects, or excessive noise persists beyond a predefined time threshold, the system triggers alerts and may terminate the exam session. This ensures strict adherence to examination rules and minimizes human intervention.

IV. RESULTS AND PERFORMANCE ANALYSIS

The proposed AI-based exam monitoring system was tested under various real-time conditions to evaluate its performance in terms of accuracy, reliability, and efficiency. The system integrates multiple modules such as face recognition, object detection, and audio monitoring, and each component was analyzed individually as well as collectively.

4.1 Face Recognition Accuracy

The face recognition module demonstrated reliable performance in identifying registered users. By using a threshold-based distance metric, the system was able to accurately distinguish between genuine and duplicate users. Experimental observations showed that maintaining a threshold value between 0.5 and 0.6 provided a balanced trade-off between false acceptance and false rejection rates. However, slight variations in lighting conditions and facial expressions occasionally affected accuracy, indicating the need for controlled environments or improved preprocessing techniques.

42 Real-Time Monitoring Performance

The real-time monitoring module effectively tracked user behavior throughout the examination. The system successfully detected the presence of multiple individuals, absence of the user, and abnormal head or eye movements. The integration of Haar Cascade classifiers ensured fast detection with minimal latency. The system maintained smooth performance during continuous monitoring, although performance slightly decreased when multiple detection modules were executed simultaneously.

4.2 Object Detection Efficiency

The YOLO-based object detection model achieved high accuracy in identifying prohibited objects such as mobile phones and laptops. The model was capable of detecting objects in real time with acceptable precision and speed. The detection accuracy was higher for clearly visible objects, while partially occluded objects resulted in reduced confidence levels. Overall, the model contributed significantly to identifying potential cheating attempts.

4.3 Audio Monitoring Effectiveness

The audio monitoring module successfully detected abnormal sound levels during the examination. By analyzing sound intensity, the system was able to identify unusual noise that may indicate communication or external assistance. However, background environmental noise sometimes triggered false alerts, suggesting that adaptive thresholding could further improve performance.

4.4 System Reliability and Response

The system demonstrated strong reliability by integrating multiple detection mechanisms. When abnormal activities were detected, the system generated alerts, captured screenshots, and recorded video evidence. The automated decision mechanism effectively terminated the exam when suspicious behavior persisted beyond the defined time threshold. This ensured strict enforcement of examination rules and minimized manual supervision.

4.5 Overall System Performance

The combined performance of all modules resulted in a robust and efficient exam monitoring system. The integration of facial recognition, object detection, and audio analysis enhanced the

accuracy of detecting malpractice. Although minor limitations such as lighting sensitivity and occasional false positives were observed, the system provides a scalable and practical solution for secure online examinations.

V. CONCLUSIONS

The proposed AI-based smart exam monitoring system provides an effective solution to address the challenges associated with online examinations, particularly issues related to impersonation and malpractice. By integrating multiple technologies such as face recognition, object detection, and audio monitoring, the system ensures a comprehensive and secure examination environment. The face recognition module enables reliable user authentication and prevents duplicate registrations, thereby enhancing system security.

The incorporation of real-time monitoring techniques allows continuous observation of user behavior throughout the examination. The system effectively detects suspicious activities such as the presence of multiple individuals, usage of unauthorized devices, abnormal head and eye movements, and unusual sound patterns. Additionally, the automated alert mechanism, along with screenshot and video recording features, provides strong evidence for further analysis and verification.

The experimental results demonstrate that the system achieves satisfactory performance in terms of accuracy, efficiency, and reliability. The use of deep learning models such as YOLO contributes to accurate object detection, while threshold-based face matching ensures balanced authentication. Although minor limitations such as sensitivity to lighting conditions and occasional false positives were observed, the overall system proves to be robust and scalable.

In conclusion, the proposed system offers a practical and intelligent approach to maintaining academic integrity in online examinations. It reduces the need for manual invigilation and provides an automated, efficient, and secure proctoring solution.

VI.FUTURE WORK

Despite the effectiveness of the proposed system, several enhancements can be incorporated to further improve its performance and applicability. One potential improvement is the use of advanced deep learning models for face recognition, such as FaceNet or ArcFace, which can provide higher accuracy and robustness under varying lighting and pose conditions. Additionally, incorporating multiple facial samples per user during registration can significantly improve recognition reliability.

Another area of enhancement is the implementation of adaptive thresholding techniques for both face recognition and audio monitoring, which can dynamically adjust based on environmental conditions. The object detection module can also be upgraded using more advanced or lightweight models to improve detection speed and efficiency, especially for real-time applications.

The system can be extended by integrating cloud-based storage and processing to handle large-scale deployments and enable remote access to logs and recordings. Furthermore, incorporating behavioral analytics using machine learning techniques can help in predicting suspicious activities more accurately. Integration with Learning Management Systems (LMS) can also provide seamless management of exams, attendance, and results.

Finally, improving user interface design and optimizing system performance for low-resource devices will enhance usability and accessibility, making the system suitable for a wider range of educational institutions.

REFERENCES

[1] P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features,” in *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, 2001, pp. 511–518.

[2] A. Krizhevsky, I. Sutskever, and G. Hinton, “ImageNet classification with deep convolutional neural networks,” *Advances in Neural Information Processing Systems*, vol. 25, pp. 1097–1105, 2012.

[3] J. Redmon et al., “You Only Look Once: Unified, real-time object detection,” in *Proc. IEEE CVPR*, 2016, pp. 779–788.

[4] J. Redmon and A. Farhadi, “YOLOv3: An incremental improvement,” *arXiv preprint*

arXiv:1804.02767, 2018.

[5] G. Bradski, "The OpenCV library," *Dr. Dobb's Journal of Software Tools*, 2000.

[6] A. Geitgey, "face_recognition library," GitHub repository, 2016.

[7] D. King, "Dlib-ml: A machine learning toolkit," *Journal of Machine Learning Research*, vol. 10, pp. 1755–1758, 2009.

[8] R. Girshick, "Fast R-CNN," in *Proc. IEEE ICCV*, 2015, pp. 1440–1448.

[9] S. Ren et al., "Faster R-CNN: Towards real-time object detection," *IEEE TPAMI*, vol. 39, no. 6, pp. 1137–1149, 2017.

[10] T. Baltrušaitis et al., "OpenFace: An open source facial behavior analysis toolkit," in *Proc. IEEE WACV*, 2016, pp. 1– 10.

[11] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *Proc. IEEE CVPR*, 2005, pp. 886–893.

[12] H. Rowley et al., "Neural network-based face detection," *IEEE TPAMI*, vol. 20, no. 1, pp. 23–38, 1998.

[13] S. Zafeiriou et al., "Face detection and tracking: A survey," *Image and Vision Computing*, vol. 30, pp. 1–20, 2012.

[14] Y. LeCun et al., "Deep learning," *Nature*, vol. 521, pp. 436–444, 2015.

[15] K. Simonyan and A. Zisserman, "Very deep convolutional networks," *arXiv preprint arXiv:1409.1556*, 2014.

[16] I. Goodfellow et al., *Deep Learning*, MIT Press, 2016.

[17] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[18] Z. Zhang et al., "Online exam proctoring using AI," *IEEE Access*, vol. 8, pp. 1–10, 2020.

[19] M. Sharif et al., "Face recognition: A survey," *Journal of Computer Science*, vol. 13, no. 2, pp. 1–14, 2017.

[20] R. Szeliski, *Computer Vision: Algorithms and Applications*, Springer, 2010.