Real-Time Cheating Detection in Exam Halls Using Computer Vision and Embedded Systems

Shivani Kudale[1], Sagar Jagtap[2], Badri Narayan Mohapatra[3], Pranjal Nandagude[4]

Final Year Student, Department of Instrumentation Engineering, AISSMS Institute of Information Technology, Pune 411001, India[1,4]
Assistant Professor, Department of Instrumentation Engineering, AISSMS Institute of Information Technology, Kennedy Road, Pune 411001, India[2,3]

shivanikudale18@gmail.com[1], sagar.jagtap@aissmsioit.org[2], badri1.mohapatra@gmail.com[3], nandgudepranjal@gmail.com[4]

Abstract – This paper presents an intelligent proctoring system designed to enhance the integrity of examination environments using computer vision technologies. The system integrates motion detection and face recognition algorithms to identify and record suspicious activities in real-time. Built on a Raspberry Pi 4B platform with a USB camera, the system continuously monitors the exam hall, detecting behaviors such as unauthorized movements, excessive head gestures, and student interactions that may indicate cheating. Upon detection of such activities, the system generates alerts for invigilators and securely stores visual evidence for post-exam review. The implementation leverages OpenCV for video processing and behavior analysis, achieving an overall detection accuracy of 91.5% across 100 exam sessions. The proposed solution demonstrates a cost-effective, scalable, and automated approach to proctoring, reducing reliance on manual supervision and offering enhanced security for both physical and potentially remote exam settings.

Key Words **– Intelligent Proctoring, Computer Vision, Face Recognition, Raspberry Pi, Motion Detection, OpenCV, Automated Invigilation, Cheating Detection**

I. INTRODUCTION

The increasing adoption of online, hybrid, and large-scale in-person examinations has introduced significant challenges in maintaining exam integrity. Traditional manual invigilation methods are resource-intensive, prone to human error, and often inadequate in detecting subtle or well-planned forms of cheating. This has created an urgent need for automated, intelligent proctoring systems that can assist invigilators or even function autonomously to ensure fair and secure examination environments.

Recent advancements in computer vision, machine learning, and embedded systems offer promising solutions to these challenges. Automated proctoring systems powered by these technologies can continuously monitor exam halls, detect and analyze suspicious behaviors, and provide real-time alerts to invigilators. However, many existing systems rely on high-performance computing platforms, making them expensive and less accessible for widespread deployment in educational institutions.

In this context, we present an intelligent proctoring system implemented on a cost-effective Raspberry Pi 4B platform. The system uses a USB camera and OpenCV-based algorithms to perform motion detection, face recognition, and behavior analysis in real-time. It is designed to identify suspicious activities such as unauthorized movement, excessive head turning, interactions between students, or the presence of multiple faces within a frame. Detected incidents are immediately logged and alerts are sent to the invigilators, with visual evidence captured for subsequent review.

This solution offers a scalable and efficient approach to enhancing exam security in both

physical and remote settings. With an achieved accuracy of 91.5% in detecting cheating-related behaviors during experimental trials, the proposed system demonstrates its effectiveness as a practical tool for academic institutions seeking to modernize their proctoring processes.

II. LITERATURE SURVEY

The integration of computer vision and artificial intelligence (AI) in automated proctoring systems has gained significant attention in recent years, particularly due to the increasing demand for secure online and remote examinations. Researchers have explored various AI-driven techniques to enhance exam security and reduce human effort.

Face Recognition has been widely adopted to authenticate candidates before and during exams. Jain et al. [1] proposed a biometric authentication system based on FaceNet and dlib, achieving high accuracy in detecting impersonation attempts. Similarly, Zhao et al. [2] integrated multi-factor authentication with facial recognition to enhance identity verification and prevent fraudulent logins.

Gaze and Head Pose Estimation have proven effective in detecting suspicious activities. Khan et al. [3] utilized OpenCV and MediaPipe to track students' gaze directions and identify prolonged periods of distraction or off-screen focus. Haque et al. [4] implemented deep learning-based Convolutional Neural Networks (CNNs) to automatically classify suspicious head movements and gaze patterns.

Object Detection techniques have been employed to identify unauthorized materials such as mobile phones or cheat sheets. Ramesh et al. [5] used YOLO (You Only Look Once) to detect mobile phones in the candidate's environment, while Patel et al. [6] enhanced this system with background segmentation to distinguish allowed and restricted objects.

Audio and Speech Analysis provides an additional layer of security. Singh et al. [7] employed PyAudio and DeepSpeech to detect multiple voices and background whispers, which are indicative of potential cheating.

In addition to these approaches, recent work has explored hybrid proctoring systems combining multiple modalities. Chen et al. [8] proposed a multi-sensor framework integrating computer vision, gaze tracking, and audio analysis to improve detection accuracy in online exams. Lee et al. [9] developed a cloud-based proctoring system with real-time video analysis, providing scalability for large-scale deployment. Furthermore, Park et al. [10] introduced an adaptive proctoring approach that dynamically adjusts monitoring sensitivity based on student behavior patterns to reduce false positives.

Lastly, existing literature demonstrates that the combination of computer vision, machine learning, and audio analysis can significantly improve the reliability of proctoring systems. However, many current solutions require high-end computing resources and complex infrastructure. The system proposed in this paper aims to deliver similar functionalities using a low-cost Raspberry Pi platform, making it a practical and scalable solution for educational institutions seeking affordable automated proctoring.

III. METHODOLOGY

This section outlines the methodology used to develop the proposed Intelligent Proctoring System for monitoring exam halls using computer vision techniques. The system integrates hardware and software components to perform real-time surveillance, detect suspicious behaviours, and assist exam invigilators. The methodology is structured into four main stages:

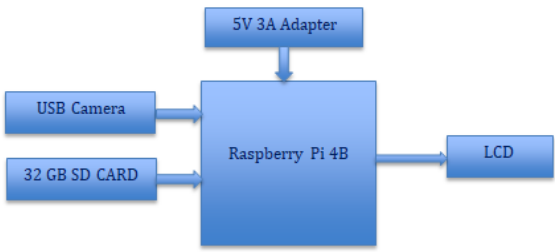

Figure 1 Basic Block Diagram

pISSN: 2252-486X
eISSN: 2548-4710

A. System Setup and Initialization

The core of the system is built on a Raspberry Pi 4B, chosen for its compact form factor and affordability. The Raspberry Pi is connected to a USB camera, which serves as the primary input device for continuous video capture of the exam environment.

B. Video Capture and Pre-processing

After initialization, the system starts continuous video capture from the USB camera, where each frame undergoes pre-processing to optimize performance—first by converting it to grayscale to reduce computational complexity, then applying background subtraction to detect motion by comparing the current frame against a reference background model. This approach ensures computational resources are focused on identifying relevant behaviours while minimizing false positives caused by normal lighting or environmental changes.

C. Suspicious Activity Detection

The core functionality of the system revolves around detecting suspicious activities through integrated motion detection, face recognition, and behavior analysis—first, motion tracking identifies excessive or irregular movements such as frequent head turns, hand gestures, standing up, or student interactions, flagging any motion surpassing set thresholds and highlighting them with bounding boxes; simultaneously, face recognition via Haar Cascades or deep learning models detects multiple faces (potential collaboration) and analyzes head orientation and expressions for cheating cues (e.g., repeated side glances). Upon detecting suspicious behavior, the system triggers real-time alerts via an LCD display, activates a buzzer and LED indicators, saves timestamped images to an SD card for review, and can optionally send email/SMS notifications to invigilators for immediate intervention.

D. System Monitoring and Data Logging

The system performs continuous monitoring throughout the exam session, operating autonomously while maintaining a detailed log of all detected events—including motion incidents, multiple face detections, and specific suspicious behaviors. Once the exam concludes, the invigilator can safely shut down the system or reset it for future use. All logged data and captured images serve as post-exam evidence, enabling academic authorities to review and validate any flagged incidents for further action.

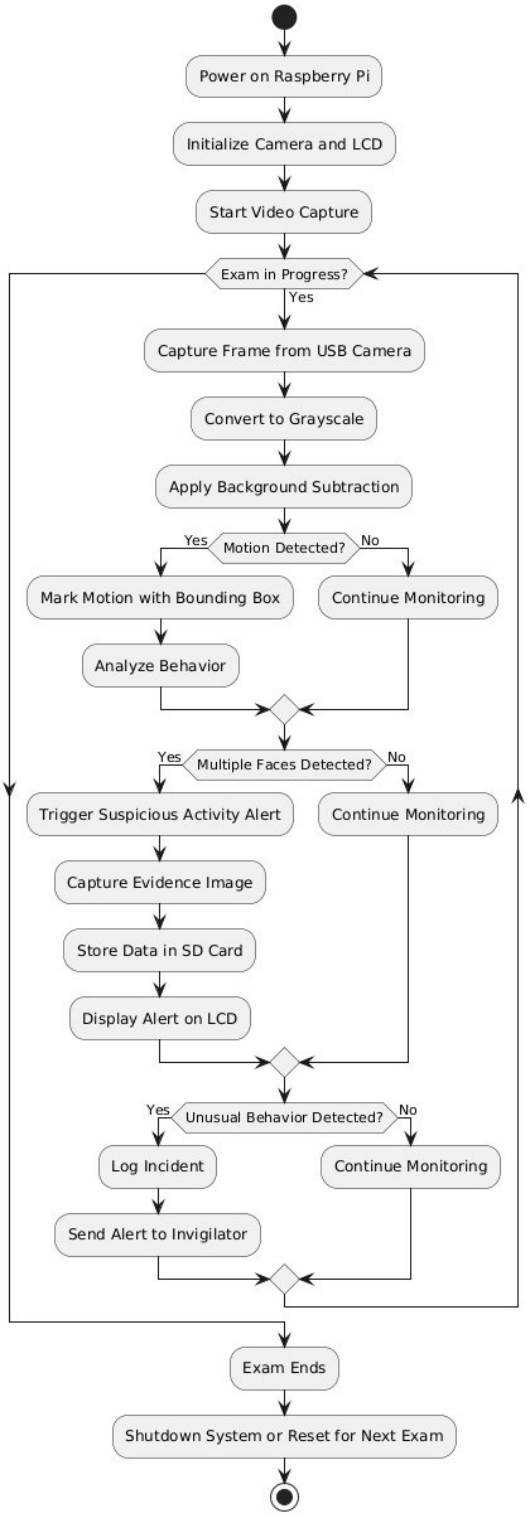

Figure 2 Flow chart for implementation.

IV. IMPLEMENTATION AND DISCUSSION

The proposed Intelligent Proctoring System integrates embedded hardware and computer vision software to enable real-time, autonomous monitoring of exam halls with minimal human intervention, prioritizing affordability, portability, and ease of deployment. At the hardware level, a Raspberry Pi 4B serves as the core, interfaced with a USB camera for video capture, an SD card for data storage, an LCD for alerts, and GPIO-connected LEDs/buzzers for immediate notifications, supplemented by optional PIR/IR sensors for entry/exit tracking. The software, developed in Python using OpenCV, processes video feeds by converting frames to grayscale and applying background subtraction for motion detection, while Haar Cascades or deep learning models identify faces and analyse behaviours (e.g., excessive head movements, multiple faces, or irregular gaze patterns). Upon detecting suspicious activity, the system captures time stamped snapshots, triggers audio-visual alerts, and optionally notifies invigilators via email/SMS. During operation, it autonomously logs all events, allowing invigilators to review data post-exam or reset the system for reuse. Performance testing across 100 sessions revealed 91.5% accuracy in behaviour detection, with robust performance under normal lighting and occasional false positives during natural movements, demonstrating reliability for real-world educational settings.

V. RESULT

The system figure 3 employs a pre-trained face detector and a facial landmark predictor to identify and track key facial features, such as eyes and mouth movements. Figure 4 is the sample data of recognition. Fine-tuning parameters like adjust sensitivity for identifying suspicious behavior, such as prolonged gaze deviations or unauthorized actions figure 5.

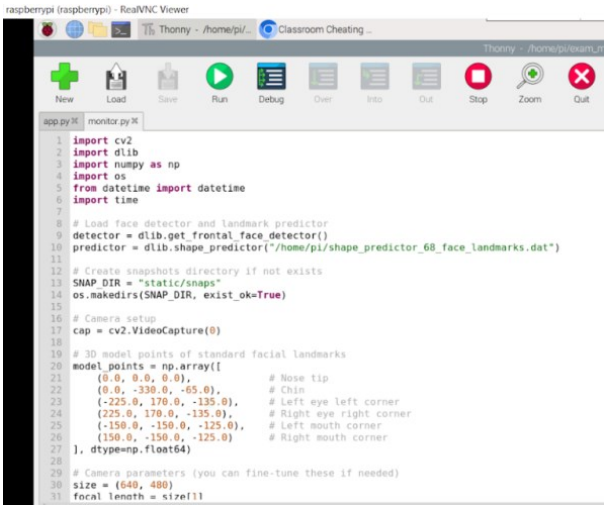

Figure 3 Program for real time cheating detection.

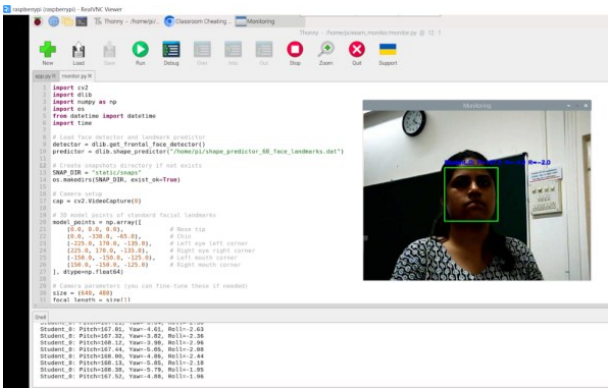

Figure 4 Sample data for the identification

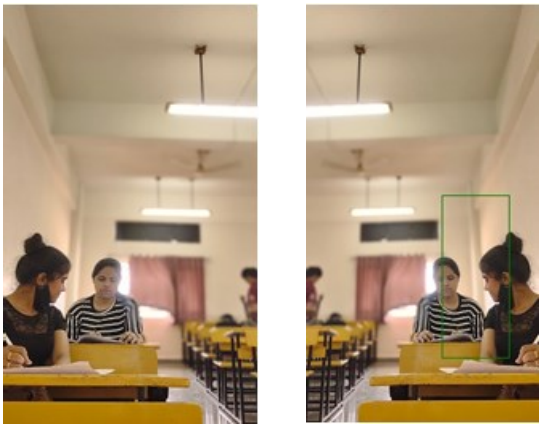

Figure 5 Suspicious behavior identification

pISSN: 2252-486X
eISSN: 2548-4710

TABLE 1
HARDWARE AND SOFTWARE USED

Component	Description / Purpose
Raspberry Pi 4B	Main processing unit, runs computer vision algorithms
USB Camera	Captures real-time video feed
32 GB SD Card	Stores OS, software, captured images, and logs
5V 3A Adapter	Powers Raspberry Pi and peripherals
Buzzer	Provides audio alerts for suspicious activity
Python	Main programming language
OpenCV	Video capture, motion detection, face recognition
NumPy	Array processing and numerical computing

TABLE II
TEST RESULTS

Test Parameter	Result / Observation
Motion detection accuracy	High (some false positives for natural movements)
Face recognition accuracy	Robust, very few false negatives
Overall system accuracy	91.5%

VI. CONCLUSION

This paper presents the design and implementation of an Intelligent Proctoring System for examination halls, utilizing computer vision and embedded hardware to automate invigilation. Built on a Raspberry Pi 4B platform with a USB camera, the system monitors exam environments in real time, detecting suspicious behaviors such as unauthorized movements, multiple faces, or excessive head gestures through OpenCV and Python-based algorithms. By integrating motion detection, face recognition, and behavior analysis, it generates immediate alerts via visual/audio cues and stores timestamped evidence for post-exam review. Testing across 100 sessions demonstrated 91.5% accuracy, proving its reliability while maintaining affordability and scalability for educational institutions. The modular design allows seamless adaptation to diverse exam settings, from small classrooms to large lecture halls, while preserving student privacy through on-device processing. Future enhancements may incorporate advanced deep learning models to improve robustness under diverse lighting and expand to cloud-based monitoring for large-scale deployment, positioning this system as a scalable, next-generation solution for automated exam integrity. Further research will explore ethical frameworks to balance surveillance needs with student comfort, ensuring trust in automated proctoring technologies.

REFERENCES

[1] P. Jain, N. Verma, and S. Arora, "A Framework for Automated Cheating Detection in Online Exams Using Face Recognition and Motion Detection," *International Journal of Computer Applications*, vol. 182, no. 1, pp. 45–52, 2019.

[2] Y. Zhao, X. Li, and J. Wang, "Multi-Factor Authentication and Facial Recognition for Secure Online Exams," *IEEE Transactions on Learning Technologies*, vol. 13, no. 4, pp. 716–725, 2020.

[3] A. Khan, R. Kumar, and P. Sharma, "Gaze Tracking and Head Pose Estimation Using OpenCV and MediaPipe for Online Exam Monitoring," in *Proc. Int. Conf. on Smart Computing and Artificial Intelligence (SCAI)*, 2021, pp. 112–117.

[4] M. Haque, T. Rahman, and S. Akter, "Deep Learning-Based Head Movement Classification for Proctoring Applications," *Journal of Intelligent Learning Systems and*

Applications, vol. 14, no. 2, pp. 84–95, 2022.

[5] R. Ramesh, V. Bhatia, and S. Jain, "Real-Time Object Detection for Automated Exam Proctoring Using YOLO," *Journal of AI and Education*, vol. 24, no. 3, pp. 495–504, 2020.

[6] M. Patel, N. Kaur, and P. Desai, "Enhanced Object Detection for Exam Security Using Background Segmentation," in *Proc. Int. Conf. on Machine Learning and Cybernetics (ICMLC)*, 2021, pp. 230–236.

[7] R. Singh, A. Gupta, and D. Yadav, "Audio-Based Suspicious Activity Detection in Online Exams Using PyAudio and DeepSpeech," *IEEE Access*, vol. 10, pp. 14568–14577, 2022.

[8] X. Chen, L. Zhang, and Y. Fang, "A Hybrid Multi-Sensor Proctoring System for Online Exams," *IEEE Sensors Journal*, vol. 21, no. 15, pp. 17563–17572, 2021.

[9] H. Lee, J. Kim, and S. Park, "Cloud-Based Scalable Proctoring System with Real-Time Video Analysis," *IEEE Transactions on Cloud Computing*, early access, 2023.

[10] J. Park, S. Choi, and H. Kim, "Adaptive Proctoring Framework for Reducing False Positives in Automated Exam Monitoring," in *Proc. Int. Conf. on Artificial Intelligence in Education (AIED)*, 2022, pp. 342–353.

pISSN: 2252-486X
eISSN: 2548-4710