International Journal of Scientific Research in Engineering & Technology
Volume6, Issue4 (July-August 2026), PP: 154-158.
https://www.doi.org/10.59256/ijsreat.20260604017
www.ijsreat.com
ISSN No: 2583-1240

AI-Based Cheating Detection System for Examination Monitoring

Sailakshmi Kumari Narava[1], Alapati Bhargava Rama Bharadwaja[2], Lenka Anusha[3], Dasari Bhaskar[4], Induri Bhuvaneswara Reddy[5], Ijju Sai Madhuri[6], Beri Bhavya[7]

[1]Assistant Professor, Department of ECE, Dr. Lankapalli Bullayya College of Engineering (Autonomous), Andhra Pradesh, India.

[2,3,4,5,6,7] Department of ECE, Dr. Lankapalli Bullayya College of Engineering (Autonomous), Andhra University, Andhra Pradesh, India.

To Cite this Article: *Sailakshmi Kumari Narava[1], Alapati Bhargava Rama Bharadwaja[2], Lenka Anusha[3], Dasari Bhaskar[4], Induri Bhuvaneswara Reddy[5], Ijju Sai Madhuri[6], Beri Bhavya[7], "AI-Based Cheating Detection System for Examination Monitoring", International Journal of Scientific Research in Engineering & Technology, Volume 06, Issue 04, July-August 2026, PP:154-158.*

Abstract: *The increasing demand for secure and transparent examination systems has highlighted the limitations of conventional human invigilation, particularly in large examination halls. Manual monitoring is prone to fatigue, limited visibility, and delayed response, making it difficult to detect sophisticated cheating behaviors in real time. This paper presents an AI-Based Cheating Detection System for Examination Monitoring that integrates computer vision, deep learning, and edge computing with low-cost IoT hardware to provide intelligent and automated exam surveillance. The proposed system combines ResNet-10 for robust face detection and counting with YOLOv8 Nano for real-time detection of unauthorized mobile devices. To overcome the blind spots of camera-based monitoring, Infrared (IR) and Passive Infrared (PIR) sensors are integrated through a Raspberry Pi Pico H, creating a hardware–software closed-loop architecture capable of detecting under-desk activities and abnormal movements. Live video streams captured through a webcam and ESP32-CAM are processed using OpenCV and displayed on a Flask-based monitoring dashboard. The system evaluates six predefined cheating scenarios, including face absence, extra person detection, student proximity, unauthorized device usage, abnormal movement, and under-desk activity, while simultaneously triggering localized buzzer alerts for immediate intervention. Experimental evaluation demonstrates reliable real-time monitoring with visual processing speeds of approximately 15–20 FPS and hardware response latency below 50 ms, ensuring rapid and accurate detection. The proposed architecture is scalable, cost-effective, and suitable for deployment in educational institutions, providing an efficient solution for enhancing examination integrity while reducing the workload of human invigilators.*

Keywords: *Artificial Intelligence (AI), Examination Monitoring, Cheating Detection, Deep Learning, YOLOv8 Nano, ResNet-10, Computer Vision, Edge Computing, ESP32-CAM, Raspberry Pi Pico H, Internet of Things (IoT), OpenCV, Flask Dashboard, Real-Time Surveillance, Smart Examination System.*

I. INTRODUCTION

The rapid advancement of Artificial Intelligence (AI) and computer vision technologies has significantly transformed surveillance and monitoring systems across various domains, including education. Ensuring fairness and academic integrity during examinations remains a major challenge for educational institutions, particularly in large examination halls where manual invigilation is often insufficient. Human invigilators are limited by fatigue, restricted visibility, and divided attention, making it difficult to identify subtle cheating behaviors such as unauthorized mobile phone usage, whispering, under-desk activities, and abnormal student movements. These limitations necessitate the development of intelligent, automated, and real-time examination monitoring systems.

Recent AI-assisted proctoring systems have employed deep learning algorithms and computer vision techniques to detect suspicious activities using surveillance cameras. However, most existing solutions rely solely on visual information, making them vulnerable to camera blind spots and environmental variations. Furthermore, many systems function only as passive surveillance tools by recording or logging incidents for post-examination review, rather than providing immediate intervention during examinations. Such approaches reduce the effectiveness of real-time cheating prevention.

To overcome these limitations, this paper proposes an **AI-Based Cheating Detection System for Examination Monitoring** that integrates deep learning with edge-based IoT hardware in a hardware–software closed-loop architecture. The proposed system combines **ResNet-10** for robust face detection and counting with **YOLOv8 Nano** for real-time detection of unauthorized mobile devices. To eliminate the blind spots associated with camera-only monitoring, **Infrared (IR)** and **Passive Infrared (PIR)** sensors are incorporated through a **Raspberry Pi Pico H**, enabling the detection of under-desk activities and abnormal physical movements. Live video streams acquired from both a webcam and an **ESP32-CAM** are processed using **OpenCV** and displayed through a **Flask-based dashboard**, providing continuous real-time monitoring.

The proposed system evaluates six predefined examination scenarios, including face absence, extra person detection, student proximity, unauthorized mobile device usage, abnormal movement, and under-desk activity. Upon detecting any suspicious event, the system immediately activates a localized buzzer alert, enabling prompt intervention by the invigilator. This multi-modal approach improves detection accuracy, minimizes false alarms, and enhances the reliability of examination monitoring while maintaining low implementation cost.

The major contributions of this work are:

- Development of a low-cost AI-enabled examination monitoring system using edge computing.
- Integration of ResNet-10 and YOLOv8 Nano for real-time face and object detection.
- Fusion of computer vision with PIR and IR sensors to eliminate camera blind spots.
- Implementation of a six-scenario detection framework for comprehensive cheating identification.
- Design of a scalable Flask-based monitoring dashboard with real-time alerts suitable for educational institutions.

The experimental results demonstrate that the proposed system provides accurate and efficient real-time cheating detection while maintaining low latency and high scalability, making it a practical solution for modern smart examination environments.

II. MATERIAL AND METHODS

Materials

The proposed AI-Based Cheating Detection System integrates low-cost hardware components with deep learning software frameworks to enable intelligent real-time examination monitoring. The materials used in the system are categorized into hardware and software components.

2.1 Hardware Components

- ESP32-CAM Module: Used as a wireless vision node to capture and transmit real-time video streams over a Wi-Fi network.
- Raspberry Pi Pico H: Functions as the edge microcontroller for processing sensor inputs and controlling the buzzer alerts.
- HC-SR501 PIR Sensor: Detects abnormal body movements around the examination desk.
- IR Obstacle Sensor: Monitors under-desk activities to identify hidden object movement beyond the camera's field of view.
- USB Webcam: Captures live video for continuous visual monitoring.
- 5V Active Piezo Buzzer: Generates localized audio alerts whenever suspicious activities are detected.
- TTL USB Programmer: Used for programming the ESP32-CAM module.
- Laptop/Computer: Acts as the central processing unit for executing deep learning models and hosting the monitoring dashboard.

2.2 Software Components

- Python 3.x: Primary programming language for implementing the AI algorithms and system logic.
- OpenCV: Used for image acquisition, preprocessing, and computer vision operations.
- YOLOv8 Nano: Performs real-time detection of unauthorized mobile phones and other objects.
- ResNet-10 Deep Neural Network: Detects and counts human faces for monitoring student presence and proximity.
- Flask Framework: Hosts the real-time web dashboard for examination monitoring.
- Arduino IDE: Used to program the ESP32-CAM and Raspberry Pi Pico H firmware.
- PySerial: Enables serial communication between the central computer and Raspberry Pi Pico H.
- Threading Library: Ensures synchronized processing of multiple camera streams.

2.3 Development Environment

- Operating System: Windows
- Programming Languages: Python and C++
- Development Tools: Visual Studio Code, Arduino IDE
- Deep Learning Frameworks: OpenCV DNN and Ultralytics YOLOv8
- Communication Protocols: Wi-Fi and USB Serial Commuication.

Procedure Methodology Methods

The proposed AI-Based Cheating Detection System employs a multi-modal approach by integrating deep learning-based computer vision with edge IoT hardware to achieve real-time examination monitoring. The overall methodology consists of image acquisition, AI-based visual analysis, sensor-based monitoring, decision-making, and alert generation.

2.4 System Architecture

The system consists of a central processing unit, an ESP32-CAM wireless vision node, a Raspberry Pi Pico H microcontroller, PIR and IR sensors, and a buzzer module. Live video streams are captured simultaneously from a webcam and the ESP32 -CAM and transmitted to the central processing unit. The Raspberry Pi Pico H continuously monitors the PIR and IR sensors and communicates with the central system through serial communication.

2.5 Image Acquisition

The webcam and ESP32-CAM continuously acquire real-time video frames from the examination hall. The ESP32-CAM transmits video wirelessly through a Wi-Fi network, while the webcam provides direct video input to the processing system. These video streams are processed concurrently for intelligent surveillance.

2.6 AI-Based Visual Analysis

Each captured frame undergoes preprocessing using OpenCV before being analyzed by two deep learning models.

- ResNet-10 is employed for face detection and counting to identify missing students, extra persons, and student proximity.
- YOLOv8 Nano performs real-time object detection to identify unauthorized mobile phones and other prohibited devices within the examination environment.

The combination of these models enables accurate and efficient detection while maintaining real-time performance on standard computing hardware.

2.7 Sensor-Based Monitoring

To eliminate the blind spots associated with camera-only surveillance, the system integrates two hardware sensors.

- The Passive Infrared (PIR) sensor detects abnormal body movements around the examination desk.
- The Infrared (IR) sensor monitors under-desk activities and detects hidden object movement that may not be visible to the camera.

The Raspberry Pi Pico H continuously processes sensor signals and immediately forwards detected events to the central monitoring system.

2.8 Decision-Making Strategy

The proposed system evaluates six predefined examination scenarios:

1. Face absence detection.
2. Extra person detection.
3. Student proximity (possible whispering).
4. Unauthorized mobile phone detection.
5. Under-desk activity detection using the IR sensor.
6. Abnormal movement detection using the PIR sensor.

Information obtained from the deep learning models and hardware sensors is combined to determine whether suspicious behavior is present. This hardware–software closed-loop approach significantly improves detection reliability.

2.9 Alert Generation and Monitoring

Whenever a violation is detected, the central processing unit immediately sends a control signal to the Raspberry Pi Pico H, which activates a localized buzzer near the corresponding examination desk. Simultaneously, the Flask-based dashboard displays the live video stream with bounding boxes and warning messages, allowing invigilators to monitor multiple examination benches in real time.

2.10 Experimental Evaluation

The proposed system was evaluated under various examination scenarios to assess its performance in detecting suspicious activities. The evaluation considered real-time detection capability, response latency, sensor performance, and system scalability. The integrated architecture demonstrated efficient real-time monitoring while maintaining reliable communication between the AI models, IoT hardware, and web-based monitoring dashboard.

III. RESULT

The proposed AI-Based Cheating Detection System was successfully implemented and evaluated under multiple examination scenarios to validate its real-time monitoring performance. The integrated framework effectively combined computer vision and IoT-based sensing to detect suspicious activities with high reliability.

The ResNet-10 model accurately detected and counted student faces, enabling reliable identification of face absence, extra person presence, and student proximity. The YOLOv8 Nano model successfully detected unauthorized mobile phones in real time by generating bounding boxes and alert notifications. Simultaneously, the PIR and IR sensors effectively identified abnormal body movements and under-desk activities that could not be captured through camera-based monitoring alone.

The developed Flask-based dashboard displayed live video streams with real-time annotations, including detected faces, mobile phones, and system status messages, allowing invigilators to monitor multiple examination benches simultaneously. Upon detection of suspicious behavior, the Raspberry Pi Pico H immediately activated a localized buzzer, providing instant physical alerts.

Performance evaluation demonstrated that the system processed live video streams at approximately **15–20 frames per second (FPS)** while maintaining **hardware response latency below 50 ms**, ensuring rapid detection and notification. The implementation of thread synchronization enabled stable processing of multiple camera streams without memory conflicts or system crashes. These results demonstrate that the proposed multi-modal architecture provides an accurate, scalable, and cost-effective solution for intelligent examination monitoring, significantly improving the efficiency of detecting examination malpractice while assisting human invigilators.

IV. DISCUSSION

The experimental results demonstrate that the proposed AI-Based Cheating Detection System provides an effective solution for intelligent examination monitoring by combining deep learning techniques with edge-based IoT hardware. Unlike conventional surveillance systems that rely solely on visual monitoring, the proposed framework integrates ResNet-10, YOLOv8 Nano, and PIR/IR sensors to improve detection accuracy while minimizing the limitations associated with camera-only monitoring.

The integration of computer vision with physical sensors significantly enhanced the system's capability to identify a wide range of suspicious activities, including unauthorized mobile phone usage, face absence, extra person detection, abnormal movement, student proximity, and under-desk activities. The use of PIR and IR sensors effectively eliminated camera blind spots, thereby reducing the possibility of undetected cheating attempts.

The implementation of edge computing and a hardware–software closed-loop architecture enabled real-time processing with low latency, allowing immediate activation of localized buzzer alerts whenever suspicious behavior was detected. Furthermore, the Flask-based dashboard provided continuous visualization of live video streams with real-time annotations, improving situational awareness for invigilators. The use of thread synchronization also ensured stable operation when processing multiple camera streams simultaneously.

Although the proposed system demonstrated reliable performance under experimental conditions, its effectiveness may be influenced by factors such as lighting variations, camera positioning, and hardware resource limitations in large-scale deployments. Future improvements may include incorporating advanced human activity recognition, multi-camera tracking, and transformer-based deep learning models to further enhance detection accuracy and scalability.

Overall, the proposed system offers a scalable, low-cost, and practical solution for smart examination monitoring, contributing to improved academic integrity through accurate and real-time cheating detection.

V.CONCLUSION

This paper presented an AI-Based Cheating Detection System for Examination Monitoring that combines deep learning, computer vision, and IoT-based edge computing to enhance academic integrity during examinations. The proposed system integrates ResNet-10 for face detection and counting, YOLOv8 Nano for unauthorized mobile phone detection, and PIR/IR sensors for monitoring abnormal movements and under-desk activities. By employing a hardware–software closed-loop architecture, the system provides real-time detection and immediate alert generation through localized buzzer activation.

Experimental evaluation demonstrated that the system effectively detected multiple cheating-related scenarios, including face absence, extra person presence, student proximity, unauthorized device usage, abnormal movement, and hidden under-desk activities. The Flask-based dashboard enabled continuous real-time monitoring, while the integration of physical sensors successfully eliminated camera blind spots and improved overall detection reliability. The system achieved stable multi-camera operation with low latency and efficient resource utilization, making it suitable for deployment in educational environments.

Overall, the proposed solution offers a scalable, cost-effective, and intelligent examination monitoring framework that assists invigilators in maintaining fair examination practices. Future work may focus on incorporating advanced behavior analysis techniques, additional camera nodes, and enhanced deep learning models to further improve detection accuracy and scalability in large examination halls.

REFERENCES

1. M. Masud, A. G. Alqahtani, S. M. M. Rahman, and M. S. Hossain, "Smart Online Exam Proctoring Assist for Cheating Detection," Computers and Electrical Engineering, vol. 101, pp. 108–120, 2022.
2. M. A. Al-Airaji, H. T. Hazim, and A. S. Abdullah, "Automated Cheating Detection in Examination Halls Using Video Surveillance and Deep Learning," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 13, no. 5, pp. 115–123, 2022.
3. Y. Li, X. Zhang, and H. Wang, "A Multi-Index Examination Cheating Detection Method Based on Neural Networks," IEEE Access, vol. 7, pp. 156789–156799, 2019.
4. "Detection of Exam Cheating through Surveillance using Face Detection with AI," International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), 2025.
5. J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 779–788, 2016.
6. G. Jocher, A. Chaurasia, and the Ultralytics Team, "YOLOv8: State-of-the-Art Real-Time Object Detection," Ultralytics, 2023.
7. K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 770–778, 2016.
8. G. Bradski, "The OpenCV Library," Dr. Dobb's Journal of Software Tools, 2000.
9. Raspberry Pi Foundation, "Raspberry Pi Pico Documentation," 2023.
10. Espressif Systems, "ESP32-CAM Technical Reference Manual," 2023.
11. A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," Advances in Neural Information Processing Systems (NeurIPS), vol. 25, pp. 1097–1105, 2012.
12. R. Girshick, "Fast R-CNN," Proceedings of the IEEE International Conference on Computer Vision (ICCV), pp. 1440–1448, 2015.
13. J. Long, E. Shelhamer, and T. Darrell, "Fully Convolutional Networks for Semantic Segmentation," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 3431–3440, 2015.
14. T.-Y. Lin, P. Goyal, R. Girshick, K. He, and P. Dollár, "Focal Loss for Dense Object Detection," Proceedings of the IEEE International Conference on Computer Vision (ICCV), pp. 2980–2988, 2017.
15. M. Everingham, L. Van Gool, C. K. I. Williams, J. Winn, and A. Zisserman, "The Pascal Visual Object Classes (VOC) Challenge," International Journal of Computer Vision, vol. 88, no. 2, pp. 303–338, 2010.
16. A. Howard et al., "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications," arXiv:1704.04861, 2017.

17. J. Deng et al., "ImageNet: A Large-Scale Hierarchical Image Database," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 248–255, 2009.
18. M. Abadi et al., "TensorFlow: Large-Scale Machine Learning on Heterogeneous Systems," Google Research, 2016.
19. Raspberry Pi Foundation, Getting Started with Raspberry Pi Pico, Raspberry Pi Press, Cambridge, UK, 2021.
20. Espressif Systems, ESP32 Technical Reference Manual, Version 4.9, Shanghai, China, 2023.
21. G. Bradski and A. Kaehler, Learning OpenCV: Computer Vision with the OpenCV Library, O'Reilly Media, 2008.
22. A. Rosebrock, Practical Python and OpenCV, PyImageSearch, 2021.
23. U. D. of Education, "Artificial Intelligence in Education: Challenges and Opportunities," U.S. Department of Education, Washington, DC, USA, 2023.
24. N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 886–893, 2005.
25. S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 39, no. 6, pp. 1137–1149, 2017.