WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

SentinelEye: AI-Based Examination Malpractice Detection System

[1]Ms.Sivadharshini R, [2]Harish N, [3]Kamalesh J,[4]John Peter D,[5]Kiruthick V

Sri Shakthi Institute of Engineering and Technology, Coimbatore
E-Mail Id: johnpeter2212007@gmail.com

ABSTRACT

The AI-Based Offline Exam Malpractice Detection System is designed to identify potentially suspicious activities during physical examinations using artificial intelligence and computer vision. The system analyses video captured through CCTV cameras or webcams to detect behaviours such as repeated head movements, interactions between students, and the presence of unauthorised materials.

The proposed system integrates video processing, face detection, object detection, and behaviour analysis to assist invigilators in monitoring examination halls. When suspicious activity is identified, the system can generate alerts and preserve relevant snapshots or records for further review. By supporting continuous video analysis, the system aims to reduce the workload of invigilators and improve the efficiency and transparency of examination supervision. All generated alerts should be reviewed by authorised personnel before any conclusion about malpractice is reached.

Keywords: Artificial Intelligence, Offline Examination, Malpractice Detection, Computer Vision, YOLO, OpenCV, Real-Time Monitoring.

INTRODUCTION

Maintaining academic integrity during offline examinations is an important responsibility for educational institutions. Traditional invigilation depends on human observation, which can become challenging when many students are seated in a large examination hall. Brief suspicious activities may be overlooked, and reviewing recorded footage can require considerable time.Artificial intelligence provides an opportunity to support examination supervision through automated video analysis. The proposed system uses CCTV or webcam input to analyse student movements, detect people and selected objects, and identify behaviour patterns that may require further investigation.

The system is intended to assist invigilators by providing monitoring information and alerts through a user interface. It does not replace human supervision or independently establish whether a student has committed malpractice.

LITERATURE REVIEW

Computer vision and deep learning are widely used in surveillance applications to detect objects and analyse visual activities. Convolutional Neural Networks and object-detection models can identify people and selected objects in video frames. These techniques can support the identification of potentially unauthorised materials, including mobile phones and paper notes.

Deep learning models, particularly Convolutional Neural Networks (CNNs), are commonly used for detecting suspicious behaviors, including:

- Head movement analysis
- Eye Gaze Analysis
- Object detection (mobile phones, paper chits)
- Body Pose and Head Orientation Analysis
- Multiple person detection

Behaviour analysis techniques can also examine head movements and interactions between nearby individuals. Combining multiple visual indicators may provide more useful information than relying on a single detection result.

However, performance can be affected by poor lighting, camera angles, occlusion, crowded seating arrangements, and variations in student behaviour. Privacy and data security are also important considerations when processing examination videos. These challenges highlight the need for appropriate testing, reliable evidence management, and human review of generated alerts.

METHODOLOGY

Requirements Analysis

- CCTV or webcam-based monitoring
- Real-time video processing
- Detection of suspicious behaviour
- Eye-gaze and head-movement analysis
- Detection of unauthorised objects

System Design

The system consists of the following modules:

- Video Capture Module
- Face Detection Module
- Eye-Gaze Detection Module
- Head and Body Pose Estimation Module
- Object Detection Module
- Behaviour Analysis Module
- Alert Generation Module
- Evidence Storage Module
- Monitoring Dashboard

Frontend

The frontend provides an interface for invigilators to monitor examination sessions and review suspicious events. It displays session status, available video information, generated alerts, and associated evidence. The interface should distinguish between active monitoring, completed sessions, and processing failures.

Backend

The backend is implemented using Python, integrating OpenCV and deep learning models for video processing and analysis.

AI Model

- Person and Object Detection: Detects people and configured objects using the available vision models.
- Person Tracking: Maintains person identities across video frames.
- Eye-Gaze Estimation: Analyses students' looking direction when the relevant model is enabled.
- Head-Pose Estimation: Analyses head orientation and turning direction.
- Person-Turning Detection: Identifies sideways or backward body-turning movements using available visual cues.
- Hand and Body-Pose Analysis: Analyses hand movements, posture, and body position when the relevant models are enabled.
- Behaviour Analysis: Generates events from configured visual behaviour patterns.
- Risk Analysis and Decision Agent: Evaluates event history and assigns a decision level based on configured risk weights.
- Review Agent: Supports incident review when an AI review provider is configured.

Working Process

1. Capture Video: Obtain video from a CCTV camera, webcam, or uploaded video file.
2. Process Frames: Process video frames through the computer vision pipeline.
3. Detect and Track People and Objects: Identify people and configured objects and maintain tracking identities across frames.

4. Analyse Behaviour Cues: Analyse head pose, eye gaze, hand movements, body posture, person-turning direction, and other available visual cues.
5. Generate Events: Generate events when configured behaviour patterns are detected, such as PHONE_VISIBLE or LOOK_AROUND.
6. Maintain Event Memory: Group recent events by person track and preserve behavioural context across frames.
7. Calculate Risk: Evaluate the event history using configured risk weights to calculate a risk score.
8. Apply the Decision Agent: Map the risk score to a decision level, such as observation, warning, or review required.
9. Generate Alerts and Preserve Evidence: Create alerts for qualifying decisions and store available snapshots and event metadata.
10. Review Flagged Incidents: Use the review agent to prepare incident reviews when an AI review provider is configured. This feature supports, but does not replace, human judgement.
11. Display Dashboard Results: Display live status, alerts, risk information, and available evidence on the dashboard for invigilator verification.

CONTENT

AI-based offline exam malpractice detection is a modern solution designed to improve fairness and transparency in physical examination environments. With the increasing number of students appearing for offline examinations, maintaining effective supervision in large examination halls has become a major challenge. Traditional invigilation methods rely heavily on human observation, which can be inconsistent and prone to errors.

The proposed system uses artificial intelligence techniques such as computer vision, deep learning, object detection, and behaviour analysis to monitor student activities through CCTV cameras, webcams, or uploaded video files. It analyses visual cues such as eye gaze, head movements, person-turning direction, hand movements, and body posture. It also detects supported objects, such as mobile phones and paper chits, when the configured detection models are trained to recognise them.

By automating parts of the monitoring process, the system assists invigilators in identifying potentially suspicious activities. The system generates events when configured behaviour patterns are detected and maintains event history to preserve context across video frames. A risk-analysis component evaluates these events and assigns a risk level based on configured weights.

When predefined conditions are satisfied, the system generates alerts and stores available snapshots and event information for further review. An optional AI review component can assist with preparing incident summaries when a review provider is configured. The monitoring dashboard displays live status, alerts, risk information, and available evidence for invigilator verification.

Overall, the system aims to provide an efficient and traceable approach to supporting academic integrity in offline examinations. AI-generated alerts are intended to assist human supervision and should not be treated as conclusive proof of malpractice.

Table 1: Overview of Key Features in AI-Based Offline Exam Malpractice Detection

Feature	**Description**	**Technology Used**
Face Detection	Identifies visible student faces in the examination hall.	OpenCV
Head Movement Detection	Detects head turning and changes in head orientation.	Computer Vision
Multiple Person Detection	Identifies multiple people in video frames	YOLO26s
Object Detection	Detects supported objects, such as mobile phones and paper chits.	YOLO
Behavior Analysis	Analyzes suspicious student actions	Computer Vision
Real-Time Monitoring	Processes live camera streams or uploaded videos.	OpenCV, Streaming
Alert System	Generates alerts when configured risk conditions are satisfied.	Risk Engine
Data Storage	Stores available snapshots and event records for review.	Database
Scalability	Supports extending the system to additional cameras and examination halls, subject to deployment capacity.	Server Infrastructure
Data Security	Restricts access to monitoring records and protects sensitive information.	Authentication / Access Control
Eye-Gaze Estimation	Analyses students' looking direction.	L2CS-Net
Person Tracking	Maintains person identities across video frames.	ByteTrack

Fig 1:Login page

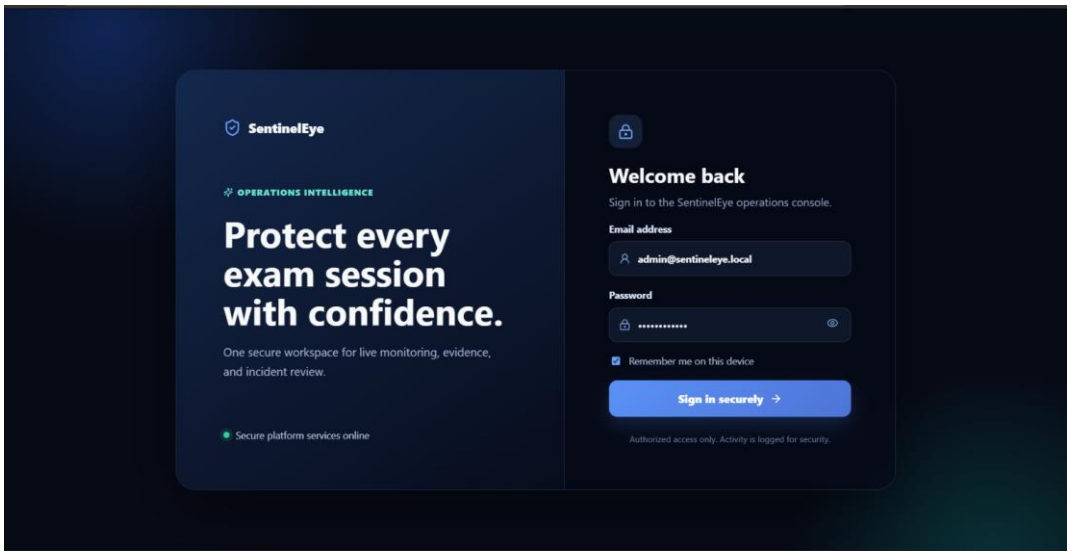
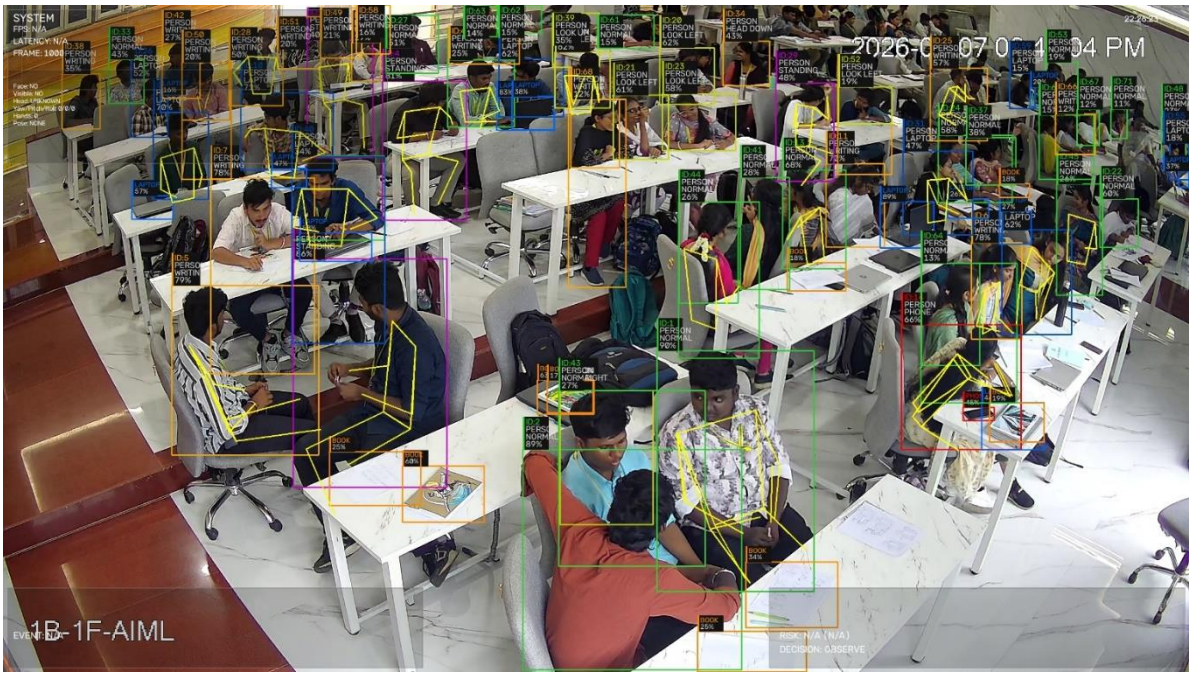


Fig 2:real time classroom monitoring and behavior detection



SYSTEM FEATURES

The proposed AI-based offline exam malpractice detection system incorporates several advanced features to ensure effective monitoring and detection of suspicious activities in physical examination halls.

Feature	**Description**	**Technology**
Face Detection	Identifies visible student faces in the examination hall.	OpenCV
Head-Pose Estimation	Analyses head orientation and head-turning movements.	OpenCV
Person-Turning Detection	Identifies sideways or backward body-turning movements.	Computer Vision / Pose Estimation
Person Detection and Tracking	Detects people and maintains their identities across video frames.	YOLO26s / ByteTrack

Feature	Description	Technology
Behavior Analysis	Analyzes suspicious activities	ML Models
Alert System	Sends real-time alerts	Real-time Processing
Data Security	Protects recorded data	Encryption
Eye-Gaze Estimation	Analyses students' looking direction to identify repeated gaze deviations.	L2CS-Net
Object Detection	Detects supported objects, such as mobile phones and paper chits	YOLO
Hand and Body-Pose Analysis	Analyses hand movements, posture, and body position.	MediaPipe / YOLO Pose

RESEARCH AND REVIEW

Recent research in AI-based examination monitoring focuses on using computer vision and deep learning to analyse student behaviour in physical examination halls. AI-based surveillance systems process CCTV footage to identify activities that may require further investigation.

Deep learning models and computer vision techniques support person detection, object detection, and behaviour analysis. These techniques can help identify head movements, eye-gaze deviations, person-turning movements, and potentially unauthorised objects such as mobile phones and paper chits.

Combining multiple visual cues can provide more useful information for examination monitoring. Person tracking helps maintain identities across video frames, while event analysis preserves behavioural context over time. Risk analysis can then evaluate detected events and generate alerts for invigilator review.

Despite these developments, challenges such as poor lighting, partial occlusion, crowded seating arrangements, and variations in student behaviour can affect system performance. Privacy and data security must also be considered when processing examination videos.

Recent development approaches focus on improving detection reliability, reducing false-positive alerts, and providing explainable results. Human review remains essential when evaluating potentially suspicious activities.

RESULTS AND DISCUSSION

Results

- Detects people and supported objects in examination video.
- Analyses eye gaze, head movements, and person-turning behaviour when the relevant models are enabled.
- Generates events when configured behaviour patterns are detected.
- Calculates risk scores using event history and configured risk weights.
- Generates alerts and preserves available evidence for review.
- Displays monitoring status, alerts, and evidence through the dashboard.

Discussion

The proposed system combines video processing, person detection and tracking, behaviour analysis, event memory, and risk assessment to support examination monitoring. By analysing multiple visual cues, it aims to help invigilators identify activities that may require further investigation.

However, performance may be influenced by:

- Poor lighting conditions.
- Camera positioning and viewing angles.
- Occlusion caused by crowded seating.
- Inaccurate gaze or pose estimation.

- False-positive alerts caused by normal student movements.
- Processing delays when analysing video in real time.
-

Further evaluation should measure detection performance, alert precision, false-positive rates, and processing speed using representative examination videos. Results should be reported only after actual testing.

CONCLUSION

The AI-Based Offline Exam Malpractice Detection System provides a proposed approach to supporting supervision in physical examination halls through computer vision and deep learning. It combines person detection, tracking, eye-gaze analysis, head-pose estimation, person-turning detection, object detection, and behaviour analysis where the relevant models are available..

The system evaluates generated events, calculates risk scores, and produces alerts with available evidence for invigilator review. Its monitoring dashboard supports the review of suspicious events and helps maintain records of detected activities.

The system aims to improve monitoring efficiency and support academic integrity in offline examinations. Its reliability depends on model performance, video quality, and appropriate configuration. AI-generated alerts should support human decision-making rather than serve as conclusive proof of malpractice.

REFERENCES

1. Python Software Foundation. Python Documentation. Available at: https://docs.python.org/3/
2. OpenCV. Open Source Computer Vision Library Documentation. Available at: https://opencv.org/
3. Ultralytics. YOLO Documentation. Available at: https://docs.ultralytics.com/
4. Zhang, Y., Sun, P., Jiang, Y., et al. (2022). ByteTrack: Multi-Object Tracking by Associating Every Detection Box. European Conference on Computer Vision (ECCV). Available at: https://arxiv.org/abs/2110.06864
5. FastAPI. FastAPI Framework Documentation. Available at: https://fastapi.tiangolo.com/
6. MongoDB Inc. MongoDB Documentation. Available at: https://www.mongodb.com/docs/
7. Google AI. MediaPipe Solutions Guide. Available at: https://ai.google.dev/edge/mediapipe/solutions/guide
8. Abdelrahman, A. A., Hempel, T., Khalifa, A., et al. L2CS-Net: Fine-Grained Gaze Estimation in Unconstrained Environments. Available at: https://arxiv.org/abs/2203.03339