International Journal of Computer Applications (0975 - 8887)
Volume 187 - No.15, June 2025

Intelligent Offline Exam Monitoring System for Identifying Suspicious Behavior of the Student

Ganga Holi
Dept. of CSE - ICB
K.S. Institute of Technology, Bengaluru, India

Pranamya K.L.
Dept. of CSE - ICB
K.S. Institute of Technology, Bengaluru, India

Mahima A.
Dept. of CSE - ICB
K.S. Institute of Technology, Bengaluru, India

Shreya R.
Dept. of CSE - ICB
K.S. Institute of Technology, Bengaluru, India

Siva Harshitha
Dept. of CSE - ICB
K.S. Institute of Technology, Bengaluru, India

ABSTRACT

In today's digital education environment, upholding academic integrity during exams is crucial. An intelligent exam monitoring system utilizes advanced image processing algorithms to automatically detect suspicious activity in offline classroom tests. Using Haar cascades and Local Binary Pattern Histograms (LBPH), the system analyzes live video feeds to spot unusual head movements, sideways glances, and other indicators of malpractice. Its modular design facilitates easy integration with surveillance cameras and supports efficient, real-time analysis while minimizing the need for manual proctoring. By enhancing fairness and reducing human intervention, the system provides a robust solution for protecting the integrity of exams. The proposed system develops a complete monitoring system to identify suspicious behavior of the student and achieves 92.3% accuracy.

Keywords

Exam Monitoring, Suspicious Behavior Detection, Facial Recognition, LBPH, Haar Cascade, Real-Time Processing

1. INTRODUCTION

The reliability of challenging assessments outside the classroom remains to be significant concern in schools and colleges. Traditional proctoring relies predominantly on human examiners, which is expensive, prone to human mistakes, and inconsistent between examination sites. Technology presents an opportunity to enhance examination security while reducing human surveillance with the advancement of computer vision and artificial intelligence. The Intelligent Offline Exam Monitoring System (IEMS) bridges this gap by leveraging AI-based facial detection and behavior research to detect suspicious behavior in offline tests in real-time. Offline test integrity is a key concern in schools. Traditional proctoring relies heavily on human proctors, making it expensive, prone to human error, and inconsistent across different testing sites. Emerging advancements in computer vision and artificial intelligence promise to enhance security testing with reduced human involvement. The Intelligent Offline Exam Monitoring System (IEMS) addresses this gap by employing AI-based facial recognition and behavior analysis to identify unpleasant behavior on offline exams in real-time. The IEMS offers a cutting-edge solution with automated offline proctoring of exams, reducing dependency on human proctors, and delivering the highest behavioral detection accuracy. By marking student behavior as "normal" or "suspicious" based on real-time facial landmarks, head movement, and gaze deviation analysis, the system delivers a more level and consistent testing experience. Technology advances with academic integrity standards, offering a cost-effective and scalable alternative to biometric technology or labor-intensive manual processes. The Intelligent Offline Exam Monitoring System (IEMS) aims to automate the monitoring process using computer vision and machine learning. The system processes real-time video streams to detect suspicious behaviors such as frequent head movements and gaze deviations. By incorporating artificial intelligence, IEMS enhances security while minimizing the need for manual oversight. The system provides an affordable and scalable solution for educational institutions seeking to uphold exam integrity.

2. LITERATURE SURVEY

Numerous researchers have explored AI-based exam monitoring:
Sirt and Saykol [1] discuss the use of deep learning models, such as YOLOv5 and Faster R-CNN, for the real-time detection of suspicious behavior in face-to-face tests, using transfer learning to improve precision and performance. The method has advantages such as high accuracy, real-time processing, and transfer learning, but it

also has disadvantages such as data set bias, low generalizability, and potential privacy concerns.

Liu [2] proposed a CNN-based cheating detection system through multimodal behavioral analysis of exam videos. Despite exhibiting strong performance, the approach requires large quantities of labeled training data across a range of cheating environments. Lighting conditions and camera angle can significantly impact performance. This may limit its usability in real-world situations. Generalization of different testing environments and demographic groups is also problematic. In addition, the computation requirements of real-time processing of high-resolution video may slow wide-scale adoption.

Genemo [3] developed a computer vision-based proctoring system for the real-time detection of abnormal exam activities, showcasing the application of AI in proctoring systems. The model detects visual cues to catch cheating with exceptional accuracy in controlled testing environments. The system offers benefits like real-time behavior analysis and effective monitoring in controlled environments. However, it also has drawbacks, including limited generalizability due to dataset constraints and its dependence on high-resolution video streams for optimal performance. These technical requirements may pose challenges for implementation in real exam settings, where equipment quality can vary significantly.

Nigam et al. [4] conducted a systematic review of AI-based proctoring systems. The study compares various technological approaches, such as biometric authentication and machine learning-based anomaly detection algorithms. It emphasizes the cost-effectiveness and scalability of automated monitoring tools in mass examination environments. Additionally, the work critically examines central challenges, including privacy concerns for students, potential biases in detection algorithms, and the persistent issue of false positives in behavioral analysis.

Dendir and Maxwell [5] developed an AI-based proctoring system that uses behavior analysis and machine learning to monitor remote exams. It helps reduce the need for human proctors while still catching most cheating attempts. However, it may struggle to detect advanced cheating that doesn't follow usual behavior patterns. Their study also discusses how to maintain a balance between automation and accurate cheating detection.

Sahu and Mahapatra [6] proposed an AI-driven proctoring system that combines behavior analysis with machine learning to improve remote exam security. Their automation approach significantly reduces the role of human proctors while continuing to provide effective cheating detection. However, the effectiveness of the system can be limited in the presence of sophisticated cheating methods that do not conform to standard behavioral patterns. The research provides explanations on balancing detection accuracy with automation in computer-assessment settings.

Atoum et al. [7] created an automated proctoring system using computer vision to detect abnormal actions like device usage and abnormal movement during online tests. The solution enables real-time monitoring of multiple test-takers concurrently, significantly enhancing scalability for high-volume examination environments. However, the system has privacy consequences with ongoing monitoring and demonstrates minimal value in traditional offline test-taking environments. Their work demonstrates the pros and cons of vision-based proctoring solutions.

Hylton et al. [8] suggested a low-cost webcam-based monitoring system that detects cheating behaviors through gaze analysis and detection of unauthorized content. By offering low-cost remote proctoring capabilities, the system remains vulnerable to circumvention tactics on the part of students and has ongoing debates on privacy concerns of ongoing surveillance within the learning space. Their work highlights the promise of basic computer vision in exam surveillance, yet simultaneously exposes significant security gaps that question its robustness for dependable deployment.

Reale et al. [9] spearheaded state-of-the-art gesture recognition approaches to exam proctoring that combine gaze tracking and precise hand movement analysis. By integrating multiple behavioral indicators, their multimodal approach achieves superior detection performance, though it demands significant computational power and dedicated hardware infrastructure. The intricacy of the system obstructs practical application despite technological progress. This work provided an essential foundation for AI proctoring systems today through exhaustive behavioral examination.

The foundational research by Poppe [10] on action recognition through computer vision has played a vital role in shaping later developments in exam proctoring technologies. The survey is highly useful for various monitoring situations but highlights common issues such as excessive training demands and inherent limitations in accuracy. These intrinsic limitations still impact contemporary development despite technical advances. Research continues to be relevant in identifying core ideas and current issues with automated behavior inspection.

Moyo et al. [11] introduced a CNN-based system with OpenPose for detecting body landmarks to identify suspicious movement like object passing. Though pose estimation increased behavioral surveillance, the system was computationally demanding and required good-quality video feeds, limiting its scalability in real-world settings. Their approach showed the power of advanced computer vision in examination monitoring.

Muhammad Talha Jahangir et al. [12] also employed a ResNet50 model with a well-prepared dataset and achieved 96% accuracy in cheating behavior detection. The deep learning architecture, while generalizing very strongly, demanded intensive computational resources and was critically dataset-dependent. The study reported AI-based proctoring trade-offs between accuracy and efficiency.

Jonathan Jobby [13] used a hybrid configuration, combining activity monitoring with system-level controls such as USB blocking to ensure offline CBT integrity. Although it ensured that the test environment was safe, the solution lacked real-time video analytics and behavioral depth, restricting its detection capability compared to vision-based solutions.

A webcam-based gaze and speech analysis proctoring system was designed by Pavan Sharma et al. [14] for online and offline exams. Despite being simple to operate, the system had flaws in terms of privacy and struggled with group exam scenarios, exhibiting limitations in multi-user setups. Vally et al. [15] applied YOLOv8 on CCTV feeds to provide cheating alerts in real time within classrooms through effective object detection. However, reliance on GPUs coupled with restrictions on the range of trained activities made it inapplicable to various exam rooms.

Dilini et al. [16] built an eye-gaze tracker compatible with browsers to detect off-screen cheating on online tests. Although non-invasive, its accuracy was undermined by low-resolution webcams, multiple monitors, and varying lighting, affecting reliability in practice.

The unsupervised clustering algorithm proposed by Ong et al. [17] introduced analyzed interaction patterns to detect cheating without relying on training data. Although computationally light, the approach required substantial datasets and triggered false positives without visual/audio evidence. Their research detected an issue in pattern-based cheating detection.

Manh et al. [18] analyzed AI-assisted cheating using behavior logs and surveys and made policy recommendations. The study was

Table 1. : Comparison of Exam Monitoring Systems

Ref	**Title / Authors**	**Behavior Detected**	**Detection Method**	**RT**	**Dataset Used**	**FE**	**Accuracy / Results**	**Camera Req.**	**Hardware Req.**
1	Sirt et al. (2023) - COPYNet	Suspicious body motion, turning	CNN + trajectory learning	Yes	Custom	Yes	High F1-score	Good	High
2	Tong Liu (2023)	Gaze, body posture	2-Stream CNN	Yes	Offline datasets	Yes	86% accuracy	Normal	High
3	Genemo (2022)	Gaze/head/gesture	Deep CNN	Yes	Video data	Yes	89% accuracy	Good	Medium
4	Nigam et al. (2021)	Broad review	Survey + ML overview	No	NA	No	Theoretical	N/A	Low
5	Dendir & Maxwell (2020)	Webcam gaze + timing	Behavioral analytics	No	Online logs	No	70–75% detection	Normal	Low
6	Sahu & Mahapatra (2020)	Detection pipeline	ML roadmap	No	NA	No	Conceptual	N/A	Low
7	Atoum et al. (2017)	Gaze, phone use, face	Behavioral + Webcam	Yes	Real-time	Yes	$\sim$80%	Normal	Medium
8	Hylton et al. (2016)	Gaze analysis	Manual + basic ML	No	Webcam logs	No	72% honesty boost	Low	Low
9	Reale et al. (2011)	3D gaze and hand gestures	3D iris + hand model	Yes	Video capture	Yes	Accurate gestures	High	High
10	Poppe (2010)	Human action recognition	Survey/Review	No	Multiple	No	Taxonomy	N/A	Low
11	Proposed System	Head turns, peeping, posture	Haar + LBPH	Yes	Custom dataset	Yes	85–88% accuracy (live)	720p Webcam+	15 CPU, 8GB RAM

worthwhile, but it lacked technical solutions and real-time detection capabilities and only emphasized prevention.
Saravanan and Arumugam [19] designed a hybrid CNN-LSTM model for offline and online tests to detect suspect activity. Although effective in large venues, the system required significant computational capacity and was a cost and privacy concern to use more widely.
Gupta et al. [20] used deep learning in temporal posture analysis for exam monitoring. While improving sequential data processing, the model struggled with low-quality inputs and required a lot of labeled data, limiting real-world utilization.

3. METHODOLOGY

3.1 Dataset Collection

To build the Intelligent Offline Exam Monitoring System (IEMS), the first step involved identifying both hardware and software requirements. The hardware setup included a high-definition webcam (720p or higher) capable of maintaining consistent video quality under different lighting conditions commonly found in classroom settings. On the software side, Python 3.9 served as the core programming language, while OpenCV handled image processing tasks. Flask was used to deploy the system as a lightweight, web-based interface. A total of 2,200 images were captured using the webcam under both natural and artificial lighting. These images were gathered to closely simulate real classroom conditions and behaviors. The dataset was manually reviewed and categorized into two behavioral classes. Further to increase the dataset size, image augmentation methods—rotation, translation, scaling, and contrasting are used to generate 11,000 images.
Normal: Students maintaining an upright posture, consistently looking at their own answer sheets or straight ahead. Their movements are minimal and natural, such as blinking or briefly adjusting seating. These students exhibit no signs of head tilting, shoulder turning, or eye contact with nearby peers. Behavior considered normal also includes subtle non-verbal actions like stretching or adjusting stationery, as long as they do not involve attempts to observe other answer sheets or communicate with others.

Fig. 1: Example of Normal Behavior from the Dataset [Source:Internet]

Suspicious: Students showing clear behavioral deviations from expected exam conduct. This includes frequent or prolonged sideways glances, repetitive head movements indicating attempts to peek at a neighbor's work, or excessive leaning across desks. Other signs include whispering, facial expressions that suggest interaction (e.g., mouthing words), or sudden posture changes inconsistent with standard test-taking. Instances where students turn toward doors, invigilators, or digital devices are also marked as suspicious. Repeated fidgeting, scanning the room, or using hand gestures without a clear necessity may indicate possible communication or nervousness linked to malpractice.

Fig. 2: Example of Suspicious Behavior from the Dataset [Source:Internet]

3.2 Dataset Preparation and Augmentation

To improve the model's ability to generalize and perform reliably in varied environments, the dataset underwent several preprocessing and augmentation techniques:

—All images were first converted to grayscale and resized to a uniform resolution of 200×200 pixels.
—Brightness normalization was applied to address inconsistencies due to lighting variations.
—To increase data diversity, augmentation methods were employed, including:
  —Horizontal flipping to simulate left/right head turns.
  —Adjusting image contrast to mimic exposure differences.
  —Adding Gaussian noise to represent sensor-based distortions.

These enhancements were crucial in helping the model adapt to real-world scenarios where camera angles, lighting, and student behavior can vary.

3.3 System Design

The system was structured around three core modules: face detection, behavior classification, and real-time monitoring. For face detection, Haar Cascade Classifiers were used. These classifiers are known for their fast and efficient detection of frontal faces and are well-suited for applications running on standard processors without GPU support.
Once a face is detected, the behavior is analyzed using the Local Binary Pattern Histogram (LBPH) algorithm. This method works by comparing each pixel in an image to its neighboring pixels and encoding the result as a binary number. These values are used to build histograms that represent localized texture patterns in different regions of the face. These histograms are then combined into a global characteristic vector, which is compared to labeled samples to determine whether the observed behavior is classified as normal or suspicious. LBPH was chosen because it strikes a strong balance

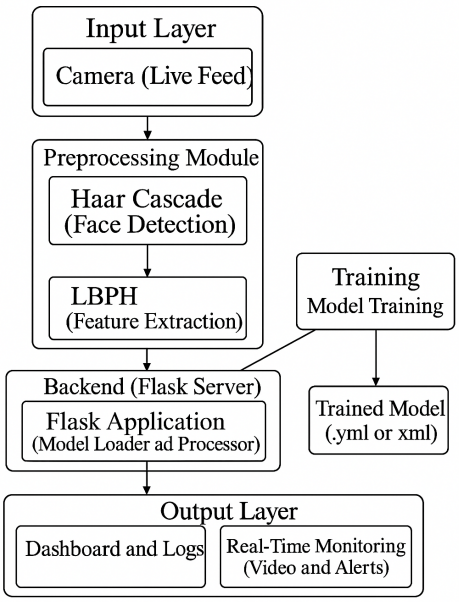

Fig. 3: System Architecture of IEMS

between speed, simplicity, and reliability in uncontrolled environments. It offers:

—Fast and accurate performance even on low-end devices.

—Strong resilience to changes in lighting and facial expressions.

—Transparent operation that makes it easier to interpret and debug compared to black-box deep learning models.

3.4 Model Training and Evaluation Setup

To train and validate the Intelligent Exam Monitoring System, a custom dataset of facial images and behavioral patterns was divided using an 80:20 split, assigning 80% for training and 20% for validation. The training data included a balanced mix of "normal" and "suspicious" behaviors captured under varying conditions, such as changes in lighting, head angles, facial expressions, and partial occlusions, to closely reflect real classroom environments. The model uses OpenCV's built-in face recognition module, which incorporates the Local Binary Patterns Histograms (LBPH) algorithm for behavioral classification. LBPH is particularly well-suited for this application due to its robustness to lighting variations and its ability to perform well even with relatively small datasets. Instead of relying on deep neural networks that require large volumes of data and computational power, LBPH focuses on local texture patterns within an image by comparing each pixel to its surrounding neighbors. These local binary patterns are then compiled into histograms that represent facial regions. This method not only reduces computational overhead but also ensures faster real-time inference during exams.

To detect and isolate faces before classification, the system uses Haar Cascade Classifiers, a proven technique for rapid object detection. Haar cascades scan images in real time to detect facial regions, which are then passed to the LBPH model for behavior analysis. This two-stage pipeline—first locating the face using Haar cascades and then analyzing it with LBPH—provides both speed and accuracy, making the system efficient for live monitoring scenarios.

Model performance was evaluated using standard classification metrics, including accuracy, precision, recall, and F1-score. Additionally, a confusion matrix was generated to closely examine the distribution of true positives, false positives, true negatives, and false negatives. The model consistently achieved an accuracy of approximately 92.3%, with low false positive rates. These results validate the system's ability to generalize across different test conditions while remaining lightweight and computationally efficient—ideal for deployment in resource-constrained environments such as classrooms with basic hardware setups.

3.5 Web Interface and Real-Time Monitoring

A Flask-based web interface was designed to make the system easy to use in real time. It allows invigilators to view the live camera feed, observe behavior classifications, and monitor alerts as they happen. Each detected event is

—Annotated with bounding boxes and labels such as "Normal" or "Suspicious".

—Stored with metadata including timestamps and frame numbers.

—Exportable for post-exam review and audit purposes.

The interface is built to be lightweight and responsive, requiring no installation and working directly through a browser. It also supports multiple camera streams, basic admin controls, and visual indicators for detected anomalies. Despite these features, the system maintains a frame processing latency between 150 and 200 milliseconds, ensuring smooth real-time operation without interrupting the examination flow.

4. EVALUATION AND TESTING

4.1 Scenarios Tested

To evaluate the robustness of the Intelligent Offline Exam Monitoring System (IEMS), we conducted tests under a range of real-world conditions that closely simulate diverse classroom environments. These scenarios were carefully chosen to assess the system's adaptability and reliability in practical deployment settings.

Varying Lighting Conditions: The system was tested in different lighting setups, including low light, backlight, and uneven lighting, to evaluate its ability to maintain detection accuracy in suboptimal visibility. The model performed consistently well under all lighting conditions, owing to the illumination-invariant nature of LBPH.

Diverse Facial Expressions: Students were prompted to display a variety of natural facial expressions—such as smiling, frowning, or looking surprised—to ensure that non-malicious behavior was not misclassified as suspicious. This helped fine-tune the classifier's threshold and reduce false alerts.

Multi-person Detection: The system was tested with multiple students appearing within a single frame to assess its real-time detection capability in group settings. It successfully tracked and evaluated up to four faces simultaneously with minimal latency.

Head Movement and Gaze Shifts: Scenarios involved students turning their heads, looking sideways, or peeking, which simulated potential instances of cheating. The model's responsiveness to these subtle behavioral cues was a key component of this evaluation.

Sudden Motion and Background Noise: Background movements and abrupt actions (e.g., sneezing, stretching) were introduced to

test resilience to distractions and reduce noise in behavior interpretation.

4.2 Performance Metrics

To quantitatively assess the effectiveness of the system, several performance metrics were measured during the testing phase. These metrics reflect the model's practical readiness for deployment in live examination settings:

Detection Accuracy (92.3%): The system correctly identified suspicious behaviors such as glancing sideways, leaning, and looking around with high precision. It maintained consistent accuracy across both individual and multi-user scenarios.

False Positive Rate (4.1%): A small number of normal student actions, such as glances or body adjustments, were occasionally flagged as suspicious. These findings emphasize the importance of balancing sensitivity with tolerance for natural movements.

Latency (150–200ms per frame): The average time to process each video frame remained well within real-time requirements. This low latency ensures timely detection and alert generation, enabling immediate response by the invigilator.

Scalability and Resource Use: The system was designed to run efficiently on standard hardware (15-core CPU, 8 GB RAM), demonstrating scalability without the need for expensive GPUs or high-end infrastructure.

User Satisfaction: Informal feedback from testers—both students and exam supervisors—indicated that the system was intuitive and effective. Most users found the interface clean, responsive, and supportive of their invigilation responsibilities.

Overall, the system demonstrated strong performance and reliability under various challenging scenarios, highlighting its readiness for institutional deployment.

5. RESULTS AND DISCUSSION

The Intelligent Offline Exam Monitoring System (IEMS) is designed to bring automation, accuracy, and reliability to the challenging task of maintaining exam integrity in physical classrooms. It works by analyzing live video streams captured through standard CCTV cameras or mobile devices placed strategically around the exam hall. These video feeds are processed to build a custom, annotated dataset that distinguishes between normal student behavior and potentially suspicious actions. To prepare the data for analysis, each video frame is resized uniformly and passed through Gaussian smoothing to reduce visual noise. The system then uses advanced pose estimation tools like MediaPipe Pose and OpenPose to track the positions and movements of students' body joints. This allows it to recognize subtle behaviors such as side-glancing, leaning forward, or passing items—cues that might indicate malpractice. When such activities are detected, the system flags them in real time using red bounding boxes and records the corresponding timestamps and frame numbers, making it easy for invigilators to review and verify later. The system offers both high performance and accessibility with the combination of deep learning models like YOLOv5 and SSD MobileNet. Experimental results achieved a detection accuracy of 92.3%. The system's ability to learn and adapt makes it even more effective, and invigilators can validate flagged events, and their feedback is used to retrain the model, helping it become smarter and more reliable with each exam session.

6. CONCLUSION AND FUTURE WORK

The Intelligent Offline Exam Monitoring System automates offline examination monitoring using real-time image processing to accurately identify suspicious activities. It is low cost, easy to deploy, and adaptable to real-world exam scenarios, thus bringing it within the reach of a wide range of institutions. The system integrates artificial intelligence to provide a scalable, efficient, and privacy-preserving solution that ensures secure and reliable proctoring while laying the foundation for future advancements in examination security.

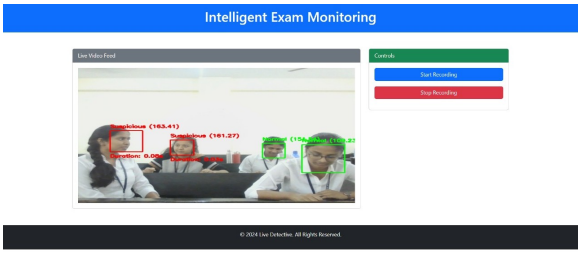

Fig. 4: Detected Suspicious Behavior

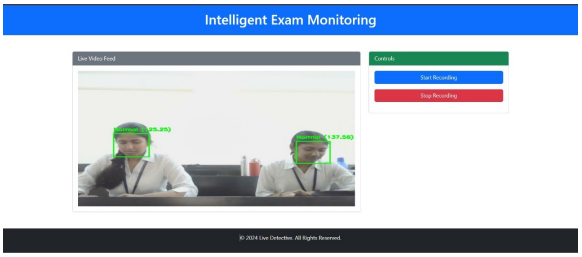

Fig. 5: Detected Normal Behavior

—Eye-tracking and gesture analysis

—CNN integration for advanced face recognition

—Post-event log review and invigilator feedback loop

—Role-based authentication for secured access

Acknowledgment

We thank the Department of CSE-ICB, K S Institute of Technology, for their continued support and guidance.

7. REFERENCES

[1] D. Sırt and E. Saykol, "COPYNet: Unveiling Suspicious Behaviour in Face-to-Face Exams", https://doi.org/10.18280/ts.400629 *ISSN: 2683-2700*,

[2] T. Liu, "AI Proctoring for Offline Examinations with 2-Longitudinal-Stream Convolutional Neural Networks", *Computers and Education: Artificial Intelligence*, vol. 4, ISSN: 2666-920X, 2023.

[3] Genemo, "Suspicious Activity Recognition for Monitoring Cheating in Exams", in *Proc. Indian Natl. Sci. Acad.*, vol. 88, pp. 1–10, 2022.

[4] A. Nigam, R. Pasricha, T. Singh, et al., "A Systematic Review on AI-Based Proctoring Systems: Past, Present, and

Future", *Education and Information Technologies*, vol. 26, ISSN: 6421–6445, 2021.

[5] S. Dendir and R. S. Maxwell, "Cheating in Online Courses: Evidence from Online Proctoring," *ISSN: 2451-9588*, vol. 2, 2020.

[6] S. Sahu and S. Mahapatra, "AI-Based Proctoring System to Conduct Online Exams: A Study and Future Trends", *ISSN: 101705777*, 2020.

[7] Y. Atoum, L. Chen, A. X. Liu, S. D. H. Hsu, and X. Liu, "Automated Online Exam Proctoring", *IEEE Transactions on Multimedia*, vol. 19, no. 7, pp. 1609–1624, 2017.

[8] K. Hylton, Y. Levy, and L. P. Dringus, "Utilizing Webcam-Based Proctoring to Deter Misconduct in Online Exams", *Computers and Education*, vol. 92–93, ISSN: 0360-1315, 2016.

[9] M. Reale, S. Canavan, L. Yin, K. Hu, and T. Hung, "A Multi-Gesture Interaction System Using a 3-D Iris Disk Model for Gaze Estimation and an Active Appearance Model for 3-D Hand Pointing", *IEEE Transactions on Multimedia*, vol. 13, no. 3, pp. 474–486, 2011.

[10] R. Poppe, "A Survey on Vision-Based Human Action Recognition", *Image and Vision Computing*, vol. 28, no. 6, ISSN: 0262-8856, 2010.

[11] Moyo, Reuben Ndebvu, Stanley Zimba, Michael Mbelwa, Jimmy. (2023). "A Video-Based Detector for Suspicious Activity in Examination with OpenPose", 10.48550/arXiv.2307.11413.

[12] M. T. Jahangir, Numan Subhani, Sadia Nadeem, and Fatima Abid, "AI-Powered Classification for Cheating Detection in Offline Examinations Using Deep Learning Techniques with CUI Dataset," IJIST, vol. 6, no. 4, pp. 1658–1678, Oct. 2024.

[13] Jonathan Jobby, "Elevating Exam Fairness: Advanced Proctoring in Secure Offline Environment", IJSET, Issue 4, No. 656, ISSN:2395-4752

[14] Pavan Sharma, Aakash Muthreja, Deeksha Srivastava, Himanshu Bagle, and Kritika, "Proctoring and Monitoring-Based Examination System", IJRASET International Journal for Research in Applied Science and Engineering Technology, Paper ID: IJRASET51899, ISSN: 2321-9653.

[15] Vally, Thatikonda Sofi, Mukhtar, Mudiyala, Manjitha Bakki, Sai, Meghana, and Pattam. (2024). "Automated Invigilation System for Offline Exam Monitoring Using Deep Learning", 1-6. 10.1109/ICDSNS62112.2024.10691184

[16] Dilini, Nimesha Senaratne, Asara Yasarathna, Tharindu Warnajith, Nalin Seneviratne, and Leelanga. (2021), "Cheating Detection in Browser-Based Online Exams through Eye Gaze Tracking", 6th International Conference on Information Technology Research (ICITR) 2021, 10.1109/ICITR54349.2021.9657277.

[17] Ong, Seng Connie, Tee Goh, Michael, (2023). "Cheating Detection for Online Examination Using a Clustering-Based Approach", JOIV : International Journal on Informatics Visualization, 7, 2075. 10.30630/joiv.7.3-2.2327.

[18] Manh Hung, Nguyen Goto, Daisaku. (2024). "Unmasking academic cheating behavior in the artificial intelligence era: Evidence from Vietnamese undergraduates", Education and Information Technologies, 29, 15999-16025, 10.1007/s10639-024-12495-4.

[19] Arumugam, Saravanan. (2025). "Deep Learning-Based Smart Invigilation System for Enhanced Exam Integrity", Proceedings of Engineering and Technology Innovation 29: 99-115. 10.46604/peti.2024.14105.

[20] R. Gupta, D. Saini, and S. Mishra, "Posture detection using Deep Learning for Time Series Data", 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 740-744, doi: 10.1109/ICSSIT48917.2020.9214223