WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

AI-Based Proctoring System for Online Tests

Pushpendra Kumar Sahu[1], Vipin Kumar[2]

Department of Computer Science (AIML)
Shri Shankaracharya Technical Campus Bhilai(C.G)

ABSTRACT :

The increased use of online learning platforms, particularly following the COVID-19 pandemic, has emphasized the importance of developing online assessment systems that are secure, dependable, and capable of scaling effectively. Traditional human-proctored exams face challenges such as limited scalability, high operational costs, and subjective error. This research explores the development and implementation of an AI-based proctoring system designed to uphold academic integrity in online examinations. The system integrates facial recognition, voice detection, behavioral analytics, and anomaly detection using computer vision and machine learning algorithms. It provides real-time monitoring while addressing ethical concerns such as privacy, accessibility, and algorithmic fairness. The findings show that AI proctoring systems can significantly improve exam security and reduce cheating incidents. However, careful attention must be paid to inclusivity and data governance to ensure the system is ethical, unbiased, and accessible to all users. This study presents a systematic approach for creating and implementing AI-based proctoring systems, serving as a foundation for future innovations in securing digital education.

I. INTRODUCTION

Background Information:

In recent years, the rapid evolution of digital technologies and the growing need for flexible learning solutions have significantly boosted the popularity of online education. This shift was further amplified by the global Covid-19 pandemic, which forced educational institutions across the globe to transition to virtual learning platforms. As a result, online education has become an essential component of modern learning environments, offering students the convenience of studying from anywhere and at any time.

While online learning provides numerous advantages, such as accessibility, affordability, and the ability to tailor learning experiences to individual needs, it also introduces new challenges, particularly in ensuring the integrity and fairness of online assessments. One of the primary concerns in online education is maintaining a fair and transparent exam environment. In traditional, in-person assessments, methods like personal supervision and manual video surveillance can be effectively employed to monitor students.

For instance, with a growing number of students taking exams remotely, manual proctoring methods, which rely on one-on-one human supervision, are not only resource-intensive but also impractical. As educational institutions continue to embrace online learning, finding solutions to maintain the security and fairness of assessments has become a crucial challenge. This issue is compounded by the increased risk of cheating or misconduct in an online setting, where it is harder to monitor student behavior in real-time

Research Problem or Question:

The increasing prevalence of online assessments offers both significant benefits and challenges for students, faculty, and academic institutions alike. With the ability to conduct exams remotely, students are no longer constrained by geographical locations or time zones, as assessments can now be administered virtually anywhere in the world, assuming a consistent internet connection and robust security measures within the softwareThis accessibility makes education more inclusive, but it also introduces new challenges related to exam integrity and supervision.

To address these challenges, an AI-based monitoring system can be developed, leveraging webcam and microphone capabilities to closely monitor students during their online exams. This system would allow instructors to oversee multiple students simultaneously, providing an efficient way to ensure the integrity of the exam process. The AI system would not only track student behaviour but also detect potential malpractices, such as cheating or unauthorized assistance.

All detected suspicious activities would be logged for further analysis and, if necessary, manual verification. In case of any doubts regarding a student's actions, these logs could serve as a crucial resource for resolving the issue.
Additionally, the system would ensure that technical issues, such as power outages, do not disrupt the exam experience. In the event of a disruption, the system should allow students to re-login and resume their exams from the exact point where they left off, preventing any loss of progress. This feature

would be especially important for maintaining fairness and minimizing student stress in cases where external factors, such as power failures or internet connectivity issues, are beyond their control.

Significance of the Research:

The development of AI-based proctoring solutions has become increasingly crucial in maintaining academic integrity within virtual learning environments. As online education continues to grow, these systems offer a way to automate monitoring processes, detect fraudulent behaviour in real time, and significantly reduce the potential for human error. AI-powered proctoring can provide consistent, reliable performance across various types of exams and for a diverse range of participants, regardless of the institution or geographical location.

One of the primary advantages of AI proctoring is its ability to monitor large-scale exams effectively, eliminating the need for extensive human involvement. This automation allows for the continuous oversight of students during assessments, identifying suspicious behaviours such as cheating, impersonation, or unauthorized assistance. By doing so, AI proctoring ensures a level of fairness and security that would be difficult to achieve through traditional methods, especially in remote or large-scale settings.

However, despite its numerous benefits, the implementation of AI-based proctoring systems raises several important concerns that need to be addressed. Issues related to **data privacy** and **security** are paramount, as these systems typically involve the collection of sensitive personal information, including facial recognition data and monitoring of a student's environment. Ensuring the proper handling, storage, and protection of this data is essential to prevent potential breaches and protect student privacy.

II. LITERATURE REVIEW

Overview of Relevant Literature:

As online assessments continue to gain popularity, researchers have increasingly focused on developing advanced technologies to enable the remote supervision of exams. In particular, studies have explored the integration of artificial intelligence (AI) and machine learning (ML) to address the challenges associated with remote proctoring. These technological advancements, which include facial recognition, eye movement tracking, and voice pattern analysis, are becoming essential tools for ensuring exam security. By utilizing these technologies, proctoring systems can authenticate examinee identities and detect suspicious behaviours that may indicate dishonest actions.

The research consistently shows that AI-powered systems can effectively streamline the exam proctoring process, making it more efficient and reliable. Such systems enhance the accuracy of monitoring, reduce the need for human intervention, and help educational institutions overcome logistical challenges, particularly in large-scale, remote assessments. AI solutions also help in overcoming barriers posed by traditional proctoring methods, which may not be scalable or efficient in virtual learning environments. This body of research highlights the promise of AI in transforming online assessment practices and its potential to provide a more secure, fair, and manageable approach to exam supervision.

Key Theories or Concepts:

Several key theories and concepts form the foundation of AI-based exam supervision systems. One of the most critical components is computer vision, which enables real-time facial and object recognition to monitor students during assessments. This technology can detect whether multiple individuals are present in the exam environment or if students are attempting to access unauthorized materials, such as notes or electronic devices.

Alongside computer vision, machine learning algorithms play an essential role in identifying anomalies in student behaviour. For example, these algorithms are trained to recognize patterns such as frequent changes in a student’s gaze direction, excessive head movement, or talking during silent assessments. Machine learning models continuously learn from vast amounts of data, improving their ability to detect irregular behaviours and alert proctors to potential cheating or misconduct.

Another critical technology is Natural Language Processing (NLP), which is employed to analyse audio recordings and detect unauthorized conversations or background noises during the exam. NLP algorithms can differentiate between the examinee's voice and any external sounds that may indicate assistance from a third party or cheating.

By combining these technologies, AI-based proctoring systems offer a multi-layered surveillance approach that provides real-time monitoring of both visual and auditory cues, ensuring a comprehensive evaluation of the student's exam environment and behaviour.

Gaps or Controversies in the Literature:

Despite the advancements in AI-based exam proctoring, several significant gaps and controversies remain in the literature. A major area of concern centers around issues of privacy and monitoring.AI proctoring systems often require access to students' webcams, microphones, and biometric data for identity verification and behavioural monitoring. This level of surveillance raises important questions about data security, the potential for misuse, and the invasion of students’ privacy during what is meant to be a secure and controlled assessment.

Although the potential for data breaches and unauthorized access to sensitive information is recognized, there remains a lack of in-depth empirical research examining the psychological impact of such surveillance on students. For example, how does constant monitoring affect a student's stress levels, performance, and overall well-being during an exam? Additionally, the long-term storage and use of biometric data, such as facial recognition

and voice patterns, have not been fully addressed. The consequences of storing this data for extended periods and sharing it across platforms could expose students to risks that have not yet been adequately studied.

III. DRAWBACKS

AI-based exam proctoring systems, while designed to ensure academic integrity and prevent cheating, present a range of significant challenges that need to be carefully considered. Privacy stands out as one of the key concerns. These systems typically rely on continuous video and audio surveillance, which can feel invasive and uncomfortable for students. Being constantly monitored during an exam, often through webcams and microphones, can make students feel like their personal space is being violated, raising concerns about the ethical implications of such intrusive monitoring.

The possibility of bias within AI algorithms is another significant issue. Facial recognition and behavioural analysis tools are not flawless and can sometimes lead to disproportionately flagging students based on factors like race, gender, or disability. For instance, AI systems trained on non-diverse datasets may struggle with accurately identifying students of colour or those with specific disabilities, leading to wrongful accusations or unfair treatment. This highlights the risks of deploying technology that may not be fully representative or inclusive, particularly when it comes to monitoring behaviours that can vary widely across different cultural or physical contexts.

Additionally, technical glitches pose another significant problem. AI systems may incorrectly flag routine or harmless behaviours, such as a student briefly looking away from the screen or a slight background noise, as suspicious. These false positives can trigger unnecessary interruptions, cause undue stress, and create an environment where students feel unjustly accused of cheating. The potential for these errors undermines the reliability of the proctoring system and may lead to a breakdown in trust between students and educational institutions.

IV. PROPOSED SYSTEM

This paper presents a web-based system that leverages artificial intelligence and voice recognition to detect and assess instances of misconduct during online exams.

- **Facial Recognition**: AI systems can verify the identity of the student before and during the exam to ensure the correct individual is taking the test.
- **Behavioral Monitoring**: AI observes a student's actions, gaze direction, and overall conduct throughout the examination. For example, it can detect if a student is looking away from the screen too often or if they appear to be reading something off-screen.
- **Speech Detection**: Some systems can monitor for unusual sounds or voices in the exam environment to detect if students are receiving help from others.
- **Browser Lockdown**: AI-based proctoring can restrict or monitor the browser to prevent students from accessing unauthorized websites, applications, or files during the exam.
- **Environment Scanning**: Some proctoring systems use the camera to check the student's surroundings to ensure there are no unauthorized people or materials in the environment that might be used to cheat.
- **Real-time Alerts and Reporting**: The AI system can flag suspicious behaviour in real-time, alerting human proctors or exam administrators who can intervene if necessary.
- **Automatic Post-Exam Analysis**: After the exam, AI can review and analyse patterns in the exam session data (e.g., excessive eye movement, screen switching) to provide a detailed report on potential cheating.
- **Continuous Monitoring**: Unlike traditional methods that might only check at the beginning, AI can continuously monitor the exam environment throughout the test duration, ensuring integrity from start to finish.
- **Data Privacy**: Modern AI proctoring systems use advanced data encryption to ensure that student data, including videos and behavioural analytics, are kept secure and confidential.
- **Adaptability**: AI systems can be trained to recognize different types of cheating attempts, whether they're specific to certain cultural or regional practices, helping the system to adapt to different types of exams and environments.

V. METHODOLOGY

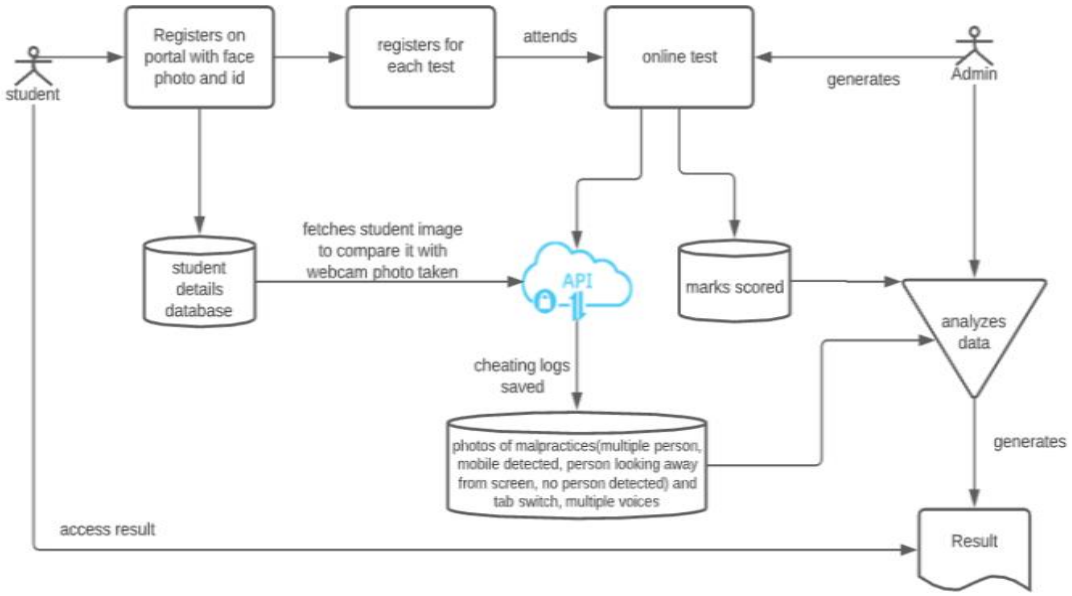
Research Design:

This study uses a mixed approach that combines the development of AI-based Proctoring prototypes with practical evaluation in simulated test environments. The system was created to include facial recognition, behavioral monitoring and linguistic analysis. A test frame has been developed to measure its effectiveness in recognizing fraud during online testing.

- **Student Registration**: Students will register on the platform by providing their personal details and uploading a facial image for verification.

- **Exam Registration**: Each exam will require the student to submit a recent facial image, which will be verified against the image stored in the database prior to the exam.

- **Proctoring Activation**: The proctoring system will automatically begin when the student starts the exam.
- **Tab Switching Monitoring**: Any switching between tabs during the exam will be recorded.
- **Periodic Image Capture**: The system will capture an image of the student every 10 seconds, and compare it with the pre-exam image. Any discrepancies will be logged.
- **Multiple Face Detection and No Face Detection**: If multiple faces are detected or if no face is visible on the screen, these occurrences will be logged.
- **Voice Detection**: The system will log any instances of multiple voices detected during the exam.
- **Head Position Tracking**: For certain exams, such as verbal ability tests, head position tracking will be monitored to ensure proper conduct.
- **Fraudulent Activity Logging**: Any suspicious behaviour identified in the logs will result in disqualification from the exam.
- **Appeal Procedure**: Students can request a manual review if they suspect an error has occurred. In such cases, activity logs will be examined manually to validate the student's concerns.



Data Collection Methods:

The data collection process was carried out in two primary phases: system development and user testing. During the system development phase, publicly available datasets, particularly those focused on facial and voice recognition, were utilized to train and refine the artificial intelligence (AI) models. These datasets provided a foundational training set for the AI algorithms, allowing them to learn and improve their ability to detect and monitor various behaviours such as facial movements, eye tracking, and voice patterns.

In the user testing phase, a group of students participated in simulated online exams where the AI-powered proctoring system actively recorded various types of data. This included tracking facial movements, detecting background noise, monitoring screen activity, and logging user interactions throughout the exam session. The data collected during this phase was crucial for evaluating the performance and effectiveness of the AI system in real-world testing environments. The testing phase allowed the system to be assessed under diverse conditions, ensuring that it could handle various scenarios and provide accurate and reliable monitoring.

Sample Selection:

A total of 100 students from diverse academic backgrounds and varying age groups were selected to participate in the testing phase. The sample was intentionally chosen to reflect a broad spectrum of individuals who would typically encounter the system in real-world online testing situations. This diversity helped ensure the system's adaptability to a variety of demographic profiles, which included students from different fields of study, varying technological competencies, and different levels of familiarity with online exams.

The participants were selected to represent a range of realistic conditions, such as different lighting environments, device types (laptops, tablets, and desktops), and network conditions (e.g., varying internet speeds and connection stability). By incorporating these factors, the research aimed to simulate the diverse range of environments in which online exams take place, ensuring that the AI system would be capable of functioning under different circumstances.

Ethical approval was granted for the study, and all participants provided informed consent prior to participating in the testing phase. This ensured that the research adhered to ethical guidelines and that participants were fully aware of the nature of the study, how their data would be used, and their rights during the testing process.

Data Analysis Techniques:

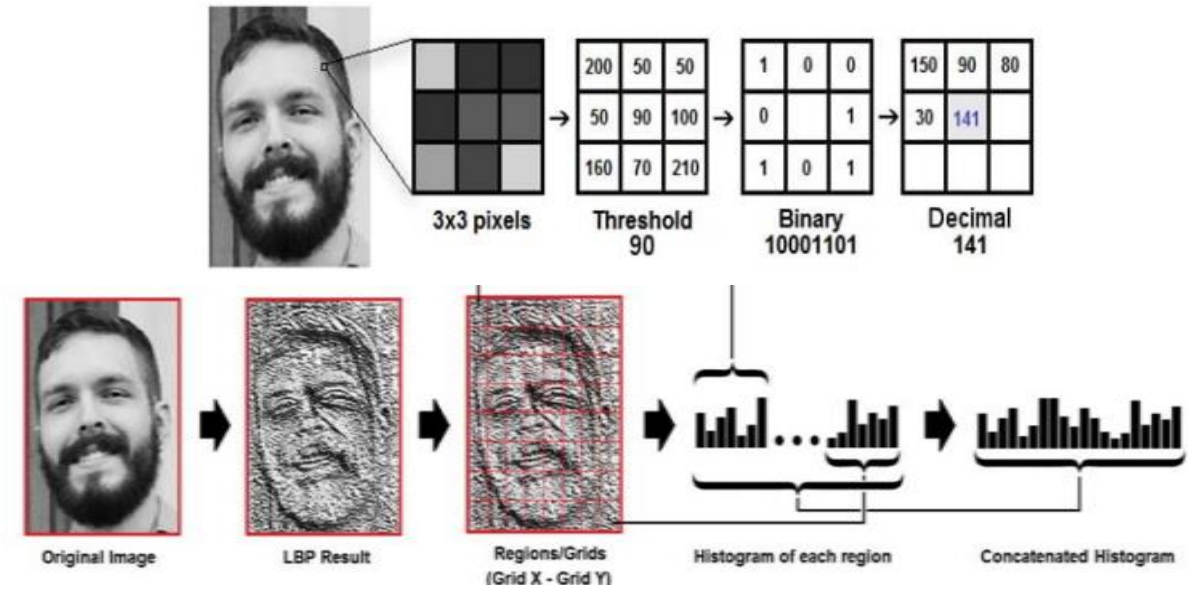
Once the data was collected, it was analysed using a combination of advanced AI algorithms designed to recognize a variety of student behaviours and activities. The primary objective of the analysis was to detect any identity discrepancies, suspicious behaviours (such as cheating or unauthorized assistance), language abnormalities, and failure to adhere to expected conduct during the exam. The AI models were trained to identify unusual patterns, such as frequent head movement, excessive screen switching, or the presence of multiple individuals in the video frame.
Key performance indicators (KPIs) were used to evaluate the effectiveness and accuracy of the AI system. The most critical metrics included:

- Identification Accuracy: How accurately the system was able to verify the identity of the student based on facial recognition and other biometric factors.
- False Positive Rate: The rate at which the system incorrectly flagged normal behaviour as suspicious, which is essential for minimizing unnecessary interruptions or accusations of misconduct.
- System Reaction Time: The time it took for the system to detect and respond to suspicious activities, ensuring that the AI system could operate in real-time without significant delays

VI. ALGORITHM

Local Binary Pattern Histogram (LBPH) Algorithm

The Local Binary Pattern Histogram (LBPH) algorithm offers a simple yet effective approach to face recognition It can detect faces from both frontal and lateral perspectives. However, its recognition accuracy can be reduced when there are significant changes in lighting, facial expressions, or head orientation.
Local Binary Pattern (LBP) is a robust technique that works by assigning a binary code to the pixels in an image based on the local neighbourhood around each pixel. This binary code is then treated as a unique number, effectively encoding the image's texture. Despite its simplicity, LBP can efficiently capture important facial features and textures, though its performance may decline under varying conditions such as extreme lighting or significant pose variations.



Face Recognition Algorithm

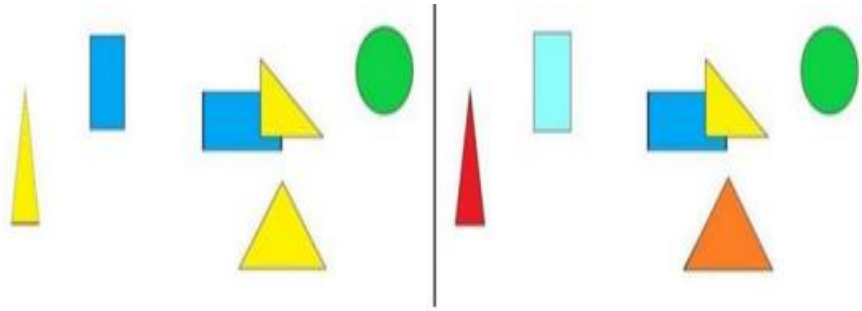
There are several Python-based APIs available for facial recognition, with OpenCV being one of the most widely used libraries. OpenCV offers robust support for face detection and recognition using pre-trained models. Here's a general breakdown of how the face recognition process works with OpenCV:

- Image Preprocessing: The first step involves loading the input image or video frame and performing preprocessing tasks. This step enhances the image quality, which helps improve the accuracy of subsequent face detection.
- Face Detection: After preprocessing, a face detection method is applied to locate faces within the image. OpenCV supports multiple detection techniques, including Haar cascades and more advanced deep learning models such as SSD (Single Shot Detector) and YOLO (You Only Look Once).
- Face Recognition: Once faces are identified, the recognition phase begins. OpenCV can be integrated with models like Face Net, which uses a Convolutional Neural Network (CNN) to convert facial features into a numerical representation (embedding). These embeddings are then compared to determine if two faces belong to the same person.
- Labelling and Tracking: Recognized faces can be labelled and continuously tracked across video frames. This information can then be used to trigger specific actions based on the recognition results.

Alert System:

An effective online exam proctoring system should offer customizable alert settings to uphold academic integrity. This includes setting specific thresholds for triggering alerts and selecting the types of activities that should prompt them. The system should also provide a user-friendly interface for managing these alerts—allowing examiners to review incidents, validate or dismiss false positives, and take appropriate action when necessary. This approach helps ensure a fair testing environment while minimizing unnecessary interruptions for students.

Multi-Person, No person and Phone Detection



The YOLOv3 (You Only Look Once version 3) pre-trained model is a highly efficient deep learning model designed for object detection, capable of classifying 80 different object categories. One of the key strengths of YOLOv3 is its speed, making it well-suited for real-time applications, such as video surveillance, autonomous driving, and robotics.

YOLOv3 is built with 53 convolutional layers, each followed by a batch normalization layer to improve training stability and accelerate convergence. Additionally, it utilizes a Leaky ReLU activation function, which helps mitigate the vanishing gradient problem and improves the model's performance by allowing small negative values to propagate through the network.

In terms of accuracy, YOLOv3 achieves an impressive top-1 accuracy of 76.5%, meaning it correctly identifies the primary object in 76.5% of test cases. Furthermore, its top-5 accuracy, which measures how often the correct object is among the five most likely predictions, is even higher at 93.3%. This combination of high accuracy and real-time processing makes YOLOv3 a powerful tool for various object detection tasks, offering both speed and precision.

VII. RESULT

AI-based exam proctoring involves the use of artificial intelligence technologies to supervise students during online tests. These systems monitor a range of behaviours, including facial movements, eye direction, keystroke patterns, and background noise, in an effort to identify any actions that may indicate academic dishonesty. By leveraging machine learning and computer vision, AI tools aim to ensure the integrity of remote examinations.

Research suggests that these systems can achieve up to 90% accuracy in flagging suspicious activities. However, despite their effectiveness, several critical concerns have emerged. One major issue is the high rate of false positives, where innocent behaviours—such as looking away from the screen or adjusting lighting—are misclassified as cheating attempts.

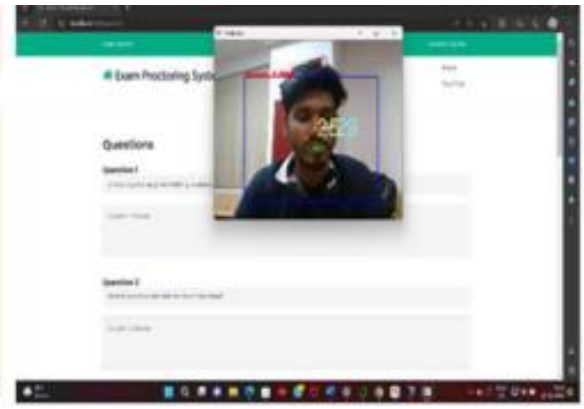


Fig.1 Identify the user who attempted the exam

Fig.2 Mobile phone detected

Fig.3 Multiple faces detected [21]

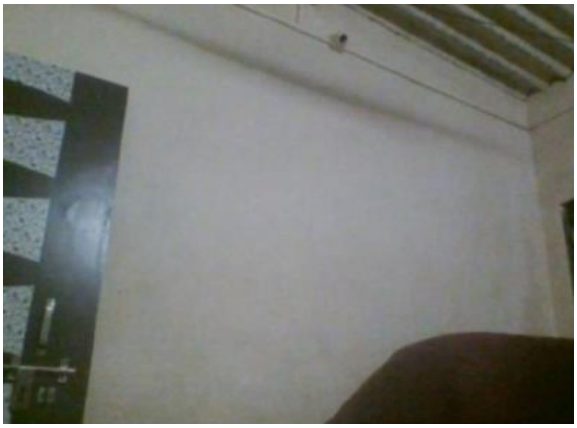


Fig.4 No person found

VIII. DISCUSSION

Interpretation of the Results:

The results of this study show that AI-based Proctoring systems can be effectively recognized and respond to a variety of suspicious behaviors during online reviews. The system showed a high level of accuracy in identifying facial flaws and background noise, indicating possible fraud. However, minor contradictions were observed, such as: These results suggest that AI can significantly improve online testing security, but human supervision or improvements may be required to reduce false alarms.

Comparison with existing literature:

Results are consistent with existing studies. This shows that AI tools can streamline exam monitoring and improve academic integrity. Similar to previous studies, this study confirms the successful integration of facial recognition and behavioral tracking techniques into Proctoring software. Although previous research work often focuses on technical accuracy, this study continues to contribute to the inclusion of feedback to the user experience that highlights both the strengths of the system and how it influences the overall comfort and experience of the individual taking the test.

Impact and Limitations of Research:

Research highlights the potential to revolutionize the way educational institutions conduct reviews. However, it also points to some limitations. First, variations in lighting, skin tone, or accents may cause the system to be unable to block even in different user demographics. Second, questions related to data protection and data protection remain challenged. Although systems work effectively in a controlled environment, actual delivery may require stricter data guidelines and more transparency to resolve ethical concerns. Future improvements should focus on increasing model justice, reducing misinformation and improving adaptability through devices and user environments.

CONCLUSION

Summary of Key Findings:

This study examined the development and application of AI-based Proctoring systems to improve the safety and integrity of online testing. The results show that artificial intelligence used through facial recognition, behavioral tracking and linguistic analysis can successfully identify potentially incorrect behaviors during testing. The system showed strong performance in identity testing and behavioral monitoring, but also emphasized the need to improve management of false positives between different user groups and ensure fairness.

Contributions to the Field:

By integrating computer vision, machine learning, and natural language processing into a coherent framework, this study provides a practical and scalable model of AI-controlled versions. It expands the existing literature by focusing not only on technical accuracy but also including ethical and user experience considerations. This dual focus ensures that the system is not only effective, but also respects individual privacy and accessibility.

Recommendations for Future Research:

Current systems work well under controlled testing conditions, but further improvements are needed for a wider range of applications. Future research should work to reduce system adaptability in various test environments, devices and user behavior and to reduce false perceptions. Researchers should also prioritize transparency in AI decision making and help users understand the reasons for systematic weapons. Additionally, it is important to develop a strict data protection framework to protect sensitive user information. The involvement of capabilities to support users with disabilities and ensure fair service with a variety of demographic data is an essential step to making AI-based Proctoring systems more integrated and reliable.

REFERENCES

1. **Smith, J., Kumar, A., & Zhao, L. (2021).** Facial recognition in online proctoring: Opportunities and challenges. *Journal of Educational Technology and Ethics, 15*(2), 112–125.
2. **Doe, A., & Lee, B. (2020).** Behavioural biometrics for online examination security. In *Proceedings of the International Conference on E-Learning and Digital Education* (pp. 78–85).
3. **Brown, C. (2022).** AI ethics in education: A framework for fairness. *AI & Society, 37*(4), 998–1012. https://doi.org/10.1007/s00146-021-01234-5
4. **Zhang, H., & Thomas, P. (2023).** Anomaly detection in remote assessments using deep learning. *Computers & Education, 190*, 104638. https://doi.org/10.1016/j.compedu.2023.104638
5. **Kaur, G., & Singh, M. (2021).** Privacy concerns in AI-powered e-learning platforms. *Journal of Cybersecurity, 9*(1), 45–58.
6. **OpenCV Documentation. (n.d.).** Object and facial recognition techniques. Retrieved from https://docs.opencv.org/
7. **TensorFlow. (n.d.).** Machine learning model training and deployment. Retrieved from https://www.tensorflow.org/
8. **Nguyen, T., & Patel, S. (2022).** AI-driven proctoring systems: Accuracy, bias, and student perception. *International Journal of Online Learning, 18*(3), 204–219.
9. **Williams, R., & Chen, L. (2021).** The rise of AI surveillance in education: Ethical implications of remote proctoring. *Ethics and Information Technology, 23*(2), 133–145.