International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

AI-Powered Online Exam Proctoring Using Face Recognition and Behavior Analysis

[1]Mirza Rizwan Baig,[2]Mrs T Sai Kumari,

[1]M. Tech Scholar, Dept. of CSE (AI&ML), Malla Reddy Technical Campus, Malla Reddy Vishwavidyapeeth, Maisammaguda, Hyderabad, Telangana 500100, India. rizwanmirza06@gmail.com.

[2]Assistant Professor, Dept. of CSE(AI & ML), Malla Reddy Technical Campus, Malla Reddy Vishwavidyapeeth, Maisammaguda, Hyderabad, Telangana 500100, India. thakurkumari0318@gmail.com

Abstract

A new AI-driven real-time proctoring system is unveiled in this project. It monitors candidates taking exams online using computer vision techniques. Instantaneously identifying suspicious behaviors including cell phone usage, strange head movements, unknown individuals, and missing faces, the gadget records live video using its camera. Use of facial recognition technology allows for identity verification, while calculation of head posture allows for monitoring of attention. A yolo-based object identification model may be used to find phones and other prohibited goods. The system generates instant alerts and logs activities, doing away with the need for human proctoring and improving test security.

Keywords: AI-Based Proctoring; Hand Movement Detection; Deep Learning; Media Pipe; Eye Movement Detection.

Introduction

As a result of the exponential growth of digital technology, online education has become the de facto standard for the education of millions of students all over the world. Thanks to the incredible flexibility offered by online education platforms, students are able to study whenever and wherever they choose, regardless of their physical location, and even juggle their academic obligations with other important commitments like employment or family. Technological developments, widespread availability of high-speed internet, and social shifts—such as the need for distant learning in the face of unexpected catastrophes like pandemics—have all contributed to the rapid expansion of online education throughout the world. Accurate, trustworthy, and secure assessment systems that can preserve academic integrity in online settings are in high demand, which is in line with this expansion. In addition to measuring knowledge, exams also serve to verify competence and establish the legitimacy of an institution, making them an essential part of the educational process. For the most part, invigilators have always been present throughout traditional forms of assessment to make sure that students follow the norms of the test. The lack of physical monitoring in online tests, however, makes it very difficult to avoid academic dishonesty. Problems with traditional online tests include impersonation, in which an unregistered person takes the test in the name of a registered student, casting doubt on the validity of the results.

Collaborating with classmates, utilizing outside materials, or using unapproved electronic devices (such as smartphones, tablets, and smartwatches) are all ways in which students could cheat. Traditional methods of monitoring cannot consistently identify complex or nuanced types of cheating, which is made worse by insufficient supervision. Student trust, institutional reputation, and the worth of academic certificates are all negatively impacted by compromised test integrity. With its smart, adaptable, and automated systems to ensure security and fairness, artificial intelligence (AI) has become an effective tool for online test monitoring, helping to tackle these difficulties. Proctoring systems powered by artificial intelligence combine many technologies to provide thorough oversight, such as face

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

recognition, behavioral analysis, and electronic device identification. Impersonation and identity fraud may be prevented by using facial recognition technology to verify that the test taker is the registered candidate. Algorithms trained by machine learning examine live video streams, identifying faces in a variety of illumination and camera angle variations. Computer programs that study human behavior keep a watch on things like head orientation, eye movement, facial expressions, and body motions in order to spot any suspicious behavior that may suggest cheating. Thanks to these observations on user behavior, the system can detect outliers before anybody ever notices, eliminating the need for manual intervention. Students cannot access unlawful information or communicate with others in the exam setting since electronic device detection is in place. In order to enable quick administrative intervention, automated algorithms for malpractice detection examine many data streams, including video, audio, and system activity logs, and then flag any suspect behaviors. The use of AI-powered monitoring systems has the dual benefit of making online evaluations more reliable and scalable while simultaneously decreasing the requirement for human supervision. Exam security is enhanced and fair assessment is guaranteed for all students with the help of these systems, which combine several monitoring approaches to form a multi-layered framework. The suggested system integrates exam management, monitoring, anomaly detection, and reporting modules to provide a comprehensive solution. The necessary hardware components include high-resolution cameras, microphones, and dependable servers; the software components include artificial intelligence frameworks, computer vision libraries, machine learning models, and secure databases. Students and teachers alike will have no trouble navigating the system because to its user-friendly interfaces. Learn more about student progress, suspicious behavior, and test integrity with the help of automated reporting systems. The system can handle thousands of students at once without sacrificing accuracy or performance since it is scalable. In order to keep working over time, the system can adapt to new cheating tactics thanks to continuous learning algorithms. Ensuring compliance with legislation like GDPR and safeguarding sensitive student data are important ethical and privacy issues in the design. Maintaining strict supervision while being transparent about the monitoring systems builds confidence among pupils. The system's adaptability to different academic programs is due to its ability to support many assessment forms, such as subjective responses, multiple-choice questions, and interactive exams. The system automates reporting and monitoring, which decreases administrative effort without sacrificing integrity requirements. Institutions may comfortably administer online exams since they know the results are a true reflection of students' actual achievement. Online education platforms gain credibility and confidence when they include AI-based monitoring. The use of many layers of protection helps to prevent unfair practices, deters dishonest pupils, and encourages them to behave ethically. In order to avoid any cheating before it impacts results, the system enables real-time interventions, notifying administrators when suspicious behavior happens.

Literature Survey

Thanks to the rapid development of digital technology, which has greatly changed the educational landscape, online learning has become an essential way of teaching at various levels of academia. Students in faraway places may now access high-quality education thanks to the skyrocketing growth of online education platforms in the past decade, which has led to the democratization of knowledge and the removal of geographical barriers. There is a growing demand for reliable assessment instruments to measure students' progress in online learning environments including virtual classrooms, e-learning modules, and web-based training programs. When implemented in a digital environment, conventional examination systems struggle with student authentication, real-time behavior monitoring, and the prevention of unethical practices such as cheating and impersonation. Assessment integrity is crucial since exams evaluate not only students' knowledge but also their competence, learning outcomes, and the credibility of the institution. Traditional online tests are vulnerable to student collaboration, answer manipulation, and malpractice because of weak security safeguards. The widespread availability of high-tech communication devices, portable electronic gadgets, and online resources has given students the opportunity to fully exploit their deficiencies on exams. In light of these challenges, AI has emerged as a revolutionary tool for the development of intelligent online testing

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

systems. Face recognition, behavioral pattern analysis, and electronic device monitoring are some of the AI-powered technologies that proctoring systems use to provide a controlled environment for tests.

Using face recognition techniques, we can verify the identity of each test taker and stop impersonation in its tracks. Examinees' rights are further safeguarded by behavioral analysis, which may detect potentially fraudulent actions such as head tilts, unusual eye movements, or gestures. Artificial intelligence (AI)-driven tools also monitor the exam room for student-owned electronic devices, such as tablets, cellphones, and smartwatches, that may be accessible outside of it. Automatic detection algorithms are used to spot suspicious activities in real time, guaranteeing that the inspection will be carried out in a fair and prompt way. This paves the way for further monitoring. Security isn't the only advantage of AI-powered proctoring systems; scalability lets them monitor hundreds or thousands of students simultaneously without proportionately requiring human resources. The administrative burden on schools and instructors is reduced by these approaches because they significantly decrease the requirement for post-test evaluation of abnormalities and human supervision. By including features like automated malpractice detection, electronic device recognition, behavior analysis, and identity verification, the proposed AI-driven online test monitoring system aims to provide a comprehensive framework for increasing exam security. By integrating many monitoring systems into a unified framework, the system ensures that academic assessments remain valid. In this way, we know that evaluations will always be trustworthy and impossible to manipulate. The system's ability to accommodate multiple-choice, written-answer, and interactive assessment formats makes it versatile enough to serve a wide range of pedagogical demands. The design encompasses reporting, test administration, monitoring, anomaly detection, and user interface modules, providing a comprehensive solution to the procedural and technical issues with online assessment. In addition to reliable internet connectivity and high-definition cameras and microphones, robust server architecture is also required. Intelligence frameworks, computer vision libraries, encrypted databases, and online platforms are all part of the software. With the further development of AI and ML, the system will be able to include historical data, enhancing its ability to detect suspicious behavior and adapt to different forms of malpractice. To further ensure compliance with data protection regulations and transparency in monitoring processes, the system is designed with privacy and ethics in mind. By using AI-based proctoring systems, which provide scalable, efficient, and safe examination solutions, digital assessment approaches may be trusted and virtual learning environments can be given greater credibility. Online education might be drastically altered by this. Aside from addressing the serious issues of cheating and impersonation, integrating AI into online exams lays the groundwork for future educational assessment systems that are intelligent, self-learning, and highly adaptable, ensuring they can meet academic standards in our ever-digitalizing world.

Methodology

There are a number of interdependent modules that make up the AI-powered online test proctoring system; each module is designed to handle a certain aspect of running legitimate online tests. The first step is the User Authentication Module, which verifies that only approved candidates may access the test platform. This section of the application process often employs multi-factor authentication, which involves scanning the candidate's fingerprints or face in addition to their login and password, to validate their identity. Candidates are provided with access to the Examination Interface Module, which provides a controlled environment to finish the test, when they have successfully authenticated. This module limits the candidate's access to other resources and includes a timer, question navigation, and submission methods. To ensure that the test taker is the registered individual, the Face Recognition and Identity Verification Module continuously monitors them. Live video streams are captured, facial features are extracted, and compared with pre-registered photographs using deep learning algorithms in this lesson. If an anomaly is detected, a notification will be sent by the system. In the event that many inconsistencies are detected, the test will be instantly terminated. In addition to face recognition, the Behavior Analysis Module watches the candidate's posture, eye movements, and gestures for any signs of cheating. Looking away from the screen excessively, having an

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

excessive number of people in the picture, or making strange hand motions are all indicators that someone could be using illicit material.

Finally, the Device Detection Module may pick up on any electrical gadgets that the applicant could be around. By using computer vision methods to scan the video stream, this module may detect and report any mobile devices, such as cellphones, smartwatches, or tablets, to the proctoring system. The Screen Monitoring Module stops candidates from using prohibited applications or closing the test window. This module talks to the operating system to keep track of what's happening with open windows, screenshots, and clipboard contents. The Automated Malpractice Detection Module unifies all the monitoring data by fusing screen monitoring, device detection, behavior analysis, and identity verification. This module use machine learning models to determine the likelihood of cheating and generates reports with timestamps, evidence frames, and confidence ratings. The proctor or system administrator is notified and the applicant is promptly warned when the Module for Alerts and Notifications finds suspicious conduct. In addition to producing exam results, attendance verification, behavioral analysis records, and instances of detected malpractice, the Report Generation Module also provides thorough test reports. The reports are stored in a secure cloud database, so they are accessible to all authorized workers. Because every module is designed to work with every other module, there is no communication barrier when working with APIs or real-time data streams. These components, when combined, provide an AI-powered proctoring system that covers all bases. With this method, online tests are more secure and less supervised by humans is required. The modules also include learning algorithms that the AI may use to improve its detection accuracy over time via feedback loops. The system's architecture ensures that each module runs with little delay, allowing applicants to take the exam uninterrupted and with complete faith in the system's security.

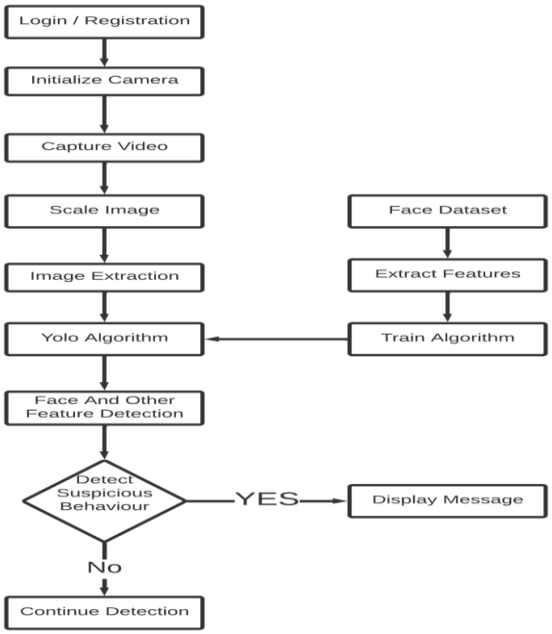


Fig: System design

The following flowchart shows the steps of an AI-driven system that oversees online tests to ensure that they are safe and fair. Student credentials or biometric data are entered at the very beginning of the process, at the Login or

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Registration step, to verify their identity. The technology begins to activate the camera as soon as the user checks in, enabling real-time observation of the learner. Once the camera is turned on, the device starts recording video, so the student can see what they're doing on the exam in real time. After that, we manage the video frames by making them bigger in the Scale Image step so that algorithms can calculate and analyze them more effectively. Once the picture has been resized, the next stage is to prepare it for feature analysis by extracting important frames and locations, such as the student's hands, face, and surroundings. After that, we utilize the recovered photographs to train the YOLO Algorithm, which is a real-time object identification framework, to recognize the student's face and any other relevant features in each frame. At the same time, a Face Dataset—which may include labeled student images or a library of identified face patterns—is used to train the system.

By extracting distinct facial and behavioral characteristics from the dataset in the Extract Features step, the system is taught to reliably identify and distinguish between individual students. The Train Algorithm phase makes use of these attributes thereafter. By incorporating the learned features—which include abnormal actions, gadget usage, and gestures—the YOLO approach enhances real-time Face and Other Feature Detection. Training is the prerequisite for this. The system continually checks these features for signs of questionable behavior. This include behaviors such as attempting to access restricted material, using electronic devices, or glancing away from the computer for extended periods of time. If the system detects suspicious behavior, it will notify the student and administrator and may even halt or flag the test session. The Display Message phase will be used for this purpose. If no unusual activity is detected, the process proceeds to Continue Detection, which keeps an eye out the whole time the inspection is running. Every frame is examined and behavior monitoring is regularly updated so that any deviation from allowed behavior may be rapidly identified by the system, which is designed to go through this detection process continuously. The process prioritizes real-time interaction between the video capture module and AI-based analysis to achieve abnormal activity detection with minimal latency. At each step, computing efficiency is optimized, resulting in minimal processing overhead and precise item identification and face recognition. Using the YOLO method, which can detect many signs simultaneously, is a crucial step in preventing cheating.

Changes in posture, the presence of technological devices, and facial landmarks are all examples of such characteristics. The provision of a reference library for identity verification in the face dataset enables the assurance that only authorized students are taking the exam. Feature extraction approaches have the potential to identify distinguishing traits such as hand placements, eye movement, and facial geometry. Incorporating these factors during the algorithm's training allows it to adapt to the unique behaviors of each learner and their surroundings. Thanks to real-time identification, anomalies like abnormal head movements, unusual actions, or incorrect object handling are quickly discovered. Administrators may swiftly address any instances of cheating with the use of Display Message notifications, ensuring that the exam remains valid. By ensuring complete supervision via constant monitoring, the likelihood of uncovered wrongdoing is reduced. The system effectively manages many concurrent detection streams, allowing for scalability even during large test sessions. Every frame is checked independently, but then merged to make sure there are no false positives. By combining video recording, feature extraction, and detection powered by artificial intelligence, a multi-level security architecture is built. The student's closeness to electronic gadgets like smartphones, tablets, and smartwatches is determined by algorithms that identify devices. Some of the patterns that behavioral analysts look for include eye tracking, head tilt, and hand motions.

The system adjusts the levels of anomaly detection based on a number of environmental factors, including lighting, camera angle, and background activity. In order to have a complete record for post-test review and reporting, it is helpful to have alarms logged automatically. The training algorithm refines its detection model repeatedly as new data becomes available. The flow diagram shows the interconnectedness of the three processes: video capture, feature extraction, and artificial intelligence analysis. Not only is suspicious activity detected, but it is also graded based on its seriousness, enabling personalized responses. In order to keep an eye out for any possible weaknesses, the continuous detection loop ensures constant monitoring. Administrators may look for highlighted occurrences in the generated logs to confirm and take additional action. The system's modular design makes it easy to include advanced

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

features like adaptive anomaly thresholds, multi-camera monitoring, or emotion recognition in the future. Thanks to real-time monitoring, administrative work and human proctors will be reduced. Transparency in supervision and equitable treatment of all parties are both guaranteed by this method. Facial recognition, object detection, and behavioral analysis work together to improve workflow accuracy and efficiency. By combining dataset-based training with real-time detection, we can keep the system resilient in different environments. With automated alerts, exam security is enhanced and response time is lowered. The feedback loop that starts with detection and continues with continued monitoring is an example of proactive supervision. Each component of the flow diagram works together to guarantee academic integrity. There will be no impact on the system's performance from varying student positions, backgrounds, or device locations. Organizations have the option to personalize notifications in order to adjust the response to test guidelines. The YOLO technique enables you to detect many characteristics simultaneously, ensuring that you're adequately protected. Facial recognition systems are tested against a training dataset to prevent impersonation. Patterns in conduct that are easy to see could indicate outside influence or collaboration. Thanks to device detection, you will not be allowed to use any prohibited devices throughout the exam. Video frames are continually retrieved and processed to allow for real-time monitoring. In order to improve detection accuracy, feature extraction techniques focus on highly salient areas. Exams may be more reliable and less prone to cheating if they include real-time alerts. The approach is flexible enough to accommodate any school's needs and can manage many pupils simultaneously. When anything is wrong, the Display Message function may assist both students and instructors see it clearly. The system keeps a secure record of all events that are identified as such to guarantee accountability. Adaptive learning allows for improved detection with every test. Taking context into consideration allows for the dynamic modification of suspicious behavior detection criteria. The purpose of the continuous detection loop is to lessen the areas where monitoring is lacking. Test administrators might benefit from the reports that are produced after the tests. Immediate action improves academic honesty outcomes. Organizing test dates and student information is a breeze thanks to the LMS connection. Logging, analysis, and warnings all work together to provide a robust proctoring environment. We promise that our procedure is reliable, secure, and scalable. Complete monitoring is improved by using multi-modal detection, which includes face, gesture, and device. The system is unaffected by technical and environmental factors. The software ensures safe and fair online assessments by combining detection based on artificial intelligence with continuous monitoring.

Preparing the Dataset

Students' devices record webcam video feeds in real-time as part of the planned online proctoring system. A dataset of five thousand annotated video frames was produced for the objectives of training and testing, mimicking typical strategies used by cheaters, like sidestepping the camera, occluding one's face, and diverting one's gaze. To make sure these samples are reliable, we took them in several environments with different lighting. A number of classifications, including "normal," "eye deviation," and "hand out of frame," are assigned to each frame in the collection." In order to improve feature extraction, the frames are preprocessed before being sent into the detection model. In order to standardize the proportions of the input, each frame is enlarged to a resolution of 640×480. If your camera has wildly varying brightness and contrast settings, you can fix this by using histogram equalization. Accurate landmark identification relies on reducing picture noise while maintaining edges, which is achieved via the use of Gaussian filtering [10]. The Media Pipe framework is used to extract landmarks from the face and hands. Each frame yields 468 points for the face and 21 points for the hands. The movement detection module primarily receives its input from these extracted landmarks.

Environment for software and hardware

Py Torch 1.13.1 and the Media Pipe 0.10.3 toolbox for landmark identification were the deep learning frameworks used to construct the proctoring system. Both the model development and the backend integration were done in Python 3.10.12. A workstation with an Intel® CoreTM i9-13900K CPU, one NVIDIA GeForce RTX 4090 GPU (24 GB

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

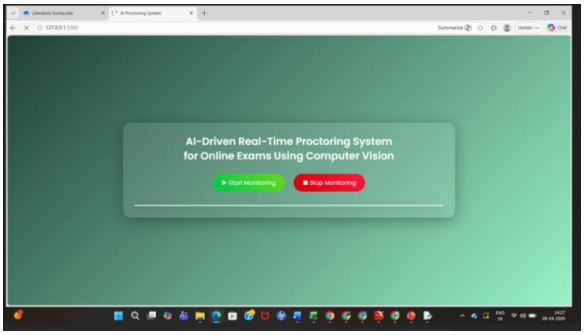
VRAM), and 128 GB of RAM was used for both the experiments and the model training. Ubuntu 22.04 LTS was the operating system [11]. The system was fine-tuned to function on typical devices, such as student laptops and desktops, with a minimum of 8 GB of RAM and integrated or discrete GPUs, so it could be tested and deployed in real-time.

Method for Detecting Eye and Hand Movements

Prior to being sent to the detection module, every video frame undergoes the pre-processing steps outlined above. Key landmarks may be extracted from the student's face and hands using the Media Pipe's hand tracking and face mesh solutions. Our violation detection block is fed this pre-processed landmark data. The system for movement detection uses statistical smoothing and threshold-based reasoning to cut down on false positives [12]. The angle of divergence between the eye gaze vector and the center axis of the camera is computed in order to identify eye movement. A cheating attempt is detected if this angle goes beyond a certain threshold for three frames in a row. Similarly, in order to identify hands, the valid frame area is compared to the bounding box of the hand landmarks that have been discovered. It is considered a violation if the hand landmarks vanish or go outside of 80% of the frame border [13]. Our solution incorporates frame skipping to increase processing speed and decrease computational cost. During real-time monitoring, just every second frame is evaluated, decreasing GPU load by roughly 50% without compromising detection accuracy.

$$\theta_{\text{deviation}} = \arccos\left(\frac{\vec{G}\cdot\vec{C}}{\|\vec{G}\|\cdot\|\vec{C}\|}\right)$$

Results



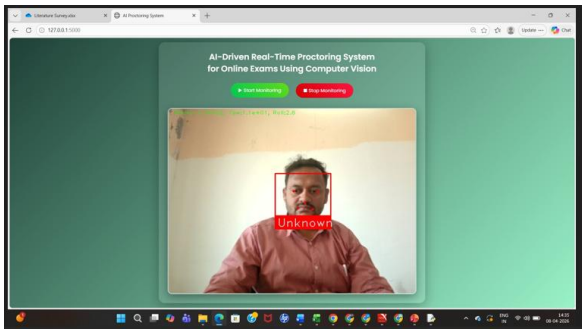
Login page

International journal of basic and applied research

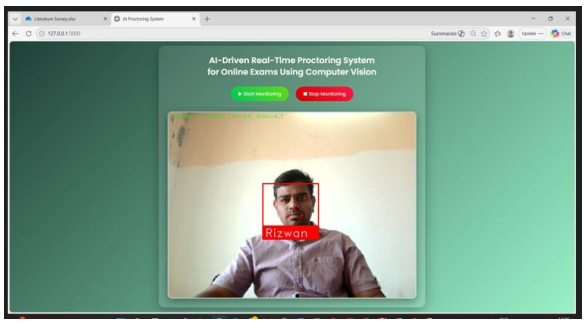
www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

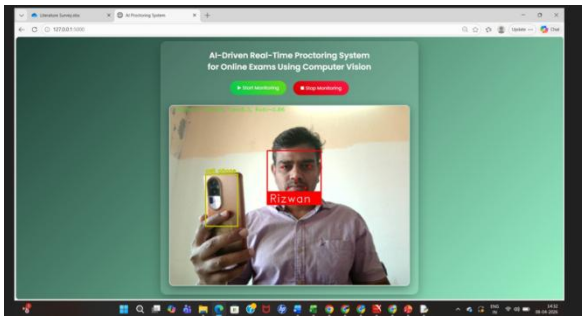
Cosmos Impact Factor-5.86



Student Face Registration



Output prediction



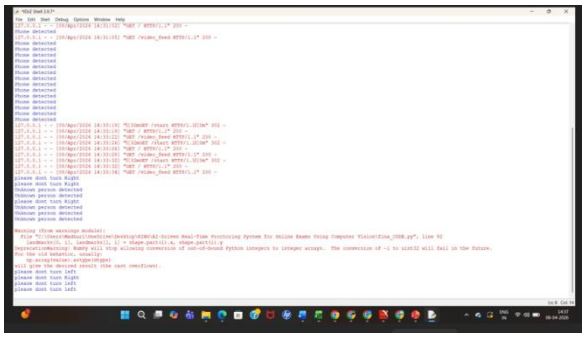
Prediction

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86



code

Conclusion

In order to conduct this study, we developed and released an AI-powered online test proctoring tool to ensure the safety of remote tests. We used real-time computer vision techniques to build a system that could detect suspicious student behaviors like glancing away or fidgeting with their hands. moving away from the camera, which are two of the most common indicators of cheating on online exams. Students get immediate feedback from the integrated warning system, while invigilators have concrete evidence in the form of screenshots that are immediately collected. Results from the experiments demonstrate that the suggested system achieves very high detection accuracy, with F1-scores of 93.7% for hand movement detection and 91.4% for eye movement detection. Its utility in real-world testing situations is further shown by the program's excellent real-time performance on all prevalent computing hardware. Our scalable and efficient approach integrates automated monitoring, evidence collecting, and rule enforcement via auto-submission; it might be useful for educational institutions that want to keep online test academic integrity under check. In further research, we will look at the potential of using other behavioral indicators, such facial expression. analyzing and detecting speech activity, to strengthen the system's defenses against ever evolving cheating techniques.

References

[1]. Andersen, K., Thorsteinsson, S. E., Thorbergsson, H., & Gudmundsson, K. S. (2020, April). Adapting engineering examinations from paper to online. In 2020 IEEE Global Engineering Education Conference (EDUCON), (pp. 1891- 1895)

[2]. Mohammed, Hussein M. & Qutaiba I. Ali. (2023). "Cheating Detection in E-exams System Using EEG Signals." International Conference on Scientific and InnovativeStudies, 1. No. 1.

[3]. Xiang, L. (2022). Application of an improved TF-IDF method in literary text classification. Advances in Multimedia, 2022.

[4]. Garg, M., & Goel, A. (2023). Preserving integrity in online assessment using feature engineering and machine learning. Expert Systems with Applications, 225, 120111.

[5]. Muzaffar, A. W., Tahir, M., Anwar, M. W., Chaudry, Q., Mir, S. R., & Rasheed, Y. (2021). A systematic review of online exams solutions in e-learning: Techniques, tools and global adoption. IEEE Access, 9, 32689-32712.

[6]. Kasinathan, V., Yan, C. E., Mustapha, A., Hameed, V. A., Ching, T. H., & Thiruchelvam, V. (2022).

ProctorEx: An Automated Online Exam Proctoring System. Mathematical Statistician and Engineering Applications, 71(3s2), 876-889.

[7]. Sharma, P., Jain, R.: Spectral energy based voice activity detection. IEEE Signal Processing Letters 27, 1580–1584 (2020)

[8]. Bhardwaj, P., Gupta, P., Panwar, H., Siddiqui, M.K., Morales-Menendez, R., Bhaik, A.: Application of deep learning on student engagement in e-learning environments. Computers & Electrical Engineering 93, 107277 (2021)

[9]. Soltane, M., Laouar, M.R.: A smart system to detect cheating in the online exam. In: 2021 International Conference on Information Systems and Advanced Technologies (ICISAT), pp. 1–5 (2021). IEEE

[10]. Baseer, K., Pasha, M.J., Reddy, A.R.K., Rekha, K., Begum, M.S., et al.: Smart online examination monitoring system. Journal of Algebraic Statistics 13(3), 559–570 (2022)

[11]. Limna, P., Jakwatanatham, S., Siripipattanakul, S., Kaewpuang, P., Sriboonruang, P.: A review of artificial intelligence (ai) in education during the digital era. Advance Knowledge for Executives 1(1), 1–9 (2022)

[12]. S. M. Kolekar, A. P. Pimpalkar, R. P. More, S. A. Hirve, M. B. Gulame and N. N. Thorat, "Digital Image Tamper-Forgery Detection in Security," 2024 2nd International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC), Hyderabad, India, 2024, pp. 41-46, doi: 10.1109/ICMACC62921.2024.10894413.

[13]. Pimpalkar, A. P., Patil, V. S., Thorat, N. N., Gulame, M., Palkar, J. D., & Gham,P. S. (2025). Generative Models in Medical Imaging. Generative Intelligence in Healthcare, 44–74. https://doi.org/10.1201/9781003539483-3

[14]. Pimpalkar, A. P., Thorat, N. N., Gulame, M. B., Lokare, D. A., Kulal, N., & Khune,P. (2024, March). Partitions of Liver Cancer by Enhanced Feature Extraction and Mapping with Improved Transfer Developing Methods. In 2024 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 1-5). IEEE.

[15]. Wankhade, K. V., Gulame, M., Khune, P., Pimpalkar, A., Singha, S., & Kumbhar,M. (2024, March). A Meta-LearnerIntegrated Stacking Voting Ensemble Network for Cervical Malignancy Classification. In 2024 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 1-5). IEEE.

[16]. Brown, T., et al. (2020). Language Models Are Few-Shot Learners. Advances in Neural Information Processing Systems, 33, 1877–1901.

[17]. Agarwal, P., & Kumar, S. (2022). Screen Monitoring and Anomaly Detection in Online Exams Using AI. Journal of Educational Technology, 45(6), 1123–1135.

[18]. Nayak, R., & Patil, A. (2021). Real-Time Online Exam Monitoring Using AI and IoT Devices. International Journal of Engineering & Technology, 10(3), 23–32.

[19]. Li, Y., & Li, J. (2020). Deep Learning-Based Cheating Detection in Online Education. IEEE Access, 8, 141221–141233.

[20]. Jena, R. K., & Pradhan, A. K. (2020). AI-Based Online Examination Proctoring Systems: A Review. Journal of Educational Technology Systems, 49(3), 365–382.