Received: 12 September 2025 | *Revised: 29 September 2025* | *Accepted: 10 October 2025* *Vol. 1 | Issue 2| December 2025*
e-ISSN: 3105-2169

International Journal of Mechatronics, Robotics, and Artificial Intelligence
Review Article

Advancements in Automated Cheating Detection Systems for Online and In-Person Examinations: A Comprehensive Review of Methods, Technologies, and Effectiveness

Maria K. Ahmed[*1], **Ghassan J. Mohammed**[1]
[1]Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq

Correspondence
*Maria Kadhim Ahmed
Department of Computer Science, College of Computer Science and Mathematics, University of Mosul
Email: maria.23csp69@student.uomosul.edu.iq

Abstract

Authenticity of tests as a measurement tool has received a lot of attention within learning institutions due to emergences of online classes and remote test administration. Supervision and invigilation methods do not always suffice to deter students from cheating, and thus Academic Cheating Detection Systems (ACDETS) have been invented. This paper presents a critical analysis of the current approaches for identifying cheating in online and face-to-face examination systems. There are plenty of approaches, including behavioral approach, facial expressions tracking, gestures recognition, voice analysis, and video monitoring. CNN (Convolutional Neural Network) algorithms, RNN (Recurrent Neural Network) algorithms, and YOLO models, for instance, have shown great enhancements in both accuracy and scalability of detecting suspicious behaviors. The paper further compares the merits and demerits of these methods and also looks at the possibility of using them for real time detection, large setting for exams, and varied testing conditions. This paper is finalized by the evaluation of the practical applicability of the findings, limitations, and further research prospects concerning the monitoring of academic integrity.

Keywords

Automated cheating detection, Online examinations, Video surveillance, Behavioral analysis, Anomaly detection.

I. INTRODUCTION

The need for better monitoring that can be implemented in academicians’ examinations has driven growing interest in invigilating technologies globally. universities and institutions of learning. Conventionally, professional proctors have been assigned the duty of overseeing examinations and identify cheaters. Nevertheless, due to the increasing use of information technology in academic institutions for both ordinary and emergency online assessments, there is a strong need to incorporate automatic procedures in both paper-based and electronic tests [1]. These systems that are already implemented in some universities have the sole purpose of improving the exam integrity as cheating is not only rife in learners accessing college education but also those in secondary and primary institutions [2].

Short-changing in particular interferes with the academic process and erodes the academic worth of a program for all students. Cheating methods have changed and enhanced and the old-fashioned ways of detecting them include manual supervision and physical monitoring are inadequate [3]. In addressing these challenges, Universities and other academic institutions are now seeking for modern technologies monitor cheating in a very efficient manner and in real-time. This increased reliance on technology has engendered a heightened awareness of automatic examination malpractice detection systems used to watch exam halls for suspicious activities without having to employ personnel to watch over them [4]. Among them, the action recognition in video surveillance is one of the most promising technologies in this area. The subfield of computer vision called action recognition has attracted much interest and can be applied in such fields as remote sensing, human-machine interaction, video surveillance, and sports analysis [5]. This technology calls for identification and analysis of human activities from videos which makes it appropriate for surveillance of exam settings. The action recognition systems can observe students’ movement and actions during exams and show signs of cheating; using prohibited equipment, communicating with others or making certain movements that are indicative of dishonesty [6].

However, it is not the same for action recognition; it poses its problems as well. Viewpoint occlusion, varying lighting, cluttered background, and camera motion are some factors which make the task of identifying cheating actions difficult. Within the context of exam surveillance, action recognition can be classified into two main types [7]: Long range recognition is the examination of extended video sequences to forecast future movements and short-range recognition gets involved with brief video clips, the events of which include cheating attempts. Each method has its advantages and disadvantages when it comes to identifying cheating during the exams [8].

This survey seeks to serve as a review of automatic cheating detection systems with emphasis on the part played by action recognition technologies in examination surveillance. Based on the findings from the scholarly articles reviewed, the survey will identify potential uses, advantages, limitations and future prospects of action recognition in protecting the credibility of academic performance.

While several prior surveys have summarized e-proctoring or academic integrity tools [23][41], our review differs by (i) integrating both online and in-person exam settings, (ii) systematically comparing deep learning action-recognition models (YOLO, RNN, CNN) with traditional behavioral and plagiarism detection, and (iii) highlighting underexplored directions such as multimodal fusion (audio+video+behavioral logs) and fairness-aware detection.

II. TRADITIONAL METHODS OF CHEATING DETECTION

Traditional techniques of cheating have been used for many years as the bedrock in enforcement of academic integrity during examinations. These methods frequently rely on the direct supervision of people, inspection of students' activity, a number of organizational measures to minimize the chances for dishonest actions [9]. The main aim of all these practices is to ensure that learners are disciplined in their practices and do their work on their own without seeking any help from other people [10]. This means having monitors, who will be overseeing the examinations rooms to prevent any cases of cheating among the students; proctoring is an example. This supervision can be from direct observation, to the use of the arrangement of the classroom that does not allow student A to sit next to student B to avoid copying. Another factor is a lack of time during exams as it inhibits people's abilities and makes them study without references to any external information [11].

In addition, the following basic methods have been used; having many sets of examinations or random questions which will reduce the probability of cheating. By ensuring that the students are given different problems it becomes difficult to copy from others when solving the problems [1]. Other body behaviors that are observed by invigilators include gestures and movements for instance when students look around nervously or when they are concealing notes. Another sign of cheating is an analysis of the student's handwriting, if it is irregular that must mean the answers are not theirs [12]. Plagiarism detection also falls under the written work detection despite it being normally employed in identifying students' work; instructors compare students' responses to recognized materials, as explained by the traditional detection strategy. While these methods are effective, they are costly and, in some cases, may not detect all cases of cheating especially due to arising technologies resulting in inventive cheating techniques. Consequently, the institutions of learning integrate new and more sophisticated approaches to learning alongside these traditional methods [13]. Table (1) summarizes Traditional Methods of Cheating Detection.

Although Table I lists long-used strategies, their detection accuracy is inconsistent (e.g., handwriting analysis is subjective vs. plagiarism detection more robust). In contrast, Table II's AI-driven tools improve scalability but trade off privacy and may trigger false positives, which limits adoption.

TABLE I.
TRADITIONAL METHODS OF CHEATING DETECTION

Method	Description	Advantages	Challenges
Proctoring (In-person supervision) [1]	Invigilators monitor students during exams, observing behavior to prevent cheating.	Provides direct oversight; can detect suspicious actions.	Relies heavily on human observation; may not catch all instances of cheating.
Multiple Question Versions [14]	Different versions of the exam are given to students, with slight variations in the questions.	Reduces the chance of copying; ensures unique exam experience for each student.	Can be logistically challenging to prepare and manage.
Time Constraints [15]	Limiting the time given for the exam to prevent students from consulting unauthorized resources.	Forces students to rely on their own knowledge.	May increase stress for students; does not eliminate the possibility of cheating under time pressure.
Handwriting Analysis [16]	Comparison of handwriting to identify inconsistencies or determine if the work is plagiarized.	Effective for identifying copied or plagiarized work.	Only useful for handwritten exams; subjective and prone to error.
Behavioral Observation [17]	Proctors look for suspicious behavior, such as excessive	Immediate detection of suspicious activity.	Can be influenced by subjective interpretation;

	glances at other students' work or cheating devices.		may miss subtle forms of cheating.
Cell Phone Checks [18]	Students are asked to place their phones in a designated area to prevent use during exams.	Prevents access to unauthorized resources.	Requires students to comply; may not detect other electronic devices.
Plagiarism Detection [19]	Manual or cross-referencing to identify instances of copying from textbooks, previous work, or online sources.	Helps detect dishonest written work; ensures originality.	Labor-intensive; may miss subtle forms of plagiarism.
Peer Reports [20]	Students are encouraged to report any cheating they observe among peers.	Can help identify cheating that goes unnoticed by invigilators.	Relies on the honesty and accuracy of students' reports; may create a distrustful environment.
Randomized Audits [21]	Random selection of students for further questioning or verification of their work during or after the exam.	Increases unpredictability, making it harder for students to cheat.	May be resource-intensive to implement and manage.
Honor Codes [22]	Students sign a pledge agreeing to adhere to academic integrity and avoid cheating.	Encourages personal responsibility and integrity.	May not be effective if students do not internalize the importance of academic honesty.

These procedures provide the framework for attempting to prevent dishonesty in academic assessments but can be time-consuming and sometimes involve a large amount of human intervention and are associated with a possible high risk of error which is why more and more educational organizations are turning to sophisticated detection tools such as AI-based monitoring and plagiarism identification software [23].

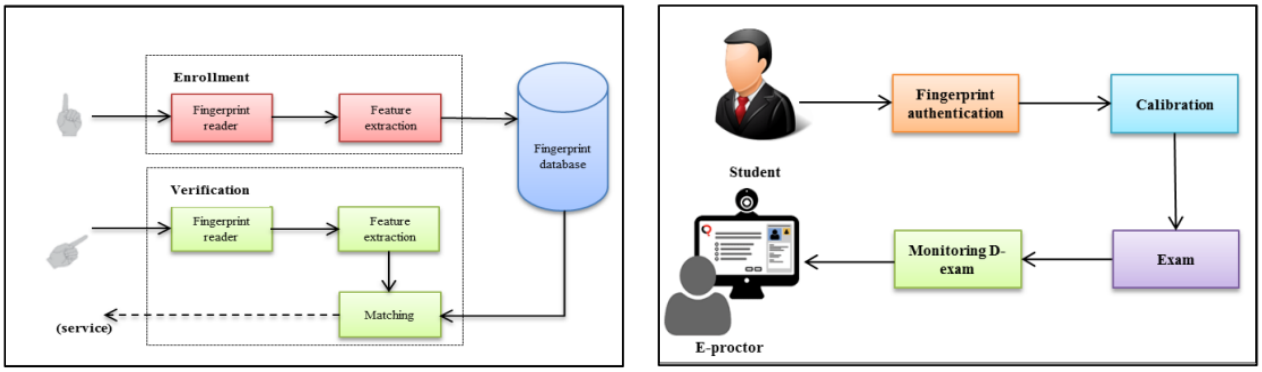
III. Technological Advances in Cheating Detection

Old-fashioned approaches to cheating prevention are being supplemented or substituted with new technologies and principles of online learning. These advances use AI, machine learning, and complex software programs to identify cheating with increased accuracy, speed and in much larger numbers [7]. Another large-scale technological application is the AI-based proctoring that relies on web cameras, microphones, and facial recognition technologies to monitor students' behavior during examinations in real time. This system is able to monitor various behaviors for example, when the face is turned away from the screen or when there are more than one people in front of the screen or when the user is using a prohibited item [24].

Another useful advance is the availability of software like Turnitin and Cityscape which can search hundreds of millions of online documents as well as a range of databases, in order to compare a piece of writing against a vast database of other texts. These tools rely on sophisticated algorithms to match the content submitted to the bibliography against other billions of documents to identify copied parts. Another technology used in online exams is browser lockdown software which limits the student's operation on the device during an exam and prevents them from finding answers or communicating with others [25]. AI can also be used in analytic to identify any behavioral issues arising from student's conducts during exams for instance, answering patterns or the time spent on a question, which may point out to cheaters. Also, in some cases an academic misconduct may be detected by means of tracking student's activity with the help of machine learning algorithms to analyze his or her academic history for any suspicious spikes as for performance for instance, getting all as in a course after failing all the previous courses. Besides the above, these technologies offer enhanced detection because they can oversee many students at the same time while at the same time do not require the involvement of human beings. Nonetheless, these systems are robust; nonetheless, they come with issues of privacy, data security and false positives [26]. Table (2) shows Technological Advances in Cheating Detection These technological solutions are the way forward in the war against academic dishonesty. However, they provide enhanced detection abilities and bring to the table problems like toughened instruct structure, privacy concerns and the probability of misuse. In the future, the development of the technology is likely to proceed and the overall approaches used by educational institutions will continue to mature with regard to the roles of security, fairness, and privacy [33]. Fig. 1 illustrates a representative deep learning architecture used in automated cheating detection. Convolutional layers extract spatial features from video frames, while recurrent layers (e.g., LSTM/RNN) or temporal 3D CNN blocks model time-dependent behavior. A final classifier predicts suspicious versus non-suspicious actions. This architecture differs from the current functional system flow (Fig. 2) by showing the internal technical components enabling high-accuracy recognition.

TABLE II.
TECHNOLOGICAL ADVANCES IN CHEATING DETECTION

Technology	Description	Advantages	Challenges
AI-based Proctoring [27]	Uses webcams, microphones, and facial recognition to monitor students' behavior during online exams.	Real-time monitoring; detects suspicious activity such as unauthorized devices or multiple people.	Privacy concerns; potential for false positives; requires high system specifications.
Plagiarism Detection Software [28]	Tools like Turnitin, Grammarly, and Copyscape scan student submissions against online databases to identify copied content.	Detects copied material quickly and comprehensively; widely used in academic settings.	May not catch all forms of plagiarism (e.g., paraphrasing); requires access to vast databases.
Browser Lockdown Software [29]	Software that restricts students' access to websites, applications, or external devices during online exams.	Prevents students from searching for answers or communicating with others during the exam.	Some students may find workarounds; requires reliable internet connections.
AI-driven Analytics [1]	Uses AI algorithms to analyze students' exam behavior (e.g., response patterns, time spent on questions).	Can detect cheating behaviors without direct human observation; scalable.	Can lead to false positives; may not be fully accurate in detecting all forms of cheating.
Machine Learning for Performance Tracking [30]	Tracks and analyzes patterns in students' performance over time, flagging suspicious grade improvements or inconsistencies.	Provides long-term insights into student behavior; helps in early detection of cheating trends.	Data privacy concerns; may not always identify honest improvements in performance.
Digital Fingerprinting of Work [31]	Digital signatures or metadata attached to submitted work that can be traced back to the original author.	Prevents unauthorized sharing or copying of work; provides clear authorship records.	Can be circumvented by students who remove metadata or alter files.
Secure Online Exam Platforms [32]	Platforms that combine various security measures, such as AI proctoring, encryption, and multi-factor authentication to secure online exams.	Comprehensive security; reduces the risk of cheating during online assessments.	Requires student cooperation; can be complex to implement; may pose technical challenges



Fingerprint Recognition

Online Proctor

Fig. 1. Advances in cheating detection [34]

IV. Action Recognition in Video Surveillance

Action recognition in video surveillance therefore refers to identifying and categorizing different actions of one or many people in sequences of videos. This task has attracted a lot of focus because of the increasing need for the application of the systems in several areas such as safety, security, health, and transport. The first goal of action recognition is to recognize the actions, behavior or interaction of human in real time to be used for preventive surveillance as well as after event analysis [35].

This process generally involves three stages: As for the demand for preprocessing (including frame extraction and noise removal), feature extraction (including spatial features, temporal features, and motion features) and classification (including the classification of activities using machine learning or deep learning). As the field of machine learning particularly deep has grown, action recognition has greatly advanced making it possible for systems to do very well even in the most complex cases [36].

A. Traditional Machine Learning Methods

These methods rely on hand-crafted features that are manually selected based on domain knowledge. Common feature extraction techniques include optical flow, histogram of oriented gradients (HOG), and spatiotemporal descriptors such as HOF (Histogram of Optical Flow) and MBH (Motion Boundary Histograms). These features are then used with classifiers like Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), or decision trees [37].

B. Deep Learning-Based Methods

Deep learning techniques, particularly Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and 3D CNNs, have revolutionized action recognition by automating feature extraction and learning spatiotemporal relationships from raw data. These models can analyze video sequences more effectively, learning from large amounts of labeled data [38].

V. Challenges in Automatic Cheating Detection

The use of ACDET has its advantages and disadvantages that if not well addressed, may hinder the effectiveness of an ACDET and pose challenges to institutions of learning. First of all, concern arises about the effectiveness of such systems, that is, their efficiency and accuracy. And thus, AI-based detection tools, for example, may generate false positives – actions that are not only legal but also legitimate, performed by students [39]. For example, a student may turn their head slightly to the side to try and remember something, or shift in their seat, and the system may think he is trying to cheat. These are some of the misinterpretations that can result into unfair punishment of students and erode confidence in the detection system [40]. Another major concern is the privacy rights of students when using products such as AI proctoring that incorporates the use of webcams and mics in an exam period. Such systems can foster concerns over the process of obtaining personal data, their storage and, in particular, their use. Students may develop unfavorable feelings towards the monitoring system by feeling uncomfortable or violated to the extent of resisting it. Institutions have to make sure that they meet different rules on privacy like the General Data Protection Regulation (GDPR) and make sure that the learners understand how their data will be used [41].

Other factors which are also attributed to include technical. An effective cheating identification system requires reasonable physical structures, internet connectivity, and the devices that will enable the running of the monitoring software. Certain students in poor families or districts may not meet these conditions; this is because there could be problems with technology or even fake alarms. This implies that, based on the distribution of the technology access, the detection process may not only be less accurate but may also bring in bias to the examination [42]. The versatility in cheating behaviors is the other challenge that automatic detection faces. Cheating is not only but has extended beyond simple acts such as copying from the person next to your desk. It may include more complex operations for example using prohibited tools, teamwork when the network is offline or by taking advantage of the system's weaknesses. The AI systems might struggle to recognize such cheating strategies, particularly if the latter entails somewhat less obvious behaviors. Cheating is not a one-time deed, and due to this, methods that are used to expose cheaters have to be developed continually [1]. Also, there is an ethical pitfall that comes with trying to implement automatic cheating detection systems. These technologies can in fact tend to identify specific groups of students, depending on specific behaviors that may not necessarily be cheating. For instance, kids who have tendency to squirm, take more time in breaks or even have other special movements may be easily marked by the system. In addition, the AI systems can be biased in that it can be designed with a biased algorithm that produces discriminated results if the machines are trained with a biased set of data. This is especially so for students from a culturally, behaviorally or neuro divergent backgrounds from which may be at higher risk of bias resulting in a lack in trust within the system [43]. These challenges put into a perspective when and how to use the automatic cheating detection technologies. Despite their learning benefits in the areas of scalability, accuracy and efficiency and, therefore, despite their potential in making the learning process more efficient and accurate they pose a number of challenges related to issues of privacy and fairness, accuracy and ethical implications which cannot go unnoticed. These technological features should be implemented in conjunction with supervision by human personnel, and the use of such technologies should be periodically reviewed in compliance with both requirements of academic dishonesty and students' rights.

VI. Datasets for Automatic Cheating Detection

The following is the summary of various data sets that can be used for developing automatic cheating detection system for exam halls. These datasets include video surveillance data and video audio data, sensor data and hybrid systems that include both video and audio data. Both datasets are different and valuable to train models to identifying malicious actions such as copying, using prohibited appliances, or talking to the other students during the test. The table also contains links to these datasets which can be useful for research and in the development of systems with regard to exam surveillance and academic integrity monitoring. Table (3) shows several samples for Datasets for Automatic Cheating Detection.

TABLE III.
Datasets for Automatic Cheating Detection

Dataset Name	Type	Description	Reference/Source
Exam Surveillance Dataset	Vision-based / Video	Contains video recordings of exam rooms with labeled instances of cheating behaviors.	https://www.kaggle.com/datasets/mateohervas/dcsass-dataset

Audio Surveillance Datasets	Audio-based	Contains audio recordings from surveillance systems, useful for detecting whispers or mobile phone use.	https://www.kaggle.com/datasets/vjcalling/speaker-recognition-audio-dataset
Multimodal Datasets (e.g., Audio+Video)	Multimodal	Combines audio and visual data to detect cheating, analyzing both student behavior and conversations.	https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2020.568825/full
Inertial Measurement Unit (IMU) Dataset	Sensor-based	Tracks head or hand movements to detect suspicious activity such as copying from others.	UCI ML Repository: IMU Dataset
Kaggle: Classroom Behavior Detection	Vision-based / Behavioral	Video dataset focusing on detecting student behaviors in classroom environments, adaptable to exams.	https://www.kaggle.com/datasets/mburakpala/student-behavior-detection
Vision-based Cheating Detection	Vision-based	Contains images and videos to train models for detecting cheating (e.g., students looking at each other's papers).	GitHub: Cheating Detection

VII. E-Exam Management System Architecture

As illustrated in Fig. 2, the operation of the e-exam management system can be divided into two more or less separate stages. During the first phase of the examination, the examinee has to first enter a username and password, then have their finger scanned before being allowed to continue and take the exam. The second phase is implemented during the exam session since the examinee's identity needs to be verified constantly throughout the examination session. To this end, eye-tracking technology is employed [34].

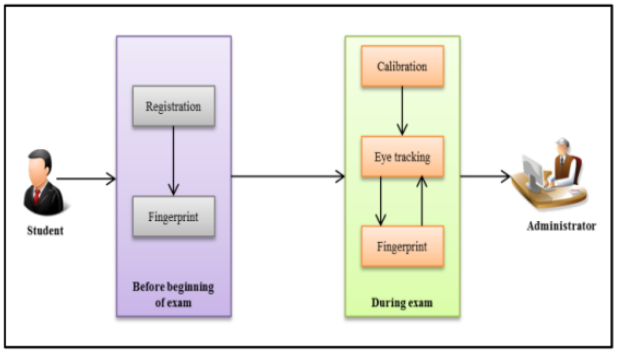


Fig. 2. Architecture of E-Exam management system [34].

First, prior to commencement of exam session, the examinee must register a username and password to open an account. On registration, the system permits the user to scan fingerprint for other subsequent identification or authentication. In the exam's duration, eye tracking is applied to make certain the identity of the examinee and prevent cheating repeatedly [44].

Eye tracking is a process of identifying where on the screen the examinee is looking by placing sensors near the eyes of the examinee. The sensor has to be placed underneath the screen and pointed toward the examinee. The examinee is required to remain within the area on the screen marked by the track box, which represents the tracking area in relation to the sensor. This also confirms the functionality of the sensor, and that the examinee is within the tracking radius [44].

After the examinee is in the correct position the calibration begins: In calibration, the examinee has to focus his or her eyes on a number of targets that appear at different positions on the screen. The targets will be displayed one by one with a specific amount of time and the goals are to achieve the highest possible results. In fact, the calibration process usually takes approximately 20 seconds to achieve. Once calibration is done, the examinee is in a position to login to the e-exam system. The eye-tracking system also authenticates the identity of the examinee throughout the exam thus greatly minimizing cases of cheating [45].

VIII. Literature Survey

The study presented in [46] focused on the analysis of the behavioral patterns of learners during online tests in order to detect cheating events. Especially, time delay and head pose variation on cheating detection in a simulated online testing scenario was discussed. The experiments indicated that the time gap and another important factor referring to head displacement with regard to computer display were significantly correlated with cheating behaviors in a student. In addition, these factors explained cheating well in a binary logistic regression test, with an overall accuracy of 75.6%. This developed algorithm provides a way to alert proctors to suspicious activities to help them monitor large enrolment online courses during the administration of remote examinations.

In Study [47] a system has been proposed to manage home appliances using interaction through voice, hand movements, and smart phones. Speech is received from users in Indonesian by the Kinect sensor the Kinect sensor and speech recognition is facilitated by a dialogue system with an additional use of Google Cloud Speech for speech processing and K-Means Clustering for gesture processing. This makes it possible for users to switch off appliances from a Smartphone application which interacts with a real-time database. The feedback from the system is twofold: an audio response through the computer speaker and a movement to control the appliances with the help of ESP8266 module. When performing accuracy tests for the system, the interaction through speech yielded 92.5% while the gesture recognition yielded only 79.25%, it was therefore clear that speech interaction was more effective. Also, the smartphone application had potential to manage the home appliances effectively.

While Researchers in [48] formed their data and used AlexNet, a deep learning model, to determine the type of cheating through the postures and facial expressions of the students during examinations. To train the model, Google Colab was used and PyTorch as the framework in which the model was implemented; The model realized a high accuracy of 96%. However, this study lacks depth in that the students were photographed only from a lateral aspect; this may have an impact on the generality of the study findings. Introducing this approach relies on studying the body posture and facial expressions in order to find out behaviors that are likely to be linked with cheating, hence offered a non-interference approach to overseeing the exam rooms.

Also, in [49] proposed a new solution for identifying academicians' misbehavior, cheating, during final examinations in online courses, based on machine learning methods. Since direct supervision is not possible during remote assessments, the authors discuss the issue of detecting cheating as an outlier detection problem. Using the example of analyzing students' continuous assessment data to identify outliers in their final examination scores, acknowledge that the data is sequential. To this effect, the study uses recurrent neural networks (RNNs) alongside anomaly detection algorithms. The proposed method which is NewAlgo surpasses other existing algorithms like, Naive Bayes, RobustCov, Isolation Forest (IsoForest) and Local Outlier Factor (LOF) with a TPR =1.00 and FPR = 0.04. These results prove that NewAlgo is capable of detecting possible cases of cheating with great efficacy thus proving it can be an effective tool is promoting academic integrity in remote assessments.

While in [50], offers research proposal idea concerning increasing examination credibility by employing computer vision for automation and surveillance. Since invigilation using individuals has drawbacks due to inherent flaws, the study recommends that closed circuit television (CCTV) camera be installed to monitor and check for irregularities in real time basis. They employed You Only Look Once (YOLOv3) as the deep learning model for the detection process and integrated residual networks that constitute the creation of its backbone. By analyzing the video stream from the exam hall, the system is a capable to identify cheating actions including but not limited to: passing papers, using any extra material or talking to other learners. The performed experiments also show that the proposed system is very effective due to the 88.03 % accuracy obtained in the detection of cheating behaviors. This automated invigilation system provides an opportunity and a probable response to issues of fairness and integrity of examination; human monitoring, and realistic assessment of students.

Also, In [51] the authors put forward a cheating detection pipeline for online interviews and exams to help designing a secure testing environment. The system only needs a video recording of the candidate during the exam and apply a series of algorithms comprising face detection, face recognition, object detection, and face tracking to determine cheating behaviors such as presence of another person, use of electronic devices and lack of presence of the candidate. The proposed pipeline is one that is efficient and more so fast in its cycle of operation thus being easily applicable through the use of an integrated webcam. To assess the proposed approach, the authors captured a private video dataset that contains 37 videos containing both legal and fraudulent behaviors. The system's performance was assessed using three different metrics: These are instance-based, segment-based and video-based. The outcome showed the high level of the model accuracy from the video-based metric that was estimated as 0.91 F1 score. In the further study, the authors propose to enrich the discussed pipeline with the voice analysis and gaze estimation to make the cheating behaviors' detection more effective.

Authors in [52] proposed "L4-BranchedActionNet" to detect the suspicious student behaviors during the examination. This model employs a 63-layer deep Convolution Neural Network that is based on the VGG-16 architecture and has four more branches for feature extraction. The system is first trained and optimized to the SoftMax function using the CUI-EXAM dataset that is particularly designed for detection of suspicious activities. Based on this expanded feature set, feature subset optimization is applied to the deep features, and then through entropy coding and the optimization of the basis using the Ant Colony System (ACS). Different classification models such as SVM and KNN are employed for classification of the features that is followed by classification model's accuracy rate of 92.99% from the cubic SVM model. Subsequent tests using CIFAR-100 set revealed enhanced accuracy of 89.80% affirming the effectiveness and resilience of the presented framework.

The study in [53] puts forward a deep learning model that is capable of real time cheating detection using video frames and speech. The system includes three modules: These include front camera-based detection, back camera-based detection, and speech-based detection and all of them use CNNs and Gaussian-based DFT techniques. Testing the system using a public dataset, the front camera module recorded test accuracies of 99.83% and 99.81% at 30% and 40% of the test set size. The back camera module was as efficient as the front camera module with an accuracy of

98.78% for either test set size and proved that the system can efficiently detect cheating during online examinations.

From the paper [54] the author presents an automated invigilation system that would help identify unethical activities during examinations. The classifier used in the system is Fast R-CNN and was trained on an invigilation dataset with training accuracy of 99.5% and testing accuracy of 98.5%. MTCNN and a face recognition module are used for the student identification and recognition with an accuracy that stands at 95%. The results from the Fast R-CNN classifier and the face recognition module are then combined to develop the student status reports in an Excel based form. This proposed model shows enhancements compared to the previous systems such as monitoring more than one hundred students on the same system without increasing computation time to provide the results.

In [55] cheating behaviors are detected by video surveillance and the Viola-Jones face detection algorithm. The dataset contains face and non-face images, and the suspicious behaviors of the subjects are labelled green and red. Criterion 3: Viola-Jones used in face detection as its efficiency is high; however, it requires much computation time when it works with big amounts of video data. However, because of the computational nature of the algorithm, this approach is a good technique for long-term observation of exam rooms without user engagement.

The work done in [56] modeling approach focuses on identifying cheating behaviors in exam rooms based on videos of the students. To process the video recorded by the system, it uses Long Short-Term Memory (LSTM) networks and a Convolutional Neural Networks (CNN). The overall accuracy of the model was 75% and F1 score was 66.7. Nevertheless, the study has some flaws, such as overfitting resulting from a small dataset and a high computational time needed for processing prevents the expansion of the solution. Nevertheless, the model reveals the possible ways of using the deep learning methods to improve cheating identification in the context of education.

Researchers in [7] the authors introduce a new dataset called “Actions of Student Cheating in Paper-Based Exams”, which collects suspicious actions during exam sessions. This dataset has been generated from recordings of eight participants doing five various cheating methods on different pairs of participants. Every step was recorded for the purpose to determine the possibility of real-time fraud detection. In evaluating the efficacy of the proposed detection framework, several action recognition methods were conducted using five types of the feature. The results have shown the percentage accuracy for each of the features; in this case, SURF with 91% of accuracy was seen to be the most accurate feature, the MSER with 89% accuracy and the HOG with 87% of accuracy. The enhancement of SURF by adding HOG features presented similar significant performance with an average of 89% accuracy, therefore underlining the efficiency of the proposed framework for automatic cheating detection in exam environments.

Authors in [57] propose an original approach to address the cheating in physical assessment by applying the modern computer vision methods. Conventional forms of invigilation are quite wanting when it comes to monitoring the large groups of students, especially in environments that are characterized by high levels of cheating. To overcome these challenges, the research uses an automated surveillance system with the help of closed-circuit television (CCTV) cameras and You Only Look Once (YOLOv5) algorithm that is improved by residual networks. This system is used to monitor the students for any shred of misconduct like; swapping of papers, writing on a banned note, or even cheating through being given assistance while sitting for the test. The model was tested in a classroom context gaining high accuracy of 88.03% in detecting cheating occurrences. The results presented here serve to support the further development of the use of AI-based monitoring systems so that exams can be evaluated equitably and with less reliance on proctors.

Scientists in [58] proposed a system to identify unlawful actions and cases of dishonesty during examinations with the help of YOLO (You Only Look Once) algorithm. It receives video streams in real-time to track and analyze students’ actions during tests, based on which sample contains different actions of students. The model proposed is of RCNN model and it has a training accuracy of 99.5%, testing accuracy of 98.5% and face recognition accuracy of 95%. The system can accommodate more than one hundred students at a learning session while using less computation time compared to the prior models. This faster invigilation system proves to be much better with increased efficiency and improvement on the general examination security.

In [59] researchers presented an automated system which is based on using computer vision and CCTV footage for immediate identification of the suspicious actions. It uses CNNs like YOLOv3, VGG-16 for object recognition, that are mobile phones, combined with LSTM for detecting sequential data, which are behaviors like frequent glances or hand movements. Consequently, our outcomes reveal that the efficiency of the system is high: The accuracy is in the range of 85–90%, the precision reaches 87%, and the recall makes 83%; thus, cheating could be identified with high confidence without many false positives.

Reported studies on eye-tracking based proctoring indicate detection accuracies ranging from 85–92% in controlled exam settings [44], though performance may drop in natural environments due to head movement and calibration drift. These metrics provide a benchmark for evaluating eye-tracking reliability in cheating detection.

Table (IV) summarizes key deep learning-based approaches, showing their model types (CNN, RNN, YOLO), datasets, and performance metrics (accuracy/F1). Such a comparison highlights that while YOLO-based systems [50][57][59] achieve ~88–90% accuracy in real-time, CNN+RNN hybrids [49] [53] exceed 95% in controlled settings but require higher computational resources.

TABLE IV.
DATASETS FOR AUTOMATIC CHEATING DETECTION

Ref.	Main Idea / System	Key Techniques	Dataset / Setup	Reported Performance
[46]	Analyze learner behavior (time delay & head pose) to detect cheating in online exams	Binary Logistic Regression	Simulated online tests	Accuracy 75.6%
[47]	Smart home control via speech & gestures (Indonesian)	Kinect + Google Cloud Speech + K-Means for gestures	Home appliance control tests	Speech acc. 92.5%, Gesture 79.25%
[48]	Detect cheating via posture & facial expressions	AlexNet (Deep CNN)	Lateral student photos (Google Colab, PyTorch)	Accuracy 96%
[49]	Outlier-based cheating detection in remote exams	RNN + Anomaly detection (NewAlgo vs NB, IsoForest, LOF)	Sequential assessment data	TPR 1.00, FPR 0.04
[50]	Automated invigilation using CCTV & CV	YOLOv3 + Residual Nets	Exam hall video	Accuracy 88.03%
[51]	Cheating detection pipeline for online exams/interviews	Face detection & recognition + Object detection + Tracking	37 video dataset	Video-based F1 = 0.91
[52]	L4-BranchedActionNet deep CNN (63 layers, VGG-16 based)	Feature subset optimization + ACS + SVM/KNN	CUI-EXAM & CIFAR-100	Cubic SVM acc. 92.99%, CIFAR 89.80%
[53]	Real-time cheating detection via video & speech	CNN + Gaussian DFT	Public dataset	Front cam 99.83%, Back cam 98.78%
[54]	Automated invigilation w/ Fast R-CNN & MTCNN	Fast R-CNN + Face recog.	Custom invigilation dataset	Train 99.5%, Test 98.5%, Face recog. 95%
[55]	Face detection for cheating monitoring	Viola–Jones algorithm	Face/non-face video data	High efficiency but computationally heavy
[56]	Video-based cheating detection	CNN + LSTM	Small dataset	Acc. 75%, F1 66.7% (overfitting & slow)
[7]	“Actions of Student Cheating” dataset & action recognition	SURF, HOG, MSER	8 participants, 5 cheating methods	SURF 91%, MSER 89%, HOG 87%
[57]	AI-based CCTV cheating monitor	YOLOv5 + Residual Nets	Classroom video	Accuracy 88.03%
[58]	Fast invigilation system	YOLO + RCNN + Face recog.	Exam session video	Train 99.5%, Test 98.5%, Face 95%
[59]	CCTV + CV cheating detection	CNNs (YOLOv3, VGG-16) + LSTM	Video & sequential behavior	Accuracy 85–90%, Precision 87%, Recall 83%

IX. Conclusions

This review demonstrates that automated cheating detection has progressed from traditional human-centric methods to AI-driven solutions integrating computer vision, behavioral analytics, and multimodal data. Among existing approaches, YOLO-based detectors and Fast R-CNN models achieve real-time detection with ~88–98% accuracy, while CNN–RNN hybrids excel in controlled environments (>95%) but demand higher computation. Eye-tracking can complement vision-based systems but typically achieves 85–92% accuracy and is sensitive to calibration. Plagiarism tools and browser lockdown remain essential for text-based exams but do not address behavioral cheating.

For practical deployment, institutions should consider privacy-friendly AI proctoring that fuses video, audio, and interaction logs, adopt bias-aware training datasets, and select lightweight architectures (e.g., MobileNet + LSTM) where hardware is limited. Future research should also focus on explainable models and federated learning to maintain student trust while ensuring fairness and compliance with data regulations.

Future research in automated cheating detection should focus on multimodal fusion, integrating video, audio, and behavioral signals such as keystrokes or mouse movement for more robust detection. Addressing fairness and bias is essential to avoid penalizing neurodivergent or culturally diverse students, while privacy-preserving approaches such as federated learning and on-device inference can help meet regulations like GDPR. Greater explainability is needed so AI decisions are transparent and reduce false accusations, and emphasis on low-resource deployment will enable lightweight models suitable for institutions with limited hardware and bandwidth.

References

[1] W. Alsabhan, “Student Cheating Detection in Higher Education by Implementing Machine Learning and LSTM Techniques,” *Sensors*, vol. 23, no. 8, 2023, doi: 10.3390/s23084149

[2] K. Lee and M. Fanguy, “Online exam proctoring technologies: Educational innovation or deterioration?,” *Br. J. Educ. Technol.*, vol. 53, no. 3, pp. 475–490, 2022, doi: 10.1111/bjet.13182

[3] K. J. Brakas, and M. Alanezi “Measuring the Extent of Cyberbullying Comments in Facebook Groups for Mosul University Students,” *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 2, pp. 337–348, 2025, https://orcid.org/0000-0003-4213-9193

[4] D. Starovoytova and S. Namango, “Factors Affecting Cheating-Behavior at,” *J. Educ. Pract.*, vol. 7, no. 31, pp. 66–82, 2016

[5] I. Jegham, A. Ben Khalifa, I. Alouani, and M. Mahjoub, “Vision-based human action recognition: An overview and real world challenges,” *Digit. Investig.*, vol. 32, p. 200901, Mar. 2020, doi: 10.1016/j.fsidi.2019.200901

[6] M. Kulbacki, M. Kulbacki, J. Segen , Z. Chaczko, J. W. Rozenblit, M. Kulbacki , R. Klempous, and K. Wojciechowski., “Intelligent Video Analytics for Human Action Recognition: The State of Knowledge,” *Sensors*, vol. 23, no. 9, pp. 1–31, 2023, doi: 10.3390/s23094258

[7] F. Hussein, A. Al-Ahmad, S. El-Salhi, E. Alshdaifat, and M. Al-Hami, “Advances in Contextual Action Recognition: Automatic Cheating Detection Using Machine Learning Techniques,” *Data*, vol. 7, no. 9, 2022. https://doi.org/10.3390/data7090122

[8] M. El-Masry, M. Fakhr, and M. A.-M. M. Salem, “Action Recognition by Discriminative EdgeBoxes,” *IET Comput. Vis.*, vol. 12, issue 4, pp. 443-452, Dec. 2017, doi: 10.1049/iet-cvi.2017.0335

[9] H. M. Mohammed and Q. I. Ali, “Cheating Prevention in E-proctoring Systems Using Secure Exam Browsers: A Case Study,” *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 8, no. 4, p. 634, 2022, doi: 10.26555/jiteki.v8i4.25094

[10] N. Doghonadze, T. Dolidze, N. Vasadze, M. Zoranyan, “Cheating in Higher Education - Causes , Results and Ways to Prevent,” June, 2024.

[11] D. Starovoytova and M. Arimi, “Witnessing of Cheating-in-Exams Behavior and Factors Sustaining Integrity,” *Journal of Education and Practice.*, vol. 8, no. 10, pp. 127–141, 2017.

[12] R. J. Fendler, M. C. Yates, and J. M. Godbey, “Proof that a simple positive approach can reduce student cheating,” *J. Instr. Pedagog.*, vol. 28, pp. 1–19, 2023, http://www.aabri.com/copyright.html

[13] T. Lancaster, “Effective And Efficient Plagiarism Detection,” no. January 2003, 2003.

[14] S. Hamady, K. Mershad, and B. Jabakhanji, “Multi-version interactive assessment through the integration of GeoGebra with Moodle,” *Front. Educ.*, vol. 9, pp. 1–15, 2024, doi: 10.3389/feduc.2024.1466128

[15] R. Fendler and J. Godbey, “Cheaters Should Never Win: Eliminating the Benefits of Cheating,” *J. Acad. Ethics*, vol. 14, Sep. 2015, doi: 10.1007/s10805-015-9240-8

[16] R. A. Hicklin, L. Eisenhart, N. Richetelli, B. Eckenrode, “Accuracy and reliability of forensic handwriting comparisons,” *Proc. Natl. Acad. Sci. U. S. A.*, vol. 119, no. 32, pp. 1–12, 2022, doi: 10.1073/pnas.2119944119

[17] C. Y. Chuang, S. D. Craig, and J. Femiani, “Detecting probable cheating during online assessments based on time delay and head pose,” *High. Educ. Res. Dev.*, vol. 36, issue 6, pp. 1123–1137, 2017, doi: 10.1080/07294360.2017.1303456

[18] W. T. Smale, R. Hutcheson, and C. J. Russo, “Cell Phones, Student Rights, and School Safety: Finding the Right Balance,” *Can. J. Educ. Adm. Policy*, no. 195, pp. 49–64, 2021, doi: 10.7202/1075672AR

[19] O. Zimba and A. Y. Gasparyan, “Plagiarism detection and prevention: A primer for researchers,” *Reumatologia*, vol. 59, no. 3, pp. 132–137, 2021, doi: 10.5114/reum.2021.105974

[20] M. Kim, “peer-reporting of academic dishonesty in classroom and online examinations : prevalence , experiences , perceptions , and beliefs of pharmacy students by”, *University of the Pacifi*c, 2020.

[21] R. Ladyshewsky, “Post-graduate student performance in ‘supervised in-class’ vs. ‘unsupervised online’ multiple choice tests: implications for cheating and test security,” *Assess. Eval. High. Educ.*, vol. 40, issue 7, pp. 1–15, May 2014, doi: 10.1080/02602938.2014.956683

[22] V. Raman and S. Ramlogan, “Academic integrity and the implementation of the honour code in the clinical training of undergraduate dental students,” *Int. J. Educ. Integr.*, vol. 16, no. 1, pp. 1–20, 2020, doi: 10.1007/s40979-020-00058-2

[23] O. L. Holden, M. E. Norris, and V. A. Kuhlmeier, “Academic Integrity in Online Assessment: A Research Review,” *Front. Educ.*, vol. 6, pp. 1–13, 2021, doi: 10.3389/feduc.2021.639814

[24] N. Taşkin, “Cheating and prevention strategies in online assessment,” *Teach. Assess. Era Educ. 5.0*, no. June, pp. 161–172, 2024, doi: 10.4018/979-8-3693-3045-6.ch009

[25] N. Das and M. Panjabi, “Plagiarism: Why is it such a big issue for medical writers?,” *Perspect. Clin. Res.*, vol. 2, no. 2, p. 67, 2023, doi: 10.4103/2229-3485.80370

[26] M. Rodrigues, R. Silva, A. P. Borges, M. Franco, and C. Oliveira, “Artificial intelligence: threat or asset to academic integrity? A bibliometric analysis,” *Kybernetes*, vol. 54, issue 5, pp. 2939-2970, 2024, doi: 10.1108/K-09-2023-1666

[27] A. Tweissi, W. Al Etaiwi, and D. Al Eisawi, “The Accuracy of AI-Based Automatic Proctoring in Online Exams,” *Electron. J. e-Learning*, vol. 20, no. 4, pp. 419–435, 2022, doi: 10.34190/ejel.20.4.2600.

[28] O. Kruse, C. Rapp, C. M. Anson, K. Benetos, E. Cotos, A. Devitt, and A. Shibani, *Digital writing technologies in higher education: Theory, research, and practice*. Springer International Publishing, 2023. doi: 10.1007/978-3-031-36033-6

[29] G. Frankl, P. Schartner, and G. Zebedin, “Secure online exams using students’ devices,”, *Proceedings of the 2012 IEEE Global Engineering Education Conference*,

pp. 1–7, Apr. 2012, doi: 10.1109/EDUCON.2012.6201111

[30] O. Ojajuni, F. Ayeni, O. Akodu, F Ekanoye, S. Adewole, T. Ayo, S. Misra, and V. Mbarika, "Predicting Student Academic Performance Using Machine Learning", *LNCS* , vol. 12957, pp. 481-491, 2021, doi: 10.1007/978-3-030-87013-3_36

[31] J. H. Yi and J. Moon, "Secure and Transparent Craftwork Authentication and Transaction System: Integrating Digital Fingerprinting and Blockchain Technologies," *Appl. Sci.*, vol. 14, no. 19, 2024, doi: 10.3390/app14199054

[32] K. Amkamaran, I. F. Kasmin, Z. M. Zainal Abidin, and H. Vasudavan, "Secured E-Examination System with Continuous Authentication to Prevent Cheating," *Int. J. Data Sci. Adv. Anal.*, vol. 4,no. 2, pp. 242–249, 2023, doi: 10.69511/ijdsaa.v4i0.172

[33] R. Djokovic, J. Janinovic, S. Pekovic, D. Vuckovic, and M. Blecic, "Relying on Technology for Countering Academic Dishonesty: The Impact of Online Tutorial on Students' Perception of Academic Misconduct," *Sustain.*, vol. 14, no. 3, 2022, doi: 10.3390/su14031756

[34] R. Bawarith, D. Abdullah, D. Anas, and P. Dr., "E-exam Cheating Detection System," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 4, pp. 176–181, 2017, doi: 10.14569/ijacsa.2017.080425

[35] M. Takahashi, M. Naemura, M. Fujii, and S. Satoh, "Human action recognition in crowded surveillance video sequences by using features taken from key-point trajectories," *IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Work.*, pp. 9–16, 2011, doi: 10.1109/CVPRW.2011.5981713

[36] G. Ranganathan, "A Study to Find Facts Behind Preprocessing on Deep Learning Algorithms," *J. Innov. Image Process.*, vol. 3, pp. 66–74, Apr. 2021, doi: 10.36548/jiip.2021.1.006

[37] A. B. Sargano, P. Angelov, and Z. Habib, "A comprehensive review on handcrafted and learning-based action representation approaches for human activity recognition," *Appl. Sci.*, vol. 7, no. 1, 2017, doi: 10.3390/app7010110

[38] K. Alomar, H. I. Aysel, and X. Cai, "RNNs, CNNs and Transformers in Human Action Recognition: A Survey and A Hybrid Model," *arXiv:2407.06162v1*, pp. 1–46, 2024, http://arxiv.org/abs/2407.06162

[39] B. Sharief and Y. Ersayyem, "LLM and RAG Powered Chatbot for the College of Computer Science and Mathematics at the University of Mosul," *Int. Res. J. Innov. Eng. Technol.*, vol. 08, pp. 59–61, Jan. 2024, doi: 10.47001/IRJIET/2024.810010

[40] K. M. Al-Tkhayneh, E. M. Alghazo, and D. Tahat, "The Advantages and Disadvantages of Using Artificial Intelligence in Education," *J. Educ. Soc. Res.*, vol. 13, no. 4, pp. 105–117, 2023, doi: 10.36941/jesr-2023-0094

[41] A. Nigam, R. Pasricha, T. Singh, and P. Churi, "A Systematic Review on AI-based Proctoring Systems: Past, Present and Future," *Educ. Inf. Technol.*, vol. 26, no. 5, pp. 6421–6445, 2021, doi: 10.1007/s10639-021-10597-x

[42] F. Noorbehbahani, A. Mohammadi, and M. Aminazadeh, "A systematic review of research on cheating in online exams from 2010 to 2021", *Education and Information Technologie*s, vol. 27, no. 6, 2022. doi: 10.1007/s10639-022-10927-7

[43] S. Mishra, S. Roopikha, S. Roshini, and S. Rithika, "Automatic Cheating Detection In Exam Hall," *techrxiv.orgR*, 2023, https://www.techrxiv.org/doi/full/10.36227/techrxiv.24538150.v1

[44] M. B. Ibrahim, A. U. Othman, B. F. Balogun, U. Musa, U. Chinalu, and U. C. Briget, "Development of a fingerprint biometric authentication scheme in electronic examination," *Int. Res. J. Adv. Eng. Sci. Briget*, vol. 2, no. 1, pp. 177–185, 2017.

[45] Z. Zeng, E. Neuer, M. Roetting, and F. Siebert, "A One-Point Calibration Design for Hybrid Eye Typing Interface," *Int. J. Hum. Comput. Interact.*, vol. 39, pp. 1–14, Jul. 2022, doi: 10.1080/10447318.2022.2101186

[46] C. Y. Chuang, S. D. Craig, and J. Femian "Detecting probable cheating during online assessments based on time delay and head pose", *Higher Education Research and Development*, 36 , 1123-1137, 2017, doi: 10.1080/07294360.2017.1303456

[47] H. Fakhrurroja, C. Machbub, A. S. Prihatmanto, and A. Purwarianti, "Multimodal interaction system for home appliances control," *Int. J. Interact. Mob. Technol.*, vol. 14, no. 15, pp. 44–67, 2020, doi: 10.3991/IJIM.V14I15.13563

[48] J. Nishchal, S. Reddy, and P. N. Navya, "Automated Cheating Detection in Exams using Posture and Emotion Analysis," *Proc. CONECCT 2020 - 6th IEEE Int. Conf. Electron. Comput. Commun. Technol.*, 2020, doi: 10.1109/CONECCT50063.2020.9198691

[49] F. Kamalov, H. Sulieman, and D. S. Calonge, "Machine learning based approach to exam cheating detection," *PLoS ONE*, vol. 16, no. 8 August. 2021. doi: 10.1371/journal.pone.0254340

[50] M. Malhotra and I. Chhabra, "Automatic Invigilation Using Computer Vision," *Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*, vol. 4. 2021. doi: 10.2991/ahis.k.210913.017

[51] A. Can, M. Uluyaˇgmur, and U. Bayraktar, "Cheating Detection Pipeline for Online Interviews and Exams," in *arXiv:2106.14483v1*, 2021.

[52] M. D. Genemo, "Suspicious activity recognition for monitoring cheating in exams," *Proceedings of the Indian National Science Academy* , vol. 88, pp. 1-10, 2022, https://doi.org/10.1007/s43538-022-00069-2

[53] S. Kaddoura and A. Gumaei, "Towards effective and efficient online exam systems using deep learning-based cheating detection approach," *Intelligent Systems with Applications*, vol. 16, 2022, https://doi.org/10.1016/j.iswa.2022.200153

[54] F. Mahmood, J. Arhad, M. T. Othman, M. F. Hayat, N. Bhatti, M.H. Jaffary, A. Rehman, and H. Hamam, "Implementation of an Intelligent Exam Supervision System Using Deep Learning Algorithms," *Sensors*, vol. 22, no. 17, 2022, doi: 10.3390/s22176389

[55] R. M. Al_Airaji, I. A. Aljazaery, H. T. S. ALRikabi, and

A. H. M. Alaidi, “Automated Cheating Detection based on Video Surveillance in the Examination Classes,” *Int. J. Interact. Mob. Technol.*, vol. 16, no. 8, pp. 124–137, 2022, doi: 10.3991/ijim.v16i08.30157

[56] S. Essahraui, M. A. El Mrabet, M. F. Bouami, K. El Makkaoui, and A. Faize, “An Intelligent Anti-cheating Model in Education Exams,” in *2022 5th International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2022, pp. 1–6. doi: 10.1109/CommNet56067.2022.9993953

[57] R. S, RoshiniS, and S. Rithika, “Automatic Cheating Detection In Exam Hall,” *International Journal of Noval Research and Development*, vol.8, issue 11, 2023.

[58] N. Sumaiya, S. Navya, R. Anjali, N. Priya, A. Nandan, “Automated Invigilation System for Detection of Suspicious Activities during Examination,” *Int. Res. J. Eng. Technol.*, vol. 10, issue 4, pp. 361–366, 2023, doi: 10.1109/AICAI.2019.8701263

[59] M. Navale, A. A. Jadhav, M. S. Kadam, S. D. Karandikar, and S. A. Kate, “From Manual to Automated: A Computer Vision-Based Solution for Exam Cheating Detection,” *International Journal of Ingenious Research, Invention and Development*, vol. 3, issue 5, 2024.