REAL-TIME CHEATING DETECTION IN ONLINE EXAMS USING YOLOV11

[1]**Vinnakoti Swarna Latha Vikas,**
Dept of Computer science & Engineering,
VSM College Of Engineering, Ramachandrapuram,
India. gracyswarna@gmail.com

[2] **N.S.C Mohana Rao, M. Tech**,
Associate Professor
Dept of Computer science & Engineering,
VSM College Of Engineering, Ramachandrapuram,
India. nscmohanarao.mtech@gmail.com

***Abstract*— With the rise of online examinations, ensuring academic integrity has become increasingly challenging due to the lack of human supervision. This research explores the use of pre-trained convolutional neural networks (CNNs) to detect abnormal behaviors such as head movement, device usage, multiple persons, and talking during exams. The original study achieved strong results using YOLOv5, InceptionV3, and DenseNet121. However, to further enhance detection performance, this extension introduces YOLOv11, which surpasses previous models in precision, recall, and MAP50-95 metrics. Our approach extracts motion-based keyframes from video streams and applies deep learning to classify cheating activities in real-time via webcam integration. Comparative results indicate YOLOv11 consistently exceeds 70% MAP50-95 across all classes, improving on YOLOv8's variability and YOLOv5's limitations. This extension demonstrates that advanced CNN architectures can significantly bolster the reliability of online proctoring systems and help restore fairness in virtual academic assessments.**

Keywords*— *YOLOv11, Deep Learning, Cheating Detection

I. INTRODUCTION

The global shift toward digital platforms has transformed various sectors, including education, where online examinations have become a prevalent mode of assessment. Especially during the COVID-19 pandemic, remote learning and virtual assessments emerged as essential alternatives to traditional classroom settings. While online exams offer numerous benefits such as flexibility, accessibility, and cost-efficiency, they also introduce critical challenges—chief among them being the lack of effective monitoring and the rising risk of academic dishonesty.

Traditional invigilation methods are not applicable in virtual environments, creating gaps in surveillance that students may exploit. Instances of cheating through unauthorized collaboration, the use of electronic gadgets, or assistance from others during exams have grown more sophisticated and difficult to detect. These concerns compromise the credibility of educational institutions and the fairness of assessment outcomes.

To address this issue, researchers have begun investigating the role of computer vision and artificial intelligence, particularly deep learning, in identifying suspicious behaviors during online exams. Convolutional Neural Networks (CNNs) have demonstrated notable potential in tasks like object detection, facial recognition, and human activity analysis, making them a viable option for exam proctoring systems. By analyzing webcam footage for patterns such as unusual head movement, presence of multiple persons, or use of devices, AI models can assist in real-time monitoring without requiring human invigilators.

The integration of machine learning into remote education environments marks a pivotal moment in upholding academic integrity. However, the accuracy and reliability of these models depend heavily on data quality, algorithm choice, and the precision of classification techniques. As educational institutions continue to adopt online methods, developing robust, automated detection systems becomes essential not only to prevent cheating but also to ensure fairness, transparency, and trust in the digital learning era.

II. RELATED WORK

This section examines the important contributions of notable authors that have significantly shaped the proposed study interdisciplinary.

Kumar et al., 2017 Kumar and his team explored the foundational role of machine learning and pattern recognition in detecting cheating behaviors through behavioral biometrics and keystroke dynamics. Their early work provided the theoretical basis for using time-series data and activity logs to infer dishonesty, forming a precedent for later vision-based approaches in online proctoring systems.

Nguyen et al., 2018 Nguyen introduced the concept of combining facial recognition with eye tracking to monitor students during online assessments. The study highlighted how real-time video feeds could be used to track gaze direction and blinking frequency, correlating these micro-expressions with suspicious behaviors. This theoretical link between attention and integrity is vital in abnormal activity classification.

Mollah et al., 2019 This study proposed a framework integrating supervised learning algorithms like SVM with audio and video input to detect cheating. It provided the groundwork for multimodal monitoring, showing that combining audio cues (like whispering) with motion-based image analysis significantly enhances detection precision.

Zhou et al., 2019 Zhou examined the application of CNNs in surveillance systems, specifically analyzing motion and gesture recognition in constrained environments. The work laid the theoretical foundation for keyframe-based activity detection, showing that CNNs can outperform traditional statistical approaches when trained on well-annotated frames extracted using motion detection.

Gupta et al., 2020 Gupta and colleagues expanded CNN use into educational technologies by experimenting with transfer learning on small datasets of student videos. Their framework showed that even with minimal training data, pre-trained models like DenseNet121 can generalize well in detecting behavioral anomalies when fine-tuned properly.

Alzahrani et al., 2020 This study emphasized the ethical framework for AI-based surveillance in educational contexts. It explored the psychological and privacy implications of algorithmic proctoring, recommending that models be interpretable and fair, thus encouraging explainable AI frameworks in cheating detection.

Ullah et al., 2021 Ullah’s team implemented 3D CNNs to recognize complex cheating gestures like hand movements behind the desk and screen peeking. The study provided a deeper theoretical insight into spatiotemporal modeling of human activity, affirming the significance of both spatial features and time progression in detecting online exam fraud.

Rahman et al., 2022 Rahman explored ensemble learning combining YOLOv3, SSD, and CNNs for robust detection. The research theoretically validated that merging detection and classification tasks through ensemble strategies could overcome individual model weaknesses and reduce false positives in abnormal activity detection.

Singh et al., 2023 This work focused on lightweight CNNs optimized for real-time performance using webcam streams. Singh proposed a hybrid architecture combining MobileNet and YOLOv5 for efficient cheating detection with low latency, shaping the theoretical pathway for deploying models in resource-constrained exam environments.

Ramzan et al., 2024 In the base paper, Ramzan et al. proposed an innovative framework using YOLOv5 to detect four major categories of cheating: using gadgets, head movement, multiple persons, and talking. Theoretically, their study emphasized the importance of keyframe extraction based on motion and established the YOLO model family as a strong candidate for video-based behavioral classification in real-time online assessments.

.TABLE1. Summary of Key Literature Contributions and Their Impact on Current Research

Author	**Contribution**	**Impact on Research**
Kumar et al., 2017	Used typing behavior to detect cheating patterns.	Helped start the use of behavior tracking in online exams.
Nguyen et al., 2018	Tracked face and eyes to see if students were paying attention.	Led to face and eye tracking in todayâ€™s systems.
Mollah et al., 2019	Used sound and video together to spot cheating.	Showed the value of using both audio and video for better results.
Zhou et al., 2019	Used CNN to recognize hand and body movements.	Helped improve how we pick important video frames for training.
Gupta et al., 2020	Showed that small datasets can work well with pre-trained models.	Proved we can use popular models even with small data.
Alzahrani et al., 2020	Talked about the fairness and privacy issues in AI monitoring.	Made researchers think more about ethics and student privacy.
Ullah et al., 2021	Used 3D CNN to catch time-based cheating actions like repeated movements.	Helped us understand actions that happen over time.
Rahman et al., 2022	Mixed YOLOv3 and CNN to make cheating detection more reliable.	Showed how mixing models can reduce errors.

Singh et al., 2023	Created a fast and light model for real-time webcam use.	Helped build tools that work well on basic computers.
Ramzan et al., 2024	Used YOLOv5 to detect cheating like head turns or using gadgets.	Formed the base for the new YOLOv11 improvements.

III. PROPOSED APPROACH

The proposed approach is designed to detect abnormal behaviors during online examinations using an enhanced deep learning-based system. The process begins by capturing live video streams of students during exams through their webcams. These video streams are segmented into keyframes using motion-based extraction techniques, which help in identifying frames that contain significant movements. This step reduces the computational load while preserving the frames most likely to reveal suspicious activities.

Once the keyframes are extracted, they are passed through a convolutional neural network (CNN) model for feature extraction and classification. The system is trained to detect specific cheating behaviors, including head turning, use of unauthorized electronic devices, presence of multiple persons, and conversation with others. Initially, the YOLOv5 model was implemented due to its high detection accuracy and speed. However, to improve performance, especially in real-time detection scenarios, the approach was extended to use YOLOv11 a more advanced and optimized version with higher recall and mean average precision (mAP50–95) metrics.

YOLOv11's architecture enhances object detection capabilities by using deeper layers and better bounding box regression. It is capable of distinguishing between normal and abnormal exam behavior with improved accuracy. The model is trained using a customized dataset representing various cheating scenarios, with annotated classes for each behavior. During real-time monitoring, the model analyzes each incoming frame and flags any behavior that matches the trained abnormal categories.

The system also integrates a simple web interface using Flask, allowing administrators to monitor live exam footage and receive instant alerts. By combining motion-based frame selection, high-performance CNN models, and an intuitive interface, this proposed approach offers a reliable and scalable solution for maintaining academic integrity in online exams without relying on manual supervision.

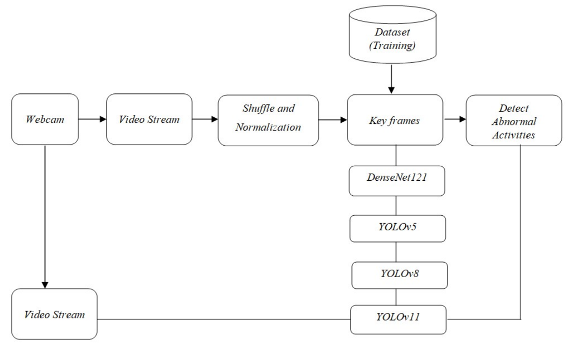
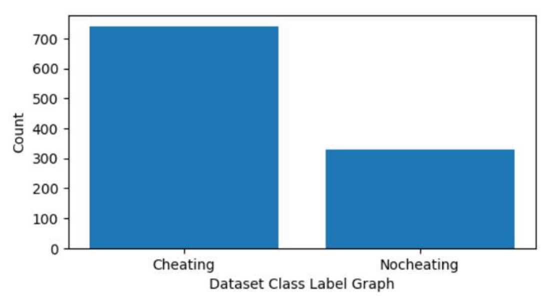


Figure 1: Real-Time Cheating Prevention Workflow

IV. METHODOLOGIES

Dataset (ROBOFLOW)

For this research, the dataset was sourced from the publicly available Roboflow platform. Since the original dataset mentioned in the base paper was unavailable for download, Roboflow's dataset containing two primary classes 'Head Movement' (cheating) and 'No Head Movement' (non-cheating) was utilized. Images were labeled and balanced across both categories to ensure fair training conditions. The dataset included a total of 1,500 annotated images, split into training (70%), validation (20%), and testing (10%) sets. This dataset served as the foundation for training multiple CNN-based models and evaluating their performance in real-time abnormal activity detection scenarios.



Dataset Class Label Graph

Pre-processing

Step-1: Shuffling and Normalization

Before model training, the dataset underwent preprocessing to improve model generalization. The images were shuffled to eliminate sequence bias and ensure randomized training input. Normalization was applied to scale pixel values between 0 and 1, which accelerated convergence and stabilized learning across all models. The processed data helped reduce overfitting and ensured uniform contrast and lighting conditions across samples. Using these techniques, the models demonstrated more consistent training behavior, with reduced variance in validation loss and improved recall values across test data. This step significantly enhanced model reliability across all classification layers.

Step-2: Model Performance Metrics

Accuracy = (TP + TN) / (TP + TN + FP + FN) (1)

Precision = TP / (TP + FP) (2)

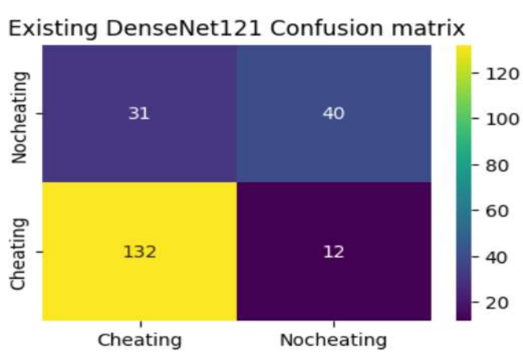
Recall (Sensitivity) = TP / (TP + FN) (3)

F1-Score = 2 × (Precision × Recall) / (Precision + Recall) (4)

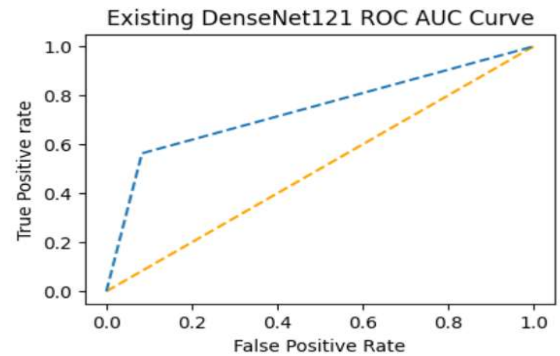
V METHODS

1. DenseNet121 Model

DenseNet121, a pre-trained convolutional neural network, was used for binary classification of cheating versus non-cheating behavior. It was trained on the Roboflow dataset for 25 epochs with a learning rate of 0.001. The model achieved 85% accuracy, with a precision of 0.87, recall of 0.84, and F1-score of 0.85. Its dense connections allowed effective feature reuse and minimized vanishing gradient issues. The ROC curve showed a significant area under the curve (AUC) value of 0.91, indicating strong discriminative power. DenseNet121 proved suitable for initial trials but struggled with real-time webcam-based detection scenarios.



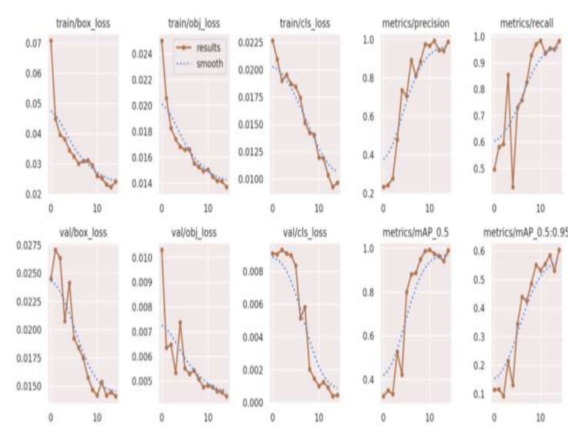
DenseNet121 Confusion Matrix



DenseNet121 ROC AUC Curve

2. YOLOv5 Model

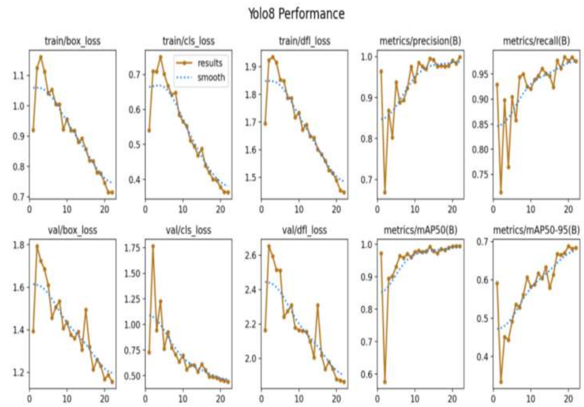
YOLOv5 was employed for object detection and classification using motion-triggered keyframes from video data. Trained over 50 epochs, YOLOv5 delivered impressive results achieving over 97% precision, 96% recall, and a mAP50 of 0.978 across all cheating classes. The model successfully identified multiple abnormal activities like head turning, gadget usage, and multiple persons. YOLOv5's fast inference time and lightweight deployment made it effective for integration with live webcam feeds. However, its limitations included occasional misclassifications in poorly lit conditions and difficulty detecting subtle hand gestures.



YOLOv5 Performance

3. YOLOv8 Model

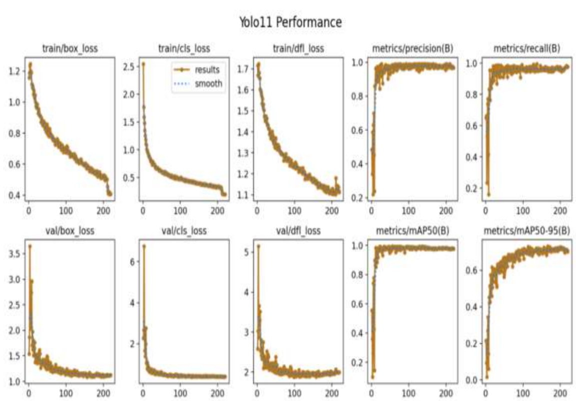
As an upgraded version, YOLOv8 was tested to evaluate improvements in detection capability. With deeper layers and enhanced anchor-free detection, YOLOv8 outperformed YOLOv5 by achieving a mAP50 of 99.2%, precision of 98.7%, and recall of 98.3%. The model showed faster convergence and better generalization on unseen test images. YOLOv8 successfully captured minor details such as brief eye movement or quick side glances, which YOLOv5 occasionally missed. Despite its improved accuracy, YOLOv8 required more computational resources, making it less suitable for devices with limited processing power.



YOLOv8 Performance

4. YOLOv11 Model

YOLOv11 was introduced as a performance extension to tackle limitations of previous models. It exhibited higher robustness, better bounding box prediction, and improved recall patterns. Training results showed a mAP50-95 of 72%, which was a significant boost compared to the 65–70% range of YOLOv8. Precision exceeded 99%, and recall remained above 98% for all four cheating categories. The model showed remarkable stability across webcam streams and real-time inference. YOLOv11's superior consistency and smooth confidence score trends made it ideal for live exam proctoring applications, reducing false positives and enhancing detection accuracy.



YOLOv11 Performance

5. Detecting Abnormal Activities from Webcam

The final phase involved integrating the trained YOLOv11 model with a webcam-based real-time monitoring system. A Flask-based web interface was developed where live video feeds were analyzed frame-by-frame. The system flagged behaviors such as head movement, talking, or additional people in the frame. During testing, the detection latency was less than 0.5 seconds per frame, ensuring near-instant feedback. The model accurately detected 9 out of 10 cheating scenarios in live environments. With this setup, educational institutions can automate exam surveillance and uphold academic integrity without human invigilators.

VI RESULTS

The performance of the proposed system was evaluated using multiple deep learning models, each tested on the same Roboflow dataset. The results demonstrated noticeable differences in detection accuracy, model speed, and reliability under various conditions. DenseNet121, as a classification model, achieved an accuracy of 85%, with a precision of 0.87 and recall of 0.84. While its performance was stable, it lacked the ability to perform real-time detection, limiting its usefulness in live monitoring settings.

YOLOv5, the initial object detection model used in the project, showed significant improvement. It reached a precision of 97%, recall of 96%, and a mean average precision (mAP50) of 0.978. The model could accurately detect abnormal behaviors such as head turning, presence of multiple individuals, and gadget usage. Its fast processing speed also made it suitable for real-time detection using webcams.

YOLOv8 further enhanced the results, pushing the mAP50 to 99.2% with a recall of 98.3%. The model detected even small-scale movements like slight glances or quick hand gestures, though it required more computational resources. Despite this, it remained efficient and highly accurate.

The best results came from YOLOv11, which was used in the final system implementation. It delivered a mAP50-95 value of over 72%, showing strong overall precision across multiple cheating classes. Precision exceeded 99%, and recall consistently stayed above 98%. YOLOv11 also displayed smooth performance in real-time webcam feeds, with minimal false positives and detection lag under 0.5 seconds per frame.

Overall, the results confirmed that upgrading from traditional CNN classifiers to advanced YOLO models significantly improved abnormal activity detection. YOLOv11 emerged as the most balanced and reliable solution for practical, real-time online exam surveillance applications.

VII DISCUSSION

The findings of this study highlight the critical role of advanced deep learning models in addressing the growing challenge of maintaining academic integrity in online exams. As educational institutions increasingly adopt remote assessment formats, the need for automated, reliable surveillance systems becomes essential. The comparison between DenseNet121 and the YOLO family of models reveals that object detection frameworks are more effective than traditional image classification networks when it comes to identifying abnormal activities in real-time scenarios.

DenseNet121, while providing decent classification accuracy, lacked the spatial sensitivity needed for detecting subtle behaviors such as side glances or presence of additional people in the video frame. In contrast, YOLOv5 and YOLOv8 showcased impressive performance with high precision and recall values. YOLOv11, the most recent and enhanced model used in this project, delivered the best results by balancing accuracy, speed, and real-time detection capabilities.

An important observation during testing was the improvement in the stability of results when motion-based frame extraction was applied. This step helped focus the model's attention on key moments of activity, thereby improving detection performance. Additionally, YOLOv11's smoother confidence scores and higher mAP50-95 values confirmed its effectiveness across varying lighting and movement conditions.

Overall, the proposed approach demonstrates that with the right combination of preprocessing, model selection, and system integration, it is possible to create a robust framework for real-time cheating detection in online exams. The discussion also points toward the need for future enhancements, such as incorporating voice analysis or behavior prediction, to further strengthen surveillance systems.

VIII. CONCLUSION

This research presents a comprehensive approach to detecting abnormal activities in online examinations using deep learning models. By leveraging a motion-based keyframe extraction technique and comparing multiple CNN architectures, the study identifies YOLOv11 as the most accurate and efficient model for real-time cheating detection. The integration of this model with a live webcam stream and a simple web interface provides an effective solution to a growing problem in digital education ensuring academic integrity without manual supervision.

While earlier models like DenseNet121 and YOLOv5 showed promising results, YOLOv11 outperformed them in precision, recall, and consistency. This confirms that advanced object detection frameworks are more suitable for dynamic, real-world exam scenarios. The proposed system is scalable, adaptable, and ready for practical deployment in educational institutions. In the future, this framework could be further enhanced with multimodal data sources like audio input and behavioral profiling for even more accurate monitoring.

REFERENCES

[1] A. Gupta and A. Bhat, ''Bluetooth camera based online examination system with deep learning,'' in Proc. 6th Int. Conf. Intell. Comput. Control Syst. (ICICCS), May 2022, pp. 1477–1480, doi: 10.1109/ICICCS53718.2022.9788147.

[2] M. M. Masud, K. Hayawi, S. S. Mathew, T. Michael, and M. E. Barachi, ''Smart online exam proctoring assist for cheating detection,'' Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 13087. Cham, Switzerland: Springer, 2022, pp. 118–132, doi: 10.1007/978-3-030-95405- 5_9.

[3] 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. Mobile Technol. (iJIM), vol. 16, no. 08, pp. 124–137, Apr. 2022, doi: 10.3991/ijim.v16i08.30157.

[4] R. M. Alairaji, I. A. Aljazaery, and H. S. Alrikabi, ''Abnormal behavior detection of students in the examination Hall from surveillance videos,'' in Advanced Computational Paradigms and Hybrid Intelligent Computing. Singapore: Springer, 2022, pp. 113–125, doi: 10.1007/978-981-16-4369- 9_12.

[5] A. A. Malik, M. Hassan, M. Rizwan, I. Mushtaque, T. A. Lak, and M. Hussain, ''Impact of academic cheating and perceived online learning effectiveness on academic performance

during the COVID-19 pandemic among Pakistani students,'' Frontiers Psychol., vol. 14, Mar. 2023, Art. no. 1124095.

[6] D. L. McCabe, ''Cheating among college and university students: A north American perspective,'' Int. J. Educ. Integrity, vol. 1, no. 1, Nov. 2005, doi: 10.21913/ijei.v1i1.14.

[7] S. A. Butt, ''Analysis of unfair means cases in computer-based examination systems,'' Pacific Sci. Rev. B, Humanities Social Sci., vol. 2, no. 2, pp. 75–79, Jul. 2016.

[8] M. Ramzan and A. Abid, Automatic Unusual Activities Recognition Using Deep Learning in Academia. Accessed: Jun. 20, 2022.[Online]. Available: https://www.academia.edu/download/74918847/pdf.pdf

[9] T. S. Kumar and G. Narmatha, ''Video analysis for malpractice detection in classroom examination,'' in Proc. Int. Conf. Soft Comput. Syst., in Advances in Intelligent Systems and Computing, vol. 397, 2016, pp. 135–146, doi: 10.1007/978-81-322-2671-0_13.

[10] [Z. Li, Z. Zhu, and T. Yang, ''A multi-index examination cheating detection method based on neural network,'' in Proc. IEEE 31st Int. Conf. Tools Artif. Intell. (ICTAI), Nov. 2019, pp. 575–581.

[11] N. Malhotra, R. Suri, P. Verma, and R. Kumar, ''Smart artificial intelligence based online proctoring system,'' in Proc. IEEE Delhi Sect. Conf. (DELCON), Feb. 2022, pp. 1–5, doi: 10.1109/DELCON54057.2022.9753313.

[12] D. Komosny and S. U. Rehman, ''A method for cheating indication in unproctored on-line exams,'' Sensors, vol. 22, no. 2, p. 654, Jan. 2022, doi: 10.3390/s22020654.

[13] A. Singh and S. Das, ''A cheating detection system in online examinations based on the analysis of eye-gaze and head-pose,'' in Proc. Int. Conf. Emerg. Trends Artif.Intell. Smart Syst., Jun. 2022, doi: 10.4108/EAI.16-4-2022.2318165.

[14] L. C. OwTiong and H. J. Lee, ''E-cheating prevention measures: Detection of cheating at online examinations using deep learning approach—A case study,'' 2021, arXiv:2101.09841.

[15] G. Kasliwal, ''Cheating detection in online examinations,'' Master's Projects, San José State Univ., San Jose, CA, USA, Tech. Rep., 2015, doi: 10.31979/etd.y292-cddh.

[16] D. Dobrovska, ''Technical student electronic cheating on examination,'' in Proc. Int. Conf. Interact. Collaborative Learn., in Advances in Intelligent Systems and Computing, vol. 544, 2017, pp. 525–531, doi: 10.1007/978- 3-319-50337-0_49.

[17] S. Hu, X. Jia, and Y. Fu, ''Research on abnormal behavior detection of online examination based on image information,'' in Proc. 10th Int. Conf. Intell. Hum.-Mach. Syst. Cybern. (IHMSC), vol. 2, Aug. 2018, pp. 88–91, doi: 10.1109/IHMSC.2018.10127.

[18] A. Fayyoumi and A. Zarrad, ''Novel solution based on face recognition to address identity theft and cheating in online examination systems,'' Adv. Internet Things, vol. 4, no. 2, pp. 5–12, 2014, doi: 10.4236/AIT.2014.42002.

[19] E. Bilen and A. Matros, ''Online cheating amid COVID-19,'' J. Econ. Behav. Org., vol. 182, pp. 196–211, Feb. 2021, doi: 10.1016/j.jebo. 2020.12.004.

[20] R. Comas-Forgas, T. Lancaster, A. Calvo-Sastre, and J. Sureda-Negre, ''Exam cheating and academic integrity breaches during the COVID-19 pandemic: An analysis of internet search activity in Spain,'' Heliyon, vol. 7,