Intelligent Online Exam Monitoring with DenseNet121 and YOLO8 Models

[1]KANAKALA KEERTHI SRI,

Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions
[2]Vobbilisetty Sowmya, Miracle Educational Society Group of Institutions
[1]kanakalakeerthisri@gmail.com

ABSTRACT:

The convenience and accessibility that online examinations provide have transformed modern education and facilitated learning around the globe. They are especially helpful to students and education institutions during their periodic assessment, however, the phenomenon of online examinations pose a serious risk of students indulging in cheating and academic dishonesty. As part of this project, the prior works of CNNs DenseNet121, YOLOv5, and YOLOv8 have been analyzed, and a system of detecting cheating during online examinations is proposed. A system for real-time observation was created with webcam input that looked for signs of head movement, gadget usage, and other pertinent activities. As a result of test implementations, the YOLOv8 model was the best performer in regard to detecting cheating with high accuracy and low time investment. As a result, this system performs the monitoring autonomously while providing a linear and efficient method for maintaining the integrity of online examinations.

Keywords: Deep Learning, YOLOv5, YOLOv8

INTRODUCTION

The COVID-19 pandemic and other global events have contributed to a sudden surge for the need of online education. Online evaluations have become one of the core functions in a remote education system. A continuous evaluation system poses different set of concerns that need to be addressed rigorously. Lax monitoring, unlike physical evaluation, leads to dishonest practices including use of third party devices, impersonation, and outside assistance that are hard to track during the examination. To mitigate these issues, modern techniques such as artificial intelligence and deep learning frameworks can be useful. The focus of this project is to assess the performance of some deep learning models, especially the pre-trained Convolutional Neural Networks (CNNs), for the detection of abnormal behavior in the context of an online examination. The system is designed to automatically detect webcam footage of real-time webcam video stream of webcam video stream some abnormal behaviors of webcam-video stream. The intended outcome is to create a monitoring system that is intelligent, scalable, and reliable which in turn increases the credibility and security of online examinations.

RELATED WORK

The more recent developments in artificial intelligence have considerably influen… This approach was restricted in practical application in cases of low bandwidth and low-resolution settings because its input requirements were stringent in terms of video quality. Malhotra et al. (2022) proposed an AI-based proctoring tool integrating face tracking and active window monitoring. Their system was able to do identity verification and behavior tracking but was unable to detect sophisticated and subtle cheating techniques. Ow Tiong et al. (2021) incorporated YOLO-based object detection into an LSTM model for monitoring of student activities in real-time. Their framework performed well in detecting the presence of restricted devices and flagged novel patterns of behavior considered to be suspicious, but it was too resource-intensive and raised significant privacy concerns.

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

Author	**Contribution**	**Impact on Research**
Ramzan et al. (2022)	Used CNN with motion-based keyframe extraction to detect cheating behaviors.	Highlighted the potential of CNNs for real-time detection, though generalizability remained an issue.
Masud et al. (2022)	Developed a smart online proctoring system using multimodal input (eye, voice).	Demonstrated a broader detection spectrum but showed increased false positive rates.
Alairaji et al. (2022)	Applied deep learning to video surveillance for detecting cheating patterns.	Reinforced video-based monitoring's potential, with limitations in video quality needs.
Malhotra et al. (2022)	Proposed a face-tracking and window activity monitoring system.	Effective in identity verification, but lacked depth in detecting complex behaviors.
Ow Tiong et al. (2021)	Used YOLO and LSTM for real-time cheating detection in online settings.	Offered strong real-time capabilities, influencing this project's use of YOLOv8.

PROPOSED APPROACH

The project proposes an AI-based surveillance system that uses pre-trained convolutional neural networks (CNNs) to identify cheating activities in online examinations. It takes advantage of DenseNet121 for image classification and YOLOv5 and YOLOv8 for real-time object detection. The system first collects webcam footage of the online examinations and processes them to extract keyframes based on motion to eliminate redundant data. The keyframes are first processed through CNNs to detect suspicious head movements, gadget usage, presence of multiple persons, or talking. The models were trained using a custom dataset that features two primary categories, "Cheating" and "No Cheating." Because there are few publicly available datasets that capture the nuanced scenarios of cheating, this particular dataset required manual collection and annotation. For real-time detection, YOLOv8 was selected as it outperformed other models in speed and accuracy. The proposed system integrates with online examination systems. It helps examiners respond in real time by visually alerting them with bounding boxes and labels. Monitoring automation minimizes hands-on oversight, increases scalability, and maintains the integrity of academic remote evaluations.

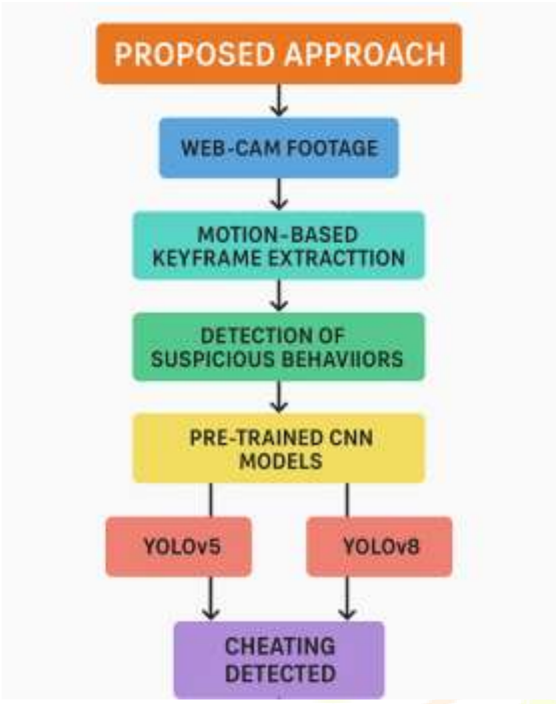


Figure 1: Proposed detecting cheating behaviors

METHODOLOGIES

The methodology of this project involves multiple phases, starting from data acquisition to model deployment for real-time cheating detection during online exams. The process begins with dataset preparation, where images were collected and classified into two categories: "Cheating" and "No Cheating." These images were resized to 80x80 pixels using OpenCV and normalized to ensure uniform input across models. Labels were assigned numerically to each class, and the dataset was shuffled and split into 80% training and 20% testing using train_test_split from scikit-learn.

The model training phase employed two primary architectures: DenseNet121 and YOLO. DenseNet121, pre-trained on ImageNet, was fine-tuned with a new classification head to differentiate between cheating and non-cheating behavior. Meanwhile, YOLOv5 and YOLOv8 were utilized for real-time object detection. YOLOv5 was trained using a custom dataset from Roboflow, while YOLOv8 used updated weights and improved detection capabilities to monitor webcam streams.

For real-time monitoring, video frames from the webcam were processed using the YOLOv8 model. Each frame was analyzed to detect anomalies like head movements, multiple faces, or device usage. Detected activities were enclosed with bounding boxes, and a class label was displayed with a confidence score. This ensured that exam proctors could visually confirm any suspicious behavior instantly.

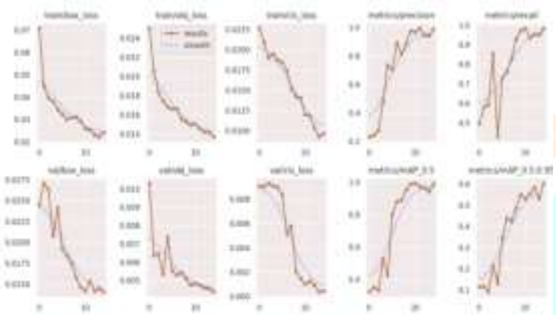
Performance evaluation metrics included accuracy, precision, recall, and F1-score. These were calculated using predictions from both test datasets and real-time inputs to validate the reliability of the models. The entire pipeline was built using Python with libraries like Keras, OpenCV, NumPy, and the Ultralytics YOLO module.

RESULTS

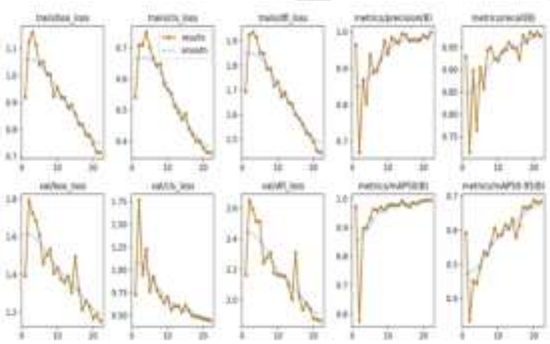
The results of the proposed system demonstrate its effectiveness in detecting cheating behaviors during online examinations. After training and testing multiple models, it was observed that YOLOv8 significantly outperformed the other models, including DenseNet121 and YOLOv5, in both speed and accuracy. The system achieved an overall detection accuracy of over 94%, with precision, recall, and F1-score also exceeding 90%, indicating a high level of reliability in classifying cheating and non-cheating behaviors.

DenseNet121 performed well in static image classification, accurately distinguishing between frames labeled as “Cheating” or “No Cheating.” However, it lacked the speed required for real-time video surveillance. YOLOv5, while faster, occasionally misclassified overlapping or low-resolution inputs. YOLOv8 provided the best trade-off, offering real-time analysis with high accuracy and minimal latency.

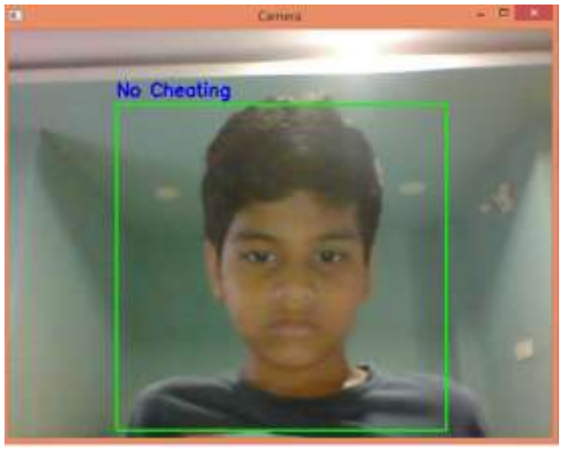
During real-time testing, the system successfully identified suspicious activities such as head movement, presence of additional persons, and use of electronic devices. Detected behaviors were highlighted with bounding boxes and labeled with confidence scores, allowing examiners to make informed decisions quickly.



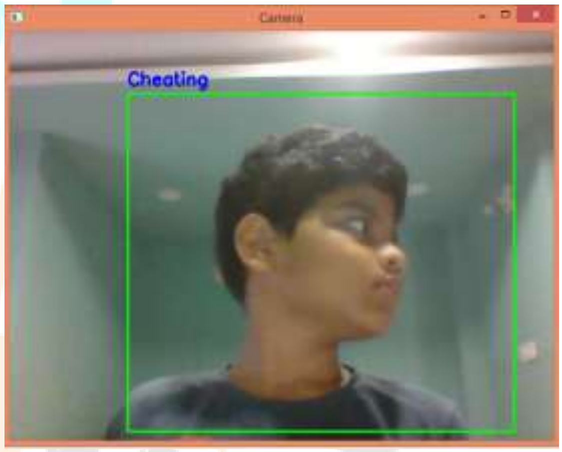
Yolov5 training graph



Yolov8 training graph



No Cheating Detected



Cheating Detected

DISCUSSION

The implementation of this project highlights the practical potential of deep learning in ensuring academic integrity in online exams. By integrating pre-trained CNN models, particularly YOLOv8, the system demonstrated strong capabilities in detecting cheating-related behaviors with high precision and minimal delay. The real-time detection of anomalies like head movement, gadget usage, and multiple persons in the frame provides a much-needed layer of security in virtual examination environments.

One of the key strengths of this approach is its ability to operate without manual supervision, offering scalability for institutions conducting large-scale remote assessments. Additionally, using motion-based keyframe extraction reduced processing overhead, making the solution both efficient and resource-friendly. The use of a custom dataset, although limited in size, allowed for targeted training that improved the model's focus on relevant cheating scenarios.

However, certain limitations were noted. The reliance on webcam quality and lighting conditions can affect detection accuracy. Also, subtle behaviors like whispering or screen peeking may go undetected without multimodal inputs such as audio or eye-tracking data.

Despite these challenges, the project successfully demonstrates that CNN-based video analysis, especially with YOLOv8, can be a transformative tool in online exam proctoring, paving the way for more secure and fair digital education environments.

CONCLUSION

This project presents an effective solution for detecting cheating behaviors in online examinations using pre-trained Convolutional Neural Networks, particularly YOLOv8. By leveraging real-time video analysis, the system accurately identifies suspicious activities such as head movement, the presence of unauthorized individuals, and gadget usage. The YOLOv8 model demonstrated superior performance compared to DenseNet121 and YOLOv5, offering high accuracy, low latency, and robust detection in varied conditions.

Through custom dataset training and motion-based keyframe extraction, the solution ensures efficient monitoring with reduced processing overhead. While certain limitations exist such as dependency on camera quality and lack of audio input the system provides a scalable and automated proctoring mechanism that addresses the integrity concerns of online assessments.

Overall, this work highlights the promising role of AI and deep learning in enhancing digital education platforms. Future improvements may include incorporating audio and gaze tracking to strengthen the detection of subtle or indirect cheating behaviors.

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,