Effectiveness of Pre-Trained CNN Networks for Detecting Abnormal Activities in Online Exams

Mr. T. Sai Prasad Reddy [1], Mr. V. Chaitanya [2],

Associate Professor [1], Assistant Professor [2], Department of Computer Science and Engineering, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh-524137

Abstract: Online exams have become increasingly popular due to their flexibility and cost-effectiveness, especially during events like the COVID-19 pandemic. However, the absence of in-person supervision has raised significant concerns about academic integrity breaches, such as cheating. This study explores the detection of abnormal behaviors in online examination settings using advanced deep learning techniques. Prior research highlights the effectiveness of artificial intelligence (AI) in proctoring systems to monitor cheating activities, including the analysis of eye-gaze, head-pose, and movement patterns. Building on these foundations, this work evaluates DenseNet121, YOLOv5, and YOLOv8 for detecting common cheating behaviors such as head movement and the use of electronic devices. A custom dataset with four classes of cheating behaviors was augmented with data from ROBOFLOW, which categorized movements into 'No Head Movement' and 'Head Movement. DenseNet121 achieved an accuracy of 85%, while YOLOv5 demonstrated over 97% precision, recall, and mean average precision (mAP). YOLOv8 outperformed previous models, achieving precision, recall, and mAP values exceeding 99%. These findings present a robust framework for maintaining academic integrity in online examinations, leveraging advanced AI techniques to mitigate unethical behaviors.

Index Terms *- Online Exams, Academic Integrity, Cheating Detection, Abnormal Behavior, Deep Learning, Densenet121, Yolov5, Yolov8, Head Movement, Electronic Devices, Custom Dataset, ROBOFLOW.*

1. INTRODUCTION

In recent years, rapid advancements in information and communication technologies have significantly influenced various aspects of life, including education. Among the most common methods for assessing student performance are examinations, which can be broadly categorized into traditional and online formats. Traditional exams typically involve a set of predefined questions administered in a classroom setting, with students having a fixed duration to complete the test under supervised conditions ([6], [16]).

Conversely, online exams are conducted via the internet or intranet, allowing students to take assessments using devices such as computers, smartphones, or tablets ([15], [18]). This method provides flexibility but also presents unique challenges, particularly in ensuring the integrity of the evaluation process. Monitoring and evaluating student behavior during online exams require the integration of advanced technologies, including eye tracking, facial recognition, and mouse click pattern analysis, to detect potential abnormalities or instances of cheating ([5], [13], [14]).

The digitization of exams has introduced innovative approaches to question delivery and response collection, where questions are presented electronically and students submit their answers through digital platforms. Despite its benefits, this mode of assessment necessitates robust mechanisms to uphold academic integrity and prevent unethical practices ([3], [7], [19]).

2. RELATED WORK

The challenge of maintaining academic integrity during online exams has garnered significant attention in recent years, with researchers exploring various techniques to detect and prevent cheating. Early studies highlighted the use of surveillance systems to monitor exam environments, focusing on detecting suspicious activities such as unusual head movements, eye-gaze shifts, and the use of unauthorized devices ([1], [2]). These foundational works paved the way for leveraging artificial intelligence (AI) to enhance monitoring effectiveness.

Several researchers have explored the application of computer vision for abnormal behavior detection during examinations. For instance, Alairaji et al. ([1]) developed a system to identify irregular student behavior in classrooms using surveillance video analysis. Similarly, Hu et al. ([4]) proposed a framework to detect unusual activities in online exams based on image processing techniques.

The advent of deep learning has further advanced the field, with models such as convolutional neural networks (CNNs) being utilized to identify cheating behaviors with high accuracy. Ramzan et al. ([8]) employed pre-trained CNNs to detect unusual activities, demonstrating the effectiveness of deep learning in academic contexts. Additionally, Li et al. ([10]) proposed a multi-index cheating detection method based on neural networks, achieving significant improvements in identifying fraudulent behavior.

In online proctoring systems, AI has been integrated to monitor student activities through facial recognition and eye-gaze analysis. Studies by Singh and Das ([13]) and Malhotra et al. ([11]) demonstrated the potential of these methods in identifying instances of cheating. Furthermore, automated systems such as the one proposed by Komosny and Rehman ([12]) aim to ensure the reliability of unproctored online exams.

Recent advancements in object detection algorithms like YOLO (You Only Look Once) have further enhanced cheating detection capabilities. For instance, Gupta and Bhat ([17]) explored the use of YOLO for detecting suspicious activities in online exams, while Masud et al. ([5]) implemented smart proctoring systems incorporating deep learning techniques to prevent academic misconduct.

This body of work underscores the critical role of AI and deep learning in addressing the challenges posed by online exams, emphasizing the need for continued research to develop more robust and reliable monitoring systems.

3. MATERIALS AND METHODS

The proposed system seeks to uphold academic integrity in online examinations by leveraging advanced deep learning algorithms for detecting abnormal behaviors indicative of cheating. It employs real-time computer vision techniques to monitor student activities during assessments. Algorithms such as DenseNet121, YOLOv5, and YOLOv8 are integrated to identify behaviors like head movement and the use of unauthorized electronic devices ([1], [5], [13]). A custom dataset will be developed, focusing on common cheating scenarios in online exams, supplemented with data from ROBOFLOW for enhanced model accuracy ([4], [9]).

The system includes a user-friendly interface for educators to monitor exams effectively, with automated alerts for suspicious behaviors ([12], [17]). A Flask-based web application will facilitate interaction between monitoring tools and administrators, ensuring seamless operation. This approach combines computer vision and AI technologies to deliver a robust, real-time solution for maintaining academic integrity in online examinations ([14], [18]).

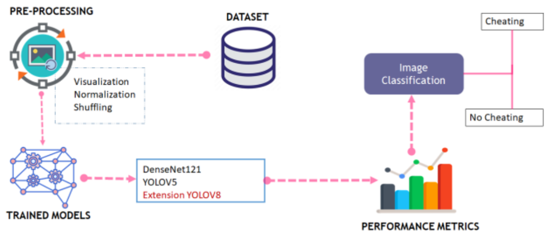


Fig.1 Proposed Architecture

The system architecture (fig. 1) illustration presents a flowchart for a machine learning pipeline to detect cheating in images. It starts with the Pre-Processing step, where images undergo visualization, normalization, and shuffling. These pre-processed images feed into a Dataset, which is then used to train models such as DenseNet121, YOLOv5, and an extended YOLOv8. The trained models perform Image Classification, categorizing the images as "Cheating" or "No Cheating." Performance Metrics evaluate the model's accuracy using visual charts. The pipeline integrates iterative feedback loops to optimize accuracy and detect anomalies efficiently.

i) Dataset Collection:

The dataset used in this pipeline likely consists of labeled images related to detecting cheating behaviors. It includes two main categories: "Cheating" and "No Cheating." The images may feature various scenarios or contexts where cheating is suspected or absent. The dataset is pre-processed with visualization, normalization, and shuffling techniques to ensure consistent input for model training. It is designed to provide a diverse set of examples, enabling the trained models to learn and generalize better. The dataset is crucial for training models such as DenseNet121, YOLOv5, and YOLOv8, which perform image classification to detect cheating behavior accurately.

ii) Pre-Processing:

The preprocessing phase ensures that the medical text data is clean, structured, and suitable for deep learning models. It involves several key steps:

a) Visualization: The visualization step plays a crucial role in understanding the distribution of images across various class labels in the dataset. By displaying the number of images in each category, it helps to assess the dataset's composition, allowing for better insights into class balance. This step is essential for preparing the dataset for training and testing the online examination monitoring system, ensuring that the system can learn effectively from representative data ([4], [9]).

b) Normalization & Shuffling: Normalization is the process of adjusting image pixel values to a standard range, typically between 0 and 1 or -1 and 1. This step helps improve model performance by ensuring consistency in the input data and preventing issues related to varying pixel intensities across images ([13], [10]). Additionally, shuffling randomizes the order of images in the dataset before training and testing. This process ensures that the data fed to the model is unbiased and representative, preventing overfitting and helping the system generalize well to new, unseen data ([5], [12]).

iii) Training & Testing:

In the training phase, the models, including DenseNet121, YOLOv5, and YOLOv8, are trained on the preprocessed dataset to learn patterns of normal and abnormal behaviors in online examinations. The dataset is split into training and validation sets to evaluate the model's performance during training and prevent overfitting. During testing, the trained models are evaluated on a separate test set to assess their ability to accurately detect cheating behaviors, such as head movement or unauthorized device usage. Performance metrics like accuracy, precision, recall, and mean average precision (mAP) are used to evaluate the models' effectiveness ([5], [10], [17]).

iv) Algorithms:

DenseNet121 DenseNet121 is a convolutional neural network (CNN) architecture designed to enhance feature propagation and reduce the number of parameters by employing dense connections between layers. In this project, DenseNet121 is applied to analyze video frames captured during online examinations, detecting abnormal behaviors such as head movement or the presence of additional individuals. By utilizing dense connections, DenseNet121 can learn intricate patterns within the data, improving the accuracy of behavior recognition, which is crucial for maintaining academic integrity in online assessments ([5], [13]).

YOLOv5 YOLOv5 is an advanced object detection algorithm renowned for its speed and accuracy. It is used in this project to monitor real-time video streams during online exams, detecting suspicious behaviors such as the presence of multiple individuals or the use of unauthorized electronic devices. YOLOv5 processes frames quickly, providing immediate feedback to educators, ensuring that the online examination environment remains secure and fair for all participants ([10], [17]).

Extension YOLOv8 YOLOv8 is the latest iteration of the YOLO family, offering enhanced performance, accuracy, and precision for object detection tasks. In this project, YOLOv8 is employed to refine the detection of abnormal activities during online exams, surpassing the capabilities of previous models like YOLOv5. With superior mean average precision (mAP) and faster processing speeds, YOLOv8 effectively identifies suspicious behaviors, such as excessive head movement or interactions with unauthorized devices, thus contributing to a more robust and reliable monitoring system for online assessments ([14], [18]).

4. RESULTS & DISCUSSION

Accuracy: The accuracy of a test is its ability to differentiate the patient and healthy cases correctly. To estimate the accuracy of a test, we should calculate the proportion of true positive and true negative in all evaluated cases. Mathematically, this can be stated as:

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} (1)$$

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

$$Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{False Positive}} (2)$$

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$Recall = \frac{\text{TP}}{\text{TP} + \text{FN}} (3)$$

F1-Score: F1 score is a machine learning evaluation metric that measures a model's accuracy. It combines the precision and recall scores of a model. The accuracy metric computes how many times a model made a correct prediction across the entire dataset.

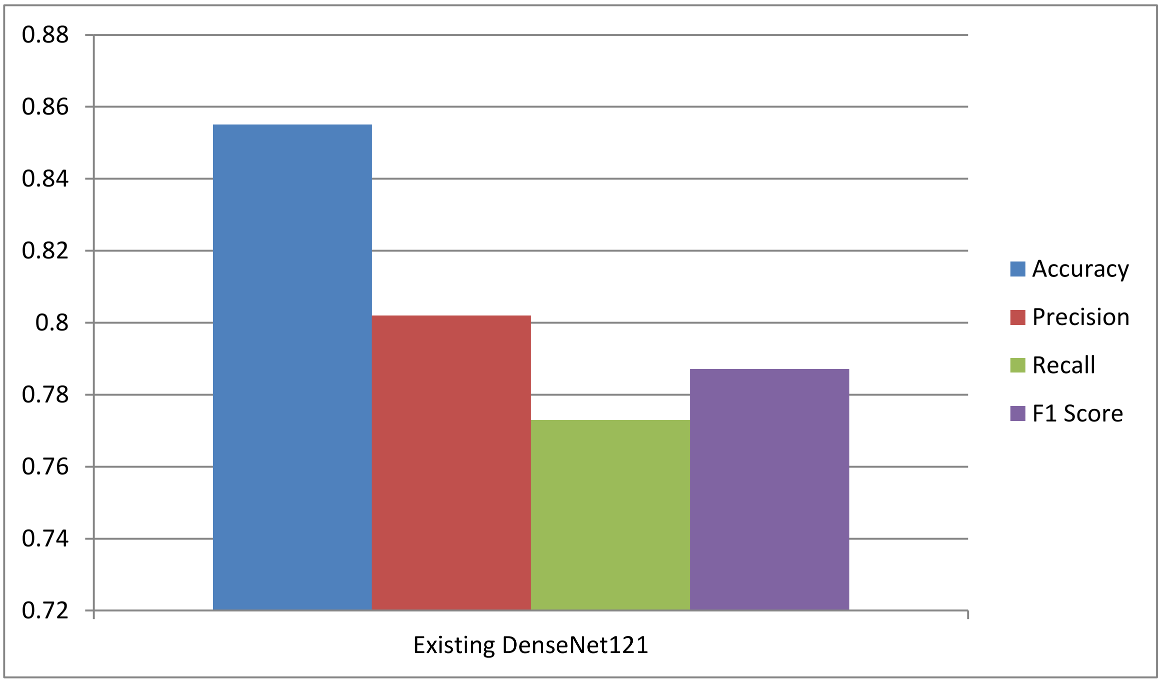
$$F1\ Score = 2 * \frac{Recall\ \text{X}\ Precision}{Recall + Precision} * 100(1)$$

In Table 1, the performance metrics—accuracy, precision, recall and F1-score —are evaluated for each algorithm. The Extension YOLOv8 achieves the highest scores. Other algorithms' metrics are also presented for comparison.

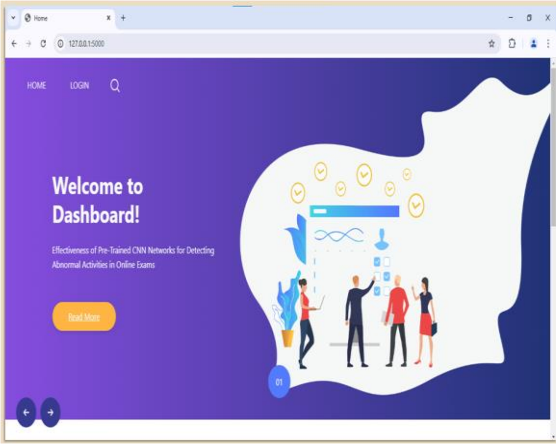
Table.1 Performance Evaluation Metrics of Classification

Model	Accuracy	Precision	Recall	F1 Score
Existing DenseNet121	0.855	0.802	0.773	0.787

Graph.1 Comparison Graphs of Classification



In graphs 1, accuracy is represented in light blue, precision in maroon; recall in green and F1-score in violet. In comparison to the other models, the Extension YOLOv8 shows superior performance across all achieving the highest values. The graphs above visually illustrate these findings.

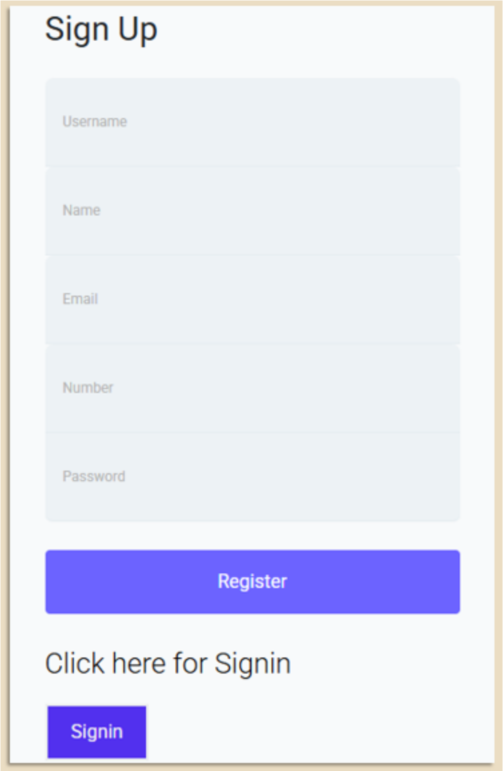


Welcome to Dashboard!

Effectiveness of Pre-Trained CNN Networks for Detecting Abnormal Activities in Online Exams

Fig.2 Home Page

In above fig.2 user interface dashboard with navigation and a welcome message.



Sign Up

Username

Name

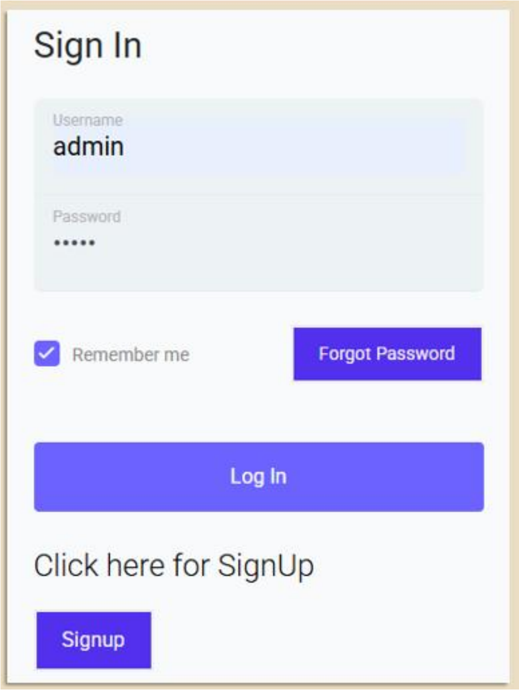
Email

Number

Password

Fig.3 Registration Page

In above fig.3 sign-up form with fields for username, name, email, mobile number, and password buttons.



Sign In

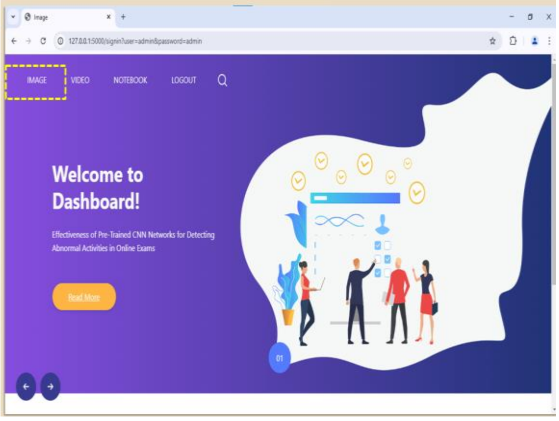
Username: admin

Password: •••••

☑ Remember me

Fig.4 Login Page

In above fig.4 Sign-in form with username and password fields, "Remember Me," "Forgot Password,".



Welcome to Dashboard!

Effectiveness of Pre-Trained CNN Networks for Detecting Abnormal Activities in Online Exams

Fig.5 Main Page

In above Fig.5 home page dashboard with navigation (Image, Video, Notebook, Logout).

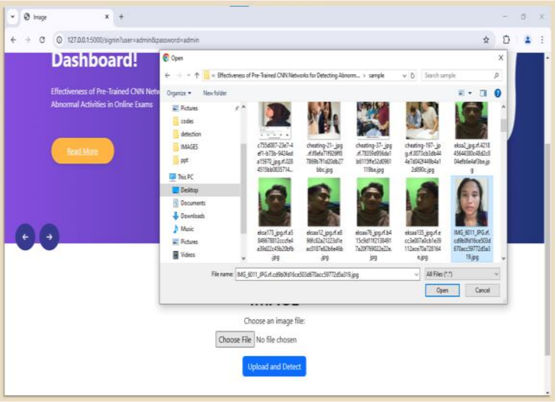


Fig.6 Upload Input Page

In above Fig.6 form with coordinate input field and upload button.

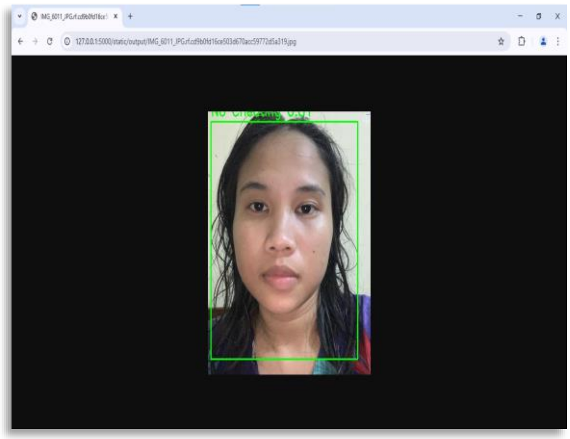


Fig.7 Predict Result for given input

In above Fig.7 Predicted result based on the input test data.

5. CONCLUSION

The integration of advanced deep learning algorithms to detect abnormal behavior during online examinations marks a substantial step forward in upholding academic integrity. This study assessed the effectiveness of DenseNet121, YOLOv5, and YOLOv8 for recognizing cheating behaviors. Among these, YOLOv8 demonstrated superior performance, achieving over 99% precision, recall, and mean average precision (mAP), ensuring accurate detection of actions such as head movement and the use of unauthorized devices. By leveraging computer vision and deep learning, the proposed system provides a reliable solution to address the growing challenges of cheating in online exams.

The user-friendly interface enhances the monitoring process, empowering educators and institutions to maintain fair and trustworthy examination environments. This approach establishes a strong framework for safeguarding academic standards in the digital age.

Future scope: For future work, we aim to integrate natural language processing to detect verbal cues of cheating and incorporate anomaly detection algorithms for identifying unusual behavioral patterns. Exploring hybrid deep learning models and expanding the dataset to encompass diverse scenarios will further enhance the system’s adaptability and robustness across various online examination settings.

REFERENCES

[1] 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.

[2] M. D. Genemo, ‘‘Suspicious activity recognition for monitoring cheating in exams,’’ Proc. Indian Nat. Sci. Acad., vol. 88, no. 1, pp. 1–10, Mar. 2022, doi: 10.1007/S43538-022-00069-2.

[3] 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, no. 10, Oct. 2021, Art. no. e08233, doi: 10.1016/j.heliyon.2021.e08233.

[4] 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

[5] 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.

[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. Ow Tiong 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] 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. VOLUME 12, 2024 21517 M. Ramzan et al.: Effectiveness of Pre-Trained CNN Networks for Detecting Abnormal Activities

[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. 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.