International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Review: Using Video Surveillance for Cheating Detection in Exam Hall

Snehajeet Jamankar[1], Harsh Sokiya[2], Minal Sonkar[3]

[1,2,3]Department of Computer Engineering, KJ Somaiya Institute of Technology, Mumbai, India - 400022

Abstract

This review delves into the assessment of video surveillance technology's role in detecting cheating within the context of examination halls. In light of the escalating concerns surrounding academic dishonesty, educational institutions are progressively turning to advanced technological measures to uphold the integrity of their examination procedures. Video surveillance has emerged as a promising tool in this domain, offering a non-intrusive means of monitoring examinees during tests. This critical analysis assesses the effectiveness, advantages, and potential limitations of deploying video surveillance for the purpose of detecting cheating, shedding light on the ramifications for educational institutions and their students. Furthermore, it delves into the ethical and privacy issues associated with this technology and suggests possible avenues for addressing them. By presenting an overview of the current landscape of video surveillance in examination settings, this review intends to provide valuable insights for educators, administrators, and policymakers aiming to fortify the credibility of their assessment procedures.

Keywords: Object detection, Cheating in exam hall, YOLO, OpenCV, Tensorflow.

INTRODUCTION

Academic integrity is a cornerstone of the education system, fundamental to ensuring that the assessments accurately reflect a student's knowledge and abilities. However, the persistent challenge of cheating in exam halls has prompted educational institutions to explore innovative solutions to uphold this integrity. Numerous educational establishments reported an increase in the prevalence of exam cheating. A McCabe investigation in 2020 was done at over 24 High Schools across United States, which was conduction on 70,000 students; resulting in students admitting to cheating on a test (64% students), admitted to plagiarism (58% students) and 95% of students claimed to have participated in either some sort of cheating on examination or copying of homework.[6] Exam results that are impartial are produced via cheating, are giving the honest student an undeserved disadvantage. The insincere student facilitates cheating in order to achieve an advantage and receives an unfair edge in the test, upsetting the honest learners. Although there are currently many established strategies in place to prevent cheating, they aren't as effective as the constantly emerging new approaches. Many novel approaches for preventing cheating are emerging as a result of this.

One such solution gaining traction is the application of video surveillance technology for cheating detection during examinations. This review delves into the world of video surveillance in exam halls, aiming to provide a comprehensive understanding of its efficacy, advantages, disadvantages, and the ethical and privacy considerations that surround its implementation. An accurate activity forecast can assist the examiner in addressing students' inappropriate behavior during the test. Furthermore, it restricts

the invigilators' biases during corrective measurement.[1] Reliable video surveillance systems that work by detecting anomalies. These techniques have shown to be effective in identifying suspicious or anomalous activity in recent times.[3]

LITERATURE SURVEY

Inspection Cheating detection is a challenging issue with several proposed approaches, all of which have positive and negative aspects. Video surveillance has been proposed as a way to deter and detect cheating in exam halls. This literature survey reviews the benefits and limitations of using video surveillance for cheating detection, as well as the latest research in this area. A comprehensive analysis of the available cheating detection techniques lists a few of these approaches.

1. CNNs(Convolutional Neural Network) with LSTM Architecture:

Combination of Artificial Neural Networks such as Convolutional Neural Networks (CNNs) along with Long short-term memory(LSTM) networks together are thought to be a very reliable approach towards detecting cheating in examinations.. LSMT is one kind of recurrent neural network (RNN) architecture used for sequential data modeling. LSTM networks are valuable in many applications including speech recognition, natural language processing (NLP), and time series analysis, since they are very good at managing and retaining long-range relationships in data. When used in conjunction with Convolutional Neural Networks (CNN), LSTM networks can enhance the capabilities of the model for tasks that involve both spatial and sequential information.

LSTM can be used with CNN in a reference to image processing. In image captioning tasks, CNNs are used to extract features from images (e.g., object recognition and localization), while LSTMs are employed to generate descriptive captions for those images. The CNN encodes the spatial information within the image and produces a fixed-length feature vector.

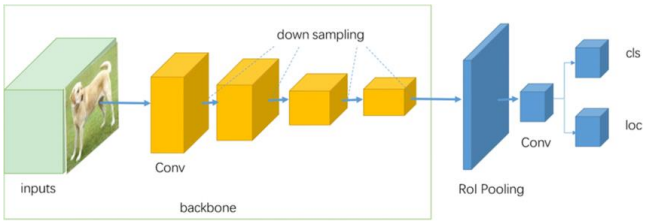

Figure 1. Generic architecture of single stage object detectors.

The LSTM network then receives this feature vector and produces a string of words to create a coherent and contextually relevant caption for the image.[7]

In [4] a Convolutional LSTM-based Residual Network which is known as CLRNet is introduced that is different from other networks. It works by accepting inputs of sequences of parallel images from videos. By capturing temporal information, this technique enables the identification of minute features. In order to identify suspicious events in real time, the study analyzes student behavior using computer vision algorithms that extract information from frames. After extraction, the video frames are classified as cheating or not using an LSTM model. The findings are sent to a supervisor so they may be used in the adjudication process, which establishes whether or not cheating occurred in the case.[6]

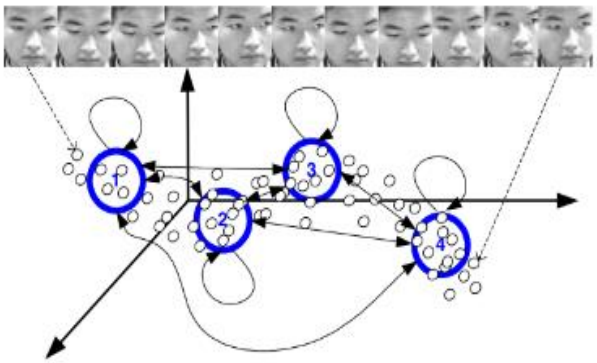

Figure 2. Face sequence modeling using Temporal HMM

2. Hidden Markov Models (HMMs):

Hidden Markov Model (HMM) are probabilistic models used in diverse fields in order to model sequential data. It comprises hidden states, which represent unobservable factors, and observable outputs, such as data or measurements, associated with those states. HMMs capture transitions between states through probabilities and determine the likelihood of observing specific outputs from each state. These models are essential for tasks involving uncertainty, temporal dependencies, and unobservable variables, making them invaluable in applications like speech recognition, bioinformatics, and natural language processing.In an educational setting, the HMM is used to identify cheating.[8] Considering a situation where an educational institution is worried about students cheating on their exams. The institution keeps an eye on student behavior during exams by using an HMM-based cheating detection system.The HMM in this instance may be in one of two hidden states: "Honest" or "Cheating." The observable data may consist of elements such as eye tracking data, suspicious item, head position, and shoulder movement.[9]

TABLE I- COMPARATIVE ANALYSIS TABLE

Sr. No	Title of the paper	Datasets used	Techniques used	Results	Limitations
1	Suspicious activity recognition for monitoring cheating in exams[1]	First dataset: CUI Exam; Second dataset: CIFAR-100.	1.Cubic SVM (CSVM) 2.Quantum Support Vector Machine (QSVM)	CSVM-92.99%, QSVM-83.22%	Usage of 3 cameras is required
2	Automated Cheating Detection in Exams using Posture and Emotion Analysis[2]	Created their own dataset	Alexnet to detect type of cheating Pytorch on Colab	96%	Only lateral view is being considered.
3	Automated Cheating Detection based on Video Surveillance in the Examination	Collection of face and non-face images	Viola-Jones Algorithm for face detection	able to detect cheating in hall	Viola-Jones Algorithm can be computationally expensive to

	Classes[3]			creating green and red label	train.
4	COVID-19: Automatic Social Distancing Rule Violation Detection using PP-Yolo & Tensorflow in OpenCV	CPID dataset and compared with their dataset	PP-Yolo is used along with Tensorflow for detection	KNN = 90 % Proposed: 97.6%	When a huge crowd is introduced with the system confusion may occur
5	An Intelligent Video Surveillance System using Edge Computing based Deep Learning Model[7]	Le2i dataset	CNN-LSMT Min-Max scaling, Edge node.	The average accuracy after multiple iterations is 90%.	The precision in a crowd is low
6	An Intelligent Anti-cheating Model in Education Exams[6]	A video collection of students in examination rooms.	1.Long Short-Term Memory (LSTM) 2.Convolution Neural Networks (CNN)	Accuracy: 75% F1 Score: 66.7%	OverFitting because of the small dataset. High computational time

PROPOSED SOLUTION

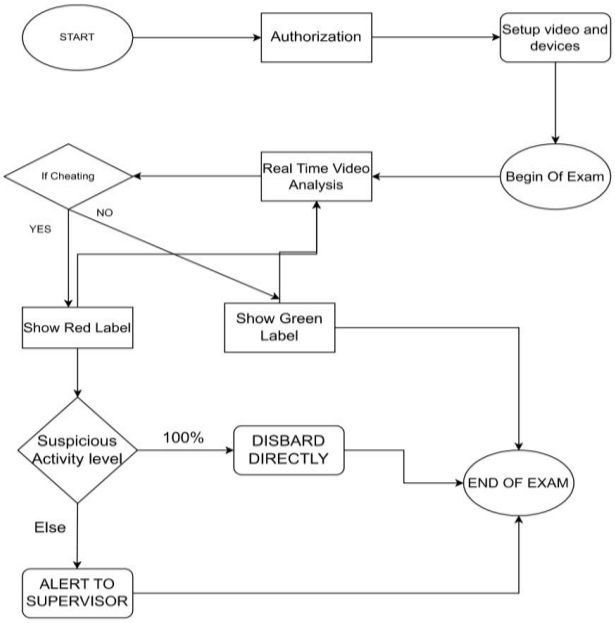

Figure 3. Workflow for proposed system

***D*atasets:** Datasets solely focused on exam cheating detection often involve sensitive and private information, and for ethical and privacy reasons, they are not readily accessible. So you need to create your own database involving a controlled group of individuals. The database needs to be divided into

normal behavior and suspicious behavior. The second division can further be classified as different suspicious behaviors such as, cheating from phone, using unethical devices, peeking into others' papers.

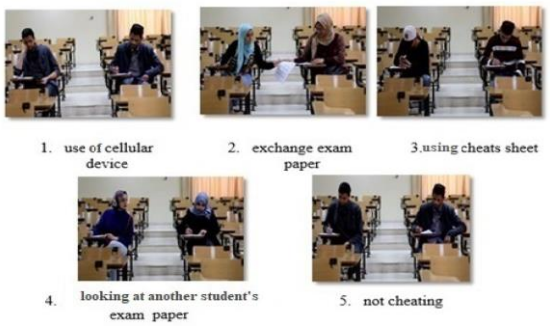

Figure 4. Workflow for proposed system

Preprocessing: The first step in the procedure is gathering video from the test hall's security cameras. Format conversion and compression are used to handle the frequently huge video files. Frame extraction makes it easier to go from a video to individual frames for finer-grained analysis, either at regular intervals or via frame differencing. Holistic model is used to extract points which are used as features. By lowering false positives, noise reduction techniques can improve the quality of the video. Individuals are identified and tracked over the frames using object detection and tracking, and the examination hall's defined areas of interest (ROIs) help to concentrate the study. The extraction of features from the frames—such as head movements, eye focus, and facial expressions—is essential for identifying instances of cheating. Relevant occurrences are labeled via data annotation, and data augmentation can broaden the variety of the dataset if necessary.

Training: In this step, after the model has been trained on one dataset, transfer learning is used to train it on further datasets with fewer samples. the dataset. Specifically, the model was trained using 108 videos consisting of 30 frames each. The training dataset is trained for 2000 epochs. Even in situations when there is a shortage of data, this approach makes use of the insights gleaned from one dataset to improve the model's performance on several additional datasets. LSTM and Densenet are used to train the model using TensorFlow.

Evaluation Metrics: For the evaluation of the model, a confusion matrix is used containing metrics like Precision, Recall, and Accuracy are considered. For input, the model used thirty frames. To give an impartial evaluation, we maintained the same percentage of real and fake photographs in the training and testing datasets. This helped to reduce the possibility of bias either from unbalanced data or from models having lower accuracy.

CONCLUSION

Video surveillance for cheating detection in exam halls represents a promising approach to maintain academic integrity. In the context of cheating detection, this review has looked at the essential elements and factors related to Hidden Markov Models (HMMs), providing a critical analysis of their possible uses. The proposed system used opencv for object detection and Holistic model to extract features. It achieved a High accuracy of 97.22 in cheating detection by CNN using LSTM architecture.

In the field of education, countermeasures and strategies for cheating must advance together with the methods themselves. Combining sophisticated modeling methods like CNN and HMM with video

surveillance provides a potent way to overcome this difficulty. However, it is still crucial to utilize this technology responsibly and ethically to preserve academic integrity without violating people's rights or privacy. Teachers, institutions, and legislators need to find a way to combine protecting test integrity with maintaining the principles of fairness and privacy in educational evaluation as new technologies develop.

REFERENCES

1. Genemo, M.D. Suspicious activity recognition for monitoring cheating in exams. Proc.Indian Natl. Sci. Acad. 88, 1–10 (2022). https://doi.org/10.1007/s43538-022-00069-2
2. J. Nishchal, S. Reddy and P. N. Navya, "Automated Cheating Detection in Exams using Posture and Emotion Analysis," 2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2020, pp. 1-6, doi: 10.1109/CONECCT50063.2020.9198691.
3. Al airaji, Roa'a M., Ibtisam A. Aljazaery, Haider Th.Salim Alrikabi, and Abdul Hadi M. Alaidi. "Automated Cheating Detection Based on Video Surveillance in the Examination Classes." International Journal of Interactive Mobile Technologies (IJIM) 16, no. 08 (n.d.): 124–37. doi:10.3991/IJIM.V16I08.30157.
4. Tariq, S., Lee, S. and Woo, S., A convolutional LSTM based residual network for deepfake video detection. arXiv 2020. arXiv preprint arXiv:2009.07480.
5. S. Verma and P. K. Jain, "COVID-19: Automatic Social Distancing Rule Violation Detection using PP-Yolo & Tensorflow in OpenCV," 2022 International Conference for Advancement in Technology (ICONAT), Goa, India, 2022, pp. 1-6, doi: 10.1109/ICONAT53423.2022.9725836.
6. S. Essahraui, M. A. El Mrabet, M. F. Bouami, K. E. Makkaoui and A. Faize, "An Intelligent Anti-cheating Model in Education Exams," 2022 5th International Conference on Advanced Communication Technologies and Networking (CommNet), Marrakech, Morocco, 2022, pp. 1-6, doi: 10.1109/CommNet56067.2022.9993953.
7. R. P. Singh, H. Srivastava, H. Gautam, R. Shukla and R. K. Dwivedi, "An Intelligent Video Surveillance System using Edge Computing based Deep Learning Model," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 439-444, doi: 10.1109/IDCIoT56793.2023.10053404.
8. Guogang, Gaozheng, Wushiqian and Yumin, "Using Hidden Markov Model to Predict the Potential Intent of User's Gaze Behavior," 2021 International Conference on Machine Learning and Intelligent Systems Engineering (MLISE), Chongqing, China, 2021, pp. 38-41, doi: 10.1109/MLISE54096.2021.00015.
9. Xiaoming Liu and Tsuhan Cheng, "Video-based face recognition using adaptive hidden Markov models," 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2003. Proceedings., Madison, WI, USA, 2003, pp. I-I, doi: 10.1109/CVPR.2003.1211373.