ISSN 2007-9737

Automated Academic Cheating Detection Using Video Surveillance and Circumstantial Action Recognition

Pratya Bhowmik, Smita Das*

National Institute of Technology Agartala,
Department of Computer Science & Engineering
India

{bhowmikpratya, smitadas.nita}@gmail.com

Abstract. Due to the aftermath of COVID-19 pandemic, educational institutions worldwide have transitioned from traditional offline teaching to online methods. Unfortunately, some students resort to unfair practices during online exams, compromising the integrity of the assessment process. In this paper, a cheating detection framework has been proposed which is specifically designed for online exams. The framework relies on eight types of Circumstantial Actions extracted from video sequences. Initially, a dataset consisting of image frames are generated from the captured video sequences. Thereafter, various feature extraction methods are employed on those images to generate the feature vectors. Finally, combination of K-Means Clustering in association with Support Vector Machines (SVM) is used to classify the data for identification of cheating in exam. Analysis of the experimental results indicate that the proposed method achieves a notably high level of accuracy in detecting cheating during exams.

Keywords. Cheating detection, circumstantial gesture recognition, computer vision, online examination, video surveillance.

1 Introduction

Cheating undermines the value of educational achievements and can lead to a general mistrust in the education system[2]. Preserving the honesty of examinations is paramount in ensuring an equitable and accurate evaluation of students' capabilities. In traditional exam setups, invigilators are pivotal in preventing cheating by monitoring behaviors like unauthorized material use, communication between students or electronic device usage. However, in the era of technological advancements, educational institutions are increasingly turning to sophisticated methods for enhanced cheating detection. One such method involves the adoption of online proctoring systems[1]. These systems can employ webcams and screen-sharing functionalities to closely observe students during online exams.

They not only record the entire exam session but also utilize artificial intelligence algorithms to promptly identify and flag any suspicious behaviors[22] in real-time, such as frequent eye movements or unusual interactions with the computer. Additionally, plagiarism detection software[7] has become an essential component of cheating detection. This software scans written responses for similarities to existing sources, both online and within institutional databases, pinpointing instances of copied or unauthorized content. This not only discourages plagiarism but also ensures the academic integrity of the assessment process. While technology can identify irregularities during exams, it remains a supportive instrument. Ultimately, human judgment is essential to uphold fairness, context, and ethical integrity.

1.1 Motivation

Despite of using all such precautions in exam system monitoring, due to COVID-19 pandemic, a sharp increment in cheating in online exam has been detected which is represented in figure 1. Cheating detection in exam system is very crucial to ensure that the academic skills and knowledge of students are assessed properly. Also, to maintain quality of education as well as reputation of educational institutes, prevention of cheating in exams

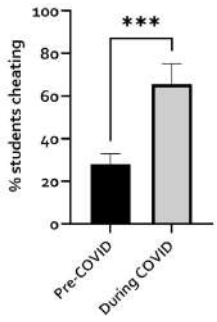

Fig. 1. Increased cheating rate due to Covid-19 Pandemic [17]

is essential. With the post-pandemic increment in online exam systems, new technologies supporting cheating have also emerged which necessitates sophisticated cheating detection frameworks. Finally, detection of cheating provides a fare amount of opportunity to all the students to qualify in the exam based on actual merit and not external help. Therefore, by detecting and preventing cheating in exam system, students can be motivated to engage more deeply with the basic concepts leading to better learning outcomes and a more meaningful educational experience.

1.2 Applications of Cheating Detection

Cheating detection is not only important for upholding standards in education but also plays a significant role in various sectors[3] where integrity and security are paramount. It helps maintain the integrity of academic assessments by identifying instances of cheating in both paper-based and paper-less exams. In professional contexts, cheating detection safeguards against fraudulent practices, maintaining the trust and reliability of various processes. For instance, in online gaming, anti-cheat systems promote fair play, contributing to a positive and competitive gaming environment. Apart from that, various machine learning techniques, for e.g. Long Short-Term Memory (LSTM) networks, are used to detect patterns of cheating behavior by analyzing student performance data which in turn is very important for behavioral analysis. Beyond education, similar techniques are used in various industries to detect fraudulent activities, like in credit card transactions or insurance claims. In video surveillance and security, cheating detection algorithms can identify unusual behavior that may indicate criminal activity.

1.3 Research Gaps and Possible Contributions

Analysis of detecting cheating during exams has primarily concentrated on technological approaches and identification mechanisms. Investigating the reasons behind cheating behaviors[12], exploring alternative assessment methods less susceptible to cheating and considering the ethical implications of detection technologies are areas requiring further exploration. Furthermore, with the surge in online learning, there's a demand for research on identifying cheating in online exams and tracking cheating behaviors across diverse educational environments. Therefore, following are some of the key contributions that our research offers:

— This paper introduces a cheating detection framework tailored for online examinations. The framework focuses on eight distinct Circumstantial Action Recognition techniques derived from video footage of online exams.

— The research consists of preparing a action recognition dataset of images, which serves as the foundation for analyzing and categorizing potential cheating behaviors captured on video. Subsequently, various feature extraction techniques have been applied to identify and extract pertinent features within this dataset.

— The culmination of this research is a comprehensive set of experiments that leverage these features to evaluate the efficacy of the cheating detection framework proposed herein.

In the rest of the paper, section 2 describes the recent literature accommodating various cheating detection methods followed by background of cheating detection in Section 3. Section 4 discusses dataset preparation and proposed method for feature extraction. Result analysis along with discussion is denoted in section 5. Finally, the paper is concluded with future direction of work in section 6.

2 Related Work

In this section, an overview of the recent literature related to cheating detection in exam system has been conducted.

2.1 Machine Learning and Deep Learning Based Approaches

In this category, a multi index examination cheating detection method based on neural network has been proposed in [13]. Authors have used the RAE algorithm and LSTM neural network to assess each student's mastery level of knowledge points, considering both their historical problem-solving performance and their mastery based on exam problem-solving. Subsequently, various indicators are derived from information such as students' cognitive levels, seating arrangements in the examination room, habitual guessing behavior, and paper similarity to evaluate potential cheating.

Finally, these diverse indicators, obtained through different approaches, are treated as features and fed into a feed-forward neural network for the classification of whether students engaged in cheating or not. Another smart system to detect cheating in the online exam has been discussed in [28]. This paper develops a completely automated online cheating detection system with the ability to identify whether a student is trying to cheat during an exam. The system will leverage deep learning techniques, specifically artificial intelligence (AI), including face recognition, sound detection, and active window detection. In [11], a machine learning based approach to exam cheating detection has been offered. Authors have presented a novel method for identifying possible instances of cheating in the final exam through the application of machine learning techniques. They frame the task of recognizing potential cheating cases as an outlier detection challenge, utilizing continuous assessment results from students to pinpoint anomalous scores in the final exam.

E-cheating prevention and detection at online examinations using deep learning approach has been proposed in [30]. Authors have employed an electronic cheating intelligence agent to identify online cheating activities, consisting of two primary components: the internet protocol (IP) detector and the behavior detector. This agent observes students' actions, capable of both identifying and thwarting any dishonest practices. It can introduce randomized multiple-choice questions in course exams and seamlessly integrate with online learning platforms for continuous monitoring of student behavior. To determine dishonesty during examinations, a machine learning model pre-configured with OpenCV, termed the Caffe Model, has been used in [27]. It ensures the integrity of the test-taking process by recognizing the examinee's face and facial markers, evaluating head movements, and monitoring eye positions. Utilizing the live webcam stream from the examinee's computer, OpenCV captures and processes multiple snapshots. Subsequently, it generates records based on the detection of distinct behaviors and actions of the individual taking the test. Towards effective and efficient online exam systems using deep learning-based cheating detection approach has been proposed by the authors in [10]. The intended study seeks to create a proficient strategy for enhancing online exam systems, employing deep learning models to promptly identify cheating through analysis of recorded video frames and speech. This involves the automatic extraction of relevant features from visual images and speech, accomplished by utilizing deep convolutional neural networks (CNNs) and the Gaussian-based discrete Fourier transform (DFT) statistical approach, allowing for the classification and detection of cheating behavior during exams.

2.2 Behavioral Analysis Based Approaches

Performance analysis of few old and some new indicators in detection of cheating on e-exams in higher education system has been proposed in [23]. The assessment focused on determining the effectiveness of various indicators in distinguishing cheaters within a subgroup from the rest of the test-takers. In their investigation, they utilized a classification tree to identify instances of induced cheating behavior. The objective was to explore the feasibility of detecting cheating in typical educational environments characterized by less-than-ideal conditions, such as the use of tests with low psychometric quality. The indicators, specifically

those related to the number of response revisions and response times, proved successful in identifying individuals who engaged in cheating. Authors in [25] proposed an exam cheating detection method with multiple human pose estimation. The suggested system utilizes Human Pose Estimation, encompassing tracking algorithms for both single-user and multiple-user scenarios.

By analyzing video footage, the system is capable of discerning whether a student is engaging in cheating activities through ongoing assessment of their head posture and hand movements during the exam. Rather than definitively labeling a student as a cheater, the system outputs a 'warning' to indicate an abnormal condition resembling cheating behavior. Cheating Detection in online exams during the Covid-19 Pandemic using data mining techniques has been proposed in [5]. This study introduced a recommendation system designed to assess students' responses and identify potential cheating in online exams. The approach involves employing statistical methods, similarity measures, and clustering algorithms. The system utilizes a set of features extracted from an online exam conducted on the Moodle platform. An automated cheating detection based on video surveillance in the examination classes has been discussed in [24].

The suggested system employs video surveillance to oversee students' actions during exams, with a particular focus on identifying unusual behavior. In instances of abnormal conduct, an automated alarm promptly notifies authorities of the detected irregularities, thus reducing the potential for errors that may arise from manual monitoring. Suspicious activity recognition for monitoring cheating in exams has been discussed by the authors in [9]. The objective of this study is to identify questionable behaviors exhibited by students in examination halls using surveillance. To achieve this, a deep 63-layer CNN model called "L4-BranchedActionNet" is proposed. This CNN structure is based on the modification of VGG-16, incorporating four additional branches.

The developed framework undergoes pre-training using the SoftMax function on the CUI-EXAM dataset to enhance its effectiveness. In more recent works, authors in [8] have introduced an automated monitoring system tailored for pen-and-paper based online examinations, taking into account the unique aspects of such tests.

This system continuously observes the examinee's head, eye, and lip positions, interpreting any shift in these as movement. Cheating is associated with regular and simultaneous movements of the head, eyes, and lips. The system quantifies a 'cheating score' that reflects the rate of these movements. An instance is flagged as cheating if this score surpasses a certain limit set by the proctor, which can be adjusted based on the particular standards of the subject matter. In [15], authors have crafted and introduced CHEESE, a framework designed to detect cheating through multiple instance learning. This system is composed of a label generator that applies weak supervision and a feature encoder that hones in on distinctive features. Moreover, the framework integrates body posture and environmental elements derived from 3D convolution with the eye gaze, head orientation, and facial characteristics recorded by OpenFace 2.0. These attributes are input into a spatio-temporal graph module, which stitches them together to scrutinize the spatial and temporal variations in video segments, thereby identifying instances of cheating. The efficacy of this method has been validated through tests on three distinct datasets: UCF-Crime, ShanghaiTech, and Online Exam Proctoring (OEP), demonstrating superior performance when bench-marked against leading-edge techniques. The summarization of the related works are represented in Table 1.

3 Background of Cheating in Online Exams

The detection of cheating has a varied history, responding to the imperative of upholding fairness and trust in education, sports, gaming, and professional contexts. Traditional methods like supervised exams and plagiarism checks are common in education, but advancements such as online proctoring[26] and AI-driven plagiarism detection are now prevalent. Technological progress, particularly in AI and machine learning, significantly contributes to more effective cheating detection, yet ethical concerns persist, necessitating a careful balance between ensuring fairness and respecting privacy rights.

Table 1. Summary of recent literature on Cheating Detection

Sl. No.	Reference No.	Functionalities of the proposed method
		Machine Learning and Deep Learning based approaches
1	[13]	Multi index exam cheating detection, RAE algorithm and LSTM neural network, cognitive levels, seating arrangements, habitual guessing behavior, paper similarity is used to detect cheating.
2	[28]	Smart system to detect cheating in the online exam, deep learning along with AI mechanisms, face recognition, sound detection, and active window detection is used.
3	[11]	ML based cheating detection, identifying cheating as detection of outlier and continuous assessment results in the final exam.
4	[30]	DL based cheating detection and prevention, intelligent agents observes students' actions and randomizes questions.
5	[27]	ML based OpenCV preconfigured Caffe Model to detect e-cheating, identifies student's face and facial markers, head movements and eye positions in live webcam.
6	[10]	DL based cheating detection, automatic feature extraction from visual images and speech, deep convolutional neural networks and Gaussian-based discrete Fourier transform.
		Behavioral Analysis based approaches
7	[23]	Indicator based cheating detection in higher education, classification tree, response revisions, response times, for identifying behaviour of student in online exam.
8	[25]	Cheating detection with multiple human pose estimation, video footage analysis, head posture and hand movements identification.
9	[5]	Data mining based e-cheating detection, students' responses are identified, statistical methods, similarity measures, and clustering.
10	[24]	Automated cheating detection based on video surveillance, observe student's actions, alarm generation for abnormal activities.
11	[9]	Video surveillance, VGG, deep 63-layer CNN model,identification of questionable behaviours of students.
12	[8]	Automated monitoring system for pen-and-paper based e-exams, head posture, eye, and lip positions based cheating score generation.
13	[15]	CHEESE framework for cheating detection, 3D CNN, Openface 2.0, label generator, feature encoder integrates eye gaze, head orientation, and facial characteristics.

3.1 Reasons behind Cheating in Exams

There are plenty of reasons [21] behind cheating in exams. First of all, there are lots of academic pressure in higher education system worldwide and fear of failure in such life-altering exams plays a key role in cheating. Sometimes, students lack in preparation or understanding of the subject material and on the other hand they desire to maintain a certain academic standard which forces them to do cheating. Also, lack of interest in a subject subsequently increases the chances of cheating.

Again, some students cheat because they believe they can escape punishment and thus insufficient awareness about the consequences of cheating contributes to their behavior during exam.

3.2 Types of Cheating in Exams

Types of cheating in exams refer to the various methods students may use to gain an unfair advantage during assessments. Cheating may be performed individually or in a group and can be of the following types which are shown in figure 2:

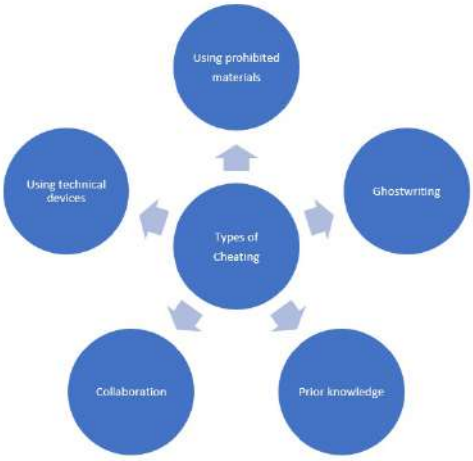

Fig. 2. Different Types of Cheating

— Using prohibited materials: This technique may further be elaborated as: copying during exam from other students, accessing unauthorized materials from books or cheat sheets. In case of online exams, materials may be collected from internet or offline digital notes can be used.

— Ghostwriting: In this technique, someone else is hired to write in the exam instead of the student. In case of online exam, someone else can make remote desktop control and even fake identity generation, credential sharing etc. can affect the authenticity of the exam.

— Prior Knowledge: Sometimes student can get unauthorized access of the question paper or exam content prior to the exam which is a type of cheating. Moreover getting help from someone knowledgeable during exam is also another kind of cheating.

— Collaboration: Sharing one's copy with another student, taking in sign language or any kind of communication, listening to other students' discussion etc may be treated as a way of cheating in exams.

— Using technical devices: Uses of different technical devices such as: mobiles or tablets, smart watches, programmable calculator, Bluetooth devices can contribute to cheating in exams.

3.3 Detection Measures for Cheating

Cheating detection in exams refers to the methods and technologies used to prevent, identify, and deter dishonest practices during assessments. It encompasses a range of strategies[1] from simple invigilation to sophisticated software that can monitor test-takers' screens, analyze their behavior, and verify their identity. The goal is to ensure the integrity of the examination process by making sure that all participants are abiding by the established rules and not gaining an unfair advantage. Therefore, detection of cheating in exam may be further subdivided in two categories as following:

— Detection of cheating throughout exam: Detection of cheating in physical exam as well as in online exam is primarily based on facial expression such as eye-gaze tracking, facial

and lip movement recognition. It may also depend on body movement such as head pose alteration, identification of hand gesture or body inclination etc. So, these types of expression or movement based cheating can be identified by human or online proctor during exam. Apart from that, behavioral analysis of keystroke pattern, mouse dynamics or voice modulation play important role in detection of cheating during exam.

— Detection of cheating afterwards exam: If cheating is not detected during the exam, still there is fair chance of cheating detection after the exam when copies are checked by the examiner. In this checking, softwares may be used to perform statistical analysis to identify the common mistakes. Several plagiarism checking tools are available to identify the copied contents. Again, searching in internet for similar content from all sources may be conducted to identify cheating. Moreover, multiple answer-script submission from same IP address, network traffic analysis of the student during exam time, time log analysis etc. is helpful in detection of cheating after exam.

3.4 Preventive Measures for Cheating

Cheating prevention[4] in exams involves proactive measures taken to discourage and reduce the likelihood of dishonest behavior during assessments. This can include designing exams that minimize opportunities for cheating, educating students about academic integrity, using technology to secure the testing environment, and implementing strict examination policies. The aim is to create a fair and honest testing atmosphere where the true knowledge and abilities of the test-takers are evaluated. Preventing measures for cheating are as following:

— Cheating prevention before exam: Several policies such as - seating arrangements, randomization of question paper, using more conceptual questions, open-book exam, reducing time limit etc. are helpful in preventing exam before it takes place. Again, various types of authentication such as - biometric authentication or continuous authentication also can secure online exam platforms' limiting access to external resources. Also, students can be motivated and informed about the consequences of cheating and thus can be prevented from doing so.

Fig. 3. Various measures for cheating in online exam

— Cheating prevention during exam: Continuous and strict offline or online proctoring is the most suitable technique to prevent cheating during exam. If a group of students are found cheating during exam, then that group may be broken with randomized seating arrangements. During online exam, internet connectivity may be stopped so that cheating can be prevented.

Figure 3 depicts the various measures for cheating in online exams. Now-a-days, various anti-cheating tools are available for maintaining academic integrity and ensuring fairness in online exams. These tools are helpful in preventing or detecting cheating via identification of external resource usage, authentication of student's identity, restricting various apps or websites during exam, live online proctoring and behavior monitoring, plagiarism checking, randomization of question bank etc. Table 2 shows a list of available anti-cheating tools.

Table 2. Anti-cheating tools for online exams

Sl. No.	Tool	Functions	URL
1	OnlineExam Maker	Face verification, browser lockdown	www.onlineexam maker.com
2	ExamSoft	Student's ID verification	www.examsoft. com
3	Exam.net	Remote proctoring, browser lockdown	www.exam.net
4	ExamDeveloper	Online proctoring	www.examdev. nccpa.net
5	Proctorio	Browser Lockdown	www.proctorio. com
6	Proctortrack	Blocks chatbots, search engines	www.proctor track.com
7	ProctorStone	AI powered online proctoring	wwwproctor stone.com
8	Questionmark	Online secure proctoring	www.question mark.com
9	Respondus	Browser Lockdown, ID verification	web.respondus .com
10	Talview	AI powered online proctoring	www.talview .com

4 Data Preparation and Implementation

One significant aspect of this research is the creation of a dataset [1] to be accessed on request. Given the absence of an openly available dataset concerning the detection of cheating in online paper-based exams, we took the initiative to design and assemble the dataset ourselves. Our dataset has been carefully crafted to encompass various actions that students might undertake during paper-based exams to facilitate cheating using video surveillance.

4.1 Video Surveillance in Online Exams

Video surveillance in online exams involves webcams or other monitoring tools to proctor students during their exams. Webcams are used generally to capture image or video of students appearing in the exam. One can check live video to detect cheating during exam or cheating may be detected after exam by scrutinizing the recorded video. But sometimes students who are unfamiliar with webcam-based proctoring may face challenges. Based on video surveillance proctoring in online exams may be of three types [18]: *online human proctoring* - where invigilator proctors the student through a software and takes action against committed cheating, *semi-automated proctoring* - where software detects cheating behaviors & patterns while human proctor takes final decision whether cheating has been done or not, and *fully automated proctoring* - where there is no human proctor involvement, software itself takes decision on cheating.

4.2 Circumstantial Action Recognition

Circumstantial action recognition involves identifying and classifying movements in real-time video streams. In online exam proctoring, this recognition is crucial for maintaining academic integrity. By detecting suspicious activities such as: glancing at another student's copy or using unauthorized materials, action recognition ensures fairness in

[1] https://github.com/PratyaBhowmik/Cheating-Detection

the process of exam. Additionally, automated monitoring helps proctors efficiently oversee the entire classroom. When suspicious behavior arises, timely intervention becomes possible with the help of proper action recognition.

In this paper, our objective is to identify eight types of exam cheating behaviors from the video of the classroom environment. From the video,initially frames are extracted and thereafter, on a frame-by-frame basis various actions are identified. In this paper, we have considered the following actions: use of mobile phone, use of earbuds, taking to each other, using cheat-sheets, exchanging answer-sheet, looking at other's copy, using smart watch and abstaining from cheating. This dataset is particularly appealing due to the prevalence of human-object interaction across most classes, which often involve similar bodily movements[13]. Different cheating actions have been illustrated in Figure 4.

4.3 Data Collection

For the experiments, we have created few classroom like environments where a 50-megapixel mobile camera has been utilized to capture scenes within those classrooms. The camera's sensor recorded scenes at a rate of 30 frames per second, with an image size of 1920 X 1080 pixels.

Additionally, the Mobile sensor captured the hand region of the subjects. The distance between the sensor and the recorded scene was approximately 3 meters. Our dataset comprises of 8 classes, totaling 42 video sequences with an average of 300 frames per video sequence. Table 3 outlines the summary of dataset with each type of action, no. of sequences, average number of frames and their average duration. Recognizing actions doesn't necessitate equal importance for every frame; only a selected few are pivotal.

4.4 Feature Extraction

In order to assess the efficacy of our proposed approach, the following five feature extraction methods has been used for each frame:

Table 3. Summary of Dataset

Actions	No. of sequence	Avg. frame No.	Avg. duration
Use of mobile	7	250	10 s
Use of earbuds	5	300	9s
Talking to each other	5	350	10s
Using Cheat sheet	4	320	11s
Exchanging answer sheet	5	280	9s
Looking at each other's copy	5	320	11s
Using smart watch	4	280	10s
Not cheating	7	400	10s

— **BRISK -** Binary Robust Invariant Scalable Keypoints[20] is a method commonly used to construct a feature descriptor by analyzing the gray scale relationships of random point pairs in the local neighborhood of an image. The obtained feature descriptor is useful for matching and recognition tasks.

— **BLOB -** Binary Large Object detection[19] mechanism identifies regions of an image that have similar intensity or color. It's useful for finding objects or regions with distinct shapes or textures.

— **LBP -** Local Binary Pattern[14] is a texture descriptor that characterizes local patterns in an image. It's commonly used for texture classifications.

— **MSER -** Maximally Stable Extremal Regions[29] mechanism detects regions in an image that are stable across different scales. It's often used for object detection and tracking.

— **HOG -** Histogram of Oriented Gradients[14] computes histograms of gradient orientations in an image. It's widely used for object recognition.

— **SURF -** Speed-Up Robust Features [29] mechanism identifies key-points based on intensity variations and computes descriptors that are robust to scale changes, rotation, and noise.

Figure 5 depicts various types of feature extraction methods.

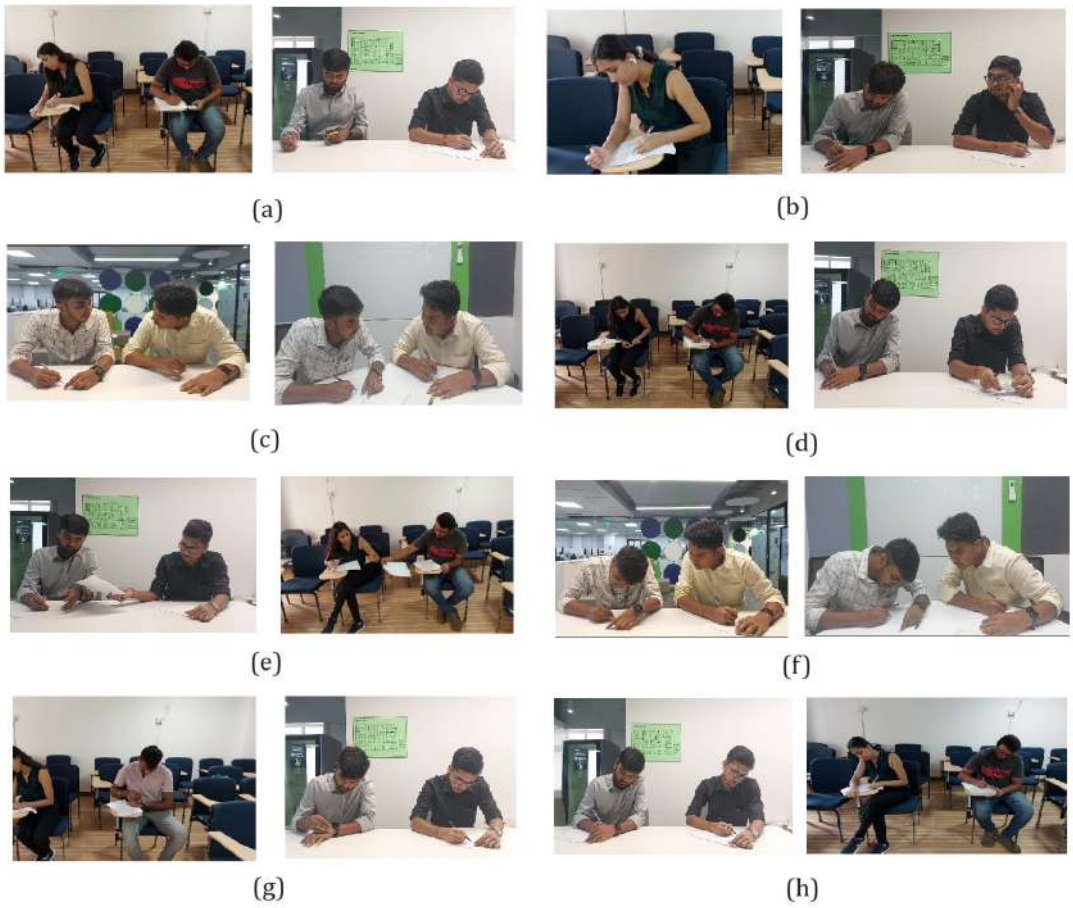

Fig. 4. Different Cheating Actions (a) use of mobile phone, (b) use of earbuds, (c) talking with each other, (d) using cheat-sheet (e) exchanging answer sheet (f) looking at other's copy (g) using smart watch and (h) no cheating

5 Experiments and Results Analysis

Before analyzing experiment results and drawing conclusions, it's crucial to carefully examine the experimental setup's details and trade-offs which are explained below:

5.1 Experimental Details

Due to the large size of training data, the experiments have been performed with Intel Core i5 3.3 GHz processor, 16 GB DDR5 RAM and 4 GB VRAM from NVIDIA GeForce RTX 3050. For testing the efficacy of the proposed system, we first prepared the dataset based on the frames collected from the video sequences. These frames are then annotated using VGG Image Annotator tool [6]. Its a lightweight tool used for manual annotation of images or video. For image annotation, a particular region is drawn inside the image and the attribute of that region is defined. If in the frame any of the items such as: mobile phone, ear bud, smart watch, cheat-sheet or answer-sheet are present then annotation is chosen as cheating. In case of frames such as: talking with each other and looking at other's copy, head movement is captured to define the region for better annotation.

Thereafter, features are identified from the frames which are resized to 1080 X 720 pixels for avoiding computational complexity. This resizing is per-

Fig. 5. Various type of feature extractions: (A) BRISK features (B) BLOB regions, (C) LBP regions (D) MSER rectangles (E) HOG blocks, (F) SURF detectors

formed using the LANCZOS filter[16] which is a high-quality, convolution-based filter available for adjusting the image dimensions to execute random cropping by ensuring the target resolution. This adjustment was made without altering their content or the primary objective of the classification task.

Finally feature vectors are generated using the extraction methods described in section 4.4.

After feature extraction, classification of image frames are carried out based on the combination of K-Means Clustering in association with Support Vector Machines (SVM). Initially, we have used the K-Means algorithm to cluster the received image features into groups. For instance, we have used BRISK, BLOB, LBP, MSER, HoG and SURF techniques to extract image features and then the extracted features are combined in a group or cluster corresponding to a pattern of features. Following to the cluster assignment, the outcome of K-Means algorithm is used in SVM to provide better detection of the action. The cluster assignment in K-means is now used as a class label such as:

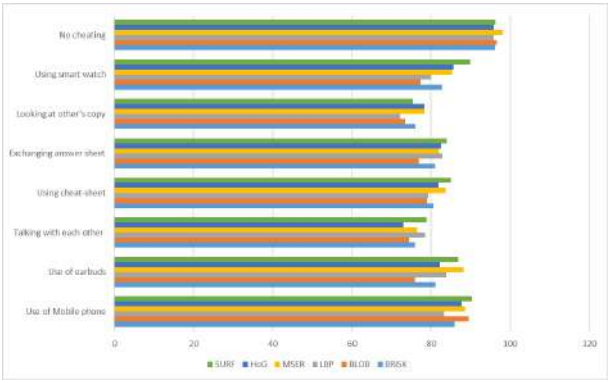

Fig. 6. Percentage of accuracy of various action classification based on different features

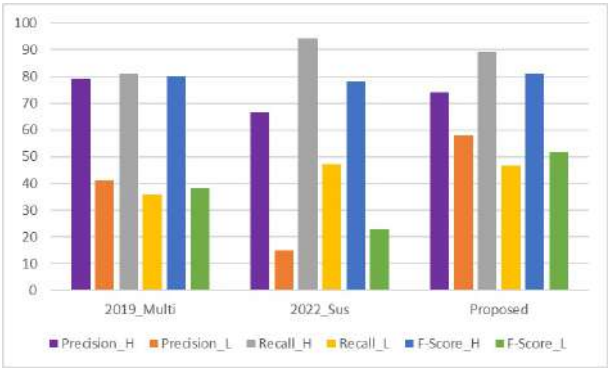

Fig. 7. Performance comparison of different methods

using mobile phone, smart watch etc. Based on this class labelling, the SVM classifier is further trained for the original annotations as well as for the K-means cluster assignments. The features those are extracted from the image frames are used to train the SVM for 8 defined classes out of which 7 classes denote cheating and a single class denote not cheating.

5.2 Results Analysis

For analyzing the results of the experiments, we have calculated the accuracy of various feature extraction methods for our dataset. Subsequently, we have compared the precision, recall and F-score values with [13] and [9].

Figure 6 depicts the percentage of accuracy of various feature extraction methods for classifying various actions for smooth detection of cheating.

Figure 7 depicts the performance comparison of our proposed method with two existing methods. The experiments in [13] provides the highest precision with 79.4%, which defines that the number of false positives (FP) is low, even if true negatives (TN) are high. Again, [9] provides the highest recall value of 94.33%, which means the algorithm is minimizing the number of false negatives. In our proposed method, the highest F-score value of 81.05% is obtained that indicates that the model performs well in correctly identifying positive instances while minimizing false negatives and false positives. In summary, a higher F-score reflects a robust classifier that achieves both accurate positive predictions and comprehensive coverage of relevant cases.

From this figure it is evident that the two actions such as: talking with each other and looking at other's copy has the lowest accuracy ranging between 72.17% to 78.89%. The computational complexity necessitates image resizing, which reduces the feature count. However, when annotating actions like "talking with each other" or "looking at other's copy," head movements play a crucial role and therefore, some features may be lost during resizing, while preserving the essential information.

On the other hand, action of using of mobile, smart watch, cheat-sheet, ear-buds etc. shows better accuracy ranging between 75.93% to 90.29%. The change in accuracy in various action recognition is due to the diverse nature of cheating behaviors present within the dataset, resulting in significant fluctuations within the feature space. Images can also vary significantly due to lighting conditions or viewpoints which may contribute to this varied accuracy rate. In these categories of actions, accuracy is much higher due to the reason that they incorporate not only actions but also the interpretation of objects, scenarios and their temporal sequences.

The 'No cheating' action shows a accuracy rate between 95.82% to 98.12%. This action achieves a high accuracy rate because of the absence of the objects such as: ear bud, mobile or smart watch in the image frames. Also, there is lack of head movement in the frames which increase the accuracy.

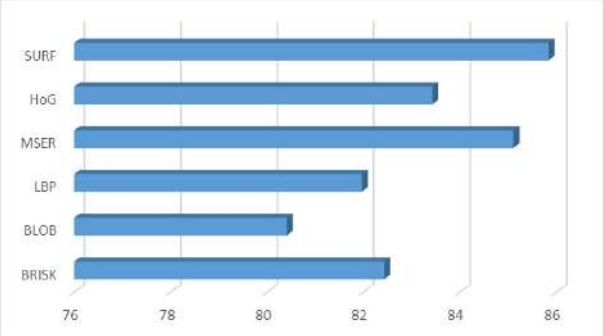

Fig. 8. Average accuracy rate of different features

Therefore, this observation indicates that classifying non-cheating behaviors leads to better outcomes compared to classifying cheating behaviors.

The average percentage of accuracy of the various features are shown in figure 8. The figure clearly indicates that the SURF feature extraction method outperforms other techniques. This superiority stems from SURF's ability to efficiently identify local texture patterns and key-points, even when specific objects like earbuds or mobile phones are present in the image frames.

6 Conclusion and Future Work

In this paper, a cheating detection framework has been proposed specifically for online exams. Initially, a dataset of frames has been curated from the captured video sequences of online paper based exam scenario. The framework leverages eight types of Circumstantial Actions extracted from those video sequences. Subsequently, various feature extraction methods have been applied to these images for identification of cheating. Finally, we employ a combination of K-Means Clustering in conjunction with Support Vector Machines (SVM) to classify the data and identify instances of cheating during exams. Our experimental results demonstrate that the proposed method achieves an average of 84.83% accuracy in detecting cheating behavior,showcasing promising and distinguishable outcomes.

The dataset presents significant challenges as many actions appear similar and involve factors beyond mere body movements which may further be enhanced. Additionally, expanding the dataset by capturing more videos and incorporating diverse dynamic factors such as varying environments, lighting conditions or camera angles could enrich its utility and effectiveness.

Acknowledgments

The authors would like to acknowledge Software Engineering & Network Lab from National Institute of Technology, Agartala for carrying out the research work.

References

1. **Alsabhan, W. (2023).** Student cheating detection in higher education by implementing machine learning and lstm techniques. Sensors, Vol. 23, No. 8, pp. 4149.
2. **Betti, A. A., Betti, G. A., Naser, A. H. (2025).** Artificial intelligence in the educational system: Theoretical perspectives and a practical application for cheating detection in examination halls. Journal of Al-Qadisiyah for Computer Science and Mathematics, Vol. 17, No. 2, pp. 272–280.
3. **Bhowmik, P., Das, S. (2023).** Cheating detection in online exam: a comprehensive survey. International Conference on Information and Communication Technology for Competitive Strategies, Springer, pp. 71–81.
4. **Cagala, T., Glogowsky, U., Rincke, J. (2024).** Detecting and preventing cheating in exams: Evidence from a field experiment. Journal of Human Resources, Vol. 59, No. 1, pp. 210–241.
5. **Duhaim, A. M., Al-Mamory, S. O., Mahdi, M. S. (2021).** Cheating detection in online exams during covid-19 pandemic using data mining techniques. Webology, Vol. 19, No. 1, pp. 341–366.
6. **Dutta, A., Zisserman, A. (2019).** The via annotation software for images, audio and video. Proceedings of the 27th ACM international conference on multimedia, pp. 2276–2279.

7. **Eshet, Y. (2024).** The plagiarism pandemic: inspection of academic dishonesty during the covid-19 outbreak using originality software. Education and Information Technologies, Vol. 29, No. 3, pp. 3279–3299.
8. **Ferdosi, B., Rahman, M., Sakib, A., Helaly, T. (2023).** Modeling and classification of the behavioral patterns of students participating in online examination. Human Behavior and Emerging Technologies, Vol. 2023, No. 1, pp. 2613802.
9. **Genemo, M. D. (2022).** Suspicious activity recognition for monitoring cheating in exams. Proceedings of the Indian National Science Academy, Vol. 88, No. 1, pp. 1–10.
10. **Kaddoura, S., Gumaei, A. (2022).** Towards effective and efficient online exam systems using deep learning-based cheating detection approach. Intelligent Systems with Applications, Vol. 16, pp. 200153.
11. **Kamalov, F., Sulieman, H., Santandreu Calonge, D. (2021).** Machine learning based approach to exam cheating detection. Plos one, Vol. 16, No. 8, pp. e0254340.
12. **Kiura, G. M. (2023).** Behavioral detection and prevention of cheating during online examination using deep learning approach. .
13. **Li, Z., Zhu, Z., Yang, T. (2019).** A multi-index examination cheating detection method based on neural network. 2019 IEEE 31st international conference on tools with artificial intelligence (ICTAI), IEEE, pp. 575–581.
14. **Liu, H., Jia, X., Su, C., Yang, H., Li, C. (2023).** Tire appearance defect detection method via combining hog and lbp features. Frontiers in Physics, Vol. 10, pp. 1099261.
15. **Liu, Y., Ren, J., Xu, J., Bai, X., Kaur, R., Xia, F. (2024).** Multiple instance learning for cheating detection and localization in online examinations. IEEE Transactions on Cognitive and Developmental Systems.
16. **Moraes, T., Amorim, P., Da Silva, J. V., Pedrini, H. (2020).** Medical image interpolation based on 3d lanczos filtering. Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, Vol. 8, No. 3, pp. 294–300.
17. **Newton, P. M., Essex, K. (2023).** How common is cheating in online exams and did it increase during the covid-19 pandemic? a systematic review. Journal of Academic Ethics, pp. 1–21.
18. **Nigam, A., Pasricha, R., Singh, T., Churi, P. (2021).** A systematic review on ai-based proctoring systems: Past, present and future. Education and Information Technologies, Vol. 26, No. 5, pp. 6421–6445.
19. **Pan, R., Li, C., Hu, B., Liu, Y. (2023).** Research on the examination technology of connector pin skewing according to blob analysis. Measurement Science and Technology, Vol. 35, No. 3, pp. 035004.
20. **Potluri, T., Sistla, V. P. K. (2023).** Mg-net: Multiple person and gadget detection for online exam proctoring system. Proceedings of Third International Conference on Advances in Computer Engineering and Communication Systems: ICACECS 2022, Springer, pp. 445–456.
21. **Radwan, T. M., Al Abachy, S., Al-Araji, A. S. (2022).** A one-decade survey of detection methods of student cheating in exams (features and solutions). Journal of Optoelectronics Laser, Vol. 41, No. 4, pp. 355–366.
22. **Ramzan, M., Abid, A., Bilal, M., Aamir, K. M., Memon, S. A., Chung, T.-S. (2024).** Effectiveness of pre-trained cnn networks for detecting abnormal activities in online exams. IEEE Access, Vol. 12, pp. 21503–21519.
23. **Ranger, J., Schmidt, N., Wolgast, A. (2020).** The detection of cheating on e-exams in higher education—the performance of several old and some new indicators. Frontiers in psychology, Vol. 11, pp. 568825.
24. **Roa'a, M., Aljazaery, I. A., Alaidi, A. (2022).** Automated cheating detection based on video surveillance in the examination classes. International Journal of Interactive Mobile Technologies, Vol. 16, No. 08, pp. 125.

25. **Samir, M. A., Maged, Y., Atia, A. (2021).** Exam cheating detection system with multiple-human pose estimation. 2021 IEEE International Conference on Computing (ICOCO), IEEE, pp. 236–240.

26. **Selwyn, N., O'Neill, C., Smith, G., Andrejevic, M., Gu, X. (2023).** A necessary evil? the rise of online exam proctoring in australian universities. Media International Australia, Vol. 186, No. 1, pp. 149–164.

27. **Singh, A., Das, S. (2022).** A cheating detection system in online examinations based on the analysis of eye-gaze and head-pose. THEETAS 2022: Proceedings of The International Conference on Emerging Trends in Artificial Intelligence and Smart Systems, THEETAS 2022, 16-17 April 2022, Jabalpur, India, European Alliance for Innovation, pp. 55.

28. **Soltane, M., Laouar, M. R. (2021).** A smart system to detect cheating in the online exam. 2021 International Conference on Information Systems and Advanced Technologies (ICISAT), IEEE, pp. 1–5.

29. **Tareen, S. A. K., Raza, R. H. (2023).** Potential of sift, surf, kaze, akaze, orb, brisk, agast, and 7 more algorithms for matching extremely variant image pairs. 2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE, pp. 1–6.

30. **Tiong, L. C. O., Lee, H. J. (2021).** E-cheating prevention measures: detection of cheating at online examinations using deep learning approach–a case study. arXiv preprint arXiv:2101.09841.

Article received on 11/09/2024; accepted on 21/08/2025.
**Corresponding author is Smita Das.*