Automated Invigilation System for Detection of Suspicious Activities During Examination

Noor Sumaiya[1], Navya S K[2], Anjali R[3], Priya N[4], Nandan A[5]

[1,] Assistant Professor, Department of Computer Science and Engineering, Jnana Vikas Institute of Technology, Karnataka, India
[2,3,4,5] Undergraduate student, Department of Computer Science and Engineering, Jnana Vikas Institute of Technology, Karnataka, India

---***---

Abstract –*Automated invigilation systems are software programs that monitor examinations and look for suspect activity using a variety of methods, including facial recognition, eye tracking, and screen recording. These systems have the power to completely alter the way exams are administered, enabling a more effective and efficient method of combating cheating. However, using such systems raises privacy and ethical issues, so the choice to do so should be carefully weighed against any potential advantages and disadvantages. To guarantee that such systems are used morally and with regard for students' privacy rights, it is essential to establish them with transparency and explicit standards. In the end, other strategies for guaranteeing academic integrity, such bettering instruction, should be balanced with the use of automated invigilation technologies.*

Education institutions resolve student strength and weakness through the examinations. Academic dishonesty has been constantly been worrying factors for the institutes in education system. Cheating and abnormal activities which includes like whispering, impersonation or hand contact these are widely involved in the exams around the globe, this research purpose is to examine and identify the abnormal/malpractices undertaking during the period of exams which results in inequality or unfair examination system. Automated video surveillance which roots image and video processing which is an optimal solution for monitoring the students activities during the offline examination. The proposed system automatically alerts the management when there is any suspicious activities are identified. The proposed system walk through various process- pre-processing, segmentation, classification, feature extraction and related works in sequential manner. The proposed model is effective, efficient and relatively less processing power.

Key Words: Video surveillance, impersonation, segmentation, feature extraction, suspicious

1. INTRODUCTION

In recent years, automated invigilation systems have drawn increased interest as a potential means of combating exam cheating. When suspect activity is observed during exams, these systems use cutting-edge technologies like facial recognition, eye tracking, and screen recording to alert human examiners for additional investigation. The process of invigilation will be made more effective and efficient, and academic integrity will be improved.

In recent years, automated invigilation systems have drawn increased interest as a potential means of combating exam cheating. When suspect activity is observed during exams, these systems use cutting-edge technologies like facial recognition, eye tracking, and screen recording to alert human examiners for additional investigation. The process of invigilation will be made more effective and efficient, and academic integrity will be improved.

The traditional method of invigilation/examinations, involves in human invigilators to present in examination hall to monitoring the students. The more number of students requires more number of invigilators to bring the quality in education and for the fair conduction of examination. A invigilation system is required to prevent cheating and to avoid any malpractices in examinations as it directly impacts the students morality.

A system based on computer artificial intelligence is proposed for the detection of cheating by the movement of head and neck movements through the surveillance camera. The system is more better and more effective than the traditional invigilation system hence it does not requires much labor, energy, effort and time.

Automated invigilation systems offer several benefits, such as reducing the likelihood of cheating, improving exam security and ensuring fairness for all students. They can also save time and resources for educational institutions as fewer human invigilators are needed to monitor the exams. There are also potential downsides including concerns about privacy, accuracy, and the potential for the technology to be misused.

The proposed system detects the suspicious activities and cheating works done by the students during the examination. Detection of the cheating activities in the classroom is implemented by the system using the YOLO (you Only Look Once) algorithm. The proposed model will be able to process the real time automated videos using the existing dataset of the student and various activities will analyzed which is happening in the examination.

Examination malpractice or cheating is any form of unlawful activity in an examination center. It is most dangerous practice, which must be avoided since this should not be a reason which impacts negative effect on the society. In this paper, proposed a system that detects and recognized the cheating done by the students in the examination hall. Despite these concerns, automated invigilation systems are still being investigated as a potential means of enhancing academic integrity in educational institutions. The effectiveness, constraints, and ethical ramifications of automated invigilation systems will all be covered in this essay. The paper will also go over the necessity for a well-rounded approach to academic integrity, which includes enhancing teaching methods, supporting students, and taking into account the application of various technologies to improve invigilation procedures.

2. LITRATURE REVIEW

Automated invigilation system is a computer based system that is used to monitor the students and detect the suspicious activities during examination among the students. It is designed to reduce the incidence of academic dishonesty and fair conduction of the exams by monitoring the students actions in real-time using a combined versions of computer vision and machine learning algorithms. The purpose of this literature review is to examine the existing research on automated invigilation system for detection of suspicious activities during the examination.

1. "Automated Monitoring and Assessment of Online Exams" by N.Arora, A.Selvaraj and M.A. Vasarhelyi (2018)

   The authors developed an automated invigilation system that uses computer vision and machine learning algorithms to monitor the student actions during the examinations. It presents multimedia analytics system for online proctoring, which aims to maintain academic integrity in e-learning. User verification, text decoration, speech detection, active window detection, gaze estimation and phone detection, these are the features acquired from the analysis and then used for the cheat detection. The capability of the system, nearly 87% segment based detection rate across all types of cheating behaviors at a fixed FAR of 2%.

2. "Detection of Cheating Behaviors in Online Exams Using an Automated Invigilation System" by R.Elangovan, N.Rajakumar and S.Suresh (2020)

   Cheating detection and prevention methods are needed to combat forbidden actions. Detection methods without applying prevention methods could not be affective. As cheating detection and prevention methods are evolved, new cheating types and technologies emerge as well. The HAR that employs a deep learning model based on MobileNetV2 architecture. The data was derived from a video clip of a person taking an online exam using a webcam capture. When employing hyper-parameters such as max epoch of 20, a learning rate of 0.0001, a batch size of 16, and a dense layer of five, the deep learning model with MobileNetV2 architecture achieved optimal performances. The evolution findings have an F1-score of 84.52% .The primary objective of, after creation of the optimal model was identified is the creation of an Indonesian-language web based application. This is unquestionably a tool that may be used to advance educational technology in Indonesia.

3. "An Intelligent Automated Online Examination Invigilation System" by Y.Wang, M.Zhang and Y,Wu (2019)

   RCNN is a deep learning model implemented for object detection and classification. It gives the accurate results and better accuracy as compared to other CNN models for invigilating purposes. The proposed model implemented as a binary classifier to classify students activities into two categories : cheating; and No cheating. The no cheating label is considered for the students who are doing their paper as obedient in a perfection manner and the cheating label is considered to those students who are continuously looking left, right and peeking to other student papers for cheating.

   Invigilation dataset with training accuracy of 99.5 and a test accuracy of the model 98.5. student identification and recognition are with an accuracy 95&. The results of the both the faster runner classifier and face recognition module are combines and students status reports are generated.

4. "A Framework for automated Online Exam Invigilation" by S.Saha, S.Biswas, and R.Choudhary (2020)

   The existing invigilator-exam assignment system in the university under consideration has some problems like time and man power needed for constructing the assignment.

A user-friendly decision support system based on a multi-objective mixed-integer programming model is introduced for invigilator-exam assignment problem with an eye to practical use. The system has a appropriate facilities for providing help to the users to implement an assignment schedule.

Comparing with the current invigilator-exam assignments for 2004-2005 spring midterm and final exam terms, it is seen that the required time for the assignments is dropped off from a few days to seconds. AIAS reaches optimum results in a few seconds.

Automated invigilation system are an effective way to reduce academic dishonesty during exams. The systems use computer vision and machine learning algorithms to monitor the student actions and detect suspicious activities such as copying pasting switching between windows, and using unauthorized access devices. The existing research on automated invigilation system that these systems are effective in reducing academic dishonesty.

Table -1: Summary of research work

Paper	Methodology	Accuracy
Automated Monitoring and Assessment of Online Exams	Feature and AdaBoost	87% segment based fixed FAR of 2%.
Detection of Cheating Behaviors in Online Exams Using an Automated Invigilation System	HAR adopts MobileNetV2 architecture	84.52%
An Intelligent Automated Online Examination Invigilation System	RCNN	98.5%
A Framework for automated Online Exam Invigilation	EM algorithm and adaptive threshold	Error rate less than 10% compared to standard computer vision algorithms

Researchers all across the world had done solid work, but there were certain accuracy flaws that could be fixed, which the proposed study aims to do.

The main contributions made to this study are as follows:

- A novel system has been developed that can identify and recognize students cheating in the examination. The yolov3 architecture was changed by replacing the parameters and backbone architecture.
- Generated the local dataset of invigilation of students in the examination.

3. METHODOLOGY

3.1 Data Preparation

Data preparation is a crucial step in developing an automated invigilation system. some of the key considerations for data preparation

The system should collect data from various sources, such as cameras, microphones, and sensors. The data should include images, videos, and other relevant information that can be used to analyze student behavior during exams then the collected data may contain noise or irrelevant information, which can affect the accuracy of the system. Therefore, it is essential to clean and preprocess the data before using it for analysis.

The collected data should be labeled with appropriate tags to indicate different activities, such as reading, writing, or looking at another screen. This labeling is essential to train the machine learning models to recognize and detect suspicious activities accurately.

Data augmentation involves creating additional training data from existing data to improve the performance of the machine learning models. For example, the system can artificially increase the number of students in an image to create a more diverse dataset. The system should use different sampling techniques to balance the data distribution. For example, if cheating activities occur less frequently, oversampling techniques can be used to increase the representation of these activities in the dataset. The collected data should be validated to ensure its accuracy and completeness. Validation includes checking the quality of the data and ensuring that it represents the activities that occur during exams.

3.2 Image acquisition

In data acquisition, a camera is utilized to record video of the students, which is afterwards turned into various frames (or images) that can be used to detect and recognize the students.

For the detection of suspicious activity and face recognition, distinct datasets have been gathered. For the aim of tracking head orientation, training and testing datasets are created for students moving their heads forward, backward, left, and right. Label image software is then used to manually generate the labels "Normal activity" and "Suspicious activity" on these photos.

To get a clean shot of every student and their desks, the cameras in the exam room should be carefully placed. In order to reduce shadows and produce high-quality photographs, the positioning of the camera should also take into account the lighting and angle of the scene. In order to ensure that the photos recorded are of good quality and provide sufficient detail to identify any potential cheating behaviors, the camera's quality is crucial. In automated invigilation systems, high-resolution cameras with good low-light sensitivity are often used. To guarantee that the images recorded are precise and reliable, the cameras must be calibrated. To produce consistent, high-quality photographs, this entails tweaking the camera's settings for brightness, contrast, and white balance. To find any potential cheating behaviors, it is necessary to process the images that the cameras captured. This entails analyzing the photos to find any suspicious activity using algorithms like object detection, facial recognition, and posture detection. To protect the privacy and confidentiality of the exam data, the photos that were taken must be maintained securely. Additionally, the system needs to have safeguards against unauthorized access and data tampering.

The collection includes 5000 photos, of which 1000 are single photographs and 4000 depict various classes where students are engaging in cheating and non-cheating activities. 80% of the dataset is utilized for training, while 20% is used for testing. After training, a live feed from an automated security camera in an exam room is used to test the model. On a labeled dataset that was head-oriented, we trained our faster RCNN model. After training, the model is tested using real-time footage from an automated security camera in an exam room. During implementation, the video is first broken up into frames, and each frame is examined for head movement before being categorized as cheating or not. For the purpose of identifying student faces, a separate database of recognized faces has been developed. The dataset includes 1000 photos of students, each of which has the front, left, and right angles of their faces captured.

The dataset produced locally for the current work. Six classes worth of physical exams were recorded using a camera with a 640 x 480 resolution and a 25 frames per second frame rate. The footage showed both the students' regular and questionable behavior. From the captured videos, 30,000 frames were taken out. Used a Python script with the OpenCV library to extract more than 5000 frames. Preprocessing of the collected frames involved manually deleting blurred frames from the folder.

The proposed model was trained on a dataset of head-oriented student data, where student head movements to the left, right, and up were classified as either cheating or not, it is limited in that it only considers the students' head orientation when determining whether or not there was any cheating. The suggested invigilation system can be improved further by training a faster invigilation system to detect hand motions and hand contact while passing sheets by extending the existing dataset to include the classes of student hand gesture photos and student hand contact images. The suggested invigilation system can be further improved by training on an expanded dataset that includes the classes of student hand gesture photos and student hand contact images. The suggested invigilation system can be further improved by training a faster RCNN system to detect hand motions and hand contact during passing sheets by extending the existing dataset to include the classes of student hand gesture photos and student hand contact images. It can also be used to identify any type of dangerous instruments, such as calculators and phones, to lessen the risk of cheating in offline exams. Several Deep Learning models, including YOLOv4, RCNN, and Mask RCNN, PCA, can be used to detect cheating behavior.

3.3 Face Recognition

Face Recognition with Open-CV is used for student identification. To identify the students, their faces are first identified. Face detection is performed using MTCNN. Students' facial traits are extracted using face embedding models. For the purpose of recognizing and identifying a student, a vector called face embedding that represents the student's facial features is employed. For the purpose of identifying students, a different database is developed. Each student's face is embedded in the system. Each student's face embedding in a live video stream has been calculated, and the results have been compared to the known face embedding that is already present in the dataset.

By matching the student faces to the pictures kept in the database, the system can confirm their identities. This reduces the possibility of impersonation and helps ensure that the appropriate student is taking the exam.

Using cameras, the system can continuously watch the test space and identify any changes in the students' facial expressions or posture. This can assist in identifying any students who might be switching positions or attempting to cheat by talking to another student.

The invigilators can be instantly alerted if the system notices any questionable activity, giving them the information they need to respond appropriately.

To assist invigilators in reviewing and analyzing exam data, including seeing trends of suspicious behavior or suspected cheating, the system can also offer analytics and reporting functions. It is significant to note that privacy and security issues are raised by the use of facial recognition technology in automated invigilation systems. The system should be built with adequate safeguards to allay these worries, including making sure that data is collected and stored securely and that the system complies with relevant privacy laws and regulations. The system should also clearly explain to students their rights and how their data will be used, as well as be honest about how it makes use of facial recognition technology.

4. IMPLEMENTATION

The architecture and design of an automated invigilation system may vary depending on the specific features and functionalities it offers. However, in general, an automated invigilation system consists of the following components :

1. Cameras and sensors
2. Data storage and processing
3. Algorithms and machine learning models
4. Alerting and reporting
5. User interface

The system is designed for the monitoring is only engaged during the test period, the system should be built to recognize and identify the exam room.

To guarantee that they capture all required areas of the exam room while minimizing any potential privacy violations, the placement of cameras and sensors should be carefully designed. Data must be gathered and processed by the system in a secure and trustworthy manner. Additionally, it ought to offer a means of storing and retrieving data for possible later review and analysis.

Machine learning models that have been trained to accurately detect dishonest behavior should be used by the system along with trustworthy and efficient algorithms. When suspicious activity is discovered, the system must to have an alerting feature that notifies the invigilator. Additionally, to produce reports containing thorough details about the activities found during the examination. The privacy and moral ramifications of using the system should be taken into account throughout design. It should make sure that the system is utilized morally and that data is only used for the intended purpose. It should also respect students' privacy rights. The technology should have a user-friendly interface that enables the invigilator to efficiently monitor the exam room. To make it simpler to spot suspicious activities, the interface should present the data in a straightforward and intelligible manner.

To guarantee a seamless experience for the user, the system should be built to interface with other systems, such as learning management systems.

To ensure its effectiveness, dependability, and ethical use, an automated invigilation system should take into account a variety of components and elements throughout design. The system can be thoughtfully designed to assist prevent exam cheating while upholding students' right to privacy.

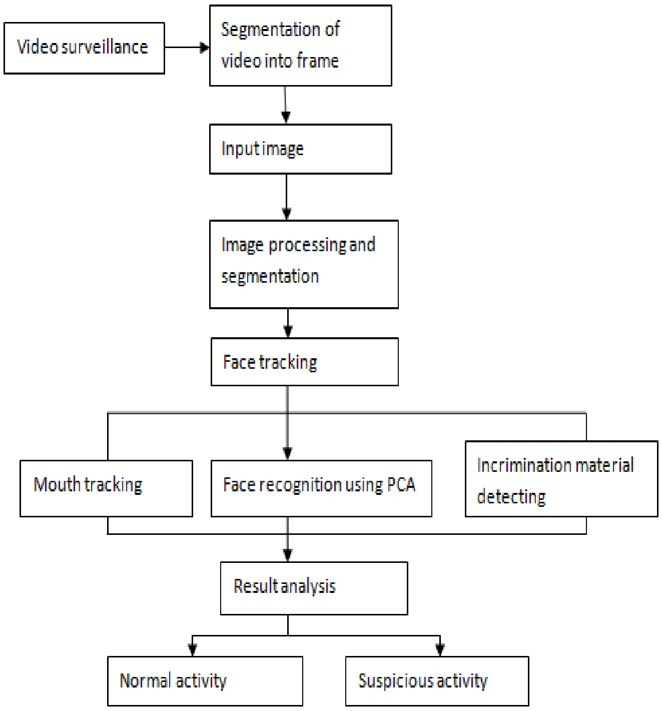

Video surveillance
Segmentation of video into frame
Input image
Image processing and segmentation
Face tracking
Mouth tracking
Face recognition using PCA
Incrimination material detecting
Result analysis
Normal activity
Suspicious activity

Fig -1: Model of proposed system

The technology uses cameras and sensors to record the exam room and keep an eye on the students' behaviors. These cameras and sensors might have features include screen recording, eye-tracking, and facial recognition. The system gathers information from the cameras and sensors, analyses it, and saves it in a safe database. Images, movies, and other pertinent information could be included with the data. The system analyses the data and looks for any unusual activity using algorithms and machine learning models. These models learn to recognize patterns of dishonest behavior through training on a sizable dataset of labeled samples. If the system notices any suspicious activity, it notifies human invigilators so they can review the video and respond appropriately. Additionally, the system produces reports that give thorough details about the activities found during the examination. The system might have a user interface that enables human examiners to keep an eye on the exam room in real-time and see the images the cameras and sensors are taking. The design of an automated invigilation system must take into account a number of criteria, including ease of use, security, and privacy. It must make sure that the system's data collection is retained securely and used only for that reason. The system should also ensure that students' privacy rights are maintained and set clear instructions on how the data will be utilized. Additionally, for invigilators to effectively watch the exam room, the user interface must be simple to use and provide all the information they need.

6. ALGORITHMS

Are speaking or whispering, which may indicate that they are collaborating or using outside resources to cheat. Computer vision and machine learning algorithms are frequently combined in automated invigilation systems to detect suspect activity during tests. Some of the algorithms that might be applied in these systems are listed below:

You Only Look Once (YOLO) or Faster R-CNN (Region-based Convolution Neural Networks) object detection algorithms can be used to find prohibited items in the exam room, such as electronic devices, books, notes, and other materials.

Algorithms for posture detection can be used to spot changes in a student's behavior or posture that can be a sign of cheating. These algorithms, for instance, are able to recognize when a student bends over towards their desk, which could indicate that they are looking at a device or a cheat sheet.

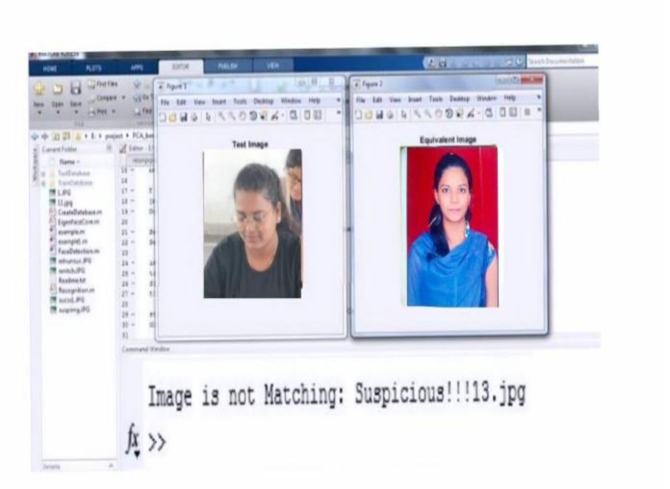
The ability to recognize specific students in the test room can be achieved using facial recognition software like Open Face or Face Net. To prevent students from switching places or using someone else's identity to cheat, these algorithms can recognize and track face traits.

Algorithms for anomaly detection can be used to spot odd or troubling exam behavior. With the use of historical data, these algorithms may recognize patterns that are inconsistent with regular behavior, such as abrupt shifts in a student's behavior or unexpected motions.

Convolution neural networks and recurrent neural networks are two examples of deep learning algorithms that can automatically identify suspicious activity by learning from the data gathered during tests. The accuracy and performance of these algorithms can be improved over time by training them on vast datasets of labeled data.

Algorithms for speech recognition can be used to examine the audio from the examination room. These algorithms are able to identify when students

To identify suspect behavior during exams, automated invigilation systems may combine object detection, facial recognition, posture detection, speech recognition, anomaly detection, and deep learning algorithms. Together, these algorithms are intended to offer a complete solution for overseeing exams and preserving academic integrity.



```
Image is not Matching: Suspicious!!!13.jpg
fx >>
```

Fig -2 : Impersonation identified after PCA face recognition

Fig -3 : sample frame of dataset

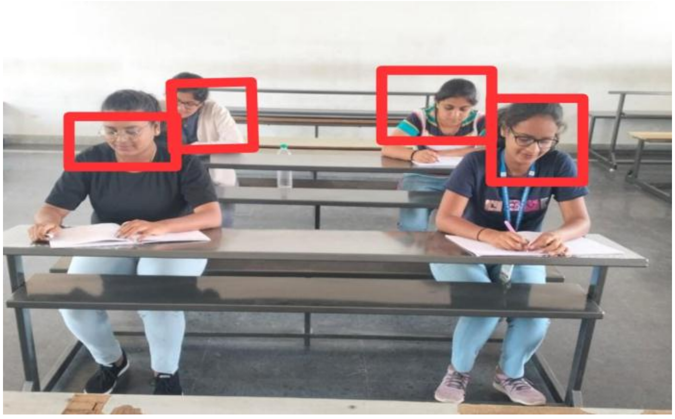


Fig -3 : Face detection

Fig -4 : Input frame for testing

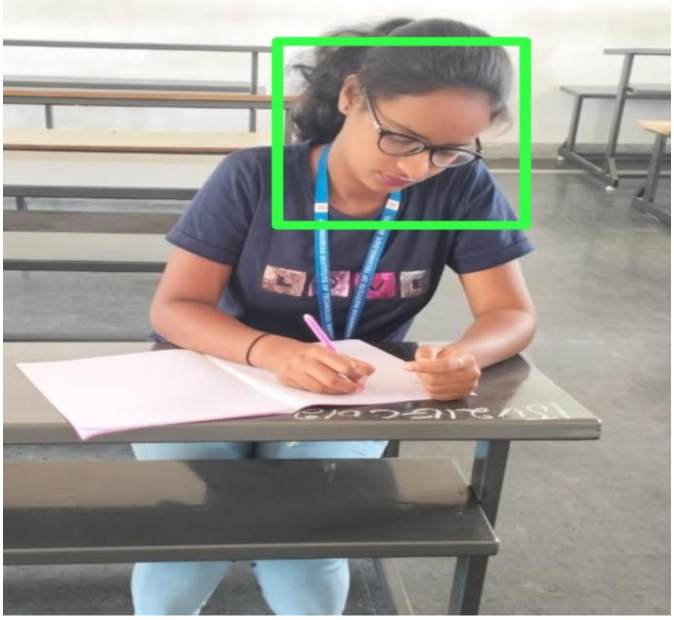


Fig -5 : Face detection in input frame

Fig -6 : Trained database image

Fig -7 : Evaluation of Impersonation

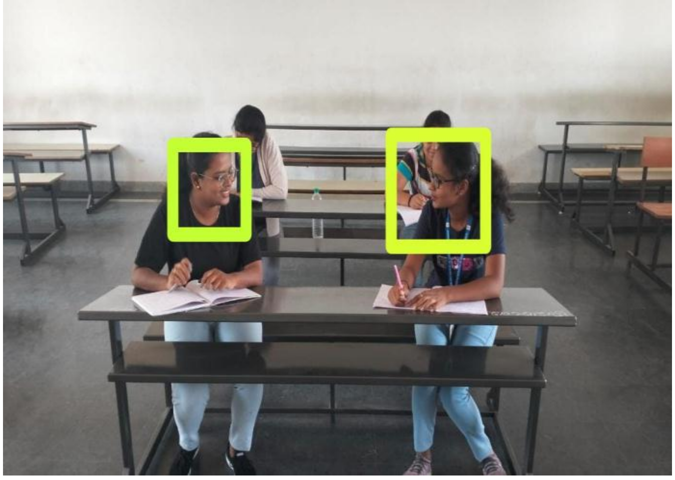


Fig -8 : Automatic Cheating Detection

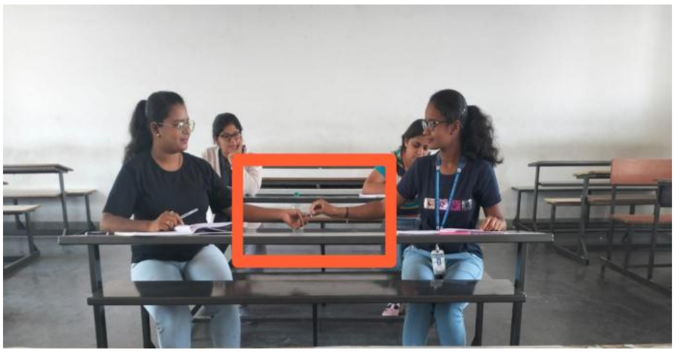


Fig -9 : Hand contact detection

6. CONCLUSIONS

Automated invigilation systems have the ability to completely change how exams are administered by enabling a more effective and efficient method of combating cheating. The technologies identify suspect activities and mark them for additional inspection by human invigilators using a variety of techniques, including facial recognition, eye tracking, and screen recording. Although it has been demonstrated that automated invigilation systems are successful at catching cheating, there are worries about the privacy and moral ramifications of deploying such systems. Some contend that the application of these systems may violate students' right to privacy and faster a stressful environment that impairs their performance

Automated invigilation systems are becoming more and more popular for spotting irregularities during inspections. These systems employ AI to track and examine the student actions throughout exams, including their head movements, eye movements, and keystrokes in order to find signs of cheating or other irregularities. The educational institutions can monitor the students during academic offline and online examinations, reducing the burden on the exam administrations. The institutions curb incidents of examination malpractice, surveillance and monitoring system can be a reliable and adequate in providing a conductive and safer environment for the students and the staff at the examination hall.

The proposed system for detection of suspicious activities during the examination is based on various computer vision algorithms such as Viola Jones and related-Like Feature and AdaBoost algorithms. The head movement and hand contact are based on color and grid manipulation and face tracking using the trained dataset. The proposed model helps educational institutions, which will be useful in detecting and recognizing cheating activities in the exam hall.

Although AI-based systems are becoming more sophisticated, there is still space for the improvement for their accuracy. Future research and development could help to reduce false positives and ensure for the fair conduction of examinations and exam integrity. As the use of artificial Intelligence in educational settings become more prevalent, it is important to ensure that privacy concerns are adequately addressed. The further work could more focus on developing more robust privacy protections that are built into the Automated Invigilation System. Future work could explore expanding scope of the system to other areas of education, such as monitoring student engagement or detecting plagiarisms in assignments and mitigate potential biases in the system and ensure that it does not discourage certain group of students.

Ultimately, the choice to utilize automated invigilation systems should be carefully considered, taking into account the special conditions and requirements of the educational institution and its students, as well as the potential advantages and disadvantages. To guarantee that such systems are used morally and with regard for students' privacy rights, it is essential to establish them with transparency and explicit standards.

The model of deep learning, the faster RCNN is implemented as a classifier with a training accuracy of 99.5 on the Invigilation dataset and a testing accuracy of 98.5. With a 95% accuracy rate, the faces Recognition module is used to identify and recognize students. Student status reports are generated. The proposed model out performs the current model since it can track more than 100 students at once and requires less computing time to get the required result than previous models. The development of a quicker invigilation system can further enhance the suggested invigilation system.

REFERENCES

[1] Zhang, Xiangyu, Xinyu Zhou, Mengxiao Lin, and Jian Sun. “Shufflenet: An extremely efficient convolutional neural network for mobile devices.” In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 6848-6856. 2018.

[2] Ahmad Salihu Ben-Musa, Sanjay Kumar Singh, Prateek Agrawal, “Suspicious Human Activity Recognition for Video Surveillance System”, International Conference on Control, Instrumentation, Communication and Computational Technologies, Research gate, 2015.

[3] B. C. Amanze, C. C. Ononiwu, B. C. Nwoke, I. A. Amaefule, “Video Surveillance And Monitoring System For Examination Malpractice In Tertiary Institutions”, International Journal Of Engineering And Computer Science, Vol. 5, January 2016, pp. 15560-15571

[4] X. Wang, M. Xia, H. Cai, Y. Gao, C. Cattani, “Hidden-MarkovModels-Based Dynamic Hand Gesture Recognition”, Mathematical Problems in Engineering, pp. 1-10, 2012.

[5] R. Lockton, A.W. Fitzgibbon, “Real-Time Gesture Recognition Using Deterministic Boosting”, Proc. British Machine Vision Conference, pp. 817-826, Sept. 2002.

[6] Paul Viola, Michael J. Jones , “Robust Real time Face Detection, International Journal of Computer Vision”, Vol 57, issue 2, pages: 137-154, 2004

[7] Richard Szeliski, “Computer Vision: Algorithms and Applications”, First Edition, Springer, 2010.

[8] Teddy Co, “A Survey on Behavior Analysis in Video Surveillance for Homeland Security Applications”, IEEE Conference on Applied Imagery Pattern Recognition Workshop (AIPR), Pages: 1 – 8, 2008.

[9] Ren, Shaoqing, Kaiming He, Ross Girshick, and Jian Sun. "Faster r-cnn: Towards real-time object detection with region proposal networks." arXiv preprint arXiv:1506.01497 (2015).

[10] N. Rajesh, H. Saroja Devi, "Emerging trends in video surveillance Applications", International Conference on Software and Computer Applications, vol. 9, 2011.

[11] Neil Robertson, Ian Reid, "A General Method for Human Activity Recognition in Video", Journal of Computer Vision and Image Understanding, Vol. 104, No. 2, pp. 232-248, 2006

[12] Arun, M., E. Baraneetharan, A. Kanchana, and S. Prabu. "Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors." International Journal of Pervasive Computing and Communications (2020).

BIBILOGRAPHY

NOOR SUMAIYA
Assistant Professor, Dept of Computer Science and Engineering, MS, Pursuing PhD from Reva University

NAVYA S K
B.E Student, Department of Computer Science and Engineering

ANJALI R
B.E Student, Department of Computer Science and Engineering

PRIYA N
B.E Student, Department of Computer Science and Engineering

NANDAN A
B.E Student, Department of Computer Science and Engineering