Original Article

A Survey on Suspicious Activity Detection in Examination Hall

Pavan Baile[1], Nandini Sutar[2], Shraddha Shinde[3], Akhilesh Brahmankar[4], Sanjeevkumar Angadi[5], Prasad Dhore[6]

[1,2,3,4]Student, Department of Computer Science and Engineering, Nutan College of Engineering and Research, Talegaon Dabhade, Pune, India

[5,6]Assistant Professor, Department of Computer Science and Engineering, Nutan College of Engineering and Research, Talegaon Dabhade, Pune, India

DOI: 10.47750/pnr.2022.13.S07.912

Abstract

Video monitoring is an ancient technique used for exam hall cheating security. Using deep learning and machine learning in conjunction with existing technology has a stronger influence on society. To increase the capabilities of security systems, we may combine machine learning with video surveillance. This technique will consist of multiple steps, the first being the collection and selection of frames, followed by the ability to apply a pre-set, pretrained machine learning model that can identify, forecast, or detect particular actions or malevolent, immoral phenomena occurring in exam rooms. Proposed system can generate a convolutional neural network-based machine learning model to improve premise security. It has two key functions. First, it will identify and detects head, hands, posture, and so on, which means system can track suspicious students who looking another student paper or using some electronics gadgets second, the network is trained on identifying suspicious activities.

Keywords: EComputer vision, feature extraction, activity recognition, machine learning, deep learning and surveillance cameras.

I. INTRODUCTION

Exams are a necessary component of every educational programme. Academic dishonesty is often dealt with administratively in the classroom or at the institutional level. Cameras are being utilised for surveillance in increasing numbers. Surveillance cameras capture a huge amount of video data. Observing human behaviour and categorising actions can be highly subjective in some situations. Gazing behind or in front of someone, making movements, looking to the side, sharing your response, copying from notes, or carrying a smartphone are all suspicious behaviours. The test environment is made up of a large number of applicants, exam conductors, and guards. Numerous human resources are necessary to keep an eye on the applicants at all times in order to prevent misbehaviour or cheating. This level of focus and concentration cannot always be applied to an exam. As a consequence, this approach for suspicious activity recognition was developed to solve the issue of exam cheating while minimising human effort.

Cheating is becoming more common at all academic levels, including secondary and primary schools. In recent years, computer vision research has shown promising breakthroughs in the field of human activity identification in videos. The importance of digital image processing is demonstrated in a variety of applications, such as remote sensing, video surveillance, video recovery, human-computer interfaces, sports video analysis, home intelligence, and feature extraction.

The proposed study's primary goal would be to infer developing action tags from temporally segmented video sequences. The proposed project includes a complete framework for recognizing and characterising unusual behaviours and activities in exam rooms that encourage cheating. This is accomplished by observing a test video and filming the students. Reputable extracted features is used to optimise the obtained model. Another notable contribution is the study's inclusion of a new dataset on exam cheating. It discusses the most common trying to cheat strategies, such as not trying to cheat, looking at another person's exam paper, swapping exam papers, and use a cheat sheet, and use a smartphone, and gazing at another person's exam paper.

The primary goal of this research is to develop a multimedia analysis system capable of recognising and categorising various behaviours that indicate exam cheating. The model extracts well-known characteristics and scales each dataset frame. To encode the visual occurrences in each frame, a visual language codebook for each type of feature is created. This codebook makes use

of words of various sizes. Finally, the stated attributes are classified using a support vector machine. The proposed dataset is used to demonstrate the utility of the proposed method.

Our machine learning-based project is called Suspicious Activity Detection in Exam Hall. Using the dataset, two training and testing models are generated. During the training phase, the machine learning algorithm model is taught using our unique dataset. We split the dataset to establish training and validation sets. 20% of the photographs in the validation set were chosen at random. Our system is a desktop programme that accepts input in the form of a computer-stored movie. After being divided into frames, the pre-processed data is sent into the model of the machine learning algorithm. Following that, feature extraction methods are used to extract attributes.

II. LITERATURE SURVEY

The literature survey on suspicious activity detection in exam halls typically focuses on the use of computer vision and machine learning techniques to automatically detect and flag suspicious behaviour. This can include the use of cameras to capture footage, image processing algorithms to analyse the footage, and machine learning models to identify patterns of behaviour that may indicate cheating. Some studies have also explored the use of frame processing and trained data recognition to detect cheating or other forms of student nature during exams. Overall, the goal of this research is to develop automated systems that can effectively detect and prevent cheating in exam halls, while also minimizing false alarms and ensuring the privacy of students. In figure 1 shows system architecture of existing work.

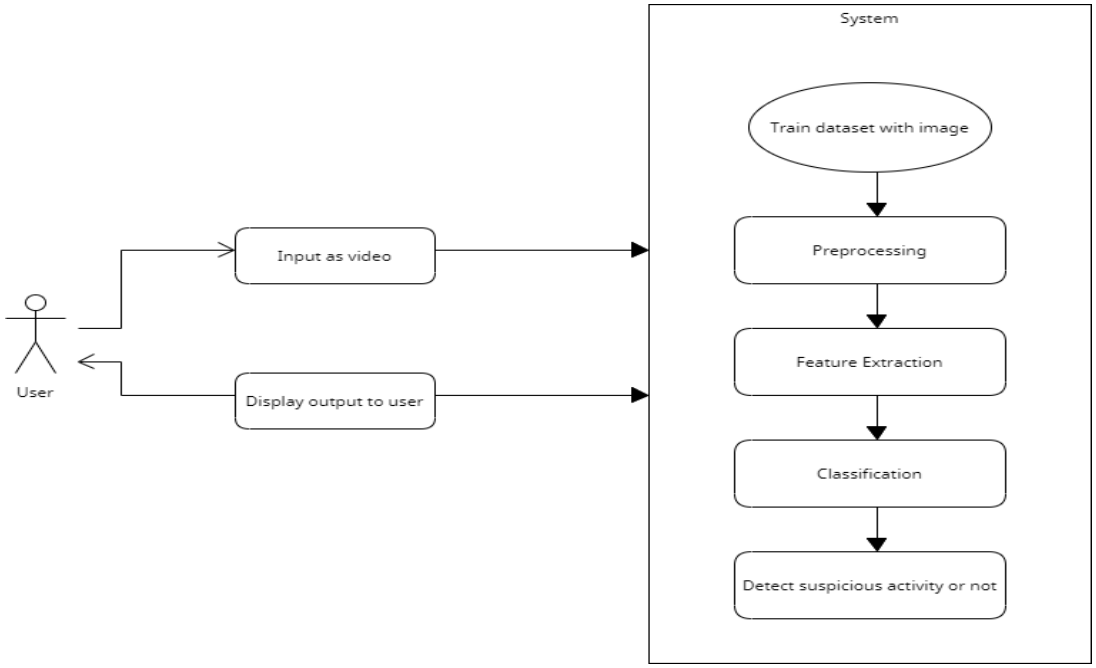

Fig 1. Existing System Architecture

In [1] this study focuses on the issue of test cheating and how it has become a worry in the educational sector. Cheating, according to the authors, has started to spread not only at the university, but also at secondary and elementary levels. The authors recommend combining visual and aural characteristics to detect suspicious conduct during an exam, such as paper showing, cheating from gadgets. These characteristics are then utilised to build a machine learning model capable of detecting cheating in real time. Computer vision-based system for detecting and classifying various actions that are indicative of cheating during an exam. The system is designed to analyse multimedia data, such as video to identify suspicious behaviour that may indicate cheating. The model incorporates pre-processing stages such as trying to scale each of the frames inside the dataset as well as extracting five well-known features to accomplish this. These characteristics are then used to generate a visual vocabulary coding scheme, which is made up of different-sized words that encapsulate the visual incidences in each frame. The proposed approach concludes with the use of a Vector Support Device (SVM) to categorise the specified features. This same

efficiency of the proposed method is evaluated using an examination hall dataset, and the results show that it can detect cheating with such a high level of precision. The authors also discuss potential applications of their method in other fields, such as surveillance and behavioural analysis. The proposed method is a computer eyesight system that detects and categorises cheating during an exam. The system uses feature extraction, a technique that reduces the dimensionality of images by identifying informative parts of the image and compressing them into a feature vector. The researchers obtained five well-known features from the experiments, including Binary Robust Discrete wavelet transform Scalable Crucial (BRISK), maximally stable singularity regions (MSER), as well as Histogram of Oriented Gradients (HOG). These characteristics were extracted from of the proposed dataset's frames, which were designed to depict cheating actions that educators could take during a journal article exam. The features extracted were then utilized to train a machine-learning model capable of real-time cheat detection.

In [2], author provides a technique to prevent cheating behaviour in educational institutions during exams. To prevent unauthorized access, the system evaluates the appearances and probable methods of cheating throughout the exam process and presents a revolutionary anti-cheating solution based on face movement recognition approach. Cheating during exams can be detected using facial expression detection. It assesses performance by administering it to a group of pupils and employing facilities and technology to detect anomalous conduct. The technology detects trying to cheat by focusing on a patient's facial gestures and motions, using a camera system and a camera to observe students' faces during an exam. The camera sends the footage to the detection, which examines it for unusual activity. The system attempts to detect students' faces in the first step. Inside the second step, a specific colour bounding box on all recognised faces can be tracked. Cheating detection is the classification of normal and abnormal student behaviour during an exam. Furthermore, it heavily relies on face recognition to detect any unusual behaviour of a student during an exam.

In [3], author proposed cheating detection system in this study uses video surveillance to monitor students' behaviour during exams, especially abnormal behaviour. The system employs three distinct techniques. one to sense when students' heads move away from of the exam script, somebody to sense whenever a patient's iris moves to duplicate responses from other source materials, and another to sense contact between a patient's face and hands or between individual students, like the sharing of inculpatory materials. Once any of these behaviours is detected, an automatic alerts authority while reducing the failure rate that really can take place with manual monitoring.

In [4], author developed model to identifying suspicious behaviour in examination rooms, a 63-layer CNN model dubbed "L4-BranchedActionNet". The model is based on Vgg with additional branches and was provided with training on the CUI-EXAM dataset. The SoftMax function, entropy coding, and an ant colony system are used for feature extraction and optimization (ACS). The enhanced features are then incorporated in to the SVM and Nearest neighbour classification techniques, with the square meter SVM outpacing the other models with a 0.9299 accuracy. The model was then tested on the CIFAR-100 set of data, and a precision of 0.89796 was obtained, confirming its efficacy. The proposed framework aims to classify students' suspicious activity in examination halls by using surveillance camera footage as input. The methodology is based on computer vision and includes several steps to process the data. Firstly, the images from the dataset are resized and converted to grayscale. This is followed by feature extraction, selection, and classification of the images. To improve the model's accuracy even further, the fused features are chosen using the principal component Analysis method. The features that have been chosen then are classified using a supported vector machine (SVM) and the K-Nearest Neighbour (KNN) algorithm. The proposed method's effectiveness is assessed using a freshly formed dataset.

In [5], author using artificial intelligence and deep learning techniques, a system has been developed to detect and prevent cheating in electronic examinations. The system captures videos of the examinee in real time using a camera and performs functions such as recognising the examinee's identity, presence/absence, numerous individuals, mobile phone use, and monitoring eye movement. Using a dataset of 20 individuals, the system obtained a detection rate of 93.9% for cheating behaviour with a fixed false alarm rate of 5%. E-learning is a type of education in which students access instructional resources outside of regular classrooms by using the internet and technology. It provides cost savings, flexibility, and student progress tracking. However, as the coronavirus epidemic has expanded, e-learning and electronic assessments have grown more common, leading to a rise in cheating during electronic tests. This has harmed the credibility of e-learning as well as the reputation of educational institutions. Using a camera, a method has been developed to monitor student behaviour and identify cheating during online tests. The system employs Python libraries to validate the student's identification, identify mobile phone use, detect the presence of numerous persons in the exam room, and other functions. The objective is to develop a completely automated, cost-effective and non-intrusive monitoring system.

In [6], author proposed research work aims to detect cheating activities in examination halls using video surveillance. The proposed system accomplishes this by extracting interest points and matching corresponding features using the SURF (Higher Speed Robust Features) method. Viola Jones item detectors are employed to locate faces, as well as monitoring algorithms are

employed to track the sensor in the video sequence. Message labelling is used to prevent false categorization if the sensors as well as monitoring algorithms fail to record the faces. The proposed methods are fast and robust. The system detects faces and hands using object detection algorithms and tracks their locations using tracking algorithms. To detect suspicious activity, the key points of two or more relevant images are also used. If any dubious activity is observed, the system will recognize the subjects' hands and faces and send an alarm to the invigilators. This system is a pioneer in real-time supervision of students during exams and eliminates the need for human supervisors. Traditional systems for recognising human activity were good for basic actions but not for complicated ones, and they were unsuitable for real-time activities, contemporary high-dimension movies, and noisy and multiple subject recognition. Examination malpractice or cheating is a dangerous practice that can have negative effects on society, including unqualified personnel, future condemnation, dishonest and corrupt minds, and unproductive brains. The system is expected to help detect and prevent cheating activities such as bringing exhibits, suspicious activities, use of electronic gadgets, verbal communication, and inscription.

In [7], the author proposes a real-time cheat detection system that uses live video to monitor students throughout written examinations for banned activities and gestures such as giving codes, staring at friends, using cheat sheets, chatting, and swapping papers. During the video's playback, the algorithm detects cheating motions and provides textual explanations based on them. The system is separated into two parts: a gesture detection model which is based on 3DCNN plus XGBoost, and an LSTM network-based sentence generation model. The gesture recognition model has a word accuracy of 95.3% and a Kappa value of 0.760 for single subject and interaction description phrases, respectively, with an average edit distance of 1.076 and 3.305. On a mid-range laptop, the system operates at 32.54 frames per second. The system consists of two stages gesture recognition and natural language creation, which are linked by a succession of gesture data representation. The gesture recognition model has a word accuracy of 95.3% and a Kappa value of 0.760 for single subject and interaction description phrases, respectively, with an average edit distance of 1.076 and 3.305. The system runs at 32.54 frames a second on a mid-range laptop. In the future, the system will be enhanced to detect cheating in scenarios involving and over two people.

In [8], this study authors goal is to create a model for monitoring and controlling unethical behaviour in real-time exams. The proposed system employs deep learning techniques such as Faster Regional Deep Neural Network (Deep convolutional neural) for suspicious behaviour detection system based on head movements and Inter Cascaded Convolutional Neural (MTCNN) enabling recognition of faces for student identification. The accuracy of training is 99.5%, while the accuracy of testing is 98.5%. During tests, the model detects and monitors more than 100 pupils in a single frame. The proposed invigilation method might be utilised in colleges, colleges, or schools to detect and track suspicious students' behaviour and to prevent cheating. The suggested approach is an Automatic Invigilation System that detects and records unethical behaviour during offline examinations. The proposed invigilation method might be utilised in colleges, colleges, or schools to detect and track suspicious students' behaviour and to prevent cheating. The method is used to monitor student activity during tests and categorise any unethical conduct as cheating based on head movements such as glancing left, right, up, or peering at other papers. Only when the student's head is inclined downward, suggesting that they are focusing on the exam, is a no-cheating label provided.

In [9], this research work author focuses on the area of suspicious human activity recognition from surveillance video in the exam hall. The objective is to develop an intelligent surveillance system that can watch human actions in real time, classify them as normal or strange, and produce alarms. The paper reviews the state-of-the-art in this field, discussing the various challenges and issues related to recognizing suspicious activities such as cheating, speaking with other candidates, and changes in position. It also goes through the many phases in identifying human activity in surveillance footage, such as foreground extraction, detection, feature extraction, categorization, activity analysis, and recognition. The system is designed to detect suspicious activities such as cheating in the exam hall, speaking with other candidates, changes in position. This study offers a surveillance video-based method for detecting suspicious actions in an examination hall. The technology monitors candidates' movements and use face recognition to detect candidates who engage in suspect behaviour such as cheating. The algorithm collects facial traits, matches them to applicants presently taking the exam, and uses a red box to show the suspect's name and details on the video frame. The information on the suspect is also saved in the system for future use.

In [10], author developed deep learning techniques, this research study focuses on identifying and recognising odd actions in an academic setting such as examination rooms. Automatic Odd Action Recognition (AUAR) is a proposed method that uses motion-based frame extractor to extract keyframes and a supervised neural algorithm to recognise odd behaviour. The assessment demonstrates that the proposed model beats existing techniques for unusual activity identification and performs well on diverse datasets.

In [11], author using convolutional neural networks and a camera, the proposed system can recognise suspects' faces and detect suspicious activity in public places. The system employs HAAR Cascade to rapidly train the neural network for face detection, and the detected faces are compared to previous images. The system extracts frames and employs a similar approach with

convolutional neural networks to identify and label the activity as normal or suspicious. For increased security, the two networks can operate independently and concurrently.

In [12], author proposed system is capable of identifying faces of suspects and detecting suspicious activities in public places using convolutional neural networks and a camera. The system uses HAAR Cascade to quickly train the neural network for face detection and matches the detected faces with previous images. For suspicious activity detection, the system extracts frames and uses a similar approach with convolutional neural networks to identify and label the activity as normal or suspicious. The two networks can work independently and simultaneously for improved security.

In [13], author developed detecting unusual behaviour of students in the examination hall is an important aspect of surveillance. This task is made more difficult by factors such as seating arrangement and strength. One of the most modern tools for spotting strange behaviour in the test hall is video monitoring. This setting works effectively to focus on everyone when combined with a high-density camera. This study looks at ways for identifying anomalous students' behaviour in the test room, which can help avoid cheating. By giving notifications to officials, anomalous equipped systems that employ video analytics prevent dangers from becoming critical. These techniques also help to prevent having a supervisor inside the hall. In addition, the technology recognises anomalous examinees in the test hall. Reduces the workload of an invigilator and offers evidence of cheating.

In [14], author proposed the goal of this study is to create a system that uses automated video surveillance to monitor and identify students who commit malpractice during an offline examination. The system is broken down into three modules: i) Impersonation detection using PCA-based face recognition and image registration to determine a student's presence or absence. ii) Based on mouth state, detection of facial malpractices such as conversations or attempts to obtain unauthorised information. iii) Detecting illegal materials or devices by training the system on positive samples and analysing a top view camera feed. When suspicious activities are detected, the system notifies the administration, lowering the error rate of manual monitoring. This work advances previous research on detecting suspicious activities in offline examinations.

In [15] today's environment, video surveillance is vital, utilising new technologies like artificial intelligence, deep learning, or deep learning to identify suspicious behaviour from live footage. Detecting abnormal human behaviour is one of the most difficult aspects of this. Deep learning is used in academic settings to detect suspicious activity, and an alert is sent to the appropriate authority if suspicious activity is predicted. The monitoring technique comprises analysing successive video frames, as well as the system is separated into two components. The first computes characteristics from video frames, and the second analyses these features to determine whether the behaviour is suspicious or typical.

In [16] author, mentioned exam proctoring, or the monitoring of students' activities during an exam, can be a difficult and costly task for supervisors. Keeping an eye on all students at once is challenging, making automatic exam activity recognition an important and active field of research. In this research, a deep learning approach is used to categorize students' activities during an exam. L2-GraftNet is a novel deep CNN architecture that combines the qualities of both AlexNet and SqueezeNet. The model is updated from AlexNet initially, and then the SqueezeNet architecture is inserted at two points inside the changed AlexNet architecture. The CIFAR-100 dataset is used to train the model, and the features are retrieved and optimised using the Atom Searching Optimization technique. These refined features are then fed to several SVM and K - nearest neighbours classifier variations, with the Course KNN classifier achieving the greatest result with an efficiency of 93.88%. This suggested categorisation lays the groundwork for automated test 12th century without the need for profs in test halls, and the findings confirm the framework's resilience.

Security [17] is very important today because of the increase in unethical and anti-social activities. Organizations use CCTV cameras to constantly monitor people and their movements. A lot of video data is generated all the time, but it's impossible for humans to watch all of it all the time. It's too time-consuming and requires a lot of people. So, we need to find a way to do it automatically. We also need to be able to see which parts of the video show unusual activity, so we can quickly tell if something is abnormal. This can be done by breaking the video into individual frames and analysing the people and their actions in each frame. Machine learning and deep learning can help us do this.

The [18] proposed system uses surveillance camera footage to discuss the use of human activity recognition, specifically anomaly detection, in security systems. The task of manually detecting abnormal activity is too time-consuming and difficult, but it can be reframed as an anomaly detection problem. To identify normal human activities, an automated activity recognition system is required, but high accuracy can be difficult to achieve due to the complexity and diversity of human actions. A CNN-based methodology is proposed for classifying and detecting suspicious activities in live or stored videos, which will improve safety and security in the premises under surveillance.

In [19] author explain today's world, abnormal activity can indicate threats and risks to others, so it is necessary to have intelligent video surveillance systems in place to detect these anomalies. One method is to employ artificial intelligence, deep learning, and deep learning techniques to differentiate between regular and suspicious behaviour in live video. A deep learning technology is utilised in an academic context to detect anomalous behaviour and deliver an alert message to authority if suspicious behaviour is expected. The system is divided into two parts: first, characteristics are collected from frames, and then, based on the recovered features, a classifier determines whether behaviour is suspect or normal. The suggested method has a 95.3% accuracy rate and may be employed in both indoor and outdoor academic contexts. The project's goal is to use CCTV video to detect and warn campus security to questionable activities. The system extracts characteristics from frames using CNN and classifies them as abnormal or normal using LSTM architecture. When suspicious behaviour is discovered, the system sends an Alert message to officials using Python and an open-source platform. The system also uses Twilio, a communication platform, to send and receive SMS programmatically.

The [20] article proposes a clever technique for detecting cheating in online tests by tracking students' eye-gaze and head-pose using their camera. By analysing these elements, the system can determine if a student is attempting to cheat. The goal is to address the issue of widespread cheating that occurs in online exams due to the lack of in-person invigilation during the COVID-19 pandemic.

III. Conclusion

Exam cheating is a big issue in the educational industry. Because many instructors and educators are concerned about the emergence of cheating as well as the failure of detection techniques, the current proposal is designing a subsystem to identify strange activities in the exam hall for this intent, primarily focused on automatic trying to cheat detection in tests. The proposed method has the potential to just be extremely useful in academic institutions in monitoring students throughout academic offline assessments, hence reducing the burden on exam administrators. Several malpractices are detected by the system, including impersonation identification, discussion between examinees, and detection of incriminating evidence. This technology may be expanded to identify and comprehend student behaviours in the test hall. The suggested technology will be able to detect whether or not any suspicious behaviour is going place. Examiners will be able to detect students' cheating behaviour during exams using this programme.

REFERENCES

1. F. Hussein, A. Al-Ahmad, S. El-Salhi, E. Alshdaifat, and M. Al-Hami, “Advances in contextual action recognition: Automatic cheating detection using machine learning techniques,” Data (Basel), vol. 7, no. 9, p. 122
2. Salah Sleibi Al-Rawi, Khattab M. Ali Alheeti, Sameera Abdul-Kader, et al. “Cheating monitoring and detection in examination from face movement recognition,” Cite as: AIP Conference Proceedings 2400, 020004 (2022) https://doi.org/10.1063/5.0115539
3. Roa’a M. Al_airaji, Ibtisam A. Aljazaery, Haider Th. Salim ALRikabi, Abdul Hadi M. Alaidi, “Automated Cheating Detection based on Video Surveillance in the Examination Classes” https://doi.org/10.3991/ijim.v16i08.30157
4. Musa Dima Genemo, “Suspicious activity recognition for monitoring cheating in exams,” Proceedings of the Indian National Science Academy (2022) 88:1–10 https://doi.org/10.1007/s43538-022-00069-2
5. Bashar H. Asker Ahmad F. Al-allaf, “Detecting cheating in electronic exams using the artificial intelligence approach,” ISSN: 0974-5823 Vol. 7 No.
6. Prateek Agrawal, Ahmad Salihu Ben Musa, Sanjay Kumar Singh, “Suspicious Human Activity Recognition for Video Surveillance System,” International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/264037010
7. Ahmad Arinaldi and Mohamad Ivan Fanany, “Cheating Video Description Based on Sequences of Gestures,” See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/316350335
8. Mahmood, F, Arshad, J, Ben Othman, M.T, Hayat, M.F.; Bhatti, N, Jaffery, M.H, Rehman, A.U Hamam, H. “Implementation of an Intelligent Exam Supervision System Using Deep Learning Algorithms”, https://doi.org/10.3390/s22176389
9. Aditya Kulkarni, Amit Dhawale, Sagar Kolhe, Amol Sawant, “Suspicious Event Detection in Examination Hall,” International Journal of Science and Research (IJSR) ISSN: 2319-7064 Research Gate Impact Factor (2018): 0.28 | SJIF (2018): 7.426
10. Muhammad Ramzan, Adnan Abid and Shahid Mahmood Awan, “Automatic Unusual Activities Recognition Using Deep Learning in Academia”, Computers,Materials & Continua Tech Science Press DOI:10.32604/cmc.2022.017522
11. Ms. Archana R. Ghuge, Mr. Rushikesh S. Wakchaure, Mr. Sagar D. Wagh, Mr. Parag S. Hude, Ms. Aishwaraya V. Pingale, “ADVANCE SUSPICIOUS ACTIVITY DETECTION,” e-ISSN: 2582-5208 International Research Journal of Modernization in Engineering Technology and Science
12. Rajesh Kumar Tripathi, Anand Singh Jalal, Subhash Chand Agrawal, “Suspicious human activity recognition: a review” Artif sIntell Rev DOI 10.1007/s10462-017-9545-7
13. Charan A, Darshan D, Madhu N, Manjunatha B S. “A SURVEY ON DETECTION OF ANOMALOUS BEHAVIOUR IN EXAMINATION HALL”, International Journal of Engineering Applied Sciences and Technology, 2020 Vol. 5, Issue 2, ISSN No. 2455-2143, Pages 583-588 Published Online June 2020 in IJEAST http://www.ijeast.com
14. G. Sandhya Devi, G. Suvarna Kumar, S. Chandini, “Automated Video Surveillance System for Detection of Suspicious Activities during Academic

Offline Examination", International Journal of Computer and Information Engineering Vol:11, No:12, 2017
15. Amrutha C.V, C. Jyotsna, Amudha J, "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video", Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020) IEEE Xplore Part Number: CFP20K58-ART; ISBN: 978-1-7281-4167-1
16. TANZILA SABA, (Senior Member, IEEE), AMJAD REHMAN, (Senior Member, IEEE), NOR SHAHIDA MOHD JAMAIL1, SOUAD LARABI-MARIE-SAINTE, MUDASSAR RAZA, (Senior Member, IEEE), AND MUHAMMAD SHARIF, (Senior Member, IEEE), "Categorizing the Students' Activities for Automated Exam Proctoring Using Proposed Deep L2-GraftNet CNN Network and ASO Based Feature Selection Approach"
17. P. Rajasekhar Reddy,B. Nirupa, Preetham Kumar, S. Vaishnavi, "SUSPICIOUS ACTIVITIES DETECTION USINGVIDEO ANALYSIS" , Science, Technology and Development Volume X Issue VIII AUGUST 2021 ISSN : 0950-0707
18. S. A. Quadri, Komal S Katakdhond, "Suspicious Activity Detection Using Convolution Neural Network", DOI: 10.47750/pnr.2022.13. S01.151
19. Muthana S. Mahdi, Amer Jelwy Mohammed, Abdulghafor waedallah Abdulghafour, "Detection of Unusual Activity in Surveillance Video Scenes Based on Deep Learning Strategies", Journal of Al-Qadisiyah for Computer Science and Mathematics Vol. 13(4) 2021, pp Comp. 1–9 https://doi.org/10.29304/jqcm.2021.13.4.858
20. Ambi Singh, Smita Das, "A Cheating Detection System in Online Examinations Based on the Analysis of Eye-Gaze and Head-Pose", DOI 10.4108/eai.16-4-2022.2318165