International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 10 | Oct 2024 www.irjet.net p-ISSN: 2395-0072

SUSPICIOUS ACTIVITY DETECTION IN EXAM USING DEEP LEARNING

Amar Kalukhe[1], Siddharthsingh Suryawanshi[2], Manish Ambuse[3], Mahesh Ravaji[4], Prof. Chaitali. A. Deshpande[5]

[1,2,3,4]Student,Department Of Information Technology, Sinhgad College Of Engineering, Pune 411041
[5] Asistant professor,Dept. Of Information Technology, Sinhgad College Of Engineering, Pune 411041

Abstract: Suspicious Activity refers to the identification of specific body parts or joint positions of individuals from images or videos. This project aims to detect unusual human behavior in real-time using CCTV footage by leveraging neural networks. The recognition of suspicious activities has been a significant challenge in computer vision for over 15 years. This area of study is crucial due to its wide range of applications, such as video surveillance, animal tracking, understanding behavior, detecting sign language, enhancing human-computer interaction, and enabling markerless motion capture. While low-cost depth sensors have limitations, primarily suitable for indoor settings, their low resolution and noisy data hinder effective human pose estimation from depth images. To address these challenges, we propose utilizing neural networks. The recognition of suspicious behavior in surveillance videos is a dynamic research field within image processing and computer vision. Through visual monitoring, human activities can be observed in critical public spaces such as bus terminals, train stations, airports, banks, shopping centers, educational institutions, parking lots, and roadways to deter threats like terrorism, theft, accidents, vandalism, and other criminal activities. Since it is impractical to monitor these areas continuously, intelligent video surveillance systems are needed to assess human activities in real-time, distinguishing between normal and abnormal behaviors while generating alerts. Most current research focuses on still images rather than videos, and there is a noticeable gap in studies employing convolutional neural networks (CNNs) for detecting suspicious actions.

Keywords: Suspicious Activity, Neural Networks, Image Processing, Surveillance Video.

1. INTRODUCTION

In today's digital era, the importance of public safety has surged, with intelligent video surveillance systems playing a crucial role. The ability to detect and predict suspicious human activities from real-time CCTV footage has become a primary focus of research in computer vision and artificial intelligence. This paper investigates the various applications of neural network technology in addressing the significant challenge of detecting suspicious behavior, particularly within the context of video surveillance.

Overcoming Limitations of Depth Sensors: While low-cost depth sensors have advanced human pose estimation, their drawbacks—such as being limited to indoor settings and providing low-resolution, noisy depth data—are evident. This study proposes a new method that employs neural networks to overcome these challenges, leading to improved accuracy and robustness in human pose estimation.

Real-World Applications: This research specifically targets the recognition of suspicious human activity in video surveillance, a field that is rapidly evolving within image processing and computer vision. Through effective visual monitoring, human behavior in key public areas, including transportation hubs, retail spaces, and educational institutions, can be scrutinized. This proactive approach acts as a deterrent against a variety of threats, from terrorism and theft to accidents and other unlawful activities.

The Need for Intelligent Video Surveillance: Continuous manual monitoring of public spaces is a significant challenge. This research advocates for the implementation of intelligent video surveillance systems that utilize neural networks for real-time observation and classification of human activities as normal or suspicious. These systems are also designed to issue alerts, enabling swift responses to any detected anomalies.

2. PROBLEM STATEMENT

Detecting Suspicious Activity And Behaviour In Examination

3. MOTIVATION

The Suspicious Activity Detection System (SADS) employs Convolutional Neural Networks (CNNs) for video analysis, specifically designed to enhance security measures in examination settings. Traditional monitoring methods often fall short in effectively identifying irregular behavior, making it essential to integrate advanced AI and deep learning technologies. SADS aims to provide a proactive and intelligent solution that exceeds conventional surveillance techniques. By harnessing the capabilities of CNNs, which excel at recognizing patterns and anomalies in visual data, this system can automatically detect suspicious activities that may go unnoticed during exams.

The primary objective of SADS is to promote academic integrity, protect the examination process, and ensure a fair testing environment by enabling rapid identification of potential misconduct. Whether implemented in crowded exam halls or controlled testing environments, this innovative system offers the promise of a more secure atmosphere, ultimately contributing to the integrity and peace of mind of students and educators alike. In a time when maintaining fairness in assessments is crucial.

4. SYSTEM ARCHITECTURE

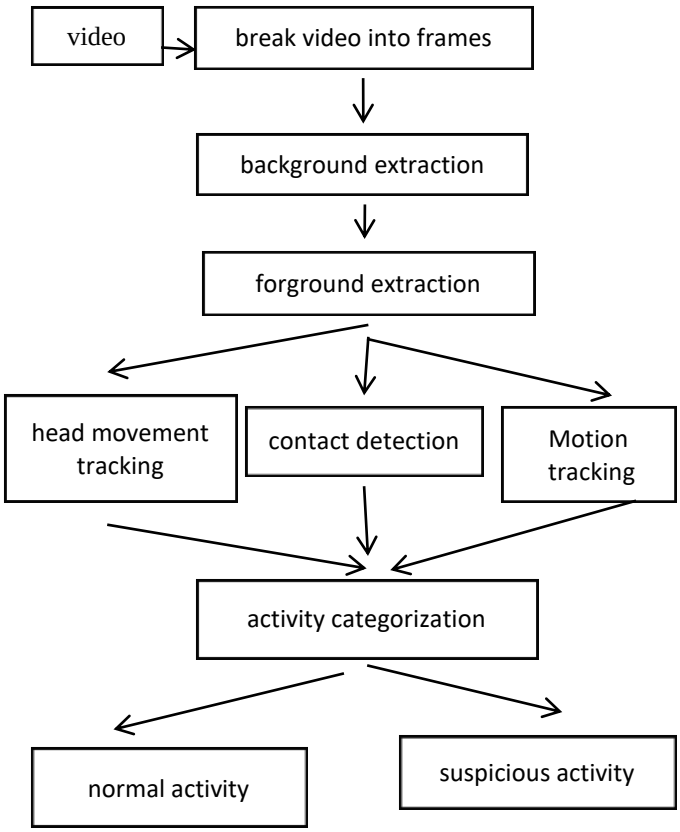

Fig 1. Flow Chart 5.

METHODOLOGY

The approach of this project follows a structured and iterative process, starting with the collection and preprocessing of data. Surveillance video datasets will be acquired to train and validate deep learning models, with preprocessing applied to improve data quality and relevance. The main focus is on developing and training deep learning models, such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs), to detect and classify various activities in surveillance footage. Transfer learning techniques may be used to enhance efficiency by utilizing pre-trained models. Anomaly detection systems will be incorporated to recognize unusual patterns or behaviors. Real-time processing capabilities will be emphasized to ensure the system operates effectively in dynamic environments. The solution will also be designed to scale, enabling it to process data from multiple surveillance cameras simultaneously. A key step will be integrating the system with existing surveillance infrastructure for smooth deployment. Throughout development, thorough testing and validation processes will be conducted, with models fine-tuned based on performance results. Ethical considerations, such as privacy and regulatory compliance, will be integral to the methodology. Continuous feedback and improvements will be incorporated to create a flexible and effective approach for developing and deploying the deep learning-based system for detecting suspicious activity.

6. PROPOSED ALGORITHM

Real-World Input Video: The process starts with receiving a video stream from a real-world environment, such as footage from a security camera.

Segmenting Video into Frames: The video is then broken down into individual frames, with each frame representing a still image.

Background Extraction: In this phase, static elements like walls and floors are isolated and extracted from each frame to identify the background.

Foreground Extraction: Once the background is removed, dynamic elements such as people or vehicles remain as the foreground.

Motion Tracking: The movement of foreground objects is tracked over time, allowing for the identification of their paths and trajectories.

Head Motion Detection: This step focuses on detecting head movements, particularly useful for tracking people's head motions within the scene.

Contact Detection: This identifies when interactions or contacts occur between objects, such as a person touching an object or interacting with another individual.

Activity Classification: The system uses the results from motion tracking, head motion detection, and contact detection to classify the overall activity in the scene, often with the help of machine learning algorithms.

Normal Activity: When behavior is classified as "normal," it indicates that the actions match typical, expected patterns, such as walking or standing.

Suspicious Activity: If the behavior is categorized as "suspicious," it suggests a deviation from normal patterns, such as running, fighting, or other potentially dangerous or unusual actions.

7. LITERATURE SURVEY

Sr No.	Publication Details	Seed Idea	Drawbacks
1	Nishchal J, Sanjana Reddy, Navya Priya N, "Automated Cheating Detection in Exams Using Posture and Emotion Analysis ", 2020.	introduces an AI-driven system designed to identify dishonest behavior by assessing students' body language and facial expressions, with the goal of enhancing exam fairness through automated surveillance	The system encounters issues related to privacy, the possibility of false positives, and restricted precision in emotion recognition, along with potential biases in facial recognition, which could affect its reliability and fairness
2	Muhammad Asad, Ahmed Hafeez, Muhammad Asif, Mateen Abbas, Ms. Munazza Sadaf, Asim, Muhammad Ahsan UL Haq "SUSPICIOUS ACTIVITY DETECTION DURING PHYSICAL EXAMS", SSRN, 15, 2013, 4676389.	The seed idea to develop an automated system that leverages deep learning algorithms to detect and prevent cheating during physical exams.	Storing and processing video data of students requires robust data security measures to prevent unauthorized access and potential breaches.
3	Jyotsna Chandran, Amudha Joseph, Amrutha C.V "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video", IEEE International Conference, 6, 2020.	The core idea is to enhance the accuracy and efficiency of detecting suspicious activities, with a specific application focus on academic environments.	Lack of discussion on scalability: It does not address the scalability of the proposed method to handle extremely large video datasets.
4	Md Adil, Rajbala Simon, Sunil Kumar Khatri, "Automated Invigilation System for Detection of Suspicious Activities during Examination," IEEE International Conference, 2024.	This paper aims to detect and identify unfair or suspicious activities, such as cheating behaviors like whispering, impersonation, or hand contact, thereby ensuring the integrity and fairness of the examination process.	The proposed algorithms, including Viola-Jones and AdaBoost, might be limited in their ability to detect all types of suspicious activities.
5	Sushmita Mishra, Roopikha S, Roshini S, Rithika S "Automatic Cheating Detection In Exam Hall," Research Gate, 2023.	This paper is designed to be more reliable and efficient than traditional human invigilation, achieving 88.03% accuracy in detecting cheating.	YOLOv3 and residual networks may not detect all types of suspicious activities, potentially missing some cheating behaviors and reducing overall effectiveness.

8. CONCLUSION

The proposed subsystem for automatic cheating detection in exam halls, which analyzes real-time video footage, shows great potential for tackling the issue of exam cheating. By utilizing advancements in suspicious activity detection, this system provides a thorough solution for monitoring student behavior during in-person assessments. Its ability to detect different forms of cheating reduces the reliance on human supervision and improves the efficiency of administrative efforts. Ongoing research in related areas can further boost its accuracy and usefulness, making it an essential tool for upholding academic integrity.

9. ACKNOWLWDGEMENT

I would like to express my heartfelt gratitude and sincere appreciation to my esteemed mentor and guide, Prof. C. A. Deshpande, Assistant Professor in the Department of Information Technology at Sinhgad College of Engineering, Pune-41. His technical guidance, continuous encouragement, and constructive feedback have been a constant source of motivation, pushing me to strive for excellence throughout this project.

REFERENCES

[1] Nishchal J, Sanjana Reddy, Navya Priya N, "Automated Cheating Detection in Exams Using Posture and Emotion Analysis, "IEEE International Conference, 2020.

[2] M. Asad, A. Hafeez, M. Asif, M. Abbas, M. Sadaf, A. Asim, and M. A. U. Haq, "Suspicious activity detection during physical exams," SSRN, vol. 15, no. 4676389, 2013.

[3] J. Chandran, A. Joseph, and A. C. V., "Deep learning approach for suspicious activity detection from surveillance video," IEEE International Conference, vol. 6, 2020.

[4] M. Adil, R. Simon, and S. Khatri, "Automated invigilation system for detection of suspicious activities during examination," IEEE International Conference, 2024.

[5] S. Mishra, R. S., R. S., and R. S., "Automatic cheating detection in exam hall," ResearchGate, 2023.

[6] Q. Chen, C. Zhang, W. Liu, and D. Wang, "Surveillance human pose dataset and performance evaluation for coarse-grained pose estimation," Athens, 2018.

[7] N. U. Khan and W. Wan, "A review of human pose estimation from single image," IEEE, 2018.

[8] P. Bhagya Divya, S. Shalini, R. Deepa, and B. Sravya Reddy, "Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras," International Research Journal of Engineering and Technology (IRJET), December 2017.

[9] Y. Yang, J. Sun, H. Li, and Z. Xu, "Deep ADMM-Net for compressive sensing MRI," in Advances in Neural Information Processing Systems, pp. 10–18, 2016.

[10] E. Eksioglu, "Decoupled algorithm for MRI reconstruction using nonlocal block matching model: BM3DMRI," Journal of Mathematical Imaging and Vision, vol. 56, no. 3, pp. 430–440, 2016.

[11] U. M. Kamthe and C. G. Patil, "Suspicious activity recognition in video surveillance system," in Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018.