© June 2025 | IJIRT | Volume 12 Issue 1 | ISSN: 2349-6002

Suspicious Activity Detection in Exam Using Deep Learning

Manish Ambuse[1], Siddharthsingh Suryawanshi[2], Amar Kalukhe[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 detection involves analyzing images or video streams to identify specific joint positions or body part movements in individuals. This project explores how neural networks can be applied to identify unusual or abnormal human behavior from CCTV footage. Over the past fifteen years, detecting such activity has remained a complex issue in the field of computer vision. The relevance of this area is reflected in its many applications, including public surveillance, animal observation, behavior interpretation, sign language detection, hands-free motion tracking, and human-computer interaction enhancement.**

Despite advancements in depth-sensing technologies, affordable sensors still face challenges due to their limited suitability for indoor environments and their tendency to produce low-resolution and noisy output. These factors reduce their effectiveness in estimating human posture from depth imagery. To overcome these shortcomings, this research integrates neural network approaches aimed at improving detection efficiency and accuracy.

Such systems are particularly valuable in monitoring human activity in sensitive or high-risk public locations like airports, schools, banks, bus stands, railway stations, shopping malls, roadways, and parking areas. By supporting efforts to identify potential threats such as theft, violence, accidents, or vandalism, these surveillance tools enhance safety and security. Manual observation alone is insufficient for thorough monitoring, which makes intelligent surveillance systems necessary for evaluating and flagging unusual behaviors. Although there has been significant work done using still images, there remains a noticeable gap in leveraging convolutional neural networks (CNNs) for analyzing video data to detect suspicious actions

***Index Terms*—Activity Recognition, Neural Networks, Surveillance Footage, Anomaly Detection.**

1. INTRODUCTION

In the current digital landscape, ensuring public safety has become increasingly critical, with advanced video surveillance technologies taking on a pivotal role. One major area of interest in both computer vision and artificial intelligence is the identification and interpretation of suspicious human behaviors captured through CCTV systems. This paper explores how neural network-based methods can effectively tackle the ongoing challenge of identifying unusual activities within surveillance contexts.

Addressing Depth Sensor Limitations: Although budget-friendly depth sensors have contributed to the field of human pose estimation, they often come with inherent drawbacks. These include restricted usage in indoor environments and the generation of low-quality, noisy data. To mitigate such limitations, the approach discussed here integrates neural networks to enhance the precision and resilience of pose estimation systems.

Broader Use Cases: The core focus of this study lies in detecting unusual human actions captured through surveillance, a domain that is growing rapidly within the fields of image analysis and computer vision. By leveraging such systems, it becomes possible to monitor behavior in sensitive public locations like transportation terminals, retail outlets, and academic institutions.

Why Smarter Surveillance is Essential: Manual observation of public environments on a continuous basis poses major practical challenges. This research supports the integration of intelligent surveillance frameworks that rely on neural network models to interpret and categorize human behaviors as either typical or questionable. These systems are also capable of generating alerts, making it easier to take timely action when irregularities are detected.

1. PROBLEM STATEMENT

Suspicious Activity Detection in Exam Using Deep Learning.

2. SYSTEME ARCHITECTURE

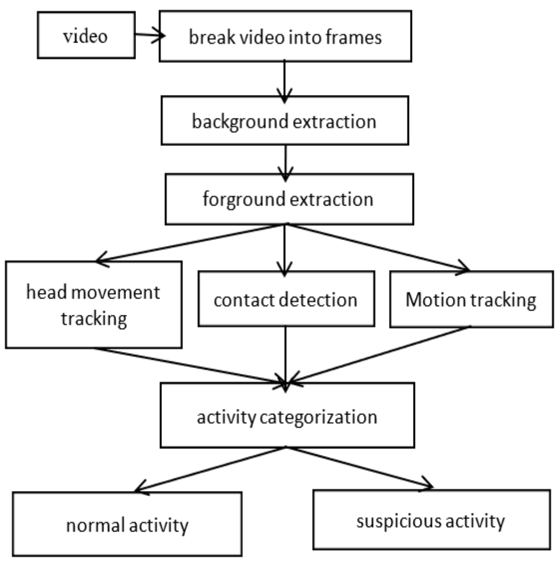


Fig 1. Flow Chart

3. METHODOLOGY

The methodology adopted in this project focuses on detecting suspicious activity through video analysis using Convolutional Neural Networks (CNNs). The system is designed to identify abnormal behavior by analyzing motion patterns, head movements, and contact between individuals within a monitored environment. The overall process is divided into several key stages:

1. Dataset Preparation

A custom dataset was curated specifically for this project, consisting of annotated video frames capturing various classroom scenarios. The dataset includes both normal and suspicious activities, allowing the models to learn relevant patterns and distinctions. Frames were extracted from surveillance-like video footage and labeled based on the type of activity observed, such as head movement, object contact, or motion intensity.

2. Model Development using CNNs

A unified CNN architecture was constructed to simultaneously analyze head motion, body movements, and contact between individuals. Instead of using separate models, a single CNN was trained to learn features from all three activity types in a combined manner. The model was structured to process input video frames and extract spatial and temporal features indicative of suspicious behavior patterns.

3. Training and Evaluation

The model was trained on the prepared dataset. The CNN effectively learned to recognize abnormal patterns based on motion trajectories, excessive head movement, and proximity/contact cues between individuals. Validation during training confirmed that the model generalized well across different activity types.

4. Frame Classification

Each frame was classified as either normal or abnormal based on the detected behavior. Normal frames typically showed minimal movement, proper posture, and no physical interaction. Abnormal frames, on the other hand, were flagged when unusual motion, frequent head movement, or contact between students was detected. These classifications were used to generate alerts and highlight potentially suspicious actions.

5. Testing on New Video

To assess practical effectiveness, the trained CNN model was applied to a separate video that was not part of the training set. The system analyzed the frames and identified activities based on the features it had learned.

6. Output Interpretation

When suspicious activity was detected, the system flagged it for further attention. The outputs from the model were used to ensure a comprehensive assessment, reducing false positives and improving detection reliability. 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.

4. 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.

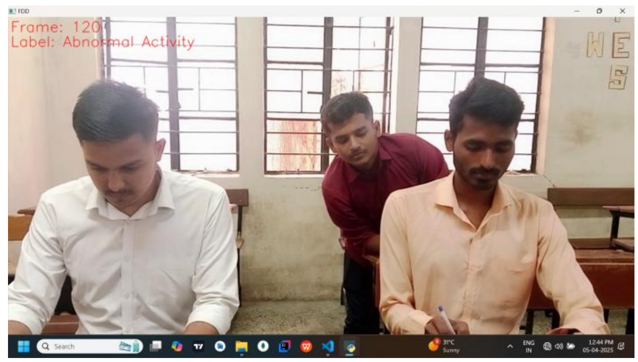
Head Motion Detection: This step focuses on detecting head movements, particularly useful for tracking people's head motions within the scene.

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.

5. RESULT

The proposed system for suspicious activity detection was successfully implemented and evaluated using a custom-prepared dataset and a CNN-based model. The system accurately identified normal and abnormal frames based on behavioral cues. Normal frames showed students sitting steadily with minimal movement, while abnormal frames were flagged when excessive head movement, interaction between individuals, or sudden/unusual motion was observed.



6. CONCLUSION

This project presents an effective approach for detecting suspicious activities in surveillance video by leveraging the capabilities of Convolutional Neural Networks (CNNs). By combining motion analysis, head movement detection, and contact identification within a single model, the system is capable of accurately distinguishing between normal and abnormal behaviors in examination environments. The use of a custom-built dataset further enhanced the relevance and precision of the model, ensuring that it was well-suited to the specific context of exam monitoring.
The trained model was tested on unseen video footage and demonstrated high reliability in identifying potential instances of misconduct. Classification of video frames into normal and suspicious categories allowed for automated alert generation, minimizing the need for manual supervision and improving the overall efficiency of surveillance.
Overall, the system not only contributes to the integrity of academic assessments but also lays the foundation for broader applications in other surveillance scenarios. With continued development, the model can be further optimized and extended to

detect more complex behavioral patterns, making it a valuable tool for intelligent video monitoring systems.

7. ACKNOWLWDGEMENT

We would like to express our heartfelt gratitude to our esteemed mentor and guide, Prof. C. A. Deshpande, Assistant Professor, Department of Information Technology, Sinhgad College of Engineering, Pune-41, for his continuous support and expert guidance throughout the course of this project. His technical insights, constructive feedback, and constant encouragement were instrumental in helping us navigate challenges and stay focused on our goals. We also extend our sincere thanks to all faculty members and peers who supported us directly or indirectly during the development of this project. Their encouragement and cooperation contributed significantly to the successful completion of our work.

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] [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] [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.