International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Anomaly Detection in Video Surveillance Using Machine Learning

Ravi Kumar. K[1], *G. Vamsi Manikanta Teja*[2], *P. Prasanth Reddy*[3], *R. Sushmitha Devi*[4], *C. Venkatesh.*[5]

[1]Assistant Professor, Dept. of CSE, Muthayammal Engineering College, Salem, Tamilnadu, India.
[2,3,4,5] UG Students, Dept. of CSE, Muthayammal Engineering College, Salem, Tamilnadu, India.

ABSTRACT

Anomaly detection in video surveillance is a critical component of modern security systems. This research presents an efficient, real-time video surveillance system capable of detecting abnormal activities using machine learning and computer vision techniques. The system captures video footage, extracts frames, and applies deep learning models to identify behavioral patterns and detect anomalies. Applications include public safety, infrastructure protection, and intelligent monitoring systems. This study introduces an end-to-end pipeline, highlights key challenges, and demonstrates the efficacy of deep neural networks for temporal and spatial anomaly detection. The proposed system achieves high accuracy in diverse conditions and contributes significantly to proactive security enforcement.

Key Words: Artificial Intelligence, Deep Learning, Machine Learning, CNN, Autoencoders, Surveillance Video, Anomaly Detection.

I. Introduction

In an era marked by increasing security challenges, surveillance systems have become indispensable. Conventional surveillance methods often rely on manual observation, which is prone to human error and inefficiency. With the advent of intelligent systems, automated anomaly detection has emerged as a solution to enhance vigilance and responsiveness. This paper presents a machine learning-based video surveillance framework for detecting unusual activities, such as trespassing, theft, or violence. By leveraging deep learning techniques and real-time video analytics, the proposed system ensures scalable, reliable, and continuous monitoring for smart cities, transportation hubs, and sensitive areas.

II. Problem Statement

Traditional surveillance systems are limited by their dependence on human monitoring, leading to oversight and delays in identifying security threats. Additionally, defining a fixed set of 'abnormal' behaviors is challenging due to context-dependent variations. Automated anomaly detection must overcome issues such as occlusions, dynamic backgrounds, and varying lighting conditions. The objective is to create a system that can learn normal behavioral patterns and flag deviations without requiring extensive manual labeling or predefined rules.

III. Objectives

The objectives of this project are:

- To develop a real-time system that can process video feeds and identify anomalous behavior autonomously.
- To use unsupervised and semi-supervised machine learning models (e.g., autoencoders, GANs) for anomaly detection.
- To improve detection accuracy using advanced video analysis and frame- by-frame behavior modeling.
- To enable the system to adapt to new environments and evolving patterns of normalcy.
- To reduce the dependency on human surveillance and improve incident response time.

IV. Sequential Diagram

The system begins by capturing live video footage from surveillance cameras. Each frame is extracted and converted to grayscale for pre- processing. Using object detection and motion tracking techniques (e.g., YOLO, DeepSORT), the system tracks individuals across frames. Behavioral features such as trajectory, speed, and posture are analyzed. These features are passed through an anomaly detection model, which flags

V. System Model and Assumptions:

Data Acquisition: Video footage is collected from static surveillance cameras.

Preprocessing: Includes frame extraction, resizing, noise reduction, and grayscale conversion.

Feature Extraction: Human motion features are extracted using deep learning.

Modeling Normalcy: Autoencoders or predictive CNN-LSTM networks are used to learn normal activity patterns.

Anomaly Detection: Frames that significantly deviate from reconstructed patterns are flagged as anomalies.

Alert Generation: Detected anomalies trigger real-time alerts for security teams.

VI. Implementation:

Data Collection: Datasets such as UCSD Pedestrian, Avenue Dataset, or custom CCTV feeds are used.

Preprocessing: Frames are extracted and converted for model readiness.

Model Training: A convolutional autoencoder is trained on normal activity sequences.

Real-Time Monitoring: The trained model is deployed on edge devices or servers for live anomaly detection.

Output: Alerts and anomaly logs are displayed on a dashboard and stored for forensic analysis.

Module Description:

Data Collection: Acquiring surveillance videos with annotated normal and anomalous events.

Data Preprocessing: Denoising, resizing, and grayscale transformation.

Feature Engineering: Using 2D/3D CNNs and optical flow for spatial- temporal features.

Model Training: Autoencoders or GANs reconstruct expected behaviors; high reconstruction error indicates anomaly.

Visualization: Anomaly scores are plotted; visual alarms highlight suspicious activities.

Frame Extraction: Enables precise frame-wise analysis for event localization.

Gray Scaling: Reduces complexity and emphasizes motion intensity for model accuracy.

Data Acquisition: Video footage is collected from static surveillance cameras.

Preprocessing: Includes frame extraction, resizing, noise reduction, and grayscale conversion.

Feature Extraction: Human motion features are extracted using deep learning.

Modeling Normalcy: Autoencoders or predictive CNN-LSTM networks are used to learn normal activity patterns.

Anomaly Detection: Frames that significantly deviate from reconstructed patterns are flagged as anomalies.

Alert Generation: Detected anomalies trigger real-time alerts for security teams.

VI. Implementation:

Data Collection: Datasets such as UCSD Pedestrian, Avenue Dataset, or custom CCTV feeds are used.

Preprocessing: Frames are extracted and converted for model readiness.

Model Training: A convolutional autoencoder is trained on normal activity sequences.

Real-Time Monitoring: The trained model is deployed on edge devices or servers for live anomaly detection.

Output: Alerts and anomaly logs are displayed on a dashboard and stored for forensic analysis.

Module Description:

Data Collection: Acquiring surveillance videos with annotated normal and anomalous events.

Data Preprocessing: Denoising, resizing, and grayscale transformation.

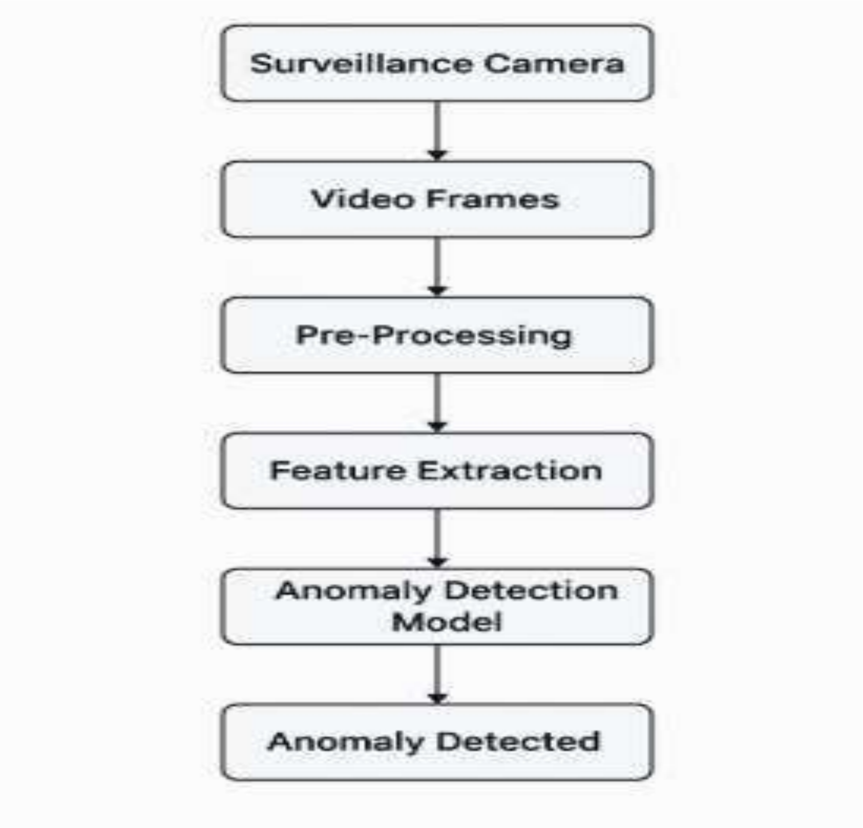
Feature Engineering: Using 2D/3D CNNs and optical flow for spatial- temporal features.

Model Training: Autoencoders or GANs reconstruct expected behaviors; high reconstruction error indicates anomaly.

Visualization: Anomaly scores are plotted; visual alarms highlight suspicious activities.

Frame Extraction: Enables precise frame-wise analysis for event localization.

Gray Scaling: Reduces complexity and emphasizes motion intensity for model accuracy.



1. Surveillance Camera

This is the starting point of the system. Surveillance cameras constantly monitor a designated area and capture live video feeds in real time.

2. Video Frame Capture

The continuous video feed is split into individual frames. These frames serve as snapshots at regular intervals, enabling analysis frame-by-frame.

3. Frame Pre-Processing

Each captured frame undergoes several preprocessing steps:

Grayscale Conversion: Simplifies the image by removing color, focusing on brightness and contrast.

Noise Reduction: Removes visual distortions to improve the clarity of the image.

Resizing: Standardizes the frame size for consistent processing**.**

4. Object Detection & Tracking

Using deep learning models such as YOLO or DeepSORT:

- Object Detection: Identifies humans or moving objects in the frame.
- Tracking: Follows each identified object across multiple frames to observe its behavior over time.

5. **Feature Extraction**

- The system extracts specific characteristics of movement and behavior:
- **Trajectory:** The path taken by each object.
- **Speed:** Rate of movement.

- **Posture/Behavioral cues:** Stance, loitering, erratic motion, etc.

6. Anomaly Detection Model

- This step uses a trained machine learning model (like Autoencoders or LSTM-CNN hybrids):
- It compares current behavior with learned "normal" behavior patterns.
- If current input deviates significantly, it's flagged as potentially abnormal.7.

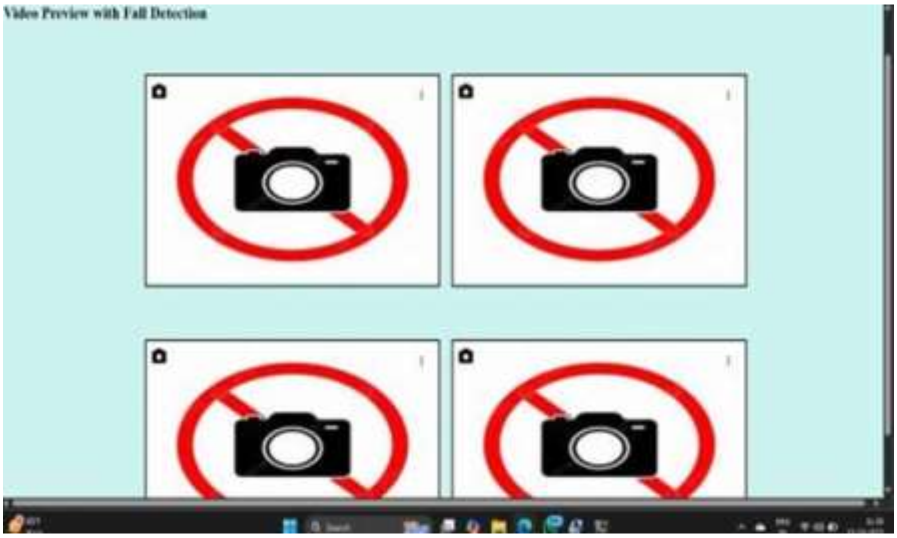
7. Anomaly Evaluation

- The system evaluates whether the observed deviation exceeds a threshold:
- Reconstruction Error or Behavioral Score is calculated.
- If this error is high, it is treated as an anomaly.

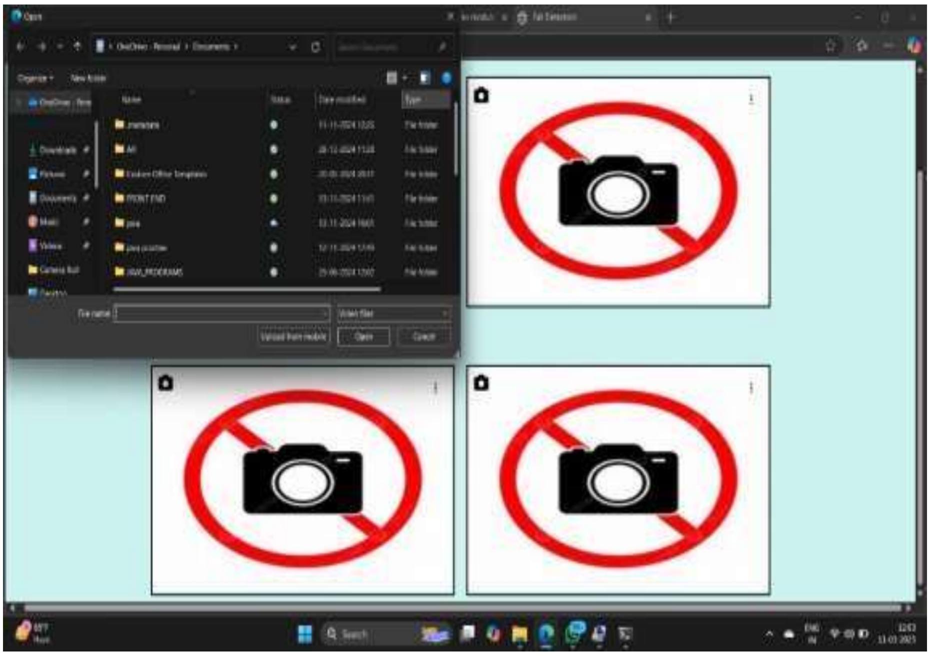
8. **Alert Generation**

- Once an anomaly is confirmed:
- Visual or Audio Alarms are triggered.
- Snapshot or Video Clip is saved for evidence.
- Logs and Notifications are sent to authorities or monitoring teams.

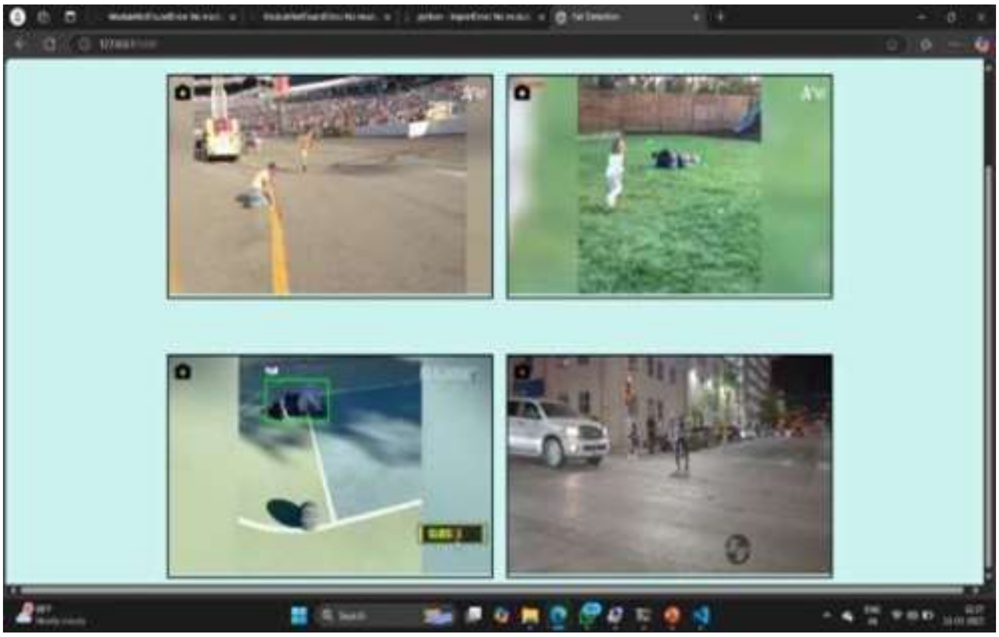
Sample Input:



Video Preview with Fall Detection



Sample out put:



Conclusion

- Anomaly detection in video surveillance using machine learning presents a transformative approach to enhancing security, reducing human monitoring workload, and enabling real-time threat detection. By leveraging advanced algorithms such as deep learning, convolutional neural networks (CNNs), autoencoders, and recurrent neural networks (RNNs), systems can learn normal behavior patterns and efficiently flag deviations indicative of potential anomalies.
- This technology not only improves the accuracy and scalability of surveillance but also adapts over time with continuous learning from new data. Despite challenges such as data imbalance, environmental variability, and real-time processing constraints, machine learning continues to push the boundaries of what's possible in automated surveillance.
- Future research should focus on improving model generalization, reducing false positives, and integrating multimodal data (e.g., audio and thermal imaging) to build more robust and intelligent surveillance systems.
- However, challenges remain, such as:
- **Data Scarcity and Imbalance**: Anomalies are rare, making it difficult to obtain large, labeled datasets for training.

- **Variability in Scenes**: Changes in lighting, weather, and camera angles can affect model performance.
- **False Alarms**: High false positive rates can reduce system reliability and user trust.
- **Real-Time Constraints**: Achieving both accuracy and speed remains a technical hurdle.
- Despite these challenges, the continued evolution of machine learning, especially with the advent of more sophisticated neural architectures and self-supervised learning methods, holds great promise. Future work should aim at developing more generalized and robust models that can adapt to new environments with minimal supervision. Additionally, integrating multimodal data (e.g., audio, thermal, and motion sensors) and focusing on ethical and privacy-preserving practices will further strengthen the applicability of these systems.
- In conclusion, anomaly detection using machine learning is a significant step forward in making surveillance systems smarter, more autonomous, and more effective in ensuring safety and security in an increasingly complex world.

Reference

1. **Sultani, W., Chen, C., & Shah, M. (2018).** *Real-World Anomaly Detection in Surveillance Videos.* In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.
2. **Hasan, M., Choi, J., Neumann, J., Roy-Chowdhury, A. K., & Davis, L. S. (2016).** *Learning Temporal Regularity in Video Sequences.* In *CVPR 2016*.
3. **Ionescu, R. T., Smeureanu, S., Alexe, B., & Popescu, M. (2019).** *Detecting Abnormal Events in Video using Narrowed Normality Clusters.*In *CVPR 2019*.
4. **Lu, C., Shi, J., & Jia, J. (2013).** *Abnormal Event Detection at 150 FPS in MATLAB.*In *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*.
5. **Sabokrou, M., Fathy, M., Hoseini, M., & Klette, R. (2017).** *Deep-anomaly: Fully Convolutional Neural Network for Fast Anomaly Detection in Crowded Scenes. Computer Vision and Image Understanding, 172*, 88–97
6. **Liu, W., Luo, W., Lian, D., & Gao, S. (2018).** *Future Frame Prediction for Anomaly Detection – A New Baseline.* In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.
7. **Ravanbakhsh, M., Nabi, M., Mousavi, H. S., Sangineto, E., & Sebe, N. (2017).** *Abnormal Event Detection in Videos using Generative Adversarial Nets.* In *ICIP 2017*.
8. **Tran, D., Bourdev, L., Fergus, R., Torresani, L., & Paluri, M. (2015).** *Learning Spatiotemporal Features with 3D Convolutional Networks.* In *ICCV 2015*. https://doi.org/10.1109/ICCV.2015.510
9. **Bishop, C. M. (2006).** *Pattern Recognition and Machine Learning.* Springer. ISBN: 978-0-387-31073-2