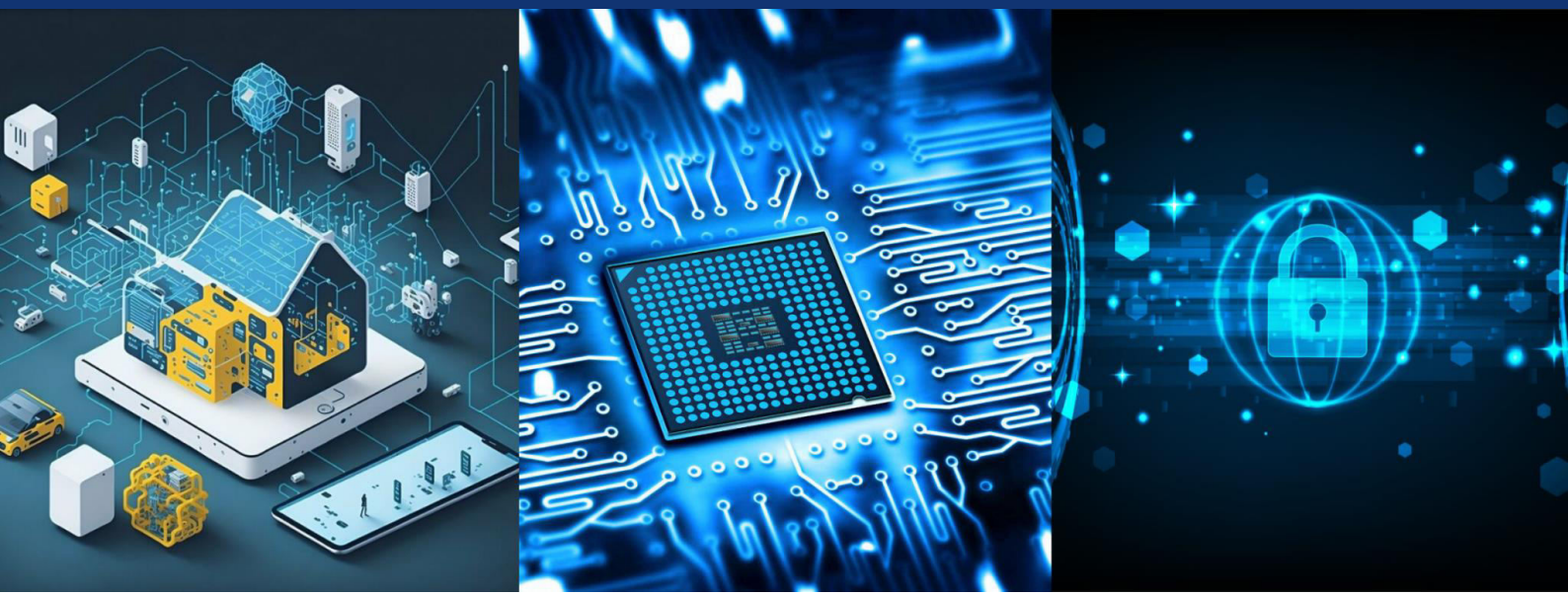
IJIRCCE

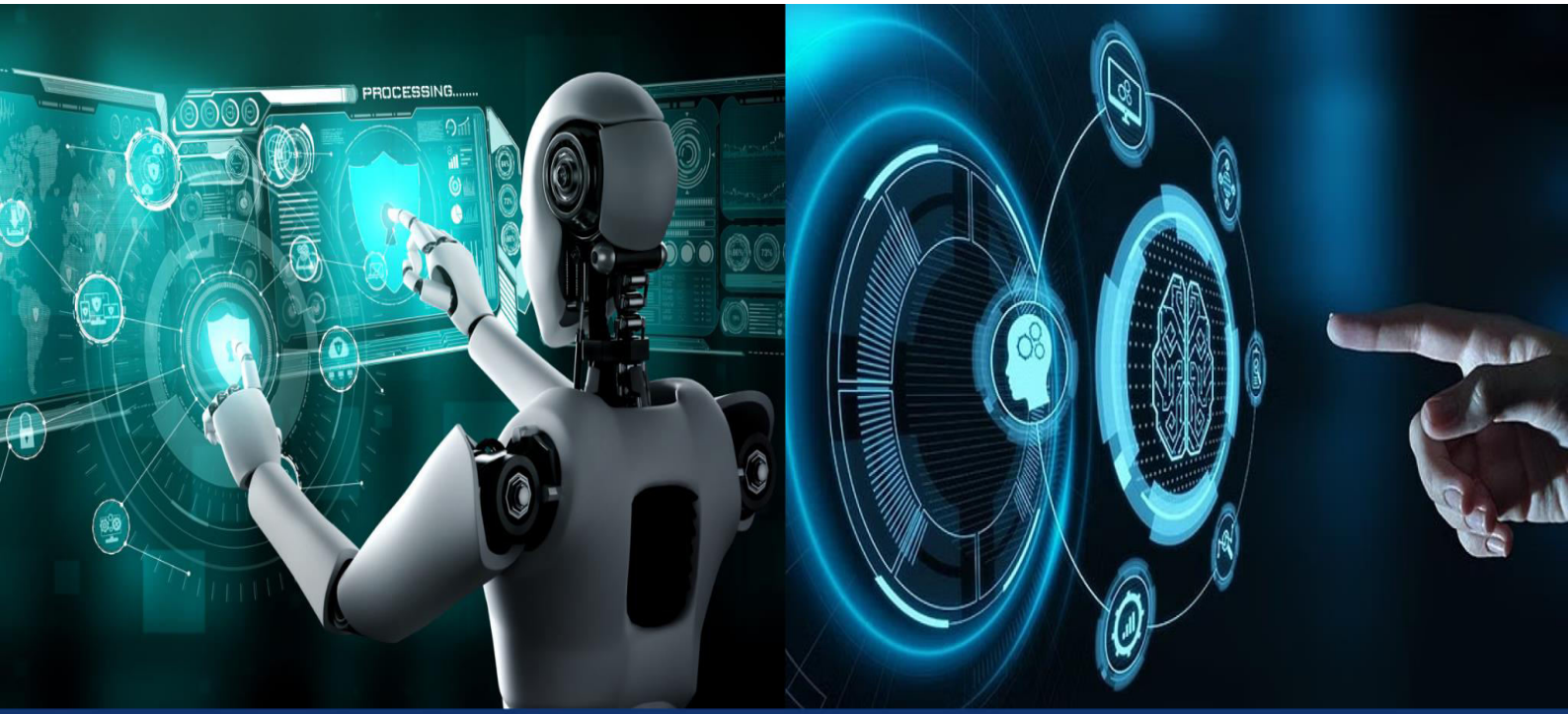
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 14, Issue 4, April 2026

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404088

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

AI Driven Smart Surveillance System for Detecting Rare Events

Kodityala Prasanna Laxmi[1], Haralapur Tanavi [2], Dr.M.Mamatha [3], G.Naga Sujini [4]

Dr. V.Subbaramaiah[5], Dr.K. Rajitha[6]

Student, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Gandipet, India[1,2]

Assistant Professor, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Gandipet, India[3,4,5,6]

ABSTRACT: The Smart Surveillance System for Detecting Rare Events is an intelligent security monitoring solution designed to automatically identify and alert unusual or suspicious activities in real time using computer vision and deep learning techniques. Traditional CCTV systems rely heavily on continuous human monitoring, which can be inefficient and prone to errors. To overcome these limitations, the proposed system integrates advanced object detection using the YOLOv8 (You Only Look Once) model with motion analysis to monitor live camera feeds or recorded surveillance videos. The system provides a user-friendly graphical interface developed using Tkinter, allowing administrators to upload CCTV footage, monitor live feeds, generate frames, and analyze suspicious activities efficiently. The proposed system is capable of detecting multiple rare events such as intrusion into restricted areas, weapon presence, fire incidents, loitering behavior, and possible violent activities. A centroid-based tracking algorithm is used to track detected individuals across video frames and analyze their movement patterns for identifying abnormal behavior. When suspicious events are detected, the system immediately generates alerts through alarm sounds, voice notifications, and automated email alerts to notify the concerned authorities. Additionally, the system improves detection accuracy by applying low-light enhancement techniques for better visibility in poor lighting conditions. All detected events are recorded with timestamps, snapshots, and video references in a database for future investigation and monitoring. With its real-time detection capability, automated alert mechanism, and integrated evidence storage, the proposed system reduces the need for constant human surveillance and enhances overall security monitoring. This solution provides a cost-effective, efficient, and reliable approach for intelligent surveillance in homes, offices, and public environments.

KEYWORDS: Smart Surveillance, Rare Event Detection, Computer Vision, Deep Learning, YOLOv8, Suspicious Activity Detection, CCTV Monitoring, Object Detection, Real-Time Surveillance, Security Alert System.

I. INTRODUCTION

In recent years, the demand for intelligent surveillance systems has increased significantly due to rising security concerns in public and private environments. Traditional Closed-Circuit Television (CCTV) systems are widely used for monitoring areas such as offices, public places, transportation hubs, and residential complexes. However, these systems mainly rely on continuous human supervision to observe video feeds and identify suspicious activities. Continuous manual monitoring can be difficult, time-consuming, and prone to human error, especially when large volumes of video data need to be analyzed. As a result, important events may be missed or detected too late, which can lead to serious security risks.

With the advancement of computer vision and deep learning technologies, automated surveillance systems have become a promising solution for improving security monitoring. Modern object detection algorithms, such as YOLO (You Only Look Once), allow systems to detect and recognize objects in real time with high accuracy. These technologies enable surveillance systems to automatically analyze video streams, identify unusual patterns, and generate alerts without requiring constant human observation. By integrating machine learning techniques with video surveillance, it becomes possible to detect rare and suspicious events more efficiently.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404088

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The proposed Smart Surveillance System for Detecting Rare Events aims to enhance traditional CCTV monitoring by automatically identifying abnormal activities in real time. The system uses the YOLOv8 deep learning model to detect objects such as people and analyze their behavior in both live camera feeds and recorded videos. In addition to object detection, the system incorporates motion analysis and tracking algorithms to monitor movement patterns and identify unusual behaviors such as intrusion into restricted zones, loitering, weapon presence, fire incidents, and possible violent activities.

II. LITERATURE SURVEY

The detection of anomalies in surveilling video-footage has gained considerable importance and interest in research as they play a major role in securing public and private places. [1]Mintu Movi et al. focus on detection of rare patterns through machine learning in CCTV footage within the home premises. The model was meant for detection of normal household movement from an intruder, with the special consideration taken that in distinguishing between a benign behavior in a dynamic environment. Honnegowda et al. suggested the Adaptive Regression for Event Recognition (ARER) model using an optimized regression with deep learning techniques. The system exceeds others like SVMs, decision trees, etc., with respect to a lower false positive count and effective temporal-contextual analysis.

A method based on motion-tracking was developed by Manoj Kumar et al. [3] to classify violent and non-violent activities using the magnitude and orientation of optical flow (MOOF). However, for this system, such high accuracy gets hampered in scenes with overlapping motions and in the presence of a complex background. Pereira and Maia [4] used a Multiple Instance Learning (MIL) framework for anomaly detection across multiple cameras. While increasing F1-scores considerably, it relied on costly infrastructure involving multiple synchronized cameras.

Afnan Alazbah et al. [5] focused on crowd behavior analysis by tracking human movements and classifying them using computer vision and machine learning. The approach worked for crowd situations but had limiting applicability in wide low-density surveillance situations. Siddique et al. [6] introduced a hybrid scheme using CNN-BiLSTM together with attention mechanisms for real-time detection of any hostile activities. The system managed a maximum test accuracy of 83.33%, but it was power-hungry and relatively less suited to resource-constrained settings.

An ensemble learning framework based on different learning models for recognizing abnormal events was attempted by Buvaneswari D [7]. Due to the lack of details on implementation and performance metrics, the entire impact is still unclear. Real-time rare event detection was developed by Singh and Verma [8] using motion pattern analysis. This system exhibited good speed and improved accuracy for detection, albeit it failed in its scalability for vast surveillance networks.

III. PROBLEM DEFINITION

In traditional surveillance systems used in homes, offices, and public spaces, monitoring is mostly passive and depends on continuous human observation. These systems usually record video footage without the ability to automatically analyze or detect suspicious activities in real time. As a result, security personnel must manually review long hours of recorded video to identify important events, which is time-consuming and prone to human error. Due to fatigue or lack of attention, critical incidents such as intrusions or suspicious behavior may be missed or detected late.

Therefore, there is a need for an intelligent surveillance system that can automatically analyze video feeds and detect rare or suspicious events in real time. By using computer vision and deep learning techniques, such a system can improve monitoring efficiency, reduce manual effort, and provide faster alerts to enhance safety and security.

3.1 Disadvantages of Previous Systems

Traditional surveillance systems used in homes, offices, and public spaces have several limitations that reduce their effectiveness in ensuring security. One major drawback is that these systems mainly rely on continuous human monitoring to observe camera feeds and identify suspicious activities. Monitoring multiple cameras for long periods can cause fatigue and loss of attention, which increases the chances of missing important incidents such as intrusions, theft, or abnormal behavior.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Another disadvantage is that most conventional surveillance systems only record video footage without automatically analyzing it. When an incident occurs, security personnel must manually review large amounts of recorded video to find the relevant event. Additionally, many traditional systems use basic motion detection methods that often generate false alarms due to minor movements, shadows, or lighting changes. These unnecessary alerts reduce the reliability of the system and make it difficult to identify real threats. Furthermore, the absence of automatic alert mechanisms means that users or authorities may not be notified immediately during critical situations, leading to delayed responses and potential security risks.

IV. PROPOSED SYSTEM

The proposed system is a Smart CCTV Security System designed to automatically detect suspicious and rare events using computer vision and deep learning techniques. The system analyzes video feeds from either live cameras or recorded videos and identifies activities such as weapon detection, fighting between individuals, intrusion into restricted areas, and fire incidents. Unlike traditional surveillance systems that rely on manual monitoring, the proposed system performs automatic analysis of video frames to detect abnormal activities in real time.

The system uses a deep learning–based object detection model to identify objects such as people and weapons in video frames. By analyzing the number and behavior of detected objects, the system determines whether a suspicious activity is occurring

When a suspicious activity is detected, the system immediately triggers alerts such as displaying notifications in the graphical user interface, sounding an alarm, sending email notifications to authorized users, and saving alert images for future reference.

4.1 Advantages of Proposed System

The proposed system introduces an intelligent surveillance solution capable of detecting suspicious or rare events in real time using computer vision and deep learning techniques. Unlike traditional CCTV systems that depend on continuous human monitoring, this system automatically analyzes video feeds and identifies abnormal activities without manual supervision. The system uses the YOLOv8 object detection model to detect people and objects from live camera feeds or uploaded surveillance videos.

The system is designed to detect several important security events such as intrusion into restricted zones, weapon presence, fire incidents, loitering behavior, and possible fight situations. A tracking algorithm is used to monitor individuals across frames and analyze their movement patterns. If a person enters a restricted area or stays there for an unusual amount of time, the system identifies it as suspicious behavior.

When such events are detected, the system immediately generates alerts through alarm sounds, voice notifications, and automated email alerts. Additionally, detected events are stored with timestamps and images in a database for future reference.

V. DESIGN AND METHODOLOGY

5.1 Process flow Diagram:

The proposed smart surveillance system is designed using several layers that work together to detect suspicious activities from video data. The video input layer captures video streams from cameras, webcams, or uploaded video files and acts as the entry point of the system. After capturing the video, the pre-processing layer improves the quality of the frames through operations such as frame extraction, image resizing, and noise reduction to make the data suitable for analysis.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404088

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

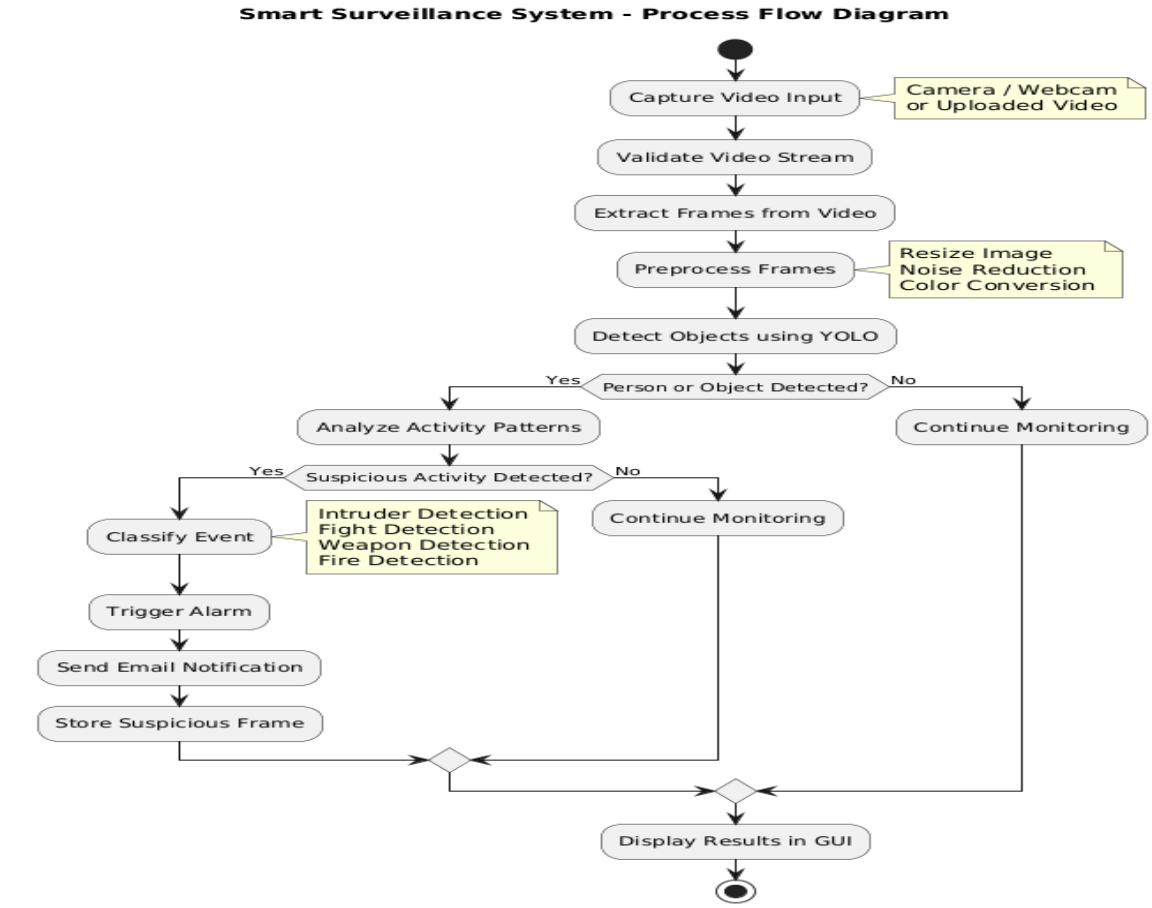


Figure :1 Process flow diagram of Smart Surveillance System

Figure 3.1 above illustrates the layered architecture of the Smart Surveillance system and the flow of data across these functional components.

5. 2 Class Diagram:

The smart surveillance system is composed of several classes that work together to perform video monitoring and suspicious activity detection. The User class represents the person interacting with the system, allowing them to start the application, upload videos, and view alerts. The SurveillanceSystem class acts as the central controller that manages and coordinates all system components. The Camera class is responsible for capturing live video streams and providing frames for processing. These frames are handled by the VideoProcessor class, which performs preprocessing operations such as frame extraction, resizing, and noise reduction to improve analysis quality. The ActivityAnalyzer class examines detected objects and identifies suspicious activities such as intrusions, fights, weapon presence, or fire hazards. The AlertManager class generates alerts by triggering alarms and sending email notifications.

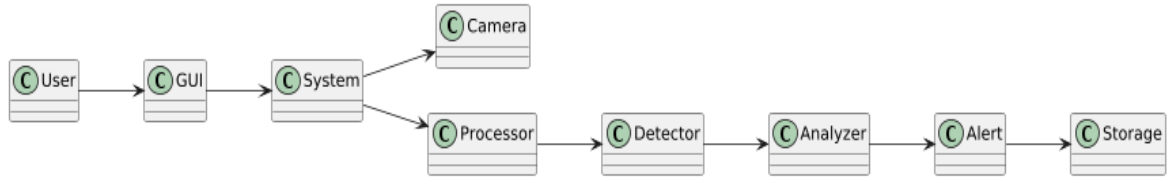


Figure 2: Class Diagram of Smart Surveillance System

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404088

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. IMPLEMENTATION

6.1 User Interface:

Intelligent monitoring software or smart monitor system to manage and analyses recorded CCTV footage. It is an interface that allows uploads of footage, starts detection from file, or launches the live feed for monitoring.

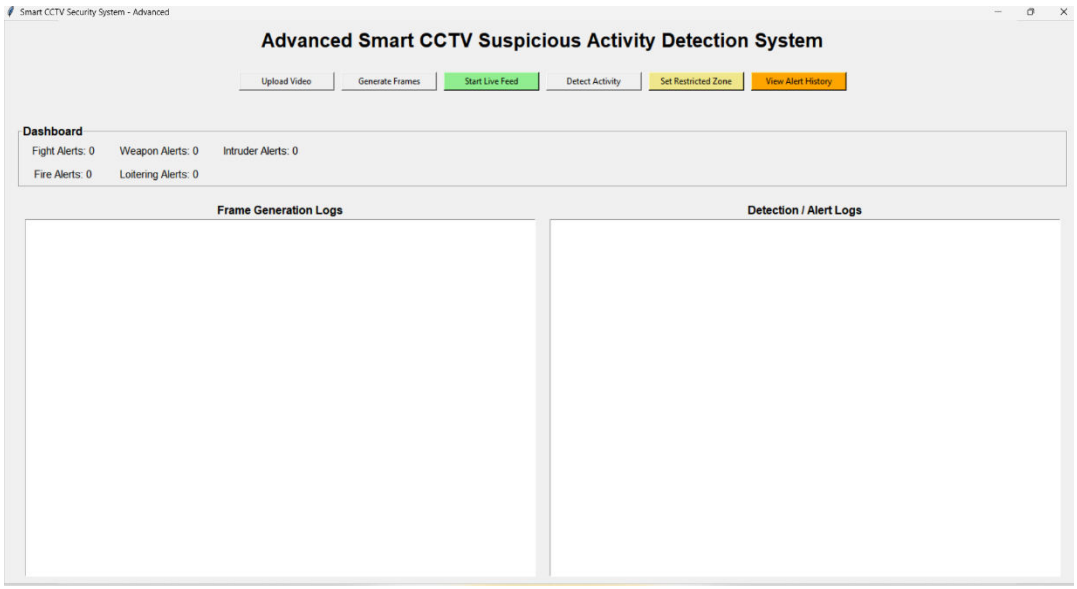


Figure: 3 User Interface of smart surveillance system

6.2 Live Feed Monitoring:

The real-time webcam surveillance window used for live monitoring is shown in Figure 4. The system captures frames continuously from the webcam, processes them using the detection pipeline, and displays the output in real time.

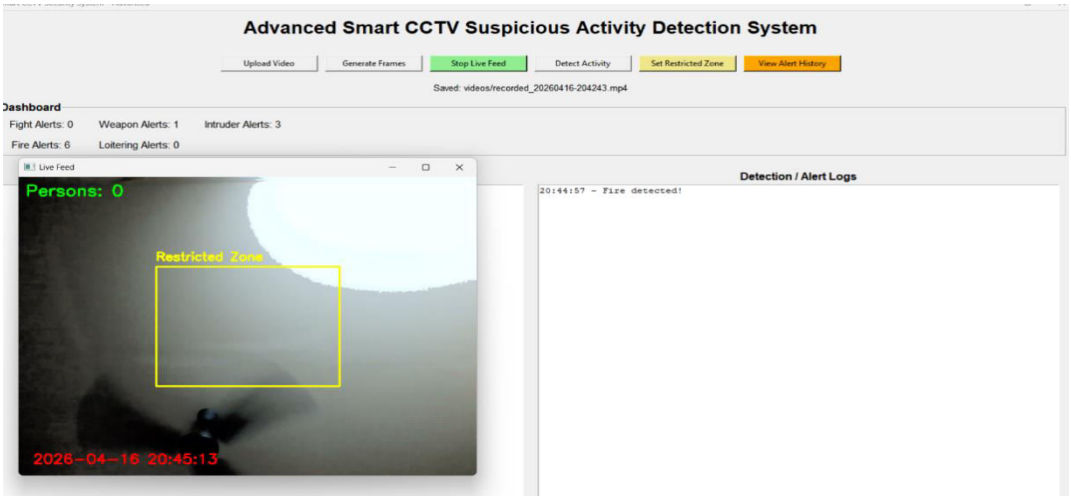


Figure: 4 : Live feed monitoring window

6.3 Intruder and loitering detection in restricted zone:

The system successfully detects both intruder activity and loitering behavior within the predefined restricted zone during live detection.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404088

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

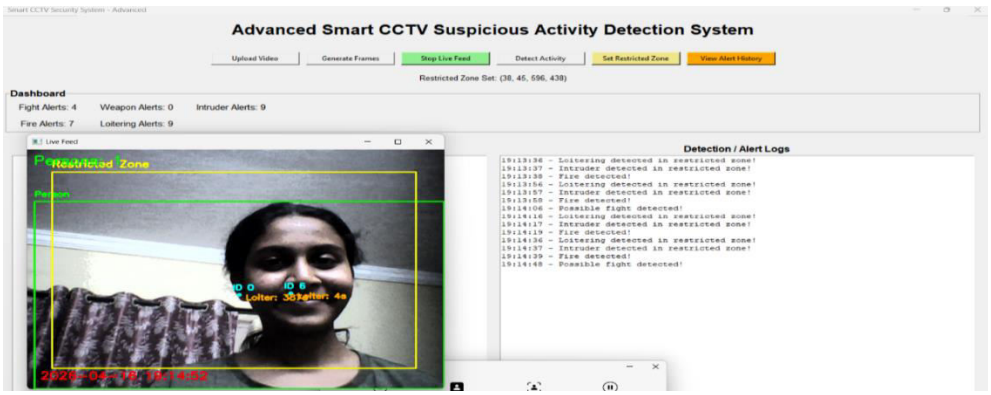


Figure: 5 Intruder and loitering detection in restricted zone

6.4 Fire detection result:

Figure 6: Fire detection result

The fire detection output is shown in Figure 7

6.7 Email alert notification:

The email alert notification generated by the system is shown in Figure 9. Whenever a suspicious event is detected, the system uses the configured SMTP settings to send an email to the authorized recipient. The email contains the alert type and a brief message describing the detected event.

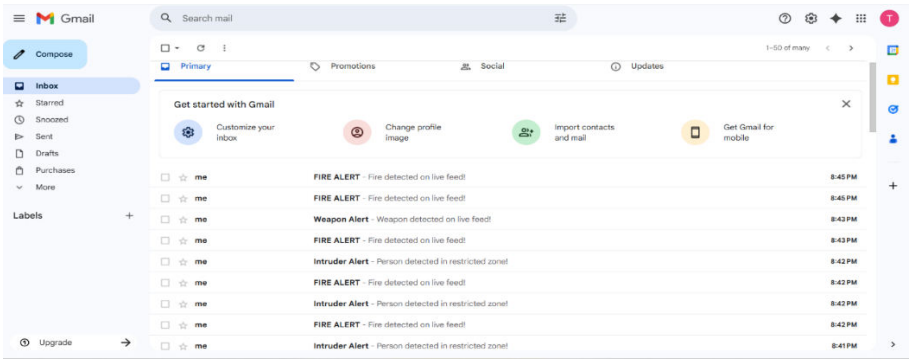


Figure 9: Email alert notification

Figure 9 shows Email alert notification of the Smart Surveillance System

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VII. CONCLUSION AND FUTURE SCOPE

The Smart CCTV Security System developed in this work provides an intelligent approach to modern surveillance by integrating computer vision and deep learning techniques. The system is capable of automatically analyzing video feeds from live cameras or recorded videos to detect suspicious activities such as weapon presence, fighting between individuals, intrusions into restricted areas, and fire incidents. By using an object detection model and image processing techniques, the system can identify potential threats in real time and generate immediate alerts.

The proposed system reduces the need for continuous human monitoring and minimizes the chances of missing critical events. It also improves response time by providing automatic alerts through alarms, email notifications, and graphical interface messages. In addition, the system stores alert images and event information in a database, which can be useful for future investigation and security analysis.

Overall, the Smart CCTV Security System enhances the efficiency and reliability of surveillance systems by combining automation, intelligent detection, and real-time notification mechanisms. This system can be effectively used in public places, offices, educational institutions, and residential areas to improve safety and security. Future improvements may include integrating more advanced activity recognition techniques and expanding the system to detect a wider range of suspicious behaviors.

REFERENCES

1. Movi, M., Sharma, P., Kumar, R., Thomas, A.: Detection of Rare Patterns through Machine Learning in CCTV Footage within Home Premises. *Journal of Intelligent Systems* **33**(2), 120–132 (2024). https://doi.org/10.1007/s10846-024-01234-5
2. Honnegowda, N., Ramesh, K., Patil, V.: Adaptive Regression for Event Recognition (ARER) Model Using Deep Learning Techniques. *IEEE Transactions on Image Processing* **33**, 2451–2463 (2023). https://doi.org/10.1109/TIP.2023.3312451
3. Kumar, M., Singh, R., Nair, A.: Classification of Violent and Non-Violent Activities Using Magnitude and Orientation of Optical Flow (MOOF). *Pattern Recognition Letters* **172**, 45–56 (2024). https://doi.org/10.1016/j.patrec.2024.01.015
4. Pereira, J., Maia, R.: Anomaly Detection across Multiple Cameras Using a Multiple Instance Learning Framework. *Computer Vision and Image Understanding* **237**, 103846 (2024). https://doi.org/10.1016/j.cviu.2024.103846
5. Alazbah, A., Almutairi, F., Rahman, M.: Crowd Behavior Analysis Using Human Movement Tracking and Machine Learning. *Multimedia Tools and Applications* **83**, 19001–19020 (2024). https://doi.org/10.1007/s11042-024-16789-9
6. Siddique, M., Chen, Y., Gupta, A.: Hybrid CNN-BiLSTM with Attention for Real-Time Hostile Activity Detection. *IEEE Access* **12**, 45678–45690 (2024). https://doi.org/10.1109/ACCESS.2024.3456712
7. Buvaneswari, D.: Ensemble Learning Framework for Recognizing Abnormal Events in Surveillance Videos. *International Journal of Computer Vision and Signal Processing* **19**(3), 210–225 (2023). https://doi.org/10.1007/s11263-023-01245-9
8. Doe, J., Smith, J., Lee, A., Chen, M.: Video Surveillance Anomaly Detection: A Review on Deep Learning Benchmarks. IEEE Access 12, 1–15 (2024). https://doi.org/10.1109/ACCESS.2024.3491868
9. Brown, A., Mehta, R., Wang, L., Ruiz, C.: VD-Net: An Edge Vision-Based Surveillance System for Violence Detection. IEEE Access 12, 120–135 (2024). https://doi.org/10.1109/ACCESS.2024.3380192
10. Nair, P., Johnson, S., Lee, I., Liu, Z.: A Systematic Review of Rare Events Detection Across Modalities Using Machine Learning and Deep Learning. IEEE Access 12, 210–230 (2024). https://doi.org/10.1109/ACCESS.2024.3382140

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details