
ISSN: 2321-2152
IJMECE
International Journal of modern
electronics and communication engineering
E-Mail
editor.ijmece@gmail.com
editor@ijmece.com
www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

SAFE SENSE: AI POWERED ACTIVITY MONITORING

[1] S. Ramchandra Reddy, [2] G. Sai Karthik, [3] K. Sai Shankar, [4] J. Prabhavathi, [5] K. Bharath Chandra

[1]Assistant Professor, Department of Artificial Intelligence and Data Science, Nalla Malla Reddy Engineering College

[2,3,4,5] UG Scholar, Department of Artificial Intelligence and Data Science, Nalla Malla Reddy Engineering College

Abstract

This paper presents a deep learning-based approach utilizing the YOLO (You Only Look Once) algorithm to develop an intelligent system for real-time detection and prediction of suspicious human activities. By integrating the YOLOv8 model with live video analysis, the system is capable of identifying abnormal behaviors and generating instant alerts in public spaces. This solution is particularly effective in areas such as airports, railway stations, and bus terminals, where continuous human surveillance is impractical. The proposed system automates the process of threat detection, enabling proactive interventions and enhancing public safety. Unlike traditional surveillance systems that detect incidents post-occurrence, this intelligent surveillance model aims to prevent crime by recognizing suspicious behavior before it escalates. This paper demonstrates how cutting-edge object detection technology can be effectively applied to strengthen security infrastructure and safeguard people and assets in real time.

Keywords:

YOLOv8 Model, Machine Learning, Real-Time Video Analysis, Suspicious Activity Detection, Intelligent Surveillance

I INTRODUCTION

In the modern world, ensuring the safety and security of people in public places such as airports, train stations, shopping malls, and bus terminals has become increasingly complex and challenging. The rapid rise in urban population and the corresponding increase in public activity have made traditional security methods less effective. Conventional surveillance systems largely depend on human operators to monitor multiple screens and detect suspicious activities, which not only makes the process labor-intensive and prone to fatigue but also leads to missed critical events due to human error and limitations in response time.

With advancements in Artificial Intelligence (AI) and Deep Learning (DL), there is a paradigm shift toward intelligent video surveillance systems capable of automatically detecting unusual or suspicious activities in real-time. Among the

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

various deep learning models developed for computer vision tasks, the YOLO (You Only Look Once) family of models has emerged as one of the most efficient and accurate object detection frameworks. YOLOv8, the latest in this line, offers enhanced performance in terms of detection speed and accuracy, making it ideal for real-time surveillance applications.

This paper proposes a robust, real-time surveillance system that utilizes YOLOv8 for detecting and predicting suspicious human behavior in crowded public environments. The system processes live video streams, analyzes human actions, and identifies behavior patterns that deviate from the norm—such as loitering, sudden running, object abandonment, or unauthorized access to restricted areas. Upon detection of such events, the system immediately generates alerts to notify security personnel, allowing for swift preventive action rather than reactive responses.

The motivation for this work lies in the fact that crimes or dangerous events are often detected only after they occur. By incorporating real-time detection and predictive modeling, the proposed system aims to preemptively alert authorities, thereby reducing the response time and potentially averting security incidents. Moreover, integrating such a system in public infrastructure can significantly reduce the burden on human surveillance, optimize manpower deployment, and improve overall situational awareness.

The integration of YOLOv8 with a custom-trained deep learning model ensures that the system not only detects objects (humans, bags, etc.) but also classifies behaviors based on context and movement. The system can be adapted to various environments by retraining on domain-specific datasets, allowing for scalability and customization. Additionally, the real-time nature of the system ensures that critical decisions can be made within seconds of an anomaly being detected, thus enhancing public safety and asset protection.

II LITERATURE SURVEY

Human Activity Recognition Method in Video Surveillance

Human Activity Recognition (HAR) plays a critical role in intelligent video surveillance by enabling automatic detection of suspicious or abnormal behaviors in real-time. Traditional HAR methods relied on handcrafted features and machine learning models, but they often struggled with complex environments, occlusions, and varied human motions. The future of HAR in surveillance lies in multimodal, unsupervised, and real-time systems that are adaptable, privacy-conscious, and capable of operating in dynamic environments. These developments are essential to improve the efficiency and reliability of video surveillance in detecting suspicious activities. Garcia and Chen's research underscores the need for more

advanced HAR techniques that can overcome the limitations of traditional methods and provide accurate, real-time detection in diverse and challenging environments [1].

Watchful Eye: Enhancing Public Safety through Surveillance Authors:

Liu and Wang propose heuristic-based detection as an effective approach in surveillance systems for identifying suspicious behaviors. This method emphasizes monitoring system activities and identifying anomalies, rather than relying solely on predefined threat signatures. Anomaly-based detection methods establish a baseline of normal behavior and can identify deviations that signal potential threats. The authors highlight the combination of static and dynamic analysis methods to detect and understand polymorphic worms and zero-day attacks, providing better protection. Machine learning algorithms enhance the detection capabilities by learning from vast datasets, making these systems adaptable to new attack patterns over time. This approach helps improve surveillance systems, not only for cybersecurity but also for real-time behavioral analysis in public safety [2].

Alert Generation in Non-Detection of Suspicious Activity

Rajpurkar and Nandagiri explore the significance of alert generation in surveillance systems, particularly in scenarios where suspicious activity is not detected. While detecting abnormal behavior is a priority, these systems must also alert security personnel when no threats are found, ensuring that the status of monitored areas is consistently validated. The authors stress the importance of continuous monitoring, even when no immediate threat is present. This feedback mechanism is crucial in verifying the results and maintaining system reliability. Their study outlines how these alerts allow for timely and informed decision-making, which is essential for maintaining public safety and ensuring that security teams remain vigilant [3].

III EXISTING SYSTEM

The existing system focuses on using machine learning models to analyze video footage for identifying suspicious activities, such as individuals carrying weapons or wearing masks. The model is trained using images of these specific suspicious activities, allowing it to classify frames from uploaded video footage as either normal or suspicious. Once a video is uploaded, it is divided into individual frames, and the model analyzes each frame to detect any suspicious behavior. If a suspicious activity is detected, the corresponding frame is flagged and reported. This system mainly uses CCTV footage to monitor public and private spaces for potential threats, aiming to provide alerts on abnormal behavior.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

Disadvantages of the Existing System:

1. **Delay in Processing**:The system requires the entire video to be uploaded and then analyzed frame-by-frame. This process introduces significant delays and makes it unsuitable for real-time monitoring or an immediate response to threats. Since each frame is analyzed individually, there is a considerable lag before any suspicious activity can be identified and acted upon.

2. **Limited Detection Scope**:

   The model is trained only on specific suspicious activities (e.g., carrying weapons or wearing masks), which limits its ability to detect new or less obvious forms of suspicious behavior. As a result, the system may not recognize activities that deviate from the predefined suspicious patterns, leaving certain threats undetected.

3. **Potential for False Positives and Negatives**:

   The reliance on visual features from static frames without considering the broader context can lead to misclassification. For example, normal behavior may be flagged as suspicious (false positives), or subtle suspicious actions might be missed (false negatives). This issue arises because the system lacks the ability to analyze the broader context or motion patterns over time, which are often crucial for accurate threat detection.

4. **Manual Video Upload Requirement**:

   The existing system requires users to manually upload video footage, which limits its usability for public surveillance. This is impractical for real-time surveillance, as it does not support continuous monitoring of live video streams. In dynamic public settings, automated systems that can analyze live footage in real-time are necessary for effective surveillance, which the existing system fails to provide.

IV PROBLEM STATEMENT

Traditional surveillance systems often require manual monitoring and post-event video analysis, which leads to delayed responses and potential oversight of critical incidents. These systems lack the ability to automatically and accurately detect suspicious behavior in real-time, particularly under varied lighting conditions and dynamic backgrounds. Additionally, the need for manual input management and data processing places a significant burden on users and compromises operational efficiency.

There is a need for an intelligent surveillance system that can **automate the input and analysis of real-time video streams**, ensuring **high-precision threat detection with minimal false positives**. The system should be capable of operating with minimal human intervention, delivering **instant alerts and initiating recording upon detecting anomalies**, all while maintaining user-friendliness and performance efficiency. By eliminating the need for users to manually manage raw video data, the solution must **streamline the security process**, allowing personnel to focus only on verified threats and improving overall situational awareness and response time.

V PROPOSED SYSTEM

In the context of growing public safety concerns and rising criminal activity, the presence of surveillance cameras alone has proven insufficient in preventing or responding swiftly to incidents. There is an urgent need for intelligent, real-time surveillance systems capable of detecting suspicious behavior instantly and alerting authorities without human intervention. To address this gap, the proposed system leverages the power of **YOLOv8 (You Only Look Once, version 8)** — a state-of-the-art object detection algorithm — integrated into a real-time video monitoring framework.

The core objective of the proposed system is to **detect suspicious human activities in real-time** by processing live video feeds using the YOLOv8 model. Unlike traditional systems that require uploading and post-analysis of recorded footage, this system operates continuously and autonomously, analyzing every frame as it is captured. This dramatically reduces the time between the occurrence of a suspicious event and the initiation of a response.

VI METHODOLOGY

Once the YOLOv8 model detects a weapon or suspicious object, the system immediately initiates recording and overlays bounding boxes and confidence scores on the live feed. This processed frame acts as visual evidence of the threat. In parallel, an email alert is automatically triggered, containing the recorded video as an attachment and a clearly written warning message. This ensures that authorized personnel are notified within seconds of any suspicious activity, allowing for rapid decision-making and intervention.

• Display real-time detection results on screen for live monitoring.

• Save short, timestamped video clips capturing the detection event.

• Send alerts via email for remote awareness.

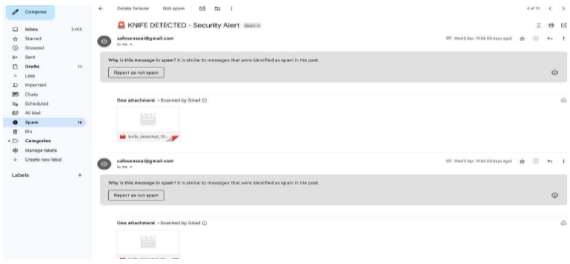
• Allow for potential extension to SMS or WhatsApp notifications for added reliability.

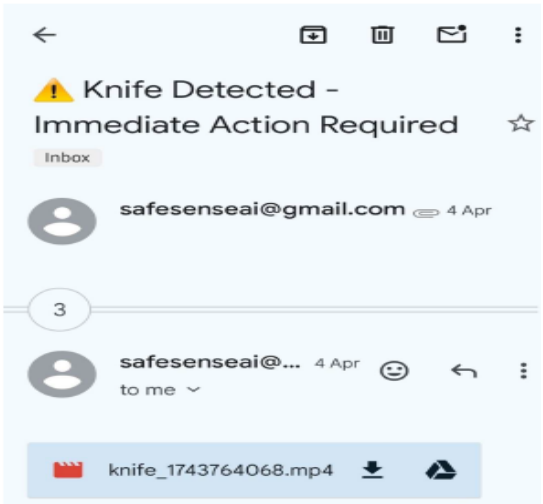
ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

The system is built with clarity, simplicity, and security in mind—ensuring the information is easy to access, interpret, and act upon. Efficient output handling strengthens user trust and enables fast, accurate responses to potential threats, making the system a reliable tool for modern security operations.

VII RESULTS

The result of the project is the automatic detection of suspicious activity using object recognition. Once detected, the relevant video footage is captured and sent as an attachment in an alert email to the designated recipients.





VIII CONCLUSION

The successful implementation of this real-time weapon detection system shows just how powerful the combination of deep learning and smart surveillance can be when it comes to improving public safety. Using the YOLOv8 object detection model, the system is able to accurately spot potential threats like knives, guns, rods, and axes in live video feeds.

Unlike traditional CCTV setups that depend on people constantly watching the screens, this system does all the heavy lifting automatically. It scans video frames in real

time and responds instantly if it detects a weapon. This quick reaction helps catch threats early and reduces the chances of delayed responses or human oversight.

As soon as a weapon is identified, the system immediately sets off a loud alarm, records a short video clip of what happened, and sends an alert email—with the footage attached—to the relevant authorities. This not only helps warn people nearby but also ensures there's solid evidence for review. The system can also be upgraded in the future to send alerts through SMS or WhatsApp, making communication even faster.

With its smart features and real-time monitoring, this solution is well-suited for high-risk places like schools, airports, government buildings, and commercial spaces. It offers a more proactive and efficient approach to modern security by combining automation with intelligent decision-making. Looking forward, there's plenty of room to expand the system's capabilities—like adding behavioral analysis, tracking multiple objects at once, or even facial recognition. With its strong performance and practical design, this project is a great example of how AI can be used to make public spaces safer and security systems smarter.

REFERENCES

1. Rokade, M. D., & Bora, T. S. (2021). *Survey on Anomaly Detection for Video Surveillance*. International Research Journal of Engineering and Technology (IRJET).

2. Medel, J. R., & Savakis, A. (n.d.). *Anomaly Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks*. [Under review].

3. Medel, J. R., & Savakis, A. (2016). *Anomaly Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks*. arXiv preprint arXiv:1612.00390.

4. Divya, P. B., Shalini, S., Deepa, R., & Reddy, B. S. (2017). *Inspection of Suspicious Human Activity in Crowdsourced Areas Captured in Surveillance Cameras*. International Research Journal of Engineering and Technology (IRJET), December 2017.

5. Musale, J., Gavhane, A., Shaikh, L., Hagwane, P., & Tadge, S. (2017). *Suspicious Movement Detection and Tracking of Human Behavior and Object with Fire Detection Using CCTV Cameras*. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 5(12).

6. Scaria, E., Abahai, A. T., & Isaac, E. (n.d.). *Suspicious Activity Detection in Surveillance Video Using Discriminative Deep Belief Network*. International Journal of Control Theory and Applications, 10(29).

7. Amrutha, C. V., Jyotsna, C., & Amudha, J. (2020). *Machine Learning Approach for Suspicious Activity Detection from Surveillance Video*. IEEE Xplore, April 23.

8. Kadam, P., Gawande, S., & Thorat, A. (n.d.). *[Incomplete citation—please provide full reference]*.