International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Anonymous Detection Using Neural Networks for Smart Surveillance

Inara Basheer, Minsiya Mol.M, Niba Naufal ,Shamsiyya.P,Ms.Anjana

1Bachelor of Technology in CSE, NCERC

2Bachelor of Technology in CSE, NCERC

3Bachelor of Technology in CSE, NCERC

4Bachelor of Technology in CSE, NCERC

5Assistant Professor, Dept. of CSE, NCERC

ABSTRACT - This project presents a real-time surveillance system that intelligently detects weapons and anomalous human behaviour using deep learning models. The system integrates YOLOv8 for object detection to identify potential threats like knives, and ResNet50 for feature extraction from video frames. These features are then analyzed by an LSTM Autoencoder trained on normal behaviour to flag any unusual activity such as loitering, panic, or sudden erratic movements. A Flask-based API ensures real-time alerts and system communication, enabling quick response without compromising individual privacy. This approach enhances public safety by combining smart surveillance with AI-driven threat detection in dynamic environments.

Keywords: Real-time Surveillance, Anomaly Detection, Weapon Detection, YOLOv8, ResNet50, LSTM Autoencoder, Deep Learning, Flask API.

1. INTRODUCTION

Ensuring security in public and private spaces has become increasingly important with the rise in criminal activities and threats. Traditional surveillance systems depend on manual monitoring, which is often inefficient, error-prone, and slow to respond to unexpected incidents. The growing need for smarter, faster, and automated surveillance solutions calls for systems that can detect unusual or dangerous behavior in real time. As a result, anomalies like unauthorized access, violent actions, or weapon appearances often go unnoticed until after the event. This limitation makes it necessary to introduce intelligent systems capable of understanding and interpreting live video streams. With advancements in artificial intelligence and deep learning, it is now possible to create models that identify abnormal behavior patterns and objects in real time.

This project presents a real-time smart surveillance system that detects anomalies and weapons using deep learning techniques. The system combines object detection with behavioral analysis, integrating YOLOv8 for weapon detection and an LSTM Autoencoder trained on normal activity patterns to identify anomalies. Features are extracted using a pre-trained ResNet50 model, allowing the system to process and evaluate each frame accurately.A webcam continuously captures live video, which is processed using OpenCV and analyzed in real time. Anomaly alerts and weapon detections are displayed on a Flask-based web interface, offering an interactive and responsive monitoring solution. By fusing computer vision with intelligent decision-making, this project demonstrates the potential of AI-driven surveillance to enhance public safety and reduce human dependency.

2. LITERATURE SURVEY

A Deep Learning Framework for Anonymity-Preserving Face Recognition

Introduces a CNN-based system for detecting human presence and behaviour while preserving privacy. It includes an anonymization layer that hides facial identities, ensuring individuals are not personally identified. This framework supports our project's goal of identity-free anomaly detection, where recognizing behaviour is prioritized over personal identification.

Real-Time Human Detection and Tracking Using YOLO

Focus: Utilizes the YOLO algorithm to detect and track humans in real time by analyzing entire video frames in a single pass. Bounding boxes are generated to follow individual movement across frames, making it suitable for real-time surveillance. The system performs well even on resource-constrained devices, such as edge computing platforms. Our project builds upon this by integrating anomaly detection and facial identity masking.

Anomaly Detection in Video Surveillance Using LSTM Autoencoders

Proposes the use of LSTM-based autoencoders to learn patterns of normal human behaviour from video surveillance footage. The model identifies anomalies by

measuring reconstruction error—higher errors indicate behaviour deviating from the norm. The system avoids reliance on facial features or personal data, aligning closely with our project's focus on behaviour-based detection without compromising individual privacy.

Smart Surveillance with Edge Computing and Deep Learning

Proposes a smart surveillance setup where edge devices handle video processing locally instead of sending data to cloud servers. This reduces latency, enhances response times, and addresses privacy concerns by keeping sensitive data within the local network. Deep learning models deployed on edge systems perform tasks like detection and classification in real time.

3. PROPOSED SYSTEM

The proposed system addresses the need for intelligent surveillance by detecting anomalous human behavior in real-time, without relying on identity recognition. It integrates deep learning models for behavior analysis and object detection, operating through a privacy-focused architecture suitable for smart surveillance applications.

The core components of the proposed system are as follows:

Real-Time Human and Object Detection: A USB webcam captures live footage of a simulated environment. The frames are processed using the YOLOv8 model to detect people and potentially dangerous objects like knives. YOLO's fast and accurate detection capability allows the system to work in real time.

Feature Extraction and Behavior Monitoring: Once humans are detected, frames are passed through a ResNet50 model to extract visual features. These features are then analyzed using an LSTM autoencoder trained only on normal behavior data. The reconstruction error helps determine whether an observed activity is anomalous.

Anomaly Detection Logic: The LSTM autoencoder calculates reconstruction error for each sequence of human activity. If the error surpasses a defined threshold, the behavior is flagged as anomalous. The system differentiates normal movement (e.g., walking) from suspicious actions (e.g., running, falling, crowding) using this unsupervised learning approach.

Flask Web API and Alert Mechanism: Upon detecting an anomaly or weapon, the system triggers an alert via a Flask API. A notification is generated on a web dashboard, and visual evidence such as bounding boxes, timestamps, and camera feed snapshots are displayed for monitoring purposes.

Embedded and Scalable Setup: The system runs on a low-cost setup using a laptop or Raspberry Pi, ensuring affordability and scalability. It can be deployed in various environments like schools, offices, or public areas where monitoring behavior is essential without compromising privacy.

By combining deep learning, real-time detection, and privacy-aware design, this system offers a practical, scalable solution for intelligent surveillance and early warning applications.

4. MODULE DESCRIPTION

Data Collection Module

Purpose: Captures real-time video feed from surveillance cameras.

Functionality: Continuously streams video to the detection and analysis pipeline.

Output: Live video frames passed to the next modules for processing.

Object Detection Module (YOLOv8)

Purpose: Detects objects such as weapons (e.g., knives) in video frames.

Functionality: Uses YOLOv8, a state-of-the-art object detection model, to identify and label objects in each frame.

Output: Bounding boxes around detected objects with class labels and confidence scores.

Feature Extraction Module (ResNet50)

Purpose: Extracts visual features from the frames to understand the context (posture, movement).

Functionality: Uses ResNet50, a deep CNN model, to process each frame and extract key features that represent human behavior.

Output: A vector of extracted features used for further analysis.

Behavior Anomaly Detection Module (LSTM Autoencoder)

Purpose: Identifies abnormal behavior such as panic, loitering, or erratic movement.

Functionality: The LSTM Autoencoder learns the normal behavior patterns over time, and any deviation from these patterns triggers an anomaly alert.

Output: Anomaly score indicating whether the behavior is normal or unusual.

Alert System Module (Flask API)

Purpose: Sends alerts based on object detection or behavior anomalies.

Functionality: Integrates with the Flask API to push real-time alerts to a web dashboard, mobile app, or messaging system when a threat is detected.
Output: Notifications containing details about detected threats (e.g., knife detected, behavior anomaly flagged).

Model Training & Saving Module

Purpose: Handles training, fine-tuning, and saving of models (YOLOv8, ResNet50, LSTM Autoencoder).
Functionality: Manages data preprocessing, training loops, and saves the best-performing models. Supports the system's adaptability to new environments and behaviors.
Output: Trained and saved models ready for deployment or future fine-tuning.

System Monitoring & Performance Evaluation Module

Purpose: Monitors the system's performance and evaluates the effectiveness of detection.
Functionality: Tracks the accuracy and performance of object detection and behavior anomaly identification in real-time. Provides feedback for system improvements.
Output: Performance metrics (accuracy, false positives/negatives) and system logs.

User Interface Module

Purpose: Provides a user-friendly interface to interact with the system.
Functionality: Displays real-time camera feeds, detected objects, anomaly alerts, and system logs.
Output: Web-based or app-based dashboard showing surveillance data, alerts, and model status.

5.TECHNOLOGIES USED

YOLOv8:

A state-of-the-art object detection model, YOLOv8, is employed for real-time weapon detection. It identifies dangerous objects like knives in video feeds, ensuring quick detection with high accuracy.

ResNet50:

This deep Convolutional Neural Network (CNN) is used for feature extraction from video frames. It analyzes human movement, posture, and context, providing essential information for behavior analysis.

LSTM Autoencoder:

A specialized neural network model, the LSTM Autoencoder, is trained to recognize normal human behavior patterns. It flags anomalies like sudden erratic movements, panic, or loitering, ensuring early detection of unusual activities.

Flask:

Flask is utilized as the web framework for the backend API. It enables the system to send real-time alerts to dashboards or messaging platforms, facilitating prompt responses to detected threats or anomalies.

OpenCV:

OpenCV handles video feed manipulation, frame extraction, and real-time processing, allowing the system to work with live video streams for object and anomaly detection.

Python:

Python serves as the core programming language, providing a versatile environment for building machine learning models and handling data processing tasks. It integrates seamlessly with the various libraries and frameworks used in the project.

TENSORFLOW/Keras:

TensorFlow, along with Keras, is the machine learning framework used for building and training deep learning models, including YOLOv8, ResNet50, and the LSTM Autoencoder. These frameworks streamline model development and deployment.

NumPy & Pandas:

These libraries are used for data manipulation and preprocessing. NumPy provides efficient numerical operations, while Pandas is used to handle and structure data, ensuring smooth data flow for model training and analysis.

Visual Studio Code (VS Code):

VS Code is the integrated development environment (IDE) used for writing, debugging, and managing the codebase. It supports Python development with various extensions.

6. SYSTEM DESIGN

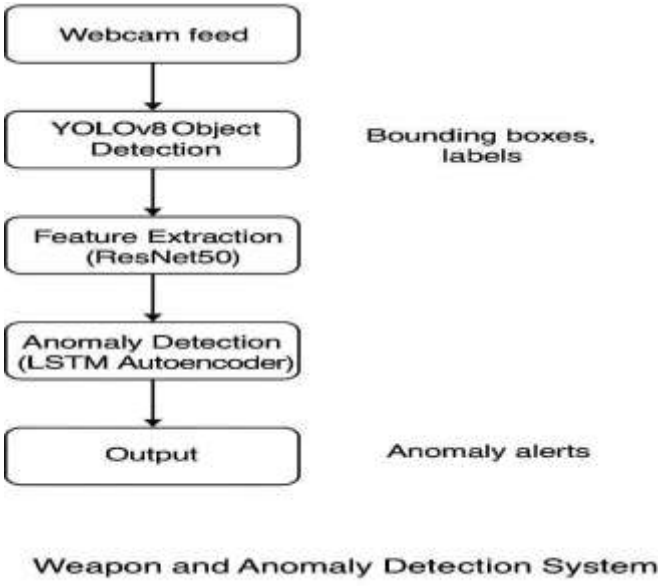

Fig 6.1- Architecture Diagram

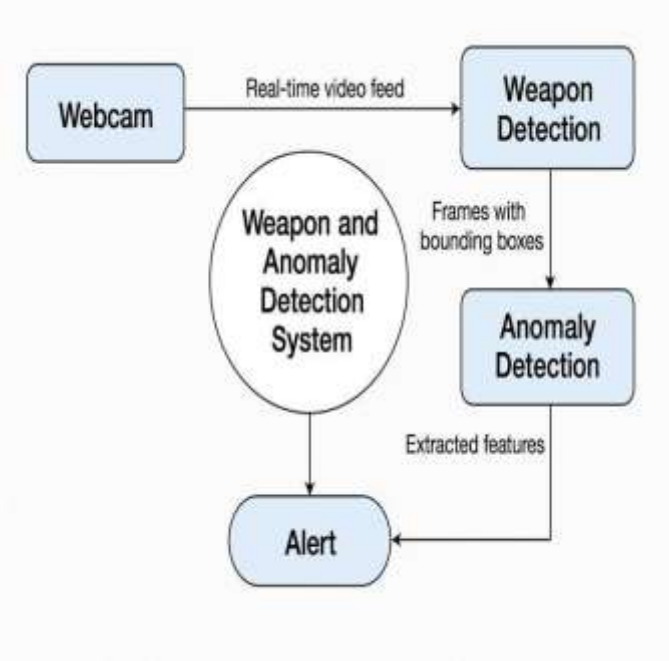

Fig 6.2- Flow Chart Diagram

7. RESULTS

Fig 7.1 Live feed, LSTM model not trained.

Fig 7.2 LSTM Autoencoder training in progress. YOLO detects persons and cellphone.

Fig 7.3 LSTM detects anomaly — knife identified.

8. DISCUSSION AND ANALYSIS

8.1 ADVANTAGES

Real-Time Threat Detection:

Instant detection of weapons (e.g., knives) and abnormal behavior (e.g., panic, loitering) without delay, which helps in improving security in real-time

Privacy-Preserving:

Unlike traditional surveillance, your system does not track faces or identities, ensuring privacy while still providing highly accurate anomaly detection.

Dual-Layer Detection:

Combines object detection (YOLOv8) for weapons with behavior analysis (LSTM Autoencoder) for anomalies, making it more comprehensive than single-focus systems.

Adaptive Learning:
The system is capable of learning from live data and can be retrained or fine-tuned over time as the environment changes (e.g., lighting, crowd behavior), ensuring continuous improvement.

Fast and Automated Alerts:
By integrating with a Flask API, it sends instant notifications to a dashboard, app, or messaging system when an anomaly or weapon is detected, enabling quick response from security teams.

Reduced Human Monitoring:
Automates the surveillance process, reducing the need for continuous human monitoring and allowing staff to focus on high-priority situations.

Scalability:
The system is designed to be scalable, meaning it can be deployed in various environments, from small spaces to large public areas, without significant changes.

8.2 FUTURE WORKS

Smart City Integration:
Enhance the system's capability to integrate with city-wide infrastructure, such as traffic management and public safety systems, to provide real-time threat detection and optimize urban security.

Traffic Violation Detection:
Incorporate AI models to automatically detect traffic violations, including red-light running and illegal turns, by analyzing real-time traffic footage, contributing to safer roads and improved traffic law enforcement.

Mobile App Integration:
Develop a dedicated mobile application that allows users and authorities to remotely monitor and control the system, providing real-time alerts, access to surveillance footage, and system settings adjustments.

Smart Pedestrian Crosswalks:
Expand the system to include smart pedestrian crosswalks that detect pedestrian presence and adjust crossing signals based on foot traffic density, improving pedestrian safety and traffic flow efficiency.

9. CONCLUSION

Our project presents a cutting-edge, AI-driven surveillance system designed to enhance security and automate threat detection. By integrating YOLOv8 for weapon detection, ResNet50 for feature extraction, and LSTM Autoencoder for behavior anomaly detection, the system provides a comprehensive and real-time solution that ensures public safety without compromising privacy.

This system is designed for scalability, allowing it to be deployed in a variety of environments, from small offices to large public spaces. With its dual-focus detection (weapons and abnormal behavior) and continuous learning capabilities, our project represents a major step forward in intelligent, automated surveillance systems.

By reducing manual monitoring and enabling faster response times, this system could play a crucial role in enhancing security in public spaces, smart cities, and sensitive areas.

ACKNOWLEDGEMENT

We express our sincere gratitude to Ms. Anjana, Assistant Professor, Department of Computer Science and Engineering, NCERC, for her valuable guidance, support, and encouragement throughout the course of this project. Her mentorship played a vital role in shaping our research and ensuring its successful completion. We also thank Nehru College of Engineering and Research Centre (NCERC) for providing the infrastructure and resources necessary to carry out this project effectively. We sincerely appreciate the efforts of all our project team members for their dedication, cooperation, and hard work at every stage of development. We are especially grateful to the volunteers who contributed fingerprint data during the testing phase, as well as to our parents and peers for their continuous support and motivation throughout this journey.

REFERENCES

1. Nejad, S. S., & Haque, A., "Weakly-Supervised Anomaly Detection in Surveillance Videos Based on Two-Stream I3D Convolution Network," arXiv preprint arXiv:2411.08755, 2024.
2. Yadav, V., & Jain, P., "A Survey on Deep Learning-Based Object Detection Techniques in Surveillance Systems," Journal of Intelligent Systems, vol. 33, no. 3, pp. 220–237, 2024.
3. Huang, S., Liu, Z., Zhang, H., et al., "Attention-Guided Temporal Feature Enhancement for Video Anomaly Detection," IEEE Transactions on Circuits and Systems for Video Technology, 2023.
4. Jiang, H., Wu, B., Chen, C., et al., "Graph Contrastive Learning for Video Anomaly Detection," Proceedings of the AAAI Conference on Artificial Intelligence, 2023.
5. Kim, D., Lee, H., & Park, S., "YOLO-Based Weapon Detection in Real-Time Surveillance Systems," Sensors, vol. 23, no. 5, pp. 2510–2522, 2023.

6. Lin, K., Ren, S., & Li, X., "Multi-Scale Feature Fusion Network for Abnormal Event Detection in Surveillance Videos," Neurocomputing, vol. 530, pp. 125–136, 2023.
7. Liu, W., Zhang, H., Yu, L., et al., "Dual-Stream Temporal Network for Efficient Video Anomaly Detection," Sensors, vol. 23, no. 2, 2023.
8. Patel, R., & Sharma, K., "Hybrid LSTM-Autoencoder for Abnormal Behaviour Detection in CCTV Feeds," International Journal of Computer Vision and Signal Processing, vol. 15, pp. 78–85, 2023.
9. Qian, Y., Wang, Y., & Zhang, J., "Spatiotemporal Transformer with Visual Memory for Video Anomaly Detection," IEEE Transactions on Image Processing, vol. 32, pp. 2956–2967, 2023.
10. Singh, A., & Saini, R., "Hybrid GAN-Based Anomaly Detection Framework in Surveillance Footage," Multimedia Tools and Applications, vol. 82, pp. 13345–13366, 2023.
11. Wang, S., Liu, B., Yang, X., et al., "Abnormal Event Detection via Spatiotemporal Feature Enhancement and Memory Modules," Image and Vision Computing, vol. 131, 2023.
12. Wu, L., Zhou, Y., & Yang, X., "Scene-Aware Self-Supervised Video Anomaly Detection," Pattern Recognition Letters, vol. 170, pp. 1–8, 2023.
13. Xia, F., Chen, X., Yu, S., et al., "Coupled Attention Networks for Multivariate Time Series Anomaly Detection," arXiv preprint arXiv:2306.07114, 2023.
14. Zhang, Y., Li, F., & Zhao, H., "Anomaly Detection in Videos Using Temporal Context Fusion Networks," IEEE Access, vol. 11, pp. 19087–19096, 2023.
15. Zhou, Y., Feng, M., & Chen, X., "Multi-Resolution Temporal Attention Network for Real-Time Abnormal Event Detection," Pattern Recognition, vol. 137, 2023.