Smart Surveillance System for Suspicious Activity Detection

Kiran Murtadak[1], Rohit Nagargoje[2], Dnyaneshwar Aher[3], Prof. A. D. Gawali[4]

Amrutvahini College of Engineering, Sangamner

Abstract

Crowd management and security are critical challenges in public spaces, where conventional surveillance methods such as CCTV primarily serve as reactive tools for incident tracking rather than proactive crime prevention. Manual monitoring is labour-intensive and inefficient, limiting real-time threat detection capabilities. This paper presents a deep learning-based model for accurate crowd behaviour detection, enabling early identification of suspicious activities to prevent crimes before they occur. The proposed system ensures secure data transmission while maintaining privacy, offering a comprehensive, end-to-end solution for real-time crowd analysis. By leveraging advanced artificial intelligence techniques, this approach enhances public safety, optimizes security operations, and paves the way for smarter surveillance systems.

Keywords: Crowd management, Deep learning, Crime prevention, Real-time monitoring, Crowd behaviour detection, Secure data transmission, Artificial intelligence, Smart surveillance

INTRODUCTION

Crowd management and security have become critical concerns in public spaces, where traditional surveillance methods such as CCTV are primarily used for tracking incidents after a crime has occurred. Manual tracking is often time-consuming and inefficient, making it difficult to prevent potential threats in real time.

To address these challenges, we propose a deep learning-based model designed for the accurate detection of crowd behaviors. Our system enhances public safety by enabling early detection of unusual activities, thereby preventing crimes before they escalate. Additionally, the solution ensures secure data transmission, maintaining privacy while providing an efficient, end-to-end approach for real-time crowd monitoring and analysis.

LITERATURE SURVEY

Sr no	Title of paper	Technique	IEEE journals/conference
1	Public Vision: A Secure Smart Surveillance System for Crowd Behavior Recognition	Real time video analysis -Deep Learning -CCTV camera	IEEE Access in PP(99):1-1

2	Suspicious Activity Recognition in Video Surveillance System	Machine Learning -GMM	IEEE Access
3	Toward trustworthy human suspicious activity detection from surveillance videos using deep learning	-Deep learning -CNN Algorithm	Springer
4	Detection of Unusual Activity in Surveillance Video Scenes Based on Deep Learning Strategies	Deep Learning VGG-16	Journal of Al-Qadisiyah for Computer Science and Mathematics

METHODOLOGY

The development of a Smart Surveillance System follows a structured approach, starting with data collection and preprocessing. Video footage from CCTV cameras in various environments is gathered and labeled with normal and suspicious activities such as loitering, aggressive behavior, or unauthorized access. Preprocessing techniques, including frame extraction, image resizing, and noise reduction, ensure high-quality input for deep learning models.Next, deep learning models such as Convolutional Neural Networks (CNNs) and YOLO (You Only Look Once) are employed for real-time object detection and activity recognition. The trained model continuously analyzes live video feeds and detects unusual behaviors with high accuracy. Upon detecting suspicious activity, the system generates real-time alerts, notifying security personnel through email, SMS, or a mobile app for quick verification and action.For efficient deployment, the system utilizes edge computing and cloud-based solutions, ensuring fast processing and scalability. Security measures like encryption and anonymization protect data privacy. The system is also scalable and adaptable, making it suitable for various environments while improving crime prevention and response times.

OBJECTIVE

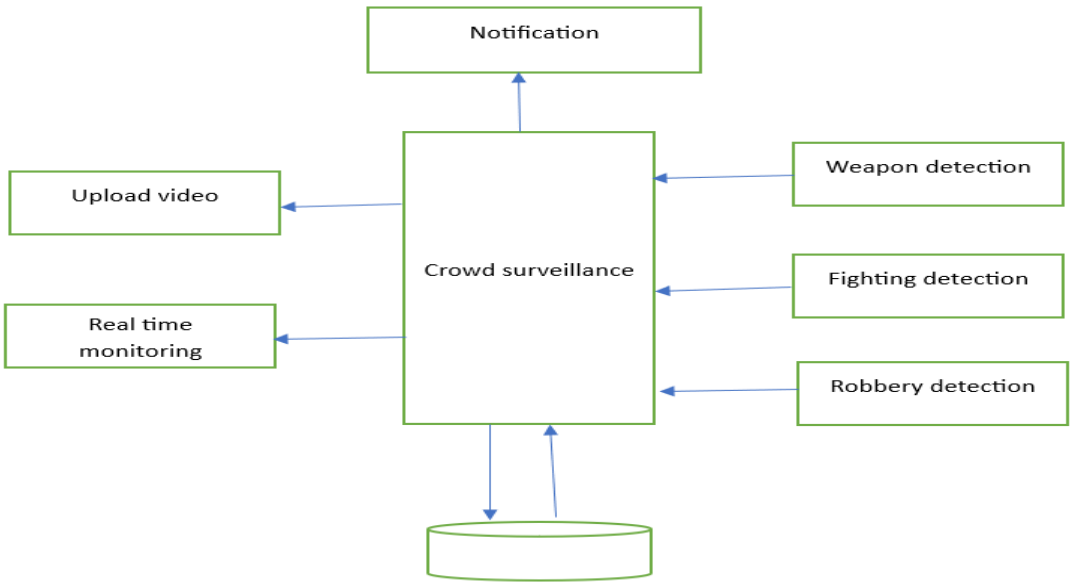
1. Automating Surveillance: Implement an AI-driven surveillance system that minimizes the need for manual monitoring, enhancing efficiency and accuracy in detecting crowd behaviours and potential security threats.
2. Prevent Crimes Quickly: Enable early detection of suspicious activities through deep learning models, allowing authorities to take proactive measures and prevent crimes before they occur.
3. Privacy Protection: Ensure secure data transmission and privacy-preserving mechanisms, maintaining ethical standards while monitoring public spaces without compromising individual identities.

4. Scalable and Adaptable: Develop a flexible system that can be easily scaled and adapted to various environments, including crowded public areas, transportation hubs, and large events.
5. Enabling Quicker Responses to Potential Threats: Facilitate real-time threat analysis and automated alerts, allowing security personnel to respond swiftly and effectively to emerging risks.

PROBLEM DEFINATIONS

The Smart Surveillance System is a deep learning-based solution designed to enhance security by monitoring live CCTV footage in real time. The system continuously analyses video streams using advanced AI models to detect suspicious activities such as unusual gatherings, aggressive behaviour, unattended objects, or unauthorized access. When any questionable activity is detected, the system instantly generates an alert message and sends it to authorized personnel via email, SMS, or a mobile application. The security personnel can then verify the severity of the situation through live video feeds, recorded clips, or AI-generated reports. Based on the assessment, appropriate actions can be taken, such as dispatching security teams or notifying law enforcement.

SYATEM ARCHITECTURE



Fig(a): System Architecture

FUCTIONAL REQUIREMENTS

1. Real-Time Crowd Monitoring – The system should continuously analyze live video feeds to detect and track crowd behaviors.
2. Anomaly Detection – It should identify unusual activities such as sudden gatherings, aggressive movements, or stampedes.
3. Automated Alerts – The system should generate real-time notifications for security personnel when a potential threat is detected.
4. Privacy Protection Mechanisms – It should implement anonymization techniques (e.g., face blurring) to ensure individual privacy.
5. Secure Data Transmission – All collected data should be encrypted and transmitted securely to prevent unauthorized access.

6. Integration with CCTV and IoT Devices – The model should be compatible with existing surveillance infrastructure, including cameras and edge devices.
7. Scalability for Different Environments – The system should be deployable in various locations such as airports, stadiums, malls, and public transport hubs.
8. User Access Control – Different user roles (e.g., security personnel, administrators) should be defined with appropriate access rights.
9. Incident Logging and Reporting – The system should store detected incidents with timestamps, video clips, and analysis for future review.
10. Multi-Camera Support – The system should be able to analyse data from multiple cameras simultaneously.

NON FUCTIONAL REQUIREMENTS

1. Performance Efficiency – The system should process video feeds in real-time with minimal latency.
2. Reliability and Availability – It should be operational 24/7 with minimal downtime to ensure continuous surveillance.
3. Scalability – The solution should support an increasing number of cameras and data sources without compromising performance.
4. Security – Strong authentication and encryption techniques should be used to protect sensitive data.
5. Interoperability – The system should be compatible with various hardware configurations and surveillance platforms.
6. Usability – A user-friendly interface should be designed for security personnel to easily access and interpret alerts.
7. Maintainability – The system should allow for easy updates, bug fixes, and improvements with minimal downtime.
8. Compliance with Legal and Ethical Standards – The solution should adhere to privacy regulations such as GDPR to ensure lawful data usage.

CONCLUSION

Effective crowd management and security require proactive measures beyond traditional CCTV surveillance and manual tracking, which are often reactive and inefficient. Our deep learning-based model provides a robust solution by enabling accurate detection of crowd behaviors, allowing for early intervention and crime prevention. By integrating secure data transmission and privacy-preserving mechanisms, our system ensures a safe and reliable approach to real-time crowd monitoring. This innovative solution enhances public safety, minimizes risks, and paves the way for smarter, AI-driven security frameworks in crowded environments.

REFERENCES

1. Marwa Qaraqe, Almiqdad Elzein, Emrah Basaran, Yin Yang , Elizabeth B. Varghese, Wisam Costandi, Jack Rizk, And Nasim Alam "*PublicVision: A Secure Smart Surveillance System for Crowd Behavior Recognition*"-IEEE Access

2. Sherief Elbiswalahai , Mohammad abdelpankey, '' *Deep learning based crowd survillence analysis*'' sept 2020 journel of imaging 6 (9): 95.

3. Guruh Fajar Shidik , Edi Noersasongko, Adhitya Nugraha, PulungNurtantioAndono ,JumantoJumanto , And Edi Jaya Kusuma ''*A Systematic Review of Intelligence Video Surveillance: Trends, Techniques, Frameworks, and Datasets*''-IEEE Access.

4.Zhengxin Zhang, HongdongLi"*Survey of Deep Learning Approaches for Crowd Behavior Analysis*"- Pattern Recognition.

5. Mohammad Alazab, Ramzi A. Haraty "*A Review of Secure Data Transmission Techniques in IoT-Based Surveillance Systems*"-IEEE Access.