CogniWatch: Advanced Scene Analysis for Threat Detection and Public Safety

Chetan Patil[1], Saurbh Moynak[2], Yash Wagh[3], Bhavana Pathare[4], Tanuja Mulla[5]

[1,2,3,4] Student, Department of Computer Engineering, Smt. Kashibai Navale college of Engineering, Pune, India
[5]Assistant Professor, Department of Computer Engineering, Smt. Kashibai Navale college of Engineering, Pune, India

---***---

Abstract - ***Ensuring the safety of life and property through the deployment of high-quality CCTV cameras has become indispensable in our modern world. Manual monitoring of every moment is not feasible, and the unpredictable nature of human behavior makes distinguishing between suspicious and normal activities a formidable challenge. In this research, we introduce a novel approach utilizing Convolutional Neural Networks (CNN) to discern between suspicious and routine activities within an environment. Our proposed system is designed to automatically alert relevant authorities upon detecting potentially suspicious behavior. The effectiveness of any suspicious activity detection system hinges on several critical factors, including the quality of training data, the architecture of the Machine Learning model, and the operational environment. To maintain the system's accuracy and keep it adaptive to new and evolving threats, continuous monitoring, regular updates, and ongoing improvement are imperative. Our work underscores the importance of robust data sources and the careful design of CNN-based models to ensure the system's reliability in real-world applications. This research not only addresses the pressing need for automated surveillance but also emphasizes the significance of staying current and vigilant in the ever-changing landscape of safety and security.***

***KeyWords**: CNN, Object Detection, Anomaly, Threat, Hyperparameter Tunning.*

1. INTRODUCTION

In today's dynamic and interconnected world, the need for advanced technologies to enhance safety and security has never been more critical. Human behavior recognition in real-world environments has found a multitude of applications, ranging from intelligent video surveillance to the analysis of shopping behavior. Among these applications, video surveillance stands out as a fundamental element of modern safety measures. It plays an indispensable role both indoors and outdoors, providing a vigilant eye on our surroundings and safeguarding our public spaces and private establishments.

The advantages of video surveillance are far-reaching. It offers efficient monitoring capabilities, significantly reduces the need for extensive manpower, provides cost-effective auditing tools, and possesses the adaptability required to keep pace with evolving security trends. As our world becomes increasingly complex and interconnected, the importance of robust video surveillance systems cannot be overstated.

In response to these needs, the "CogniWatch" project emerges as a pioneering initiative that harnesses the power of advanced scene analysis. Its primary objective is to augment threat detection and elevate public safety. In doing so, it aligns seamlessly with the broader goals of security and surveillance in the digital age. By leveraging cutting-edge technologies and methodologies, "CogniWatch" strives to enhance our ability to recognize and respond to potential threats, ultimately creating a safer and more secure environment for all. This project is not merely a technological endeavor; it is a commitment to safeguarding the well-being of communities and individuals in an ever-evolving world.

2. LITERATURE SURVEY

[1] This paper has effectively proposed a model for suspicious activity detection using Convolutional Neural Networks (CNN) with a remarkable detection rate of up to 90% accuracy, surpassing previous models. The integration of CNN and surveillance footage processing demonstrates significant potential for real-time threat recognition. While the proposed model shows promise, it is essential to acknowledge some limitations. The system's performance may still be impacted by challenging environmental conditions, such as poor lighting or occluded scenes. Additionally, the paper does not address the potential computational resources required for real-time implementation, which can be a concern in practical applications.

[4] The paper's focus on developing a deep learning-based framework for suspicious activity recognition is notable. It leverages a 63-layer CNN architecture for feature extraction, demonstrating the effectiveness of the proposed method. However, limitations include the need for a larger and more diverse dataset for comprehensive evaluation. In future work, expanding the dataset and exploring real-time implementation would enhance the practicality and reliability of the system.

[5] This paper proposes a real-time system using the Kalman Filter and Kanade-Lucas-Tomasi (KLT) Tracking Algorithm to

detect and monitor suspicious or non-suspicious human behavior for ATM video surveillance. On a real-time ATM Surveillance database, experimental results are carried out. A drawback of the proposed system is that it heavily relies on the quality of the input video data. The effectiveness of the Kalman Filter and Kanade-Lucas-Tomasi (KLT) Tracking Algorithm in detecting and monitoring human behavior may be compromised in situations where the video quality is poor, such as low-resolution footage, low lighting conditions, or camera angles that hinder clear visibility. In such scenarios, the system's accuracy in distinguishing between suspicious and non-suspicious behavior may be reduced, potentially leading to false alarms or missed security threats.

[6] The paper's focus on object detection using YOLOv3 demonstrates the potential for robust image analysis in real-world scenarios, addressing some of the challenges associated with complex environments. To further enhance its applicability, future work could explore adapting the model for specific use cases and refining its generalization across diverse settings. Additionally, incorporating real-time processing capabilities could be a promising avenue for improving practical applications in surveillance and security.

[8] The paper's focus on detecting potential gun-based crimes and abandoned luggage in surveillance footage highlights the critical importance of improving public safety. However, observed limitations include the need for further optimization in real-time gun detection and addressing sudden illumination changes in the abandoned luggage detection method. Future work should explore different architectures, enhance real-time detection, and consider additional features for more robust surveillance solutions.

[10] The paper's focus on using an Advanced Decision Tree Algorithm for detecting suspicious emails related to criminal activities highlights the potential of data mining in enhancing crime detection. However, it is important to note that the limited dataset used for experimentation may introduce bias into the results. Future work could involve incorporating larger, more diverse datasets, exploring additional feature selection methods, and adapting the tool for mobile environments. This would help improve the tool's accuracy and widen its applicability in real-world crime detection scenarios.

[11] The paper's focus on the development of a surveillance camera system for threat detection and public safety using Motion Quantity is a notable highlight. It presents a promising approach to automate the monitoring process and identify suspicious activities. However, the limitations include the need for further real-world testing and validation to ensure the reliability of the proposed method. Future work should explore the integration of advanced machine learning techniques and large-scale deployment to enhance the system's accuracy and practicality.

3. RELATED WORK

This project involves the utilization of cutting-edge technologies and methodologies to enhance security measures and protect public safety. A thorough review of related work in this field reveals a range of techniques and innovations aimed at achieving this objective. Here is an in-depth exploration of some key areas of related research and developments:

1. Real-Time Threat Detection in Video Surveillance Systems using CNNs

In this work, the authors focus on real-time threat detection in video surveillance systems using Convolutional Neural Networks (CNNs). They demonstrate the effectiveness of CNNs in detecting threats such as suspicious objects and individuals. The research highlights the significance of real-time processing and its applicability in public safety.

2. Deep Learning for Improved Object Detection and Classification in Surveillance Videos

This study delves into the application of deep learning, specifically CNNs, for object detection and classification in surveillance videos. It addresses the challenge of recognizing both known and unknown threats in crowded public spaces and highlights how enhanced CNN models can improve accuracy.

3. Enhanced CNN Models for Anomaly Detection in Smart Cities

Anomaly detection in smart cities is a critical aspect of public safety. This research explores the use of enhanced CNN models to detect anomalies in various urban scenarios, from traffic patterns to unusual human behavior. The study emphasizes the need for advanced CNN architectures to achieve better anomaly detection results.

4. Drones and Deep Learning for Aerial Threat Detection

Aerial threats pose a unique challenge for public safety, especially in crowded events and urban areas. This work discusses the integration of drones and deep learning techniques, including enhanced CNNs, for the early detection of threats from the air, such as drones carrying potential dangers.

5. Privacy-Preserving Threat Detection using Deep CNNs

Balancing public safety with privacy concerns is crucial. This research explores methods for privacy-preserving threat detection using deep CNNs. It discusses how enhanced CNN models can be trained on encrypted data, ensuring that privacy is maintained while still effectively identifying potential threats.

6. Scalability and Resource Optimization for CNN-Based Threat Detection

Scalability and resource optimization are crucial for deploying CNN-based threat detection systems in real-world scenarios. This study investigates techniques to make CNN models more efficient, enabling their deployment in resource-constrained environments for public safety applications.

These related works highlight the evolving landscape of threat detection and public safety using enhanced CNN algorithms. They address a variety of challenges, including real-time processing, object recognition, privacy concerns, and resource optimization, providing valuable insights for the development of advanced scene analysis systems for public safety.

4. METHODOLOGY

The development of an advanced scene analysis methodology for threat detection and public safety using an enhanced Convolutional Neural Network (CNN) algorithm is a crucial endeavor in the field of surveillance and security. In this discussion, we will compare and contrast various aspects of this methodology.

The initial step in this research was to define the specific suspicious activities that the system would focus on. In this context, five activities were selected for classification: shooting, punching, kicking, knife attacks, and sword fights. This selection is fundamental, as it serves as the foundation upon which the enhanced CNN algorithm is built. The methodology's effectiveness greatly depends on the accuracy and comprehensiveness of this initial activity selection.

To enhance the performance of the CNN algorithm, several key considerations come into play. The architecture and design of the CNN play a pivotal role in achieving high accuracy in threat detection. Parameters such as the depth of the network, the number of layers, and the use of pre-trained models must be carefully considered. Additionally, data quality and quantity are vital factors. The availability of a diverse and representative dataset that includes a wide range of instances of the chosen suspicious activities is essential for training the algorithm effectively.

Furthermore, the methodology must incorporate real-time analysis capabilities, allowing for the immediate identification and response to potential threats. Latency in threat detection can significantly impact public safety, so optimizing the algorithm's efficiency is paramount.

An advanced scene analysis methodology also needs to address scalability and adaptability. As new types of suspicious activities emerge or evolve, the algorithm should be able to accommodate these changes without a complete overhaul. Moreover, it must be deployable in a variety of environments, including public spaces, transportation hubs, and critical infrastructure.

Ensuring public safety is a multifaceted challenge that extends beyond algorithmic accuracy. The implementation of a threat detection system requires collaboration with law enforcement, emergency response teams, and relevant authorities. Proper procedures for responding to detected threats and for maintaining the privacy and civil rights of individuals in public spaces must be established.

Continuous improvement and updates to the algorithm are integral to its long-term effectiveness. The evolving nature of technology and the adaptability of potential threats necessitate ongoing research and development efforts. Regularly updating the CNN model, reevaluating the chosen activities, and improving data collection and analysis methods will ensure that the system remains reliable and relevant.

In conclusion, the methodology for advanced scene analysis for threat detection and public safety using an enhanced CNN algorithm is a multifaceted approach that requires careful consideration of activity selection, algorithm design, data quality, real-time analysis, scalability, and adaptability. The success of such a system is contingent on its ability to efficiently and accurately detect threats, while also ensuring public safety and upholding ethical standards. Continuous improvement and collaboration with relevant stakeholders are keys to its long-term success in an ever-evolving security landscape.

5. SYSTEM ARCHITECTURE

The system architecture for this project is a sophisticated framework that combines cutting-edge technology to enhance public safety. This architecture integrates Convolutional Neural Networks (CNNs) for advanced scene analysis and threat detection.

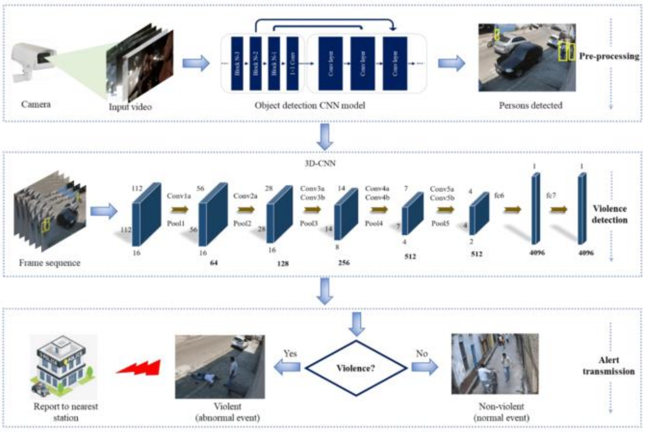

Figure 5.1 System Architecture

It comprises multiple layers, including data input from various surveillance sources, preprocessing modules for image and video data, and CNN-based deep learning models for real-time analysis.

The system processes data through these layers, detecting anomalies and potential threats within public spaces. When a threat is identified, the system triggers immediate alerts to the relevant authorities for swift response, thereby bolstering public safety through the power of artificial intelligence and advanced scene analysis.

6. CONCLUSION AND FUTURE WORK

In conclusion, this research presents a promising approach using CNN architectures for the detection of suspicious activities, highlighting the importance of enhancing model performance and accuracy. In the future, a comparative analysis of various CNN architectures will guide the selection of the most suitable one. Fine-tuning hyperparameters, optimizing training processes, and implementing data augmentation techniques are essential steps to improve model robustness.

Expanding the model's scope to address a wider range of suspicious activities requires a more extensive and diverse dataset, including CCTV footage images. Collaborating with local authorities for real-world data access will be invaluable. This strategic move ensures the model's adaptability to an evolving security landscape, ultimately advancing its capabilities, accuracies and effectiveness of surveillance.

7. REFERENCES

[1] *Bhagyashri Kumbhar1, Pranav Pisal2, Kunal Kene3, Aditi Raut4 , "Suspicious Activity Detection Using Machine Learning", ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 11 Issue V May 2023*

[2] *K. Kranthi Kumar, B. Hema Kumari, T. Saikumar, U. Sridhar, G. Srinivas, G. Sai Karan Reddy, "Suspicious activity detection from video surveillance*", *IJRPR, Vol 3, June-2022*

[3] *Ms. Archana R. Ghuge, Mr. Rushikesh S. Wakchaure, Mr. Sagar D. Wagh, Mr. Parag S. Hude, Ms. Aishwaraya V. Pingale ,"Advance suspicious activity detection",IRJMETS , Volume:03, July-2021*

[4] *Tanzila saba rabia latif , Amjad rehman ,Suliman Mohamed fati , Mudassar raza and Muhammad sharif ," Suspicious Activity Recognition Using Proposed Deep L4-Branched-Actionnet With Entropy Coded Ant Colony System Optimization", Volume 9, 2021*

[5] *Suvarna Nandyal ,Sanjeevkumar Angadi, "Recognition of suspicious Human Activaties using KLT and Kalman Filter for ATM Surveillance System, ICIPTM-2021*

[6] *Shriya Akella, Priyanka Abhang, Vinit Agrharkar, Dr. Reena Sonkusare , "Crowd Density Analysis and Suspicious Activity Detection" , IEEE International Conference for Innovation in Technology (INOCON) Bengaluru, India. Nov 6-8,2020*

[7] *Malika Ben Khalifa, Zied Elouedi, Eric Lefevre, " An Evidential Spammer Detection based on the Suspicious Behaviors' Indicators", IEEE - 2020*

[8] *Sathyajit Loganathan, Sathyajit Loganathan , Sathyajit Loganathan , "Suspicious Activity Detection in Surveillance Footage", ICECTA -2019*

[9] *Md Adil, Rajbala Simon, Sunil Kumar Khatri," Automated Invigilation System for Detection of Suspicious Activities during Examination", IEEE – 2019*

[10] *Mugdha Sharma, " Z - CRIME: A Data Mining Tool for the Detection of Suspicious Criminal Activities Based on Decision Tree", IEEE - 2014*

[11] *Miwa Takai ,''Detection of Suspicious Activity and Estimate of Risk from Human Behavior shot by Surveillance Camera'', IEEE- 2010.*