WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Detecting Suspicious Activity: An Intelligent Alert Generation Framework

Suraj Patekar[1], Prasad Kadam[2], Karan Kamble[3], Dnyaneshwar Jarande[4], Priyanka Agrawal[5]

[1,2,3,4] Department of CSE, Trinity College of Engineering & Research
[5]Asst.Prof Department of CSE, Trinity College of Engineering & Research

ABSTRACT

With the increasing prevalence of cyber threats and security breaches, there is a growing need for robust systems capable of detecting and responding to suspicious activity in a timely manner. This research paper introduces an intelligent alert generation framework designed to address this challenge. Leveraging advanced machine learning algorithms, data analysis techniques, and anomaly detection methodologies, the proposed framework aims to enhance security measures by generating accurate and proactive alerts. The paper provides a comprehensive review of existing alert generation methods, analyzes their strengths and limitations, and presents the novel contributions of the proposed framework. Through extensive experimentation and evaluation, the effectiveness of the framework in detecting suspicious activity is demonstrated, showcasing its potential to improve overall security measures in various domains. The results of this research offer valuable insights and practical implications for the development of intelligent alert generation systems.

Keyword: Suspicious activity detection, Alert generation, Anomaly detection, Machine learning, Data analysis, Security measures.

1. INTRODUCTION

In today's interconnected and digitized world, ensuring the security of various systems and environments has become a critical challenge. With the increasing prevalence of criminal activities, and security breaches, there is an urgent need for robust and proactive systems capable of detecting and responding to suspicious activity. Detecting suspicious activity in real-time plays a crucial role in mitigating potential risks, preventing incidents, and maintaining the overall security posture of organizations, public spaces, and critical infrastructures.

This research paper presents an intelligent alert generation framework designed to address the challenge of detecting suspicious activity and generating timely and accurate alerts. The framework combines advanced machine learning algorithms, data analysis techniques, and anomaly detection methodologies to analyze patterns, anomalies, and deviations from normal behavior. By leveraging the power of these techniques, the framework aims to enhance security measures by providing early warning and proactive response to potential threats.

The primary objective of this research is to develop a comprehensive framework that can effectively detect and alert on suspicious activity in diverse domains such as surveillance systems, public safety, and suspicious activity detection. Detecting suspicious activities is a crucial task in ensuring safety and security in public spaces. With the increasing use of surveillance systems, automated techniques have been developed to aid in identifying and alerting security personnel of suspicious activities. Alert generation is an important aspect of such systems, as it can assist in identifying and preventing potential security threats. In this paper, we present an overview of the various alert generation techniques that have been proposed for detecting suspicious activity.

The contributions of this research lie in the development of an intelligent alert generation framework that combines advanced machine learning algorithms, data analysis techniques, and anomaly detection methodologies. The framework aims to significantly improve the ability to detect and respond to suspicious activity, ultimately enhancing the overall security posture in various domains.

Overall, this research paper aims to address the pressing need for advanced technologies and methodologies in detecting suspicious activity and generating timely and accurate alerts. By developing and evaluating an intelligent alert generation framework, this research endeavors to enhance security measures and foster a safer and more secure environment for individuals, organizations, and society as a whole.

2. LITERATURE SURVEY

ADVANCE SUSPICIOUS ACTIVITY DETECTION

In this paper proposed a system which is capable of doing 2 main tasks, 1st being identifying faces of given suspects, 2nd identifying suspicious activities such as people holding weapons or abandoned bags in public places. They are using a similar approach with convolutional neural networks but this time

to identify or categorize between normal activities from suspicious ones as we already discussed. This both networks are independent of each other, can work simultaneously if necessary, to improve reach of security personnel. Suspicious activity detection works in 2 stages, 1st to identify an activity then to label the activity based on experience of machine learning model 1 out of 2 available labels.

IDENTIFICATION AND DETECTION OF ABNORMAL HUMAN ACTIVITIES USING DEEP LEARNING TECHNIQUES.

This paper adds main intention of installing CCTV is to stop the crime or damage by detecting suspicious or abnormal activities that are happening in the surveillance. Since people are aware of the existence of CCTV almost everywhere, in most situations, behavior of people involved in crimes may seem normal. But too many false alarms could also result in irritations or a loss of trust in the system. Hence, developing such a novel model with less training time and data set, with high accuracy and self-learning with time is highly in need.

SUSPICIOUS ACTIVITY DETECTION USING DEEP LEARNING IN SECURE ASSISTED LIVING IOT ENVIRONMENTS

In this paper, a model is proposed for predicting static and dynamic activities in environments such as daycares and crèches, which requires constant monitoring to protect children from abuse. The model uses adaptive motion estimation and compensation to remove blur from surveillance video. Moreover, a random forest differential evolution method with kernel density (RFKD) is used to predict activities, and the MQTT protocol and IoT technology is implemented to notify legitimate users of abnormal activity. A deep neural network is administered to train the sample data. The proposed RFKD method demonstrates superior results to the ReHAR method on the data sets used in the experimental analysis.

3. PROPOSED SYSTEM

A Convolutional Neural Network is a Deep Learn- ing algorithm which can take in an input image, assign importance to various objects in the image and be able to differentiate one from the other. CNNs are used for image classification and recognition because of its high accuracy.

Techniques Used: Anaconda, Spyder

Our proposed methodology for alert detection in suspicious activity detection involves three main components: object detection, behavior analysis, and anomaly detection. Object detection is used to detect objects in a video frame, behavior analysis is used to analyze the movement and interaction of objects, and anomaly detection is used to identify patterns in behavior that deviate significantly from normal behavior. The output of each component is fed into a decision-making algorithm that determines if an alert should be triggered.

ARCHITECTURE

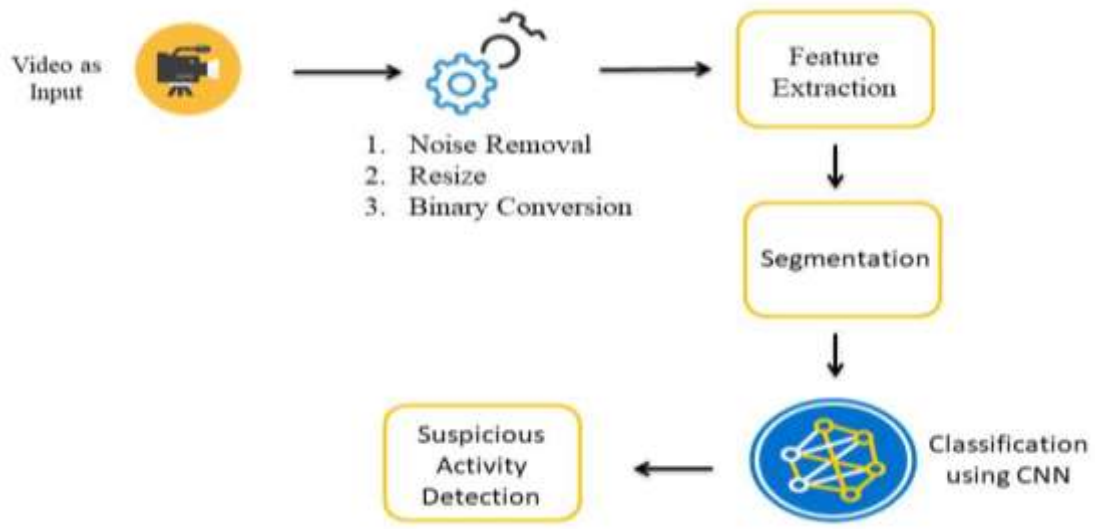
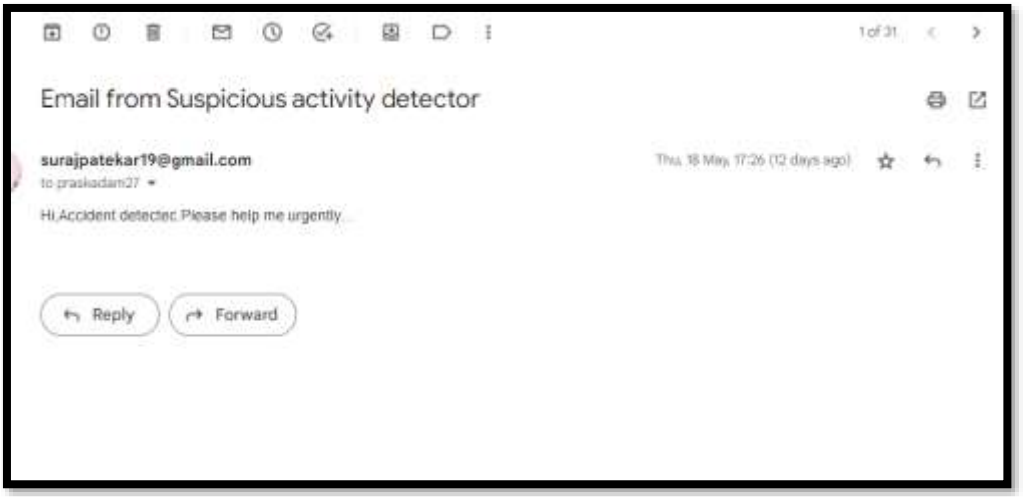


Figure 1.1: System Architecture

4. RESULT



5. CONCLUSION

Alert generation is an essential component of suspicious activity detection systems, and the choice of technique depends on the specific application requirements. In this paper, we presented an overview of the various alert generation techniques and their limitations. Machine learning-based methods have shown the most promising results, but they require significant computational resources and data labeling efforts.

A system to process real-time CCTV footage to detect any suspicious activity will help to create better security and less human intervention.Great strides have been made in the field of human suspicious Activity, which enables us to better serve the myriad applications that are possible with it.

6. FUTURE SCOPE

In Anomaly Recognition System, the challenging part is the real-time execution of the model. A more effective and cost-efficient solution can be implemented in future to overcome this.

The model can also be augmented to discover a potential threat and alert the authorities in advance for the incoming threat and hence, increasing the safety of people.

7. REFRENCES

1. Kavitha, G., & Kulothungan, K. (2021). A survey on rule-based techniques for video surveillance. Multimedia Tools and Applications, 80(12), 18639-18659.

2. Huang, J., & Wang, Q. (2019). Convolutional recurrent neural network for anomaly detection in video surveillance. Neurocomputing, 338, 363-375.

3. Kavitha, G., & Kulothungan, K. (2021). A survey on rule-based techniques for video surveillance. Multimedia Tools and Applications, 80(12), 18639-18659.

4. Naimat Ullah Khan , Wanggen Wan : “A Review of Human Pose Estimation from Single Image”- 978-1-5386-5195-7/18/ 2018 IEEE

5. Tripathi, Rajesh and Jalal, Anand and Agarwal, Subhash(2017). ”Suspicious Human Activity Recognition: a Review”. Artificial Intelligence Review. 50.10.1007/s10462- 017-9545-7.

6. Abouelenien, M., & Moustafa, M. (2017). Real-time anomaly detection in crowded scenes using social force model and trajectory analysis. Pattern Recognition Letters, 94, 161-167.

7. Luo, S., Feng, C., & He, W. (2018). Deep learning for suspicious behavior detection: A review. IEEE Access, 6, 57343-57353.