IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205023 |

Survey towards Suspicious Activity Detection from Surveillance Video

Mr. Pawankumar Shedage, Mr. Tejas Satpute, Mr. Prasad Gharge, Mr. Rohit Gupta,

Prof.Shinde Babaso

Department of Computer Engineering, Shree Ramchandra College of Engineering, Wagholi, Pune, India

ABSTRACT - The important role that human suspicious activity recognition—more specifically, anomaly detection—plays in ensuring people's safety and security is covered in this essay. Closed-circuit television (CCTV) is a common surveillance technique, however it is ineffective since it requires regular human supervision. It is necessary to have an automated security system that can identify suspicious activity in real-time and offer victims immediate assistance. The suggested method examines and finds suspicious human actions in live CCTV footage using machine learning techniques like convolutional neural networks and image processing. The approach has demonstrated improved accuracy and efficiency when evaluated on a dataset that includes both typical and atypical activity. In today's world, where risks are continually growing, the article emphasises the significance of video surveillance and anomaly detection in maintaining people's safety and security. It also emphasises how machine learning methods could be used to create automated security systems that could offer victims real-time support.

KEYWORDS: Video Surveillance, Anomaly Detection, Machine learning, Convolutional neural networks, Image processing.

I. INTRODUCTION

Human Activity Recognition focuses on the importance of anomaly detection in security systems and highlights the challenges associated with it. Anomaly detection aims to detect unexpected actions or patterns, and it is difficult to list all possible negative (anomaly) examples. It is also challenging to collect enough negative samples due to their rarity. Therefore, the paper proposes the use of videos of normal events as training data to learn a model for anomaly detection. The proposed system utilizes machine learning techniques, such as neural networks, to analyze surveillance videos and detect anomalous behavior. An activity recognition system is used to identify the basic day-to-day activities performed by humans, and the activities are categorized into normal and anomalous activities. The model is trained on videos of normal activities, and it is used to detect suspicious events that do not fit into the learned model.The highlights limitations of low-cost depth sensors in estimating human poses from depth images. Therefore, the use of neural networks is proposed as a solution to overcome these limitations. In summary, this emphasizes the importance of detecting anomalous human activity in surveillance videos to ensure safety and security. The use of machine learning techniques, such as neural networks, is proposed to automate the process and improve accuracy. The paper also highlights the challenges associated with collecting negative samples for anomaly detection and proposes the use of videos of normal events as training data.

II. RELATED WORK

According to [1] The use of video surveillance has become increasingly important for ensuring the safety and security of various indoor and outdoor areas. One of the key components of video surveillance is the ability to recognize, understand, and classify human activities as normal or suspicious. This paper presents a hierarchical approach to detect different suspicious activities, including loitering, fainting, and unauthorized entry, based on motion features between objects. The approach first defines different suspicious activities using a semantic approach, which helps in reducing the computational complexity of the system. The object detection is then performed using background subtraction, which helps in detecting the objects present in the surveillance footage. The objects detected are then classified as living (human) or non-living (bag).The next step involves tracking the objects using a correlation technique, which helps in monitoring the movements of the objects in the video footage. Finally, using the motion features and temporal information, the events are classified as normal or suspicious. This approach is highly efficient as it reduces computational complexity and improves the overall efficiency of the system.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205023 |

According to [2] YOLOv3 (You Only Look Once version 3) is a deep learning algorithm that is widely used for object detection in real-time. YOLOv3 can detect multiple objects within an image and provide their location as well as their class label. YOLOv3 is based on convolutional neural networks (CNNs) and is designed to be fast and accurate.In the context of human activity detection, YOLOv3 can be used to detect different types of suspicious activities such as bag-snatching, lock-breaking, and other potentially dangerous activities. The system works by processing video frames and identifying regions of interest where suspicious activities may be taking place. YOLOv3 can then classify these regions of interest into different categories based on the type of suspicious activity being detected. One of the advantages of using YOLOv3 for human activity detection is its speed and accuracy. YOLOv3 can process video frames in real-time and provide accurate detection results with high confidence levels. This makes it an ideal solution for real-time surveillance applications where quick decision-making is crucial.

Then Research paper [3] The paper presents two specific use cases for the application of intelligent surveillance systems: detecting potential gun-based crimes and detecting abandoned luggage. The paper argues that with the increase in criminal activities in urban and suburban areas, it is necessary to detect suspicious activities to minimize risks to human lives.The first case involves the use of a deep neural network model to detect handguns in images. The model is trained on a dataset of images containing handguns and uses convolutional neural networks (CNNs) to learn features that can distinguish between images of handguns and non-handguns. The proposed model can be integrated into an intelligent surveillance system to detect potential gun-based crimes in real-time.The second case involves the use of a machine learning and computer vision pipeline to detect abandoned luggage on frames of surveillance footage. The pipeline involves multiple stages, including object detection, tracking, and classification. The proposed pipeline can be used to identify potential threats caused by abandoned luggage in public spaces.

According to the paper [4] The deep learning model used for this system is based on convolutional neural networks (CNNs) which are trained on a large dataset of labeled video footage. The features are extracted using a pre-trained CNN model and then fed into a fully connected neural network for classification. The model is trained to distinguish between normal and suspicious activities in an academic environment, such as fighting, vandalism, and theft.To improve the accuracy of the model, the system also uses transfer learning, where a pre-trained model is fine-tuned on the specific task at hand. This helps to reduce the amount of training data required and improves the generalization of the model.The system is designed to work in real-time, with the video footage being continuously processed and analyzed. If a suspicious activity is detected, an alert message is sent to the corresponding authority, such as campus security. This allows for quick intervention and prevention of potential incidents.

The research paper from Springer [5] presents an efficient technique for identifying anomalies in videos. This approach takes advantage of the capabilities of convolutional neural networks (CNNs) for object detection and recognition in images. While CNNs have shown great success in image recognition tasks, they are supervised learning models and require labeled data for training. To overcome this limitation, the authors propose a technique called unsupervised feature learning. This approach involves training a deep neural network to extract features from unlabeled data. The features learned in this way can then be used to train a supervised learning model for the target task of anomaly detection.The proposed spatiotemporal architecture combines both 2D and 3D CNNs to extract both spatial and temporal information from the video data. The 2D CNN is used to extract spatial features from individual frames, while the 3D CNN is used to capture the temporal information across multiple frames. The extracted features are then combined and fed into a fully connected network for classification. The authors evaluate their proposed method on several publicly available datasets and show that it outperforms several state-of-the-art methods for anomaly detection in crowded scenes. The proposed method is computationally efficient and can be used in real-time applications.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205023 |

III. System Architecture

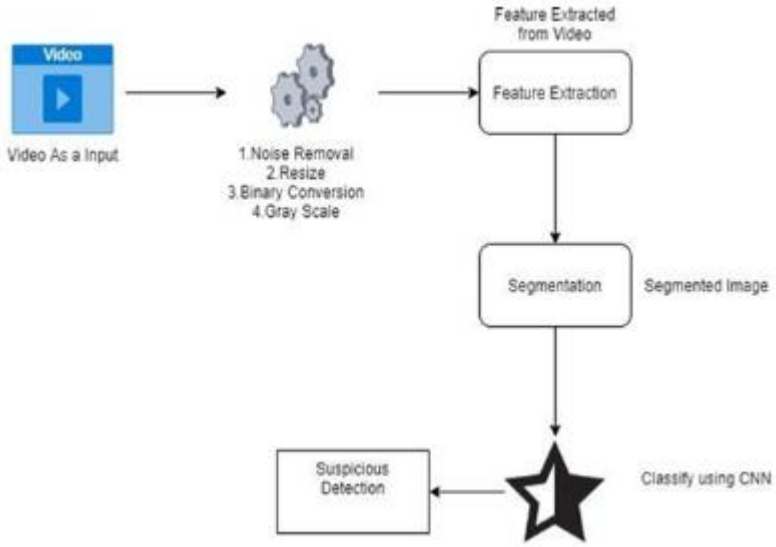

Fig. 1 System Architecture

Proposed model's work:

1.Video Input: The first step is to obtain the video data from a surveillance camera. This video data could be in various formats such as MPEG, AVI, etc. It is important to ensure that the video quality is sufficient and there is no loss of data during transmission.

2.Preprocessing: The next step involves preprocessing the video data. This includes techniques such as resizing, cropping, and normalization of the video data to ensure that it is consistent in size and format.

3.Noise Removal: The video data is often corrupted with noise that can negatively impact the detection accuracy. Therefore, noise removal techniques such as median filtering, Gaussian filtering, etc. are used to remove the noise.

4.Binary Conversion: Binary conversion is a process where each pixel value in the video data is converted to either 0 or 1. This simplifies the data and makes it easier to process further.

5.Grey Scale: Grey Scale is the process of converting the binary image into a grayscale image. This helps to reduce the complexity of the data and also allows for easier feature extraction.

6.Feature Extraction: In this step, features such as edges, corners, and blobs are extracted from the grayscale image. These features help to identify different objects and their movement in the video.

7.Segmentation: Segmentation is the process of dividing the video data into smaller regions based on the features that have been extracted. This helps to identify regions where suspicious activity may be occurring.

8.Classification using CNN: In this step, a Convolutional Neural Network (CNN) is used to classify the segmented regions as either normal or suspicious. CNNs are well suited for image and video classification tasks as they are capable of learning and detecting complex patterns in the data.

9.Suspicious Detection: The final step is to use the output of the CNN to detect suspicious activity. If a segment is classified as suspicious, an alert can be sent to security personnel to investigate further.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205023 |

IV. CONCLUSION

The proposed system is an innovative approach to address the need for improved security systems to detect criminal activities in real-world scenarios. The system is designed to analyze surveillance videos and identify abnormal behavior that may be indicative of criminal activity. The increasing incidence of crime has made it necessary to develop such a security system that can help detect criminal activities in real-time. Traditional approaches to surveillance, such as human monitoring or rule-based systems, have been found to be inadequate in identifying complex and evolving criminal behavior. Therefore, there is a need for an automated system that can accurately detect and respond to abnormal behavior. The proposed system uses a convolutional neural network (CNN), a deep learning approach that has proven to be highly effective in various image and video recognition tasks. The CNN is trained on a large dataset of annotated surveillance videos to learn the patterns and features that are indicative of criminal behavior. The CNN-based system has several advantages over traditional methods, including high accuracy and efficiency in detecting criminal activity. Unlike rule-based systems, which rely on pre-defined rules, the CNN can learn from data and adapt to new and evolving criminal behavior.

REFERENCES

[1] U.M Kamthe and C.G. Patil, "Suspicious Activity Recognition in Video Surveillance System," 4th International Conference on Computing Communication Control and Automation (ICCUBEA), 16–18 August 2018, Pune, India.
[2] "Suspicious Activity Detection From Videos Using YOLOvs"-2020 IEEE 17TH INDIA COUNCIL INTERNATIONAL CONFERECE (INDICON), 10-13 DECEMBER 2020, NEW DELHI, INDIA. Nipunjita Bordoloi, Anjan Kumar Talukdar, and Kandarpa Kumar Sarma.
[3] "Suspicious Activity Detection in Surveillance Footage," Sathyajit Loganathan, Gayashan Kariyawasan, and Prasanna Sumathipala.-2019 INTERNATIONAL CONFERECTION ON ELECTRICAL AND COMPUTING TECHNOLOGIES AND APPLICATIONS (ICECTA), 19–21 NOVEMBER 2019, RAS AI CHAIMAH, UNITED ARAB EMIRATES.
[4] C.V. Amrutha, C. Jyotsna, and J. Amudha, "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video," 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangaluru, India, March 5–7, 2020.
[5] Wazha Mmereki, Rodrigo S. Jamisola, Dimane Mpoeleng, Tinao Petso: "YOLOv3-Based Human Activity Recognition as Viewed from a Moving High-Altitude Aerial Camera"- 2021 7TH INTERNATIONAL CONFERENCE ON AUTOMATION, ROBOTICS AND APPLICATIONS (ICARA), 04-06 FEBRUARY 2021, PRAGUE, CZECH REPUBLIC.
[6] "Alert Generation on Detection of Suspicious Activity Using Transfer Learning" by Om M. Rajpurkar, Siddesh S. Kamble, Jayram P. Nandagiri, and Anant V. Nimkar.- KHARAGPUR, INDIA, 01–03 JULY 2020, 11TH INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND NETWORKING TECHNOLOGIES (ICCCNT).
[7] "Human Suspicious Activity Detection Using Ensemble Machine Learning Techniques," by Aqil Shamnath and Meena Belwal.- HUBLI, India, 24-26 JUNE 2022, 2nd International Conference on Intelligent Technologies (CONIT).

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details