IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

Smart Video-Based Threat Analysis and Detection using CNN

Shubhada P. Mone[1], Mukul Borole[2], Devashish Shahakar[3], Dnyanesh Mahajan[4]
Assistant Professor, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2,3,4]
Marathwada Mitra Mandal's College of Engineering, Pune, Maharashtra, India

Abstract: *In recent years, more and more video surveillance devices like drones, CCTV's have been deployed due to an increase in demands related to public security and smart cities. There is a need to overcome the existing drawbacks of post-investigation techniques of video surveillance systems by providing a pre-alert generation system. The video surveillance system has become an important part of the security and protection of modern cities. So we are going to focus on video surveillance by giving video contents containing early fire events detection, suspicious activities and smart parking systems, and crowd estimation. Smart monitoring cameras equipped with intelligent video analytics techniques can monitor and pre-alert systems by capturing suspicious activity and events. Our work is based on deep learning techniques for video analysis with better performance and event detection with the advantages of alert generation.*

Keywords: Video surveillance, background subtraction**,** Suspicious Activity, Suspicious Object, Alert generation, CNN.

I. INTRODUCTION

From the Stone age era, security was a top priority for humans. They were threatened by being attacked by wild animals. Today, the world has evolved tremendously. Now, humans are threatened by being attacked by other humans. The recent rise of anti-social activities such as violent protests, theft, bomb attacks, and other terrorist attacks have highlighted the need for clever video surveillance systems. In the last few decades, video surveillance systems have gained tremendous attention. Because of their huge application prospects, it has attracted more and more researchers. These systems help in monitoring and alerting the surrounding threats in real-time.

Suspicious activity is any observed behavior that could indicate a person may be involved in a crime or about to commit a crime. An object is suspicious when it is unattended for a long period[4]. The problem with the current surveillance system is that it is not smart enough to report a crime and suspicious thing to the security personnel at the same time as it is recording [1]. Hence, we are proposing a system that will help to detect suspicious things as fast as possible. And at same time it will send alert messages to security personnel.

II. LITERATURE REVIEW

According to the review carried out, the researchers have resolved various methods to detect suspicious activity in a very efficient way. For detecting anomalous behavior, the CNN i.e. convolution neural network has been used[1]. It is based on extracting key features from each frame of the video.

For systematic proceeding, 5 suspicious activities are selected which are shooting, punching, kicking, knife attack and sword fight. After extracting images from the video frame, cleaning of images takes place (removal noise and background effects)[5]. The ResNet model of CNN is used for processing. Accuracy of 94.85% is obtained with the use of ResNet-50

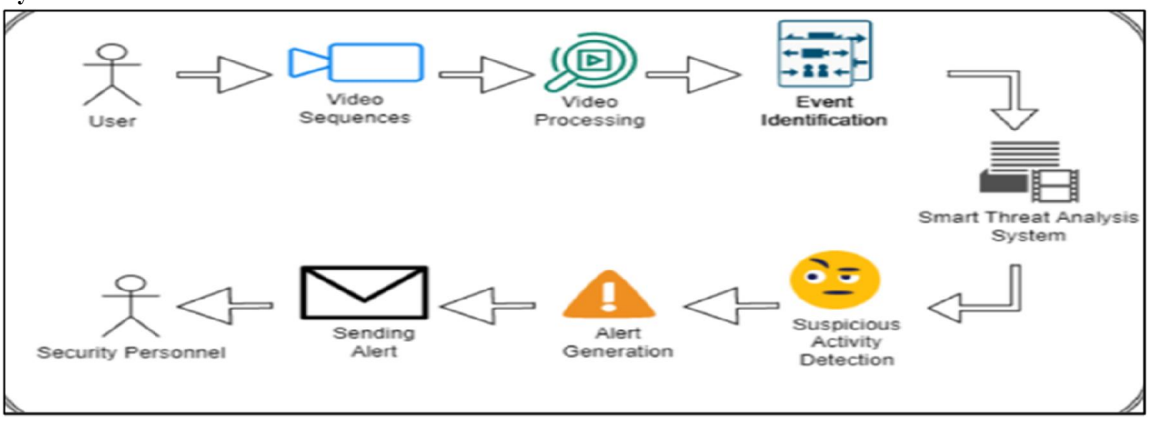
A method for decision making from sequences of video frames using ML techniques and sending notifications of abnormal activities to IoT notification devices is proposed in [3]. Main focus is on developing the system for continuous monitoring of children who are kept in day care centers by their parents. For video processing, Random Forest classifier is used. The average accuracy of suspected activity prediction rate was measured to be 98.88%.

A method to detect suspicious objects in a real time environment is proposed in [4]. For detection of objects, they used a mixture of Gaussian methods. Morphological filtering is used for better detection.

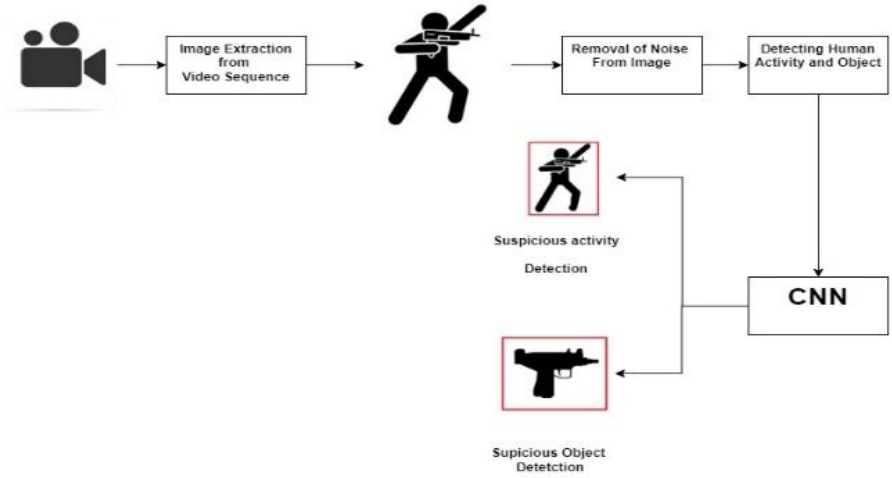
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

III. FIGURES

3.1 System Architecture



IV. PROPOSED SYSTEM



V. ALGORITHM

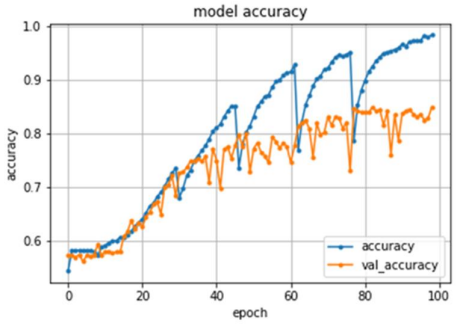
- **Step 1**: Input is given as video.
- **Step 2**: Extraction of image from video takes place.
- **Step 3**: Then many different filters are applied to the extracted image to create a feature map.
- **Step 4**: Next a ReLU function is applied to increase non-linearity.
- **Step 5**: Then apply a pooling layer to each and every feature map.
- **Step 6**: The algorithm compresses the pooled images into one long vector.
- **Step 7**: In the next step, input the vector to the algorithm into a fully connected artificial neural network.
- **Step 8**: Processes the features via the network. At the end fully connected layer delivers the "voting" of the classes.
- **Step 9**: Train through forward propagation and back propagation for numerous epochs. This repetition occurs until we have a well-defined neural network with trained weights.

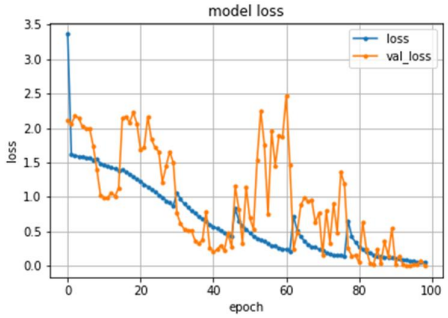
VI. RESULTS

The proposed model was trained and tested using data from the UCF Crime Dataset. It has a total of 14 classes, one of which is Normal. Because there were so many normal videos, we had to delete some of them to keep the proportionality.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

The dataset contains many sub-videos that together form a single video feed. The proposed model is trained by feeding extracted video frames. We created a CSV file to define the labels, which links the video to the appropriate label and helps the model understand what the video represents. The trained model is about 192 MB in size. We only need to provide video as the input and gives a particular label as output. The proposed model aims to detect anomalous behavior in the video, and the system achieves an accuracy of 85%. The graphs that represent loss and accuracy are shown below.





VII. Conclusion

All the implementation mentioned is based on the processing of video sequences, giving it to a deep learning model to give the required results. This model tries its best for early detection of the occurrence of suspicious activities and report it to the security personnel. This model will be helpful for every CCTV and drone camera. This model will perform better than the original one.

References

[1]. Tejashri Subhash Bora, Monika Dhananjay Rokade "Human suspicious activity detection system using CNN model for video surveillance". International Journal of Advance Research and Innovative Ideas in Education

[2]. C. V. Amrutha, C. Jyotsna and J. Amudha, "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)

[3]. Vallathan, G., John, A., Thirumalai, C. et al. "Suspicious activity detection using deep learning in secure assisted living IoT environments". J Supercomput 77, 3242–3260 (2021).

[4]. Trupti M. Pandit, P.M.Jadhav, A.C.Phadke, "Suspicious Object Detection In Surveillance Videos For Security Applications". in 2016 International Conference on Inventive Computation Technologies (ICICT),added in IEEE Xplore 19 January 2017

[5]. Rachana Gugale, Abhiruchi Shendkar, Arisha Chamadia, Swati Patra, Deepali Ahir "Human Suspicious Activity Detection using Deep Learning" in International Research Journal of Engineering and Technology (IRJET) ,Volume: 07 Issue: 06 | June 2020

[6]. Patel Parin, Gayatri Pandi " Traffic Monitoring using Video Stream with Machine Learning: Based on Big Data Process with Cloud". International Journal of Innovations & Advancement in Computer Science 2017

[7]. Jeany Son,Mooyeol Baek,Minsu Cho,Bohyung Han "Multi-Object Tracking with Quadruplet Convolutional Neural Networks" Dept. of Computer Science and Engineering, POSTECH, Korea 2017