IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

Suspicious Activity Detection

[1]Aditya Chapke, [2]Sohel Bagwan, [3]Rohit Gadge, [4]Dr.B. D. Jadhav
[123]Students, Department of Electronics and Telecommunication
[4]Proffesor , Department of Electronics and Telecommunication
JSPM'S Rajarshi Shahu College of Engineering, Pune, Maharashtra, India

Abstract: *Video Surveillance plays a significant role in today's world. Various technologies have been utilized to implement the safety of life and property by installing high quality CCTV cameras. It is impossible to manually monitor each and every moment activity. Furthermore, in practical scenario the most unpredictable one is human behavior and it is very difficult to find whether it is suspicious or normal. In this work the notion of Convolution Neural Network is used to detect suspicious or normal activity in an environment, and a system is proposed that sends an alert message to the corresponding authority, in case of predicting a suspicious activity. This project will entail detectingsuspicious human Activity from real-time CCTV footage using neural networks. Human suspicious Activity is one of the key problems in computer vision that has been studied for more than 15 years. It is important because of the sheer number of applications which can benefit from Activity detection. Hence, we plan to use neural networks to overcome these problems. Suspicious human activity recognition from surveillance video is an activeresearch area of image processing and computer vision. Through the visual surveillance, human activities can be monitored in sensitive and public areas such as bus stations, railway stations, airports, banks, shopping malls, school and colleges, parking lots, roads, etc. to prevent terrorism, theft, accidents and illegal parking, vandalism, fighting, chain snatching, crime and other suspicious activities. It is very difficult to watch public places continuously, therefore an intelligent video surveillance is required that can monitor the humanactivities in real-time and categorize them as usual and unusual activities; and can generate an alert.*

Keywords: Convolution Neural Network, Anomaly, CCTV, Video Surveillance, etc

I. INTRODUCTION

Now a day's human behavior and activity pattern research are more important in surveillance. Detection and tracking the object of behavior is important factor in video surveillance system. Over a last decade it has been seen the rapid growth and an extraordinary improvement in real- time video analysis. Main goal of video analytics is to identify the potential threaten events with less or no human intervention. Video surveillance is a prominent area of research which includes recognition of human activities and categorization of them into usual, unusual or suspicious activities. The primary goal is to find unexpected events in videos using a surveillance system that might be human, semi-automatic, or fully automated. Humans are completely reliant on the manual surveillance system. Analyzing behavior or distinguishing abnormal from regular conduct required physical labor. Semiautomatic systems require less human interaction, whereas fully automatic video surveillance systems do not require human intervention to make decisions. Face recognition is another approach for detecting intrusions. A criminal dataset is built and saved in the system. Python's OpenCV package is used to recognize faces. This recognition procedure involves internal picture processing and deep learning. The system becomes more accurate as a result of such advanced technology.

We plan to build an application for detection of suspicious activity of people in public places in real time. Our application can be used in surveillance at places like malls, airports, railway stations, etc. where there is a risk of robbery or a shooting attack. We will be using deep learning and neural networks to train our system. This model will then be deployed as a mobile and desktop app which will take real time CCTV footage as input and send an alert on the administrator's device if somesuspicious pose is found. Human suspicious activity is related to identifying humanbody parts and possibly tracking their movements. Real life applications of it vary from gaming to AR/VR, to healthcare and gesture recognition. Compared to image data domain, there is relatively little work on applying CNNs to video

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

classification. This is because, a video is more complex than images since it has another dimension-temporal. Unsupervised learning exploits temporal dependencies between frames and has proven successful for video analysis.
Some suspicious activity approaches use CPU instead of GPU so that suspicious activity can run on low cost hardware like embedded systems and mobile phones. Low cost depth sensors are another newtechnology in computer vision. They are present in gaming consoles like the Kinectfor Xbox 360. They are motion sensors which allow the user to interact with the console without a game controller, through just hand gestures. These are RGB-D sensors that obtain depth information by structured light technology. The structuredlight sensors infer the depth values by projecting an infrared light pattern onto a scene and analyzing the distortion of the projected light pattern. However, these sensors are limited to indoor use, and their low resolution and noisy depth information makeit difficult to estimate human poses from depth images.

II. LITERATURE SURVEY

According to [1] Sparse coding has constructed anomaly detection which shown better performance, even contain the theories are feature learning, sparse representation, and dictionary learning. In this paper, a innovative neural network is proposed for anomaly detection which is also labeled as AnomalyNet by deeply accomplishing feature learning, sparse representation as well as dictionary learning in three joint neural processing blocks. Specifically, to learn improved features, the authors design a motion fusion block accompanied by a feature transfer block to relish the benefits of eliminating background noisy, capturing motion and improving data insufficiency.
According to [2] An suspicious activity is any observation of action that could state a person may be involved in a crime or is about to commit a certain criminality. Anomaly detection is the process detecting suspicious activity. Surveillance cameras are one of the best solution to the issue of security in various places. Present-day system needs man power for monitoring the system as detecting and identifying criminal and abnormal activity is so challenging. So this paper carry out a survey on anomaly detection for video surveillance using different concepts like deep learning, RNN etc.
Then Research paper [3] automates the detection of anomalous actions within long video series is challenging due to the uncertainty of how such events are defined. The authors tactic the problem by learning generative models that can discover anomalies in videos using restricted supervision. Projected end-to-end trainable complex Convolutional Long Short-Term Memory (Conv-LSTM) networks that are able to predict the development of a video sequence from a minor number of input frames.
According to the paper [4] , authors inspired by the capability of sparse coding based suspicious detection, projected a Temporally-coherent Sparse Coding (TSC) where they implement similar neighboring frames be encoded with alike reconstruction coefficients. Then mapped the TSC with a distinct type of stacked Recurrent Neural Network (sRNN). The contributions of the paper are- i) proposed a TSC, which can be recorded to a sRNN which facilitates the parameter optimization and speed up the doubtful prediction. ii) Build a very huge dataset that is even larger than the summation of all existing dataset for finding anomalous activity.
The research paper from Springer [5] presented an efficient technique for identifying anomalies in videos. Recently applications of convolutional neural networks have shown possibilities of convolutional layers for object detection and recognition, specifically in images. Though, convolutional neural networks are supervised and have need of labels as learning signals. Authors as well as proposed a spatiotemporal architecture for suspicious detection in videos with crowded scenes.
The paper [6] proposed end-to-end trainable complex Convolutional Long Short-Term Memory (Conv-LSTM) networks. These Conv-LSTM networks are capable to predict the evolution of a video sequence from a minor number of input frames. Consistency scores are derived from the reconstruction errors of a set of estimates with irregular video sequences yielding lower regularity scores as they separate further from the actual sequence over time. The models employ a composite structure and observe the special effects of conditioning in learning more meaningful representations.
According to [7], the approach for this problem by learning a generative model for consistent motion patterns using multiple resources with very restricted supervision. Specifically, paper contains two methods that are built upon the auto encoders for their capacity to work with little to no supervision. The first method is to leverage the conventional

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

handcrafted spatio-temporal local features and then study the fully connected autoencoder. Secondly, construct a fully convolutional feed-forward autoencoder to learn together the local features and the classifiers as an end-to-end learning structure. The proposed model is able to capture the regularities from numerous datasets.

The paper [8], authors has proposed the technique for actual time anomaly detection and localization in crowded scenes. Each video is well-defined as a set of non-overlapping cubic spots, and is explained using two local and global descriptors. The descriptors used here capture the video assets from different phases. By integrating simple and cost-effective Gaussian classifiers, we can distinguish normal events and anomalies in videos.

Then Research paper [9] is basically on inherent redundancy of video structures, authors propose an effective sparse combination learning framework. It accomplishes decent performance in the detection phase deprived of compromising result quality. The short running time is fail-safe because the new method efficiently turns the original complex problem to one where only a few less in cost small-scale least square optimization steps are considered. The process scopes high detection rates on benchmark datasets when figuring on a usual desktop PC by using MATLAB.

III. SYSTEM DESIGN

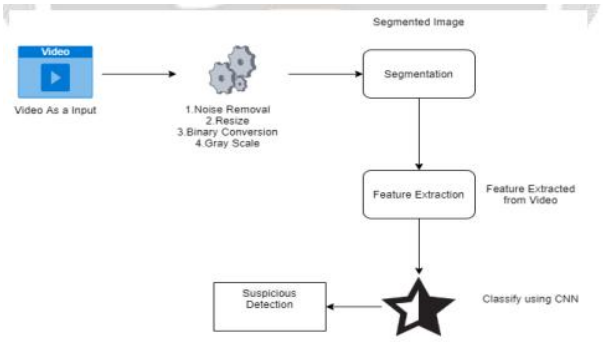

Fig-1: System Architecture

In our proposed system, for detecting anomalous behavior, the CNN i.e. convolution neural network has been used. For effectively classification of anomalous activities, it is essential to recognize the temporal data in the video. Recently, CNN is mostly used for extracting key features from each frame of the video. CNN is only the algorithm best suited for this purpose. For classifying the given input successful, it is necessary that the features get extracted from CNN, therefore CNN should be capable of knowing and extracting the needed features from the frame of videos.

IV. ALGORITHM

Convolutional Neural Network (CNN) algorithm is used to implement the project.

Steps for CNN Algorithm is as follows:

Step 1: Input is given as image / video.

Step 2: Then many different filters are applied to the input to create a feature map.

Step 3: Next a ReLU (Rectified Linear Unit) function is applied to increase non-linearity.

Step 4: Then applies a pooling layer to each and every feature map.

Step 5: The algorithm compresses the pooled images into one long vector.

Step 6: In next step, inputs the vector to the algorithm into a fully connected artificial neural network.

Step 7: Processes the features via the network. At the end fully connected layer delivers the “voting” of the classes.

Step 8: In this last step training is conducted through forward propagation and back propagation for numerous epochs. This repetition occurs until we have a well-defined neural network with trained weights and feature detectors.

V. RESULT AND DISCUSSION

The dataset of the proposed model includes videos of anomalous behavior which are Arson, Burglary, fighting as well as it also contains videos of normal behavior. Since the surveillance videos are very sensitive and hard to get, the videos for the normal behavior had to be created manually with the help of standard camera and for the anomalous behavior the videos are taken from the work dataset and through social media.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

We extract various existing data as well as currently posted information through various websites. The dataset includes a total of 15 videos for training purposes and 7 videos for the testing purpose. We downloaded about 4-5 GB data as a video samples to use machine learning algorithms for testing the proposed method.

VI. CONCLUSION

In this work, suspicious activity detection application is presented based on convolution neural network. The proposed model is successfully trained with CCTV footage instead of normal training datasets. Spatiotemporal analysis is implemented. The proposed system is a machine approach to detect real-world criminal activity identification in surveillance videos. The necessity to develop such a security system is increasing with the increasing number of crimes that are happening every day. The result of the proposed system is detection the anomaly. Manual process is substituted by intelligent automation process

REFERENCES

[1]. Joey Tianyi Zhou, Jiawei Du, Hongyuan Zhu, Xi Peng, Rick Siow Mong Goh, ”AnomalyNet: An Anomaly Detection Network for Video Surveillance, 2019.

[2]. Monika D. Rokade and Tejashri S. Bora, "Survey On Anomaly Detection for Video Surveillance" 2021 International Research Journal of Engineering and Technology(IRJET).

[3]. Jefferson Ryan Medel, Andreas Savakis, “Anomaly Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks” under review.

[4]. W. Luo, W. Liu, and S. Gao, “A revisit of sparse coding based anomaly detection in stacked rnn framework,” in The IEEE International Conference on Computer Vision (ICCV), Oct 2017

[5]. Y. S. Chong and Y. H. Tay, “Abnormal event detection in videos using spatiotemporal autoencoder,” in International Symposium on Neural Networks. Springer, 2017, pp. 189–196.

[6]. J. R. Medel and A. Savakis, “Anomaly detection in video using predictive convolutional long short-term memory networks,” arXiv preprint arXiv:1612.00390, 2016.

[7]. M. Hasan, J. Choi, J. Neumann, A. K. Roy-Chowdhury, and L. S. Davis, “Learning temporal regularity in video sequences,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 733–742.

[8]. M. Sabokrou, M. Fathy, M. Hoseini, and R. Klette, “Real-time anomaly detection and localization in crowded scenes,” in The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, June 2015.

[9]. C. Lu, J. Shi, and J. Jia, “Abnormal event detection at 150 fps in matlab ,” in Proceedings of the IEEE international conference on computer vision, 2013, pp. 2720–2727.

[10]. H. Mousavi, M. Nabi, H. K. Galoogahi, A. Perina, and V. Murino, “Abnormality detection with improved histogram of oriented tracklets,” in International Conference on Image Analysis and Processing. Springer, 2015, pp. 722–732.

[11]. Monika D.Rokade, Dr. Yogesh Kumar Sharma, "MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE 2021.

[12]. Monika D.Rokade, Dr. Yogesh Kumar Sharma, "Identification of Malicious Activity for Network Packet using Deep Learning “, in 2020