|| Volume 6 || Issue 5 || May 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

METHODOLOGY FOR HUMAN SUSPICIOUS ACTIVITY DETECTION

Tejashri Subhash Bora[1], Monika Dhananjay Rokade[2]

PG Student and Asst. Prof., Department of Computer Engg., SPCOE, Pune, India[1 2]

boratej283@gmail.com[1], monikarokade04@gmail.com[2]

Abstract: - The crime is increasing day by day. So for the security, the demands for surveillance cameras are also increased. Surveillance cameras are more and more being used in public places e.g. streets, intersections, banks, shopping malls, etc. However, the monitoring ability of law enforcement agencies has not kept pace. The outcome is that there is a deficiency in the utilization of surveillance cameras and an unworkable ratio of cameras to human monitors. One critical task in video surveillance is detecting anomalous events such as traffic accidents, crimes or illegal activities Such systems require frequent rule-base updates and signature updates, and are not capable of detecting unknown attacks. So to overcome from this problem we proposed a system which will analyze and detect the suspicious human activity from real-time CCTV footage using neural networks.

Keywords: - *Anomaly detection, Video Surveillance, CNN, Machine learning, Image processing*.

I INTRODUCTION

Seen the increasing demand for security, surveillance cameras have been widely set up as the infrastructure for video analysis. One of the major challenges faced by surveillance video analysis is detecting abnormal activity which requires exhausting human efforts. Fortunately, such a labour-intensive task can be recast as an anomaly detection problem which aims to detect unexpected actions or patterns. Anomaly detection varies from the traditional classification problem in the following aspects: 1) It is very difficult to list all possible negative (anomaly) illustrations. 2) It is a daunting job to collect adequate negative samples due to the rarity.

To achieve anomaly detection, one of the most widespread method is using the videos of normal events as training data to learn a model and then detecting the suspicious events which would do not fit in the learned model. For example, human pose estimation is used in applications including video surveillance, animal tracing and actions understanding, sign language recognition, advanced human-computer interaction, and marker less motion capturing. Low cost depth sensors have restrictions like limited to indoor use, and their very low resolution and noisy depth information make it problematic to estimate human poses from depth images. Hence, we are to using neural networks to overcome these problems. Anomalous human activity recognition from surveillance video is an active exploration part of image processing and computer visualization. Through the visual observation, human activities can be detected in sensitive and public areas such as bus and railway stations, airports, banks, shopping malls, universities (school and college), parking lots, roads, etc. to prevent terrorism, theft, accidents and illegal parking, vandalism, fighting, chain snatching, crime and other doubtful activities. It is very tough task to watch public places constantly, therefore an intelligent video surveillance is required that can monitor the human activities in real-time and classify them as normal and strange activities; and can generate an alert.

II HISTORY AND BACKGROUND

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 autoencoders for their capacity to work with little to no supervision. The first method is to leverage the conventional 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.

III METHODOLOGY

The algorithm, implemented in our model is CNN. CNN stands for Convolutional neural network which is a category of artificial neural networks(ANN) that has become leading in multiple digital vision tasks, is attracting the attention across many of the domains. CNN is intended to automatically and adaptively learn spacial orders of features through back-propagation by implementing multiple stages, like as convolution layers, pooling layer, flatten and fully connected layers. Several researchers has been carried out with totally different ways for positive and negative classification, aspect base classification, etc. Maximum of the existing approaches make use of unsupervised algorithm and techniques for anomaly detection. We are using supervised learning approach having one preparation dataset and a test dataset for classification.

Training set is completely having input feature courses and their consistent class labels. Employing this training dataset, an classification model is generated which tries to order the input courses into equivalent class names or labels. Then a test set is used to confirm the model by deriving the class labels of anonymous feature courses. A variety of machine learning and deep learning techniques like Long short term Memory(LSTM) along with Advance Motion Detection (AMD) algorithm, SURF (Speed Up Robust Features), ANN (Artificial Neural Network), Gaussian Classifiers, sparse auto encoder are used.

IV PROPOSED SYSTEM

Proposed work of model:-

- **Data Collection:**

First of all, the information form various Websites and Social Media applications based on certain parameters is extracted data.

- **Pre- Processing**

Then we are going to apply numerous pre-processing steps like as Noise removal, resizing, binary conversion and gray scaling in order to make our dataset proper to use.

- **Noise Removal**

Noise is detached from the input video. In image processing, the key method for denoising is filtering. Generally average filters, median filters, Wiener filters and Kalman filters are utilized to diminish noise.

- **Resizing**

Image resizing is necessary when the necessity is to increase or decrease the total number of pixels, whereas remapping can be

done when we are adjusting for lens distortion or rotating an image.

- **Binary Conversion**

A binary image is one that holds the pixels that can have any one of precisely two colors, classically black and white. Binary images are also entitled as bi-level or two-level. This means that each and every single pixel is stored as a solitary bit—i.e., in value of 0 or 1.

- **Gray Scaling**

Gray-scaling is the method of transforming a continuous-tone image to an image that a computer can manipulate effortlessly.

- **Segmentation**

Image segmentation is the significant process in which isolation of a digital image into multiple segments is carried out i.e. (sets of pixels, also recognized as image objects).

- **Feature Extraction**

Feature extraction is a part of the dimensionality decrease procedure, in which, an initial set of the raw data is separated and compact to more controllable groups.

- **Classification**

Classification is the method of sorting and labeling groups of pixels or vectors with in an image based on definite rules and instruction.

- **Data Training**

We compile artificial as well as real time using social media data and provide training with any machine learning classifier.

- **Data Testing with Machine Learning**

We give testing dataset to system and apply machine learning algorithm to detect the activity accordingly.

- **Analysis**

We determine the accuracy of proposed system and estimate with other existing systems.

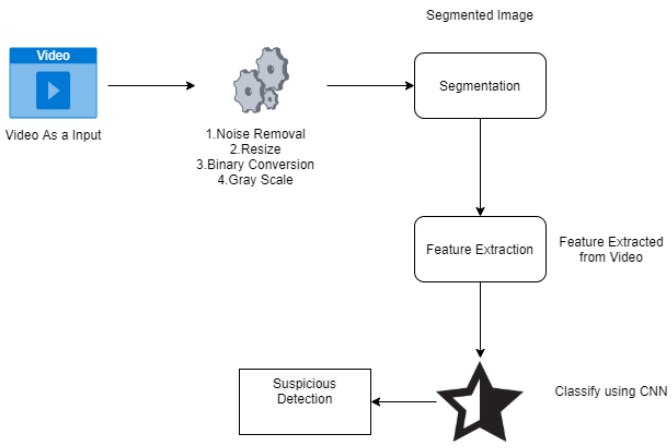

Figure 1: *System Architecture*

V . RESULT AND DISCUSSION

The results and discussion may be shared into Expected result is given as follows:

a) System service providers detect anomaly activity.

b) Classify anomalous action using trained classification, which can automatically predict some predefined class with anomaly detection.

c) No. of computation are less.

d) Performance has been increased with the reduced cost.

VI . CONCLUSION

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 everyday. The result of the proposed system will be able to detect whether any anomaly action is taking place or not. And most of the previous researches had lower accuracy in determining the abnormal behavior. Therefore, in this a new approach CNN is used for better results.

ACKNOWLEDGMENT

Authors want to acknowledge Principal, Head of Computer department Prof. S.S. Khatal and the guide Prof. M.D. Rokade for all the support and help rendered. To express profound feeling of gratitude to the regarded guardians for giving the motivation needed for finishing of paper.

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] Tejashri S. Bora and Monika D. Rokade, "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] Z. Zhu, J. Wang, and N. Yu, "Anomaly detection via 3d-hof and fast double sparse representation," in Image Processing (ICIP), 2016 IEEE International Conference on. IEEE, 2016, pp. 286–290.

[12] T. Xiao, C. Zhang, H. Zha, and F. Wei, "Anomaly detection via local coordinate factorization and spatio-temporal pyramid," in Asian Conference on Computer Vision. Springer, 2014, pp. 66–82.

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

[14] M. D. Zeiler, "Adadelta: an adaptive learning rate method," arXiv preprintarXiv:1212.5701, 2012.