IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Surveillance-based Suspicious Activity Detection: Techniques, Application and Challenges

[1]Nandini Fal Dessai, [2]Prof. Shruti Pednekar,

[1]Student, [2]Professor

[1]Department of Computer Science and Engineering,

Goa College of Engineering, Goa, India

Abstract: Suspicious activity identification from surveillance video is an effective research area of image processing and computer vision. Detecting suspicious activities is significant for maintaining the security of organizations and communities. Surveillance cameras are mostly used in public areas to monitor and secure safety. It is difficult to observe public places continuously, so hence intelligent video surveillance is needed that can detect human activity in real-time and classify them as non-suspicious & suspicious activities. To solve these problems, we will create a Long-term recurrent convolutional network (LRCN) system to record the CCTV footage and to detect suspicious & non-suspicious activities. The system is also used to generate an alarm that will inform the user if any suspicious activities are detected.

Keywords- CNN, LRCN, Suspicious Activity, Non-Suspicious Activity.

I. INTRODUCTION

In today's modern world CCTV surveillance is the primary & impactful security feature a premises can have. CCTV can be establish in Hospitals, Universities, Malls, etc. being the most popular way of preventing and detecting the unfavorable activities. human activity recognition is useful in numerious situations, which includes detecting abnormal behavior in security systems. With the growing need for security, surveillance cameras have become common for analyzing video footage. Many organizations have installed CCTV cameras to monitor people and their actions. One big problem with analyzing surveillance videos is figuring out when something unusual is happening.

Human behavior identification in real-world environments discover plenty of applications. Understanding how people behave in the real world is really useful for things like smart security cameras and figuring out how people shop. Security cameras are used to keep people safe and are found in many places both inside and outside. Watching these cameras all the time is impossible, and even if something has happened, finding the right video clip takes a lot of time. Now, there is new technology that can automatically analyze videos and spot unusual things happening. This is really helpful for making sure people stay safe.

Human behavior detection in video surveillance systems is an automated way of intelligently detecting any suspicious activity. Numbers of efficient algorithms are available for the automatic detection of human behavior in public areas like airports, railway stations, banks, offices, examination halls, etc. Automated video surveillance systems are crucial for security purposes. These systems detect and track moving objects in video sequences, and can automatically identify potential security incidents. Computer Vision researchers are currently focused on developing automated video surveillance systems that can handle dynamic and complex scenes. Video surveillance is the emerging area in the application of Artificial Intelligence, Machine Learning and Deep Learning. Artificial intelligence helps the Scomputer to think like a human. In machine learning, important components are learning from the training data and making predictions on future data.

Nowadays GPU (Graphics Processing Unit) processors and huge datasets are available, so the concept of deep learning is used. Deep Neural Networks is one of the best architectures used to perform difficult learning tasks. Deep Learning models automatically extract features and build high-level representation of image data this is more generic because the process of feature extraction is fully automated. From the image pixels, convolutional neural networks (CNN) can learn visual patterns directly. In the case of video streams, long short-term memory (LSTM) models are capable of learning long term dependencies. The LSTM network has the ability to remember things. The proposed system will use security camera footage to keep an eye on what people are doing on a college campus. If something seems strange, people will be alerted. The most important parts of the system are figuring out when something strange is happening and understanding how people usually behave.

II. LITERATURE REVIEW

The related work suggests different approaches for detecting human behaviors from video. The objective of the works was to detect any abnormal or suspicious events in video surveillance. Video surveillance is crucial for indoor and outdoor security. The system's components, such as behavior recognition, can classify activities as normal or suspicious in real-time [01, 02].

P. Bhagya [03] uses a hierarchical approach to detect suspicious activities based on motion features between objects. The Semantic approach defines suspicious activities, background subtraction detects objects, correlation technique tracks them, and motion features and temporal information classify events. The semantic approach reduces computational complexity and improves efficiency [03].

Detecting abnormal events in video surveillance is difficult but significant for security systems. Making sure that security cameras can spot unusual things happening is really important, but it's not easy. Wang [05] came up with a way to do this using a special computer program. He proposed an algorithm efficiently that solves this problem using an image descriptor that encrypts movement information and classification method and the abnormality indicator is derived from a hidden Markov model, which measures similarity between observed and normal frames using histograms of optical flow orientations. This method has been tested on many different videos and has been proven to work well [05].

Hussein Kassem [04] presents a video surveillance system in a crowded Campus area and the system detects unusual events using simple procedures and is split into three parts: dividing the video frame into zones, computing the optical flow magnitude in each zone, and analyzing and classifying the data as normal or abnormal events using a logical threshold. The system implements results based on the Histogram of Magnitudes for each zone (HOM), and the outcome meets expectations.

Kwang-Eun [07] proposes a deep convolutional framework to detect abnormal human behavior in video surveillance systems. The framework includes a human subject detection and discrimination module, a posture classification module, and an abnormal behavior detection module based on LSTM and the proposed method provides satisfactory performance in detecting abnormal behavior in a real-world scenario, as evaluated on a benchmark dataset [07].

Surveillance research is increasingly important with growing technology and population. The author Prajakta Jadhav[12] aims to automate camera event detection, as manual monitoring is impractical and time-consuming. The author also focuses on efficient storage and indexing of surveillance data as Video surveillance is a critical security measure for theft prevention, traffic control, and public safety in various settings[12].

Advance Motion Detection (AMD) algorithm was used to detect an unauthorized entry in a restricted area. In the first phase, the object was detected using background subtraction and from frame sequences, the object is extracted. The second phase was the detection of suspicious activity. The advantage of the system was the algorithm works on real-time video processing and its computational complexity was low. But the system was limited in terms of storage service and it can also be implemented with a hi-tech mode of capturing videos in the surveillance areas [2].

A semantic-based approach was proposed in [13]. The captured video data was processed and the foreground objects were identified using background subtraction. After subtraction, the objects are classified into living or non-living using a Haar-like algorithm. Object tracking was done using a Real-Time blob-matching algorithm. Fire detection was also detected in this paper[13].

The author[15] discusses how surveillance videos can capture realistic anomalies and proposes a new method for learning anomalies by using both normal and anomalous videos. To avoid manually labeling each abnormal segment, the authors suggest using a deep multiple instances ranking framework that leverages weakly labeled training videos. They consider normal and anomalous videos as bags and video segments as instances, and use this approach to automatically learn a deep anomaly ranking model that can predict high anomaly scores for anomalous video segments. They also introduce a new large-scale dataset of 1900 surveillance videos, containing 13 types of realistic anomalies as well as normal activities. This dataset can be used for general anomaly detection or recognizing each of the 13 anomalous activities. The authors' method achieves significant improvement on anomaly detection performance compared to previous methods, and the dataset is challenging and offers opportunities for future research[15].

The unusual events in video footage could be detected by tracking of people. Human beings are detected from the video using background subtraction methods. The features are extracted using CNN and which was fed to a DDBN (Discriminative Deep Belief Network). Labeled videos of some suspicious events are also fed to the DDBN and their features are also extracted. Then a comparison of features extracted using CNN and features extracted from the labeled sample video of classified suspicious actions was done using a DDBN and various suspicious activities were detected from the given video[14].

III. PROPOSED APPROACH

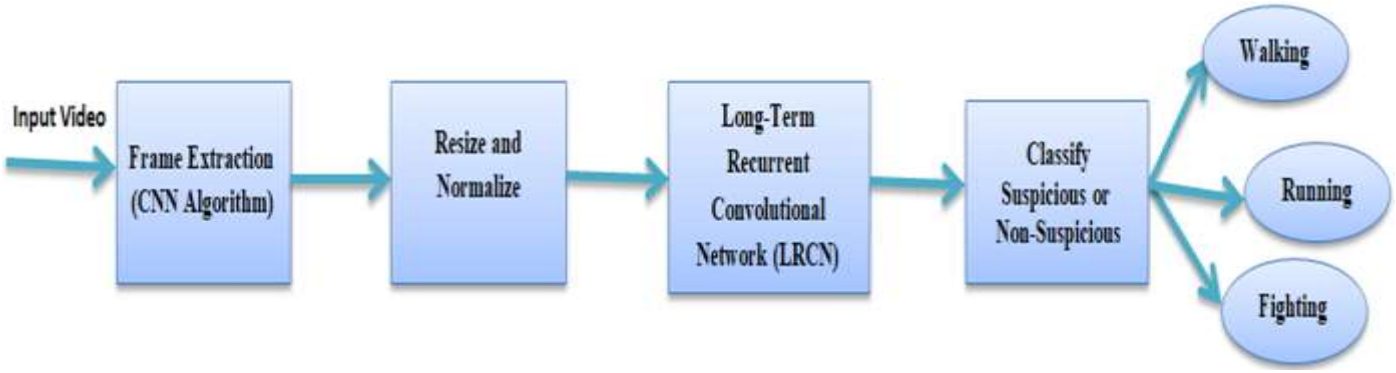

Fig: Data Flow Diagram for Detecting Suspicious Activity

A. Dataset Description

In this paper, an LRCN model is proposed for the detection of suspicious activities. This model uses the Dataset which contains 3 types of activities. This dataset has been preprocessed and given to our LSTM model as input. The dataset consists of 3 different types i.e. Running, Walking, and Fighting. Each of them consists of 100 videos. Some of the videos are taken from Kaggle and others are from YouTube and other sources.

B. Pre-processing of Data

i. Read Video and Label: Using an OpenCV library the videos are read from their respective Class folder and their Class label is stored inside numpy array.

ii. Splitting into frames to make one single sequence**:** In this process, each Video is read using the OpenCV Library, and the videos are broken down into smaller parts as 30 frames so that they can be analyzed more easily.

iii. Resizing**:** Image resizing is done to increase or decrease the total number of pixels. So, the frames are resized to a width of 64px and height of 64px so that they can have the same size.

iv. Normalization: the images are made easier to analyze by normalizing them and changing the values so they all fall between 0 and 1.

v. Store in Numpy Arrays: The sequence of 30 Normalized and resized frames are kept in a numpy array and it is given as Input to the Model.

C. Train Test Split Data

- 75% of the data is used for Training
- 25% of the data is used for Testing

D. Model Creation

A deep learning (DL) network, a Long-term recurrent convolutional network (LRCN) is used to proposed the system for suspicious activity detection from video surveillance. LRCN processed the variable length as visual input with a CNN and those outputs are fed into a stack of recurrent sequence models (LSTMs), which finally produce a variable-length prediction. Both CNN and LSTM weights are shared over time, which results in a representation that scales to arbitrarily long sequences. The LRCN idea is to use two types of computer programs to understand videos. One type looks at the individual images in the video and tries to understand what is happening. The other type looks at how the images change over time and tries to understand what is happening in the bigger picture. Together, these two types of programs can help understand what is happening in a video and even predict what might happen next. LSTM networks are well-suited to process, classify, and make predictions that are based on time series data, as there can be lags of unknown duration between important events and in a time series. LSTMs were designed to deal with the vanishing gradient problem that can be encountered when training traditional RNNs.

IV. CONCLUSION

The system which we are building is originally designed for academic settings. In the future, it can also be used in other places like public or private areas to detect suspicious activities. This system needs to be trained to recognize the suspicious activities that might happen in those places. It can become better if it can identify not only the activity but also the suspicious individual.

Nowadays, people know that CCTV cameras are essential for security purposes. But, usually, these cameras are checked only after something bad has already happened. This new system can analyze the footage in real-time and warn the authorities if something bad might happen. Therefore, we can prevent bad incidents from occurring.

REFERENCES

1. Amrutha, C. V., C. Jyotsna, and J. Amudha. "Deep learning approach for suspicious activity detection from surveillance video." In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 335-339. IEEE, 2020.

2. Divya, P. Bhagya, S. Shalini, R. Deepa, and Baddeli Sravya Reddy. "Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras." International Research Journal of Engineering and Technology (IRJET) (2017).

3. Kamthe, U. M., and C. G. Patil. "Suspicious activity recognition in video surveillance system." In 2018 Fourth international conference on computing communication control and automation (ICCUBEA), pp. 1-6. IEEE, 2018.

4. Kain, Zahraa, Abir Y. Ouness, Ismail El Sayad, Samih Abdul-Nabi, and Hussein Kassem. "Detecting abnormal events in university areas." In 2018 International Conference on Computer and Applications (ICCA), pp. 260-264. IEEE, 2018.

5. Wang, Tian, Meina Qiao, Yingjun Deng, Yi Zhou, Huan Wang, Qi Lyu, and Hichem Snoussi. "Abnormal event detection based on analysis of movement information of video sequence." Optik 152 (2018): 50-60.

6. Fenil, E., Gunasekaran Manogaran, G. N. Vivekananda, T. Thanjaivadivel, S. Jeeva, and A. J. C. N. Ahilan. "Real time violence detection framework for football stadium comprising of big data analysis and deep learning through bidirectional LSTM." Computer Networks 151 (2019): 191-200.

7. Ko, Kwang-Eun, and Kwee-Bo Sim. "Deep convolutional framework for abnormal behavior detection in a smart surveillance system." Engineering Applications of Artificial Intelligence 67 (2018): 226-234.

8. Li, Yuke. "A deep spatiotemporal perspective for understanding crowd behavior." IEEE Transactions on multimedia 20, no. 12 (2018): 3289-3297.

9. Sreenu, G., and Saleem Durai. "Intelligent video surveillance: a review through deep learning techniques for crowd analysis." Journal of Big Data 6, no. 1 (2019): 1-27.

10. Radha, D., J. Amudha, P. Ramyasree, Ranju Ravindran, and S. Shalini. "Detection of unauthorized human entity in surveillance video." International Journal of Engineering and Technology 5, no. 3 (2013).

11. Kavikuil, K., and J. Amudha. "Leveraging deep learning for anomaly detection in video surveillance." In First International Conference on Artificial Intelligence and Cognitive Computing: AICC 2018, pp. 239-247. Springer Singapore, 2019.

12. Jadhav, Mrs Prajakta, Mrs Shweta Suryawanshi, and Mr Devendra Jadhav. "Automated Video Surveillance." (2017).

13. Musale, Jitendra, Akshata Gavhane, Liyakat Shaikh, Pournima Hagwane, and Snehalata Tadge. "Suspicious Movement Detection and Tracking of Human Behavior and Object with Fire Detection using A Closed Circuit TV (CCTV) cameras." *International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume* 5 (2017).

14. lizabeth Scaria, Aby Abahai T and Elizabeth Isaac, "Suspicious Activity Detection in Surveillance Video using Discriminative Deep Belief Netwok", International Journal of Control Theory and Applications Volume 10, Number 29 - 2017.

15. Tripathi, Rajesh Kumar, Anand Singh Jalal, and Subhash Chand Agrawal. "Suspicious human activity recognition: a review." *Artificial Intelligence Review* 50 (2018): 283-339.