ISSN 2277-2685
IJESR/Jan. 2024/ Vol-14/Issue-1/1-7
Dr . P. Ravinder Rao et. al., / International Journal of Engineering & Science Research

Digital Watchman Using Deep Learning

Dr.P. Ravinder Rao	G. Sairam	J. Dayamani	V. Likitha
Assistant Professor	21EG505828	21EG505831	21EG505870
Anurag University.	Anurag University	Anurag University	Anurag University
Email-ravinderraocse@anurag.edu.in	sairamgundlapally11@gmail.com	dayamanij044@gmail.com	likithav293@gmail.com

Abstract:

In response to the increasing instances of fraudulent and offensive activities occurring in real-time, the need for continuous monitoring of CCTV surveillance footage becomes crucial. Human surveillance alone is not feasible due to the sheer volume of footage to be analyzed. Furthermore, it is important to quickly identify and assess frames or sections of the recordings that contain exceptional or suspicious behaviour. This project addresses these challenges by utilizing various Deep Learning models, specifically Convolutional Neural Networks (CNN) and Long-term Recurrent Convolutional Networks (LRCN), to detect signs of violence in real-time. The Deep Learning models are trained on labelled datasets containing examples of violent and nonviolent activities. By leveraging the power of CNNs, the models can extract relevant features from video frames, enabling the identification of violent behaviours. LRCNs are employed to capture temporal dependencies and analyse the sequence of frames, providing a comprehensive understanding of the activities. By implementing these Deep Learning models, the project aims to provide a rapid and automated method for identifying and flagging exceptional or suspicious activities. This technology assists security personnel in efficiently monitoring surveillance footage, enabling them to focus their attention on specific frames or sections of the recordings that require immediate assessment or intervention. Ultimately, the goal is to enhance security measures, facilitate timely response, and improve public safety in real-time surveillance environments.

Keywords – Suspicious Activity, Video Surveillance, LRCN, CNN, LSTM

I. INTRODUCTION

Security and safety is a big concern for today's modern world. In today's insecure world the video surveillance plays an important role for the security of the indoor as well as outdoor places. This hierarchical technique detects various suspicious activities such as loitering, fainting, illicit access. Then it sends an alarm message to the proper authorities. By this we can protect our society from harmful activities. We need state of the art deep learning algorithms, fast processing, and hardware, advanced CCTV cameras in real time.

Applications: Retail stores, Banks and ATMs, Airports and Transportation Hubs, Smart Cities, Schools and Campuses, and in Parking Lots.

To overcome this challenge and improve efficiency, there is a growing need to automate the surveillance system with high accuracy. Deep learning algorithms, such as Convolutional Neural Networks (CNN) and Long Term Recurrent Neural Networks (LRCN), can play a crucial role in automating threat recognition systems. These

algorithms can be trained to identify signs of aggression and violence in real-time, effectively filtering out irregularities from normal patterns. Implementing deep learning algorithms in an automated threat recognition system can significantly reduce the reliance on human monitoring, minimizing both time and labour requirements. It enhances the overall security infrastructure and enables a more proactive approach to identifying and addressing potential threats

II. Proposed System

In Real-time there has been huge amount of fraudulent and offensive activities have been taking place. As most places are under CCTV surveillance, it's quite impossible for humans to be on a constant watch over the surveillance footage. Additionally, it's essential to show which frames and sections of the recording have the exceptional activity, which enables a more rapid assessment of unusual or suspicious behaviour. In this project, we are using different Deep Learning models (CNN and LRCN), for identifying signs of violence in real-time and performance of these Deep Learning models is also evaluated.

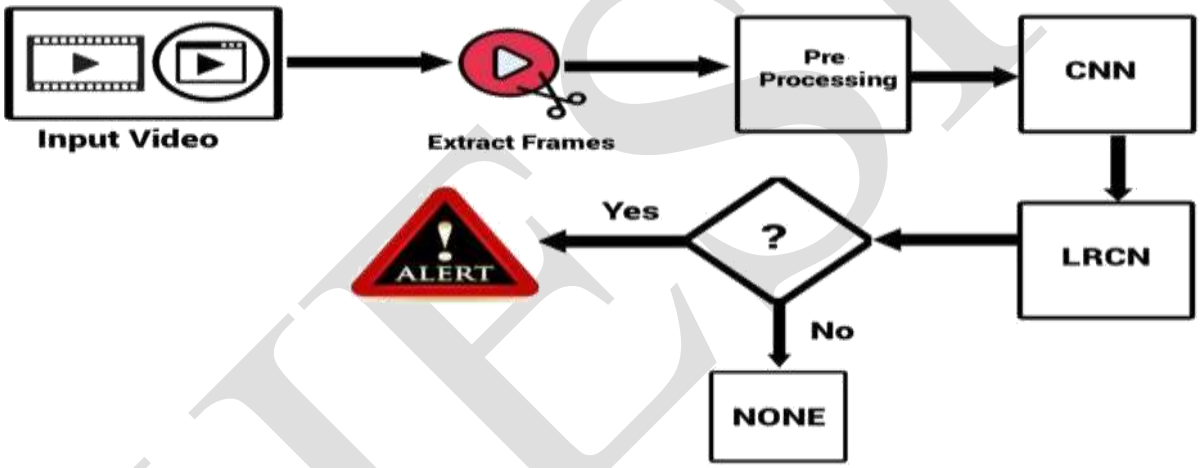

Figure 1 System Architecture

1. **Extract frames from the video:** The first step is to extract frames from the video surveillance footage. This can be done using a standard video processing library.

2. **Pre-process the frames:** Once the frames have been extracted, they need to be pre-processed before being passed to the CNN and LRCN. This may involve resizing the frames to a fixed size, normalizing the pixel values, and converting the frames to grayscale.

3. **CNN:** Pass the pre-processed frames to a CNN to extract spatial features: The next step is to pass the pre-processed frames to a CNN to extract spatial features. The CNN will learn to extract features from the frames that are relevant to the task of detecting suspicious activity.

4. **LRCN:** Pass the spatial features to an LRCN to model the temporal relationships between the frames: The spatial features extracted by the CNN are then passed to an LRCN to model the temporal relationships between the frames. The LRCN will learn to identify patterns of activity in the video that are indicative of suspicious behaviour.

5. **Output:** The output of the LRCN is then used to predict whether or not the video contains suspicious activity. This can be done by using a simple softmax classifier.

6. **Generate an alert:** If the video is predicted to contain suspicious activity, an alert can be generated. This alert can be sent to a human security officer or to an automated system for further investigation.

This process continues until all frames of the input video are processed

III. EXPERIMENT AND RESULT

1. Data Collection and Input Module:

This module encompasses the processes involved in gathering and preparing the data that the model will be trained on. The effectiveness of the data collection and input module significantly impacts the model's performance, as a well-curated and appropriately pre-processed dataset is essential for training a robust model.

2. Data Preprocessing and Model Creation Module:

The data is pre-processed by resizing images or videos to a consistent resolution, normalizing pixel values. The model is created by relu and sigmoid activation functions and then the model is trained using train dataset.

3. Data Analysis and Detecting Module

This module involves the utilization of deep learning models, such as Convolutional Neural Networks (CNNs) and Long-term Recurrent Convolutional Networks (LRCNs), to analyse the processed data and detect suspicious or exceptional activities. As a developer, you can perform the following using Google Colab.

Write and execute code in Python

- Create/Upload/Share notebooks
- Import/Save notebooks from/to Google Drive
- Import/Publish notebooks from GitHub
- Import external datasets
- Integrate PyTorch, TensorFlow, Keras, OpenCV
- Free Cloud service with free GPU

Test case ID	Input	Expected Output	Actual Output	Rate
1.	Test the model's ability to avoid misclassifying non- suspicious activities as suspicious	The model should correctly Classify these non-Suspicious activities as non- suspicious	The model correctly classified the non-suspicious activities	Success
2.	Test the model's Performance and real-time capabilities by processing a stream of CCTV surveillance Video footage	The model should detect suspicious activities, ensuring timely intervention and prevention of potential conflicts	The model detected suspicious activities	Success
3.	Test the model's resilience to environmental changes, such dynamic backgrounds or moving objects	The model should remain effective in detecting and classifying suspicious and non-suspicious activities despite environmental changes and potential distractions	The model detected suspicious and non-suspicious activities despite of environmental changes	Success
4.	The model's performance in low lighting conditions where visibility may be limited	The model should be able to detect and classify suspicious activities accurately, even when in low lighting	The model detected suspicious activities accurately in low lighting	Success

SCREENSHOTS

IV.CONCLUSION

REFERENCES

1. Amrutha C.V, C. Jyotsna, Amudha J. "Deep Learning Approach for Suspicious Activity

Detection from Surveillance Video" Dept. of Computer Science & Engineering, Amrita School of Engineering, Bengaluru, Amrita Vishwa Vidyapeetham, India.

2. Ms.U.M.Kamthe, Dr. C.G.Patil " Suspicious Activity Recognition in Video Surveillance System" Dept. of E & TC SAE, Pune, India.

3. Virender Singha, Swati Singha, Dr. Pooja Gupta. Real-Time Anomaly Recognition Through CCTV Using Neural Networks 1877-0509 © 2020 The Authors. Published by Elsevier B.V

4. Human Behaviour Recognition Model Based Feature and Classifier Selection by GeGeo, Zhixin Li, Zhan Huan, Ying Chen, Jiuzhen Liang, Bangwen Zhou, Chenhul Dong. Published:

23 November 2021Sensors 2021, 21(23), 7791; https://doi.org/10.3390/s21237791

5. DaeHyoen Joe and Min-Suk Kim proposed about the Deep Learning Based Sequence Casual Long-Term Recurrent Convolutional Neural Network for Data Fusion Using Video

Data. Published: 24 February 2023 Electronics 2023, 12(5),1115; https://doi.org/10.3390/electronics12051115