JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ALERT GENERATION ON SUSPICIOUS ACTIVITY DETECTION FROM VIDEOS USING CNN

[1]Auti Mayuri, [2]Yendhe Kirti, [3]Temkar Siddhi, [4]Pabale Snehal

[1]Professor, [2]Student, [3]Student, [4]Student
Department Of Computer Engineering,
SPPU JCOE Kuran, Pune, India

Abstract: The main goal of the system is to find out the doubtful activates without the interference of any human being. The moto of the paper is to identify the doubtful activity and observation for the alertness to the shop owner when doubtful activity is seen. Electronic Article Surveillance (EAS) systems are broadly used in most of the retail stores, still this system is incapable as some of the shop lifters can remove the tags from the product. So, this system takes the videos from the CCTV as an input and after passing to the CNN model developed by the help of transfer learning and detect shoplifting, robbery or breakin in the shop and inform it to the shop owners as sooner as it happens. At the end the main motive is to provide a system that finds doubtful activities without interference of human and create alert. Hence making the vast revolution in today's surveillance system.

***Keywords*- Deep Learning, Suspicious Behavior, Alert Generation, CNN.**

I. INTRODUCTION

This model will then be deployed as a mobile and desktop application which will take real-time CCTV Footage as input and send an alert on the manager device if some doubtful pose is found. Thus, supplying a machine that determine suspicious activity is must in today's global and hence this machine promises such offerings of tacking all such deception and forgery and for that reason creating a large revolution in today's surveillance machine. This concept is applied in many research-based applications related to suspicious-activity detection, pickpocket detection, chain-snatch-event detection, and other social-security detection.
Human behavior identification in the today's world environment finds lot of applications including intelligent video surveillance, shopping behavior analysis. Video surveillance has broad application areas especially for indoor, outdoor and places. Surveillance is an essential part of security. At this moment security camera becomes part of life for the welfare and security purposes. E-Surveillance is one of the main agendas in digital India, development program of Indian government. Video surveillance remains as a part of it. This model will then be deployed as a mobile and desktop application which will take real-time CCTV Footage as input and send an alert on the manager device if some doubtful pose is found. Machine learning works on a principle that if provide data to machines such that data is labeled into useful and not useful format. Use this approach for various purposes such as to identify faces, to identify suspicious activities and others.

II. MOTIVATION

The main motive is to provide a system that detects suspicious activities without human intervention and generates alert, thus making a huge revolution in today's surveillance system. In this project, we track people's behaviour as suspect or not. Now a day's everywhere CCTV cameras are installed which capture videos and store at centralized server and manually scanning those videos to detect suspicious activity for that human required lots of efforts and time.

III. PROBLEM DEFINITION

To develop suspicious human activity recognition from surveillance video is an active research area of image processing and computer vision. This project will entail detecting suspicious human activity from Video dataset using neural networks.

.

IV. RELATED WORK

Om M. Rajpurkar, Siddesh S. Kamble, Jayram P. Nandagiri and Anant V. Nimkar, "Alert Generation On Detection Of Suspicious Activity Using Transfer Learning" 2020@IEEE Department of Computer Engineering Sardar Patel Institute of Technology Mumbai, India IEEE – 49239.

• Since the past two decades, due to the advent of various information systems and technologies, the surveillance system has experienced a tremendous increase and development.
• Various methods such as motion detection, object detection, object tracking, fractal concepts, as well as different clustering techniques are used to achieve the highest accuracy.
• There have been drastic changes in the surveillance system and also in the different ways in which they are implemented.
K Kranthi Kumar 1, B. Hema Kumari 2, T. Sai Kumar 3, U Sridhar 4, G. Srinivas 5, G Sai Karan Reddy 6." Suspicious Activity Detection from Video Surveillance."
• Suspicious activity recognition is bored phrase that refers to a different actions that require different detection methods.
• Crowd behavior such as crowd movement such as necessary methodologies that capture crowd's overall features rather than individuals.
• This method is focus on detecting suspicious activity in system automatically. This type of conduct might happen over a long period of time.
• They frequently include several objects, necessitating the consideration of issues such as finding paths, identification tracking, and object classification
Amrutha C.V, C. Jyotsna, Amudha J. "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video" 2020@IEEE Dept. of Computer Science Engineering, Amrita School of Engineering, Bengaluru, Amrita VishwaVidyapeetham, India ISBN: 978.
• Related works suggest different approaches to detect human behavior from video.
• The Advanced Motion Detection (AMD) algorithm was used to detect unauthorized entry into a restricted area. In the first stage, the object is detected using background subtraction and from the frame sequence the object is extracted.
• The goal of the job is to detect any unusual or suspicious events in the surveillance video.
NipunjitaBordoloi, Anjan Kumar Talukdar, Kandarpa Kumar Sarma, "Suspicious Activity Detection from Videos using YOLOv3" Dept. of Electronics and Communication Engineering Gauhati University, Guwahati, Assam, India 2020@IEEE.
• Here, ongoing work in the area of suspicious action detection is reviewed. Different researchers have used different systems according to their needs.
• Their test results show that the MIL method for anomaly detection significantly improves detection performance compared to the most advanced methods.
• Used a general anomaly detection model using an intensive Multi-Instance Learning (MIL) framework. Frame-based receiver operating characteristic curves (ROC) and corresponding area under the curve (AUC) were used to evaluate the performance of the method.

.

V. PROPOSED METHODOLOGY

The Proposed system will use video obtained from cameras for monitoring activities in a banks or bus stations and send alert message to the when any suspicious event occurs.The Proposed system will use video obtained from cameras for monitoring activities in a banks or bus stations and send alert message to the when any suspicious event occurs. In this system we detect person behavior as suspicious or not. now a day's everywhere CCTV cameras are installed which capture videos and store at centralized server and manually scanning those videos to detect suspicious activity for that human required lots of efforts and time. To overcome this issue, we automate such process using Deep Learning Algorithms. In this study, convolutional neural networks will be used to identify suspicious activity.

1. ALGORITHM

CNN- A CNN is a kind of network architecture for deep learning algorithms and is specifically used for image recognition and tasks that involve the processing of pixel data. There are other types of neural networks in deep learning, but for identifying and recognizing objects, CNNs are the network architecture of choice. The convolutional layers are the key component of a CNN, where filters are applied to the input image to extract features such as edges, textures, and shapes. The output of the convolutional layers is then passed through pooling layers, which are used to down-sample the feature maps, reducing the spatial dimensions while retaining the most important information.

Convolutional Neural Networks have the following layers:

A. Convolutional Layer

B. ReLU Layer

C. Pooling Layer

D. Fully Connected Layer

Convolutional Layer-
This is the first step in the process of extracting valuable features from an image. A convolution layer has several filters that perform the convolution operation. Every image is considered as a matrix of pixel values.

ReLU Layer-
ReLU stands for the rectified linear unit. Once the feature maps are extracted, the next step is to move them to a ReLU layer. ReLU performs an element-wise operation and sets all the negative pixels to 0.

Pooling Layer-
Pooling is a down-sampling operation that reduces the dimensionality of the feature map. The rectified feature map now goes through a pooling layer to generate a pooled feature map.

Fully Connected Layer-
All neurons from the past layers are associated with the other next layers. The CNN has classified the label according to the features from convolutional layers and reduced with any pooling layer.

VI.SYSTEM ARCHITECTURE

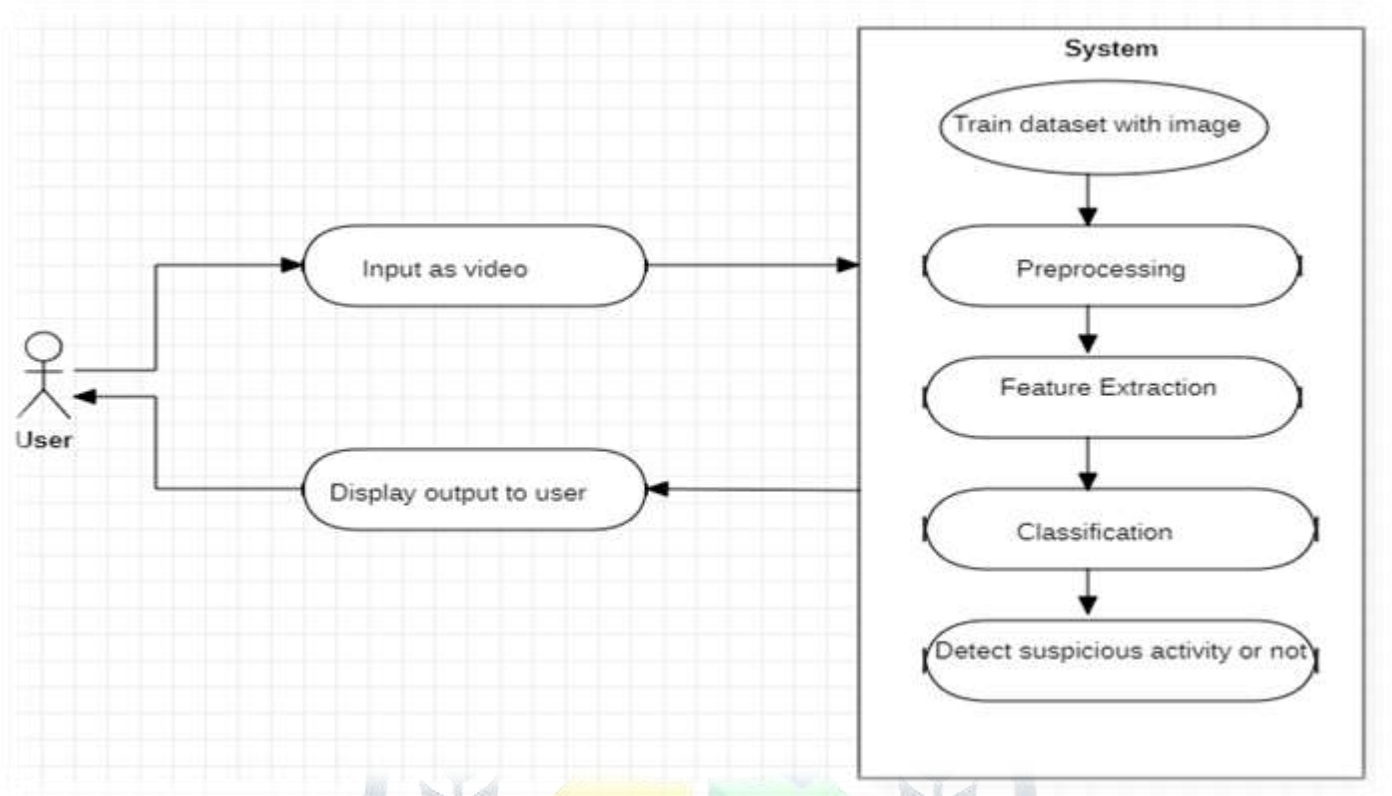

Fig.1.System Architecture

VII. RESULTS

Fig.2.Home Page

Fig.3.Result

VIII. FUTURE SCOPE

- Detect the suspicious activity in public areas such as bus station, banks.
- Anyone can use this application easy.

Conclusion

The human suspicious activities can be detected using this system. Further, this system can be extended to detect and understand the activities of people in various places. The result of the proposed system will be able to detect whether any suspicious activity is taking place or not.

References

[1 Om M. Rajpurkar, Siddesh S. Kamble, Jayram P. Nandagiri and Anant V. Nimkar, "Alert Generation On Detection Of Suspicious Activity Using Transfer Learning" 2020@IEEE Department of Computer Engineering Sardar Patel Institute of Technology Mumbai, India IEEE.

[2] Amrutha C.V, C. Jyotsna, Amudha J. "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video" 2020@IEEE Dept. of Computer Science Engineering, Amrita School of Engineering, Bengaluru, Amrita VishwaVidyapeetham.

[3] Nipunjita Bordoloi, Anjan Kumar Talukdar, Kandarpa Kumar Sarma, "Suspicious Activity Detection from Videos using YOLOv3" Dept. of Electronics and Communication Engineering Gauhati University, Guwahati, Assam, India 2020@IEEE.

[4] Tejashri Subhash Bora1, Monika Dhananjay Rokade "Human Suspicious Activity Detection System Using CNN Model For Video Surveillance" Vol-7 Issue-3 2021.

[5] K Kranthi Kumar 1, B. Hema Kumari 2, T. Sai Kumar 3, U Sridhar 4, G. Srinivas 5, G Sai Karan Reddy 6." Suspicious Activity Detection from Video Surveillance."

[6] Prof. Malan Sale1 , Arvind Patkal 2 , Harshal Mahale3, Jyoti Lavhale4 , Sunayana Apsingekar, "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video" Volume 2, Issue 4, May 2022.

[7] Digambar Kauthkar1,,Snehal Pingle2 ,Vijay Bansode3,Pooja Idalkanthe4, prof. Sunita Vani "Suspicious Human Activity and Fight Detection using Deep Learning Volume 7, Issue 6, June 2022.