



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423

9940 572 462

6381 907 438

ijrset@gmail.com

www.ijrset.com

Implementation towards Suspicious Activity Detection from Surveillance Video

Mr. Pawankumar Shedage, Mr. Tejas Satpute, Mr. Prasad Gharge, Mr. Rohit Gupta,
Prof. Shinde Babaso

Department of Computer Engineering, Shree Ramchandra College of Engineering, Wagholi, Pune, India

ABSTRACT – Predicting a person's body part or joint placement based on an image or a video is considered suspicious activity. The study will include applying neural networks to real-time CCTV data to find suspect human activity. One of the main issues in computer vision that has been researched for more than 15 years is human suspicious activity. The sheer amount of apps that can profit from Activity detection makes it crucial. For instance, human position estimation is utilised in marker-less motion capturing, improved human-computer interaction, tracking and understanding of animal behaviour, sign language identification, and video surveillance.

Low-cost depth sensors are only useful indoors, and estimating human poses from depth photos is challenging due to their low resolution and noisy depth information. We therefore intend to use neural networks to solve these issues. The detection of suspicious human activity in surveillance footage is a current field of study for image processing and computer vision. Human activity can be observed visually in sensitive and open spaces like bus stops, train stations, airports, banks, retail centres, schools, and colleges. Parking garages. Roads, etc. to stop crime, terrorism, unlawful parking, accidents, fights, chain snatching, and other suspicious activity.

Since it is exceedingly challenging to constantly monitor public spaces, it is necessary to install sophisticated video surveillance that can track people's movements in real-time, classify them as routine or exceptional, and provide alerts. The majority of the study being done focuses on photos rather than videos. Additionally, none of the published articles make an effort to use CNNs to identify suspicious activity.

KEYWORDS: Video Surveillance, Anomaly Detection, Deep learning, Convolutional neural networks, Image processing.

I. INTRODUCTION

In order to detect suspicious activity of persons in public places in real time, we intend to develop an application. We can use our application to monitor areas like malls and airports. Where there is a chance of robbery or a gun attack: railway stops, etc. To train our system, deep learning and neural networks will be used. Then, this model will be implemented as a mobile and desktop programme that will accept real-time CCTV footage as input and, if any suspect poses are discovered, send an alarm to the administrator's device. The identification of human body parts and potential surveillance of their movements are related to human suspicious activity. Its real-world uses range from gaming to AR/VR, to healthcare, to gesture detection.

DETECTION OF ABNORMAL BEHAVIOR

Unusual behaviour plays a key role in the identification of suspicious activities in surveillance footage. Using several video analytics approaches, abnormal behaviour can be identified as a potential threat or criminal behaviour. One method for looking for typical conduct in a certain location, like a street or a building. To accomplish this, analyse either watching the region during regular operation hours or using prior video footage. Any departure from the baseline can be marked as odd conduct and possibly suspicious if it has been established. Utilising machine learning algorithms to identify patterns of typical conduct and spot any anomalies is another method for identifying aberrant behaviour. These algorithms can learn to recognise patterns of behaviour that are connected to questionable behaviours, including loitering or strange movements, by being trained on vast amounts of video footage.

OBJECT TRACKING OR ACTIVITY DETECTION

In object tracking, objects are tracked as they move through a video feed, and any odd behaviour—such as objects moving unexpectedly or at extraordinary speeds—is noted. This can be helpful in spotting suspicious activity like a car travelling the wrong way down a one-way street or someone leaving an unsecured gift in a public place. Contrarily,

human activity identification focuses particularly on identifying and assessing human motions and behaviours in a video feed. This can be helpful for spotting unusual activity, like someone scaling a fence or entering a forbidden zone.

II. RELATED WORK

The security of both indoor and outdoor spaces is greatly aided by video monitoring in today's unstable environment. Real-time applications can make advantage of video surveillance system components like behaviour identification, comprehension, and classification of action as normal or suspicious. The hierarchical technique is utilised in this paper to identify several suspicious behaviours, like loitering, fainting, unauthorised entry, etc. This method is based on how the various items move in relation to one another. First, a semantic method is used to define the various questionable activities.. [1]

An automated method of analysing video clips and deducing conclusions about the actions in the video is human activity detection for video systems. It is one of the fields of artificial intelligence and computer vision that is expanding. The technique of identifying unauthorised human activity in settings and circumstances is known as suspicious activity detection. This is accomplished by breaking down video into frames and then using the processed frames to analyse people's actions. Due to the non-rigid nature of human bodies and their propensity to change shape at will, human detection has always been a difficult problem. [2]

When it comes to the potential risk it poses to people, suspicious activity is a problem. It is essential to detect criminal activity given the rise in it in urban and suburban areas in order to reduce such occurrences. In the early days, surveillance was carried out manually by humans, which was a taxing task because suspicious activity was rare compared to everyday activity. Different methods of surveillance were introduced with the introduction of intelligent surveillance systems. We concentrate on examining two situations where, if neglected, there is a considerable risk to human lives: identifying prospective crimes involving firearms and identifying abandoned luggage on surveillance tape. In order to identify probable gun-related crimes and abandoned luggage scenarios in surveillance footage, we offer a deep neural network model that can recognise firearms in photos as well as a machine learning and computer vision pipeline that can detect abandoned luggage. Key words: Computer vision, surveillance footage, gun detection, and abandoned luggage identification. [3]

Convolutional deep architectures have been shown to be very efficient and are frequently utilised in computer vision. There has been an increased focus on utilising GPU processing capacity for deep learning methods since the Graphics Processing Unit (GPU) was introduced for general purpose problems. Additionally, the abundance of data available online has made it easier to effectively train deep neural networks. examine the state-of-the-art in research on Convolutional Neural Networks (CNN) and deep learning-based computer vision systems. As a potential computer vision problem to investigate in our research, we opt for human position estimation in video frames. After careful consideration, we suggest three distinct lines of inquiry into: enhancing current CNN implementations, utilizing, Recurrent Neural Networks (RNNs) for human pose estimation, with unsupervised learning paradigm as the final step in NN training.[4]

Item a detailed explanation of the algorithms used in machine learning In the age of big data, pose estimation is highly appreciated in surveillance systems. However, the challenges of pose estimation in outside surveillance scenarios are not fully covered by the present human pose datasets. We present a brand-new Surveillance Human Pose Dataset (SHPD) in this research.[5].

Real-time multi-person 2D pose estimation is essential for giving machines the ability to recognise individuals in pictures and movies. In this study, we offer a real-time method for identifying numerous people's 2D poses in a picture. The proposed method learns to link body parts with persons in the image using a nonparametric representation that we call Part Affinity Fields (PAFs). The bottom-up approach system achieves high accuracy and realtime performance, regardless of the number of people in the image.[6]

In this research, we offer depth-based algorithms for human position estimation and gesture identification. The suggested approaches are created so that the algorithm can be run on a cheap platform, like an embedded board, using only a CPU (central processing unit). With no prior knowledge of a human body model, the human posture estimation approach is based on an SVM (support vector machine) and superpixels. In the gesture recognition approach, a human body's stance information is used to identify gestures..[7]

III. SYSTEM ARCHITECTURE

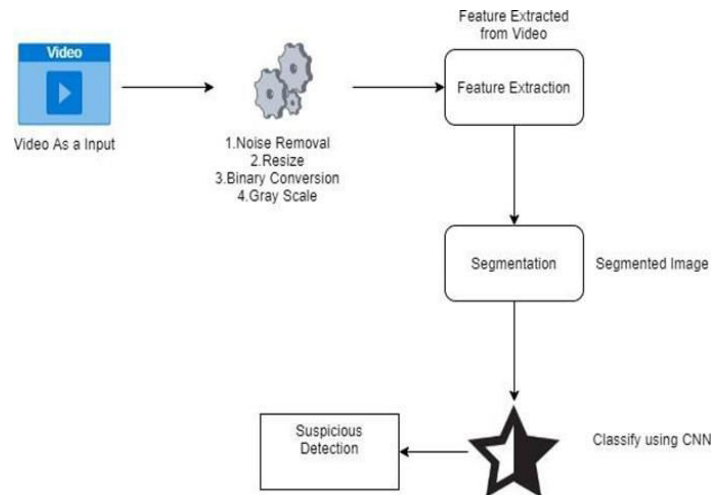


Fig. 1 System Architecture

Proposed model's work:

1.Data Collection: To begin with, data is retrieved from various Websites and Social Media applications based on predetermined criteria.

2. Preprocessing: In order to make our dataset suitable, we will then apply several pre-processing techniques as noise removal, resizing, binary conversion, and grey scaling.

3. Noise reduction: The input video's noise is reduced. The main technique for denoising in image processing is filtering. In order to minimise noise, average filters, median filters, Wiener filters, and Kalman filters are frequently used.

4. Resizing: Remapping can be used to correct for lens distortion or rotate a picture, whereas image resizing is required when we need to increase or decrease the total number of pixels.

5. Binary conversion: In a binary image, which traditionally consists of black and white, each pixel can only have one of just two colours. Binary images work just well too.

6. Gray-scaling is a technique for converting a continuous-tone image into one that a computer can easily alter.

7. Segmentation: Image segmentation is a crucial technique that isolates a digital image into various segments, or groups of pixels that are also known as image objects.6. Data Training: We gather synthetic and real-time news data from web sources and offer training for any machine learning classifier.

8. Feature extraction: Feature extraction is a step in the dimensionality reduction process that separates and compacts a starting set of raw data into more manageable categories.

9. Classification: Sorting and labelling groupings of pixels or vectors inside a picture based on specific criteria is known as classification.

10. Training with data: We gathered synthetic and live social media data and offered training with any machine learning classifier.

11. Testing using machine learning: We provide the system with a testing dataset and use a machine learning technique to detect activities in accordance with that.

12. Analysis: We compare the proposed system's accuracy to other existing systems to estimate.

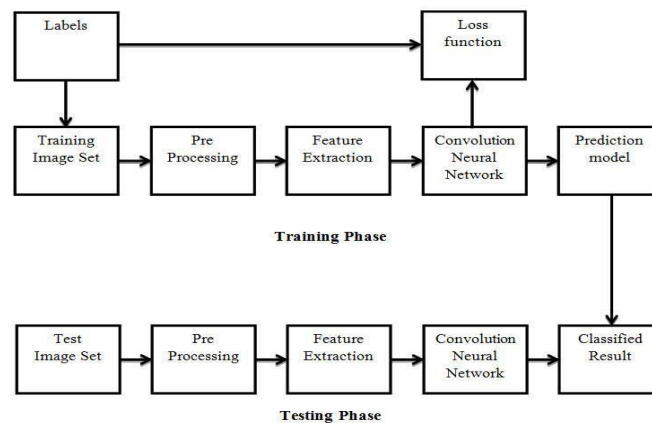


Figure 1: Block diagram of proposed brain tumor classification using CNN

IV. ALGORITHM

Convolutional Neural Network:

Step 1: An image or video is provided as input.

Step 2: After applying numerous filters to the input, a feature map is produced.

Step 3: To further increase non-linearity, a ReLU function is then used.

Step 4: After that, each and every feature map is given a pooling layer.

Step 5: The method merges all of the pooled images into a single long vector.

Step 6: The final step involves feeding the algorithm's vector into a completely linked artificial neural network.

Step 7: Utilizes the network to process the features. The "voting" of the courses is delivered by a fully connected layer at the conclusion.

Step 8: This final phase involves training across several epochs using both forward and back propagation. This cycle is repeated until we have a neural network that is clearly defined and This cycle is repeated until the neural network is well-defined, with trained weights and feature detectors.

V. RESULT

Videos showing abnormal behaviour, such as arson, burglary, and fighting, as well as regular behaviour, are included in the dataset of the proposed model. The movies for typical behaviour had to be manually generated using a standard camera because surveillance videos are so sensitive and difficult to obtain, while the videos showing anomalous behaviour were obtained from the work dataset and shared on social media.

Through a number of websites, we pull diverse existing data as well as recently posted information. There are 7 videos included in the dataset for testing and a total of 15 videos for training. We downloaded roughly 4-5 GB of data in the form of video clips to evaluate the proposed methodology using machine learning techniques.

The proposed method achieves an accuracy of 85% on the provided data set and is designed to identify aberrant behaviour occurring in the video. Here are some pictures showing how the suggested model performed.



Fig2: No Suspicious Activity



Fig 3: Suspicious Activity

VI. CONCLUSION

Better security will result from fewer human interventions and real-time CCTV processing that can identify any suspicious activity. Human Suspicious Activity has advanced significantly, allowing us to better service the countless applications that are feasible. Additionally, research in adjacent domains, like activity tracking, can significantly improve its beneficial application in other fields. The suggested solution uses a machine learning algorithm to identify actual criminal activity in CCTV footage. With more crimes occurring every day, it is becoming more and more important to create a security system. The suggested system's output will be able to determine whether any abnormal action is occurring or not. Additionally, the majority of earlier studies were less accurate at identifying aberrant behavior. CNN is therefore employed in this new strategy for better outcomes.



REFERENCES

- 1.U.M Kamthe, C.G Patil : “Suspicious Activity Recognition in Video Surveillance System”-2018 FOURTH INTERNATIONAL CONFERENCE ON COMPUTING COMMUNICATION CONTROL AND AUTOMATION (ICCUBEA), 16-18 AUGUST 2018, PUNE, INDIA.
- 2.Nipunjita Bordoloi, Anjan Kumar Talukdar, Kandarpa Kumar Sarma : “Suspicious Activity Detection From Videos Using YOLOvs”-2020 IEEE 17TH INDIA COUNCIL INTERNATIONAL CONFERENCE (INDICON), 10-13 DECEMBER 2020, NEW DELHI, INDIA.
- 3.Sathyajit Loganathan, Gayashan Kariyawan, Prasanna Sumathipala : “Suspicious Activity Detection in Surveillance Footage”-2019 INTERNATIONAL CONFERENCE ON ELECTRICAL AND COMPUTING TECHNOLOGIES AND APPLICATIONS (ICECTA), 19-21 NOVEMBER 2019, RAS AI CHAIMAH, UNITED ARAB EMIRATES.
4. C.V Amrutha, C. Jyotsna, J. Amudha : “Deep Learning Approach for Suspicious Activity Detection from Surveillance Video”- 2020 2ND INTERNATIONAL CONFERENCE ON INNOVATIVE MECHANISMS FOR INDUSTRY APPLICATIONS (ICIMIA), 05-07 MARCH 2020, BANGALORE, INDIA.
5. Wazha Mmereki, Rodrigo S. Jamisola, Dimane Mpoeleng, Tinao Petso : “YOLOv3-Based Human Activity Recognition as Viewed from a Moving High-Altitude Aerial Camera”- 2021 7TH INTERNATIONAL CONFERENCE ON AUTOMATION, ROBOTICS AND APPLICATIONS (ICARA), 04-06 FEBRUARY 2021, PRAGUE, CZECH REPUBLIC.
6. Om M. Rajpurkar, Siddesh S. Kamble, Jayram P. Nandagiri, Anant V. Nimkar : “Alert Generation on Detection of Suspicious Activity Using Transfer Learning”- 2020 11TH INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND NETWORKING TECHNOLOGIES (ICCCNT), 01-03 JULY 2020, KHARAGPUR, INDIA.
7. Aqil Shammath, Meena Belwal : “Human Suspicious Activity Detection Using Ensemble Machine Learning Techniques”- 2022 2ND INTERNATIONAL CONFERENCE ON INTELLIGENT TECHNOLOGIES (CONIT), 24-26 JUNE 2022, HUBLI, INDIA.



INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.423



ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 **6381 907 438** **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details