iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52486

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Suspicious Activity Detection Using Machine Learning

Bhagyashri Kumbhar[1], Pranav Pisal[2], Kunal Kene[3], Aditi Raut[4]
[1, 2, 3, 4]*Computer Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India*

Abstract: ***Various technologies have been utilized to implement the safety of life and property by installing high quality CCTV cameras. It is not possible to manually monitor each and every moment activity. Furthermore, in practical scenario the most unpredictable one is human behaviour and it is very difficult to find whether it is suspicious or normal. In this work the notion of CNN is used to detect suspicious or normal activity in an environment, and a system is proposed that sends an alert message to the similarity authority, in case of predicting a suspicious activity. It's worth noting that the effectiveness of a suspicious activity detection system relies on the quality of the training data, the architecture of the Machine Learning model, and the deployment environment. Ongoing monitoring, regular updates, and continuous improvement are important for maintaining the system's accuracy and adapting it to new and emerging types of suspicious activities.***
Keywords: Anomaly, CNN(Convolution Neural Network), CCTV, Video Surveillance.

I. INTRODUCTION

Suspicious Activity Detection Using MachineLearning can indeed be used to detect various types of suspicious activities, including thoserelated to human behaviour. However, thespecific activities that can be detected depend onthe training data and the design of the Machine Learning model.

If the model is trained on a dataset that includesexamples of suspicious human activities, it can learn to recognize patterns and behaviours associated with those activities. For example, it could detect activities such as fighting, stealing,trespassing, or engaging in potentially dangerousbehaviour.

Human behaviour recognition in the real-world environment finds bumper of applications including intelligent video surveillance, shopping behaviour analysis. Video surveillancehas vast application areas particularly for indoor outdoor and places. Surveillance is an integral part of security. Today security camera becomespart of life for the safety & security purposes. Today, manual monitoring of all the events on the CCTV camera is impossible. Even if the event had already happened, searching the same event in the recorded video wastes a lot of time. Analysing abnormal events from video is an emerging topic in the domain of automated video surveillance systems.

Video surveillance is the emerging area in the application of AI, Machine Learning and Machine Learning. AI helps the computer to think like human. In machine learning, importantcomponents are learning from the training data and make prediction on future data. Nowadays GPU (Graphics Processing Unit) processors andhuge datasets are available, so the concept of Machine Learning is used.

Deep Neural Networks is one of the best architectures used to perform difficult learning tasks. Machine Learning models automatically extract features and builds high level representation of image data. This is more generic because the process of feature extractionis fully automated. From the image pixels, convolutional neural network (CNN) can learn visual patterns directly. In the case of videostream, long short-term memory (LSTM) models are capable of learning long term dependencies. LSTM network has the ability to remember things. The proposed system will use footage obtained from CCTV camera for monitoring the human behaviour in a term warn when any suspicious event occurs. The major components in intelligent video monitoring are event detection and human behaviour recognition.

It's worth noting that the effectiveness of a suspicious activity detection system relies on the quality of the training data, the architecture of the Machine Learning model, and the deployment environment. Ongoing monitoring, regular updates, and continuous improvement are important for maintaining the system's accuracy and adapting it to new and emerging types of suspicious activities.

II. MOTIVATION OF THE PROJECT

By developing an automated system that can detect and alert authorities or relevant personnel to suspicious activity, it may be possible to prevent or mitigate potential harm. Machine learning and Machine Learning techniques can be used to analyse large amounts of data and identify patterns that may indicate suspiciousbehaviour.

III. GOALS AND OBJECTIVES

1) To convert video to image.
2) To frame segmentation using K means clustering.
3) To extract frame by background subtraction and frame sequence. To detection the object.
4) To action recognition using Deep Belief Network (DBN).
5) To classify normal activity or suspiciousactivity with trained dataset.
6) To alert a security.

IV. SYSTEM ARCHITECTURE

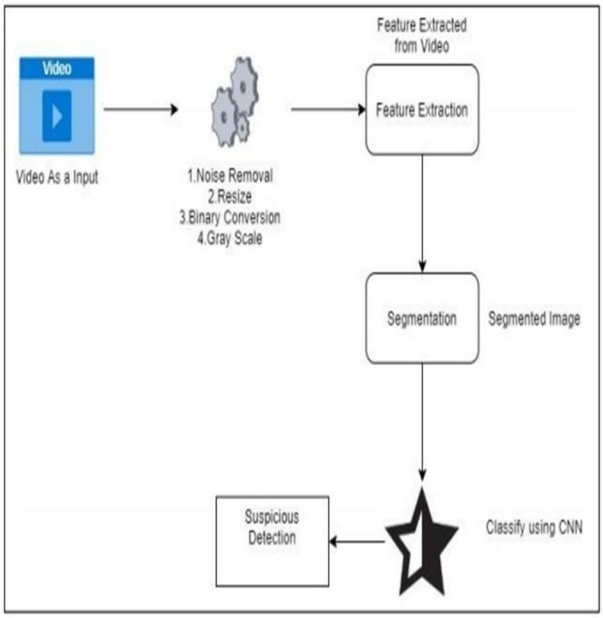


Fig. SYSTEM ARCHITECTURE

V. RELEVANT ALGORITHM ASSOCIATEDWITH THE PROJECT

1) Step 1: Input is given as image and video.
2) Step 2: Then many more different filters areapplied to the input to create a feature map.
3) Step 3: Next step is a ReLU (Rectified Linear Unit) function is applied to increase non- linearity.
4) Step 4: Then step is a applies a pooling layer to each and every feature map.
5) Step 5: Then the next step is algorithm compresses the pooled images into one longvector.
6) Step 6: In next step is inputs the vector to the algorithm into a fully connected artificial neuralnetwork(ANN).
7) Step 7: Next step is processes the features via thenetwork. At the end fully connected layer delivers the "voting" of the classes.
8) Step 8: In this final step training is conducted through forward propagation and back propagation for numerous epochs.

VI. LITERATURE SURVEY

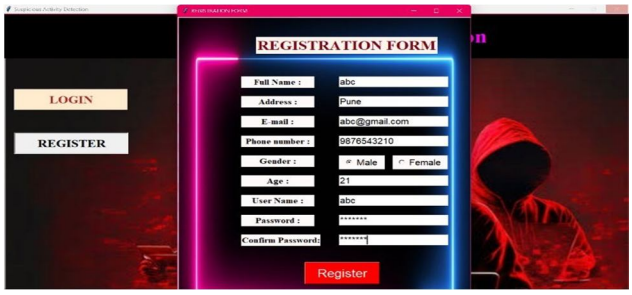
Paper Name:- Suspicious Actions Detection System Using Enhanced CNN (Convolutional neural network) and Surveillance Video
Author:- Govindaraju Karthi
Description:- Work is proposed for human- action recognition (HAR), with two human activity datasets. This work was used for monitoring the elderly, suspicious-people monitoring, and objects in public places. This skeletal-joint motion was activated with image pre-processing and Deep Learning algorithms. Motion sets are limited and their lead disadvantage. A computer-vision and image- processing-based solution for the detection of violent activities was discussed. This review work suggested various Machine Learning and Deep Learning algorithms. A work was created as a solution for violence-detection techniques for the Internet of Things (IoT) surveillance network for industry. The technique was called artificial intelligence assisted vision . Violence- detection (VD) and behaviour analysis have been measured with accuracy on surveillance and non-surveillance datasets. In this work convolutional long short-term memory was usedto extract features based on the violence- detection concept.

VII. CONCLUSION

A project model is used to process real-time CCTV footage to detect any suspiciousactivity would help in creating better security and less human interface in activities. Inaddition, research in related areas such as activity can increase like tracking its productiveuse in many areas. A system to process real-timeCCTV footage to detect any suspicious activity will help to create better security and less humanintervention. Great act have been made in the field of human suspicious Activity, whichenables us to better serve themyriad applications that are possible with it. Moreover, research in related fields such as Activity Tracking can greatly enhance its productive utilization in several fields.

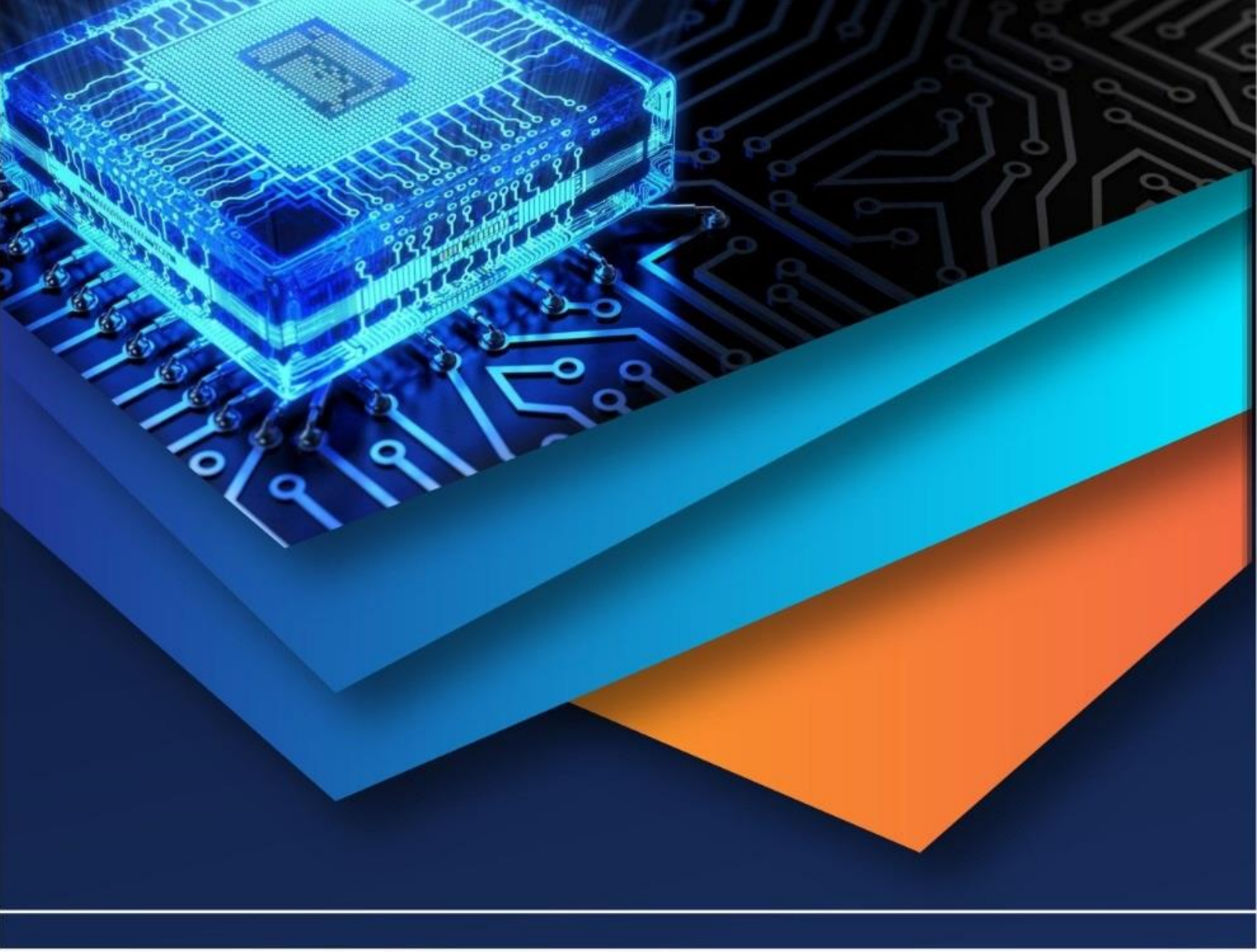
VIII. RESULTS

We studied existing methods and offered an alternative approach to trace suspicious activities and fighting using CCTV footage taking place in public places. Our approach used CNN(Convolutional neural network) to ascertain whether activity was distrustful. In ourmodel the detection rate is increases up to the 90
% accuracy then previous model.



REFERENCES

[1] Monika D. Rokade and Tejashri S. Bora, "Survey On Anomaly Detection for Video Surveillance" 2021 International Research Journal of Engineering and Technology(IRJET).
[2] Jefferson Ryan Medel, Andreas Savakis, “Anomaly Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks” under review.
[3] J. R. Medel and A. Savakis, “Anomaly detectionin video using predictive convolutional long short-term memory networks,” arXiv preprintarXiv:1612.00390, 2016.
[4] P.Bhagya Divya, S.Shalini, R.Deepa, Baddeli Sravya Reddy,“Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras”,International Research Journal of Engineering and Technology (IRJET),December 2017.
[5] Jitendra Musale,Akshata Gavhane, Liyakat Shaikh, Pournima Hagwane, 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 Issue XII December 2017.
[6] Elizabeth Scaria, Aby Abahai T and Elizabeth Isaac, “Suspicious Activity Detection in Surveillance Video using Discriminative Deep Belief Netwok”, International Journal of ControlTheory and Applications Volume 10, Number 29
[7] -2017
[8] Amrutha C.V, C. Jyotsna, Amudha J. “MachineLearning Approach for Suspicious ActivityDetection from Surveillance Video” , IEEE Xplore , Issue 23 April 2020
[9] Phalguni Kadam , Shweta Gawande , Akshita Thorat , Rohini Mule. “Suspicious Activity Detection using Image Processing”, Journal of Science and Technology, Issue 01, August 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY