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.2023.51438

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

Deep Learning Approach for Suspicious Activity Detection from Surveillance Video

Prof. Dr. Sarang Patil Sir[1], Gaurav Borse[2], Shubham Tanpure[3], Sanket Chavan[4], Rohit Dolas[5]
[1, 2, 3, 4, 5]*Department of Computer Science SKN Sinhgad Institute of Technology and Science , Lonavala Pune, India*

Abstract: ***In today's uncertain world, video surveillance plays a vital role in maintaining indoor and outdoor security. Video surveillance system components such as behaviour detection, behaviour understanding, and normal or suspicious activity classification can be used for real-time applications. This article uses a hierarchical approach to detect various suspicious activities such as loitering, fainting, and trespassing. This approach is based on motion properties between different objects. First, various suspicious activities are defined using a semantic approach. Object detection is then performed by background subtraction. Detected objects are classified as live (human) or non-live (bag). These objects need to be tracked and this is done using correlation techniques. Finally, motion features and temporal information are used to classify events as normal or suspicious. A semantics-based approach is used, resulting in low computational complexity and high efficiency of the approach.***
Keywords: Video Surveillance; Suspicious Activities; Motion Features; Semantic Approach; Object Detection

I. INTRODUCTION

In recent years, there has been an increase in violence and crime rates around the world. Various tools are used to minimize or control the situation. Video surveillance is the best option available for both private and public places. Video surveillance can be effective in efficiently detecting anomalous/suspicious activity. Most of today's surveillance systems are operated by humans. Therefore, human attention is always required to detect anomalous activity. Due to human involvement, the efficiency of the system decreases over time due to the human fatigue factor. This problem can be solved by automating video surveillance. The function of the automated system is to issue an alarm or other form of indication when a predefined abnormal activity occurs.

II. METHODOLOGY

A. System Model

The shows the flow of the system for the detection of suspicious activity. The different block is explained as follows-

1) *Input Data:* The input for the system is video stream. As the system is to be implemented to detect the suspicious activity its input is to be taken from the CCTV. Background image acquisition- The illumination effect can be corrected by the background image. A reference image/ standard background is taken as reference for the further image processing.
2) *Image Preprocessing:* The different image preprocessing techniques are used to improve the image so that the unwanted distortions are get suppressed or some required features enhanced.

B. Implementation Object Detection

The template matching is used for the object detection. In this method the cross correlation between a template image & the new image is performed. The different geometrical parameters are used for matching the reference image with the input image to find the required object. Suppose S(x, y) is the input image & we have to find the object from this input image. Then the image T(xt, yt) is taken as the template image. This template is considered as a mask & the centre of the mask is moved over each pixel in input image. Then the sum of product between coefficient of input image S(x, y) & template image T(xt, yt) is calculated over the whole area spanned by the template. By considering all the position of the template the position which has the highest score is considered as the best position where object can be detected.

© IJRASET: All Rights are Reserved |

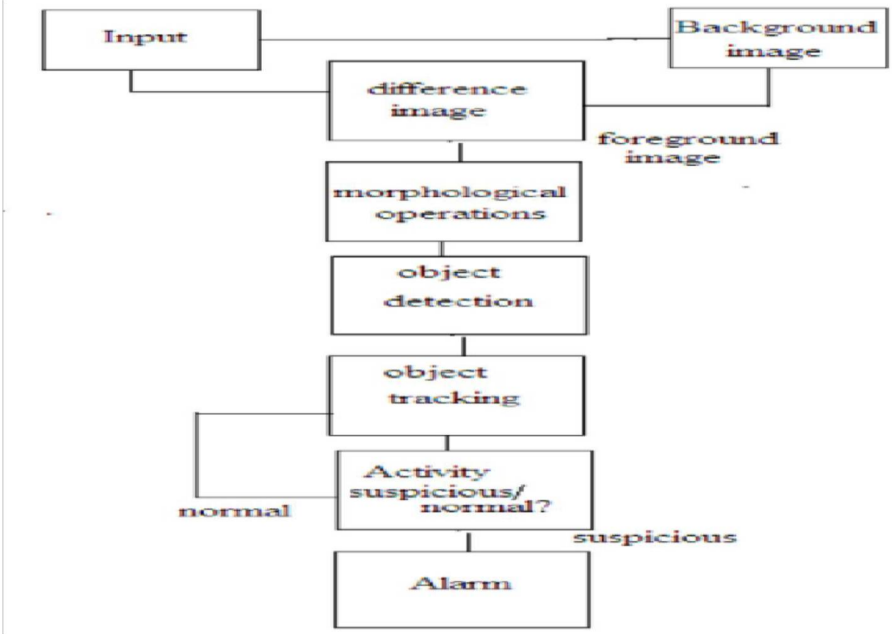


Fig 1. Workflow

1) *Object Tracking:* Use correlation-based tracking methods to track detected objects in the scene. This method places a small tracking window in the center of the object on the first frame. This object is considered a target. Its color histogram is calculated for each object in the frame. So, a red, green and blue histogram is calculated for each object. Objects are identical if their color histograms in the current frame and the previous frame match. Knowing the color histogram allows us to track a particular object over multiple frames. Also, when new objects enter the frame, they are easily identifiable.
2) *Object Features Extraction:* Once the object is fixed to the tracked frame, we need to extract its features. Most of the work uses shape-based functions, but they require large training data sets with many variations in both animate and inanimate shapes. This work uses the motion function. Objects are classified into four different categories based on their motion characteristics. Here is the state diagram for this classification:
3) *Defining the Suspicious Activities:* There are lots of activities which come under the suspicious activity. But for the project work we have selected the following activities-
4) *Abandoned Luggage:* Researchers define abandoned bag as- stationary object that is not touched by a person for some time duration.
5) *Unauthorized Access:* In the restricted area the entry for common people is not allowed. If somebody tries to access the place without any authentication then it is harmful and it should be detected. Loitering- If the presence of a person in a particular place exists for a period longer than the time required for a activity then it is called as loitering.

III. LITERATURE SURVEY

Automatic detection of anomalous events in long video sequences is difficult due to the vague definition of such events. We tackle this problem by training a generative model that can identify video anomalies with limited supervision. We
propose an end-to-end trainable complex convolutional long-short-term memory (Conv-LSTM) network that can predict the evolution of video sequences from a small number of input frames. A regularity score is derived from the reconstruction error of a set of anomalous video sequence predictions, with regularity scores decreasing as the sequence deviates further from the actual sequence over time. The model uses composite structures and examines the effects of 'conditioning' in learning more meaningful representations. The best model is selected based on reconstruction and prediction accuracy. The Conv-LSTM model has been qualitatively and quantitatively evaluated and shows competitive results on the questionable detection dataset. The Conv-LSTM unit has proven to be an effective tool for modelling and predicting video sequences. Introduces an efficient method to detect video anomalies. Recent applications of convolutional neural networks show the potential of convolutional layers in object detection and

detection, especially in images. However, convolutional neural networks are supervised and require labels as training signals. We propose a spatiotemporal architecture for suspicious detection in videos containing crowded scenes.

IV. EXPERIMENTS AND RESULTS

1) The system's main page is designed with user-friendliness and intuitive navigation in mind.
2) Upon accessing the main page, users are presented with two modules: Login and Register.
3) These modules enable users to create an account or sign in to an existing one quickly and easily.
4) Overall, the system's main page offers an account and convenient user experience.

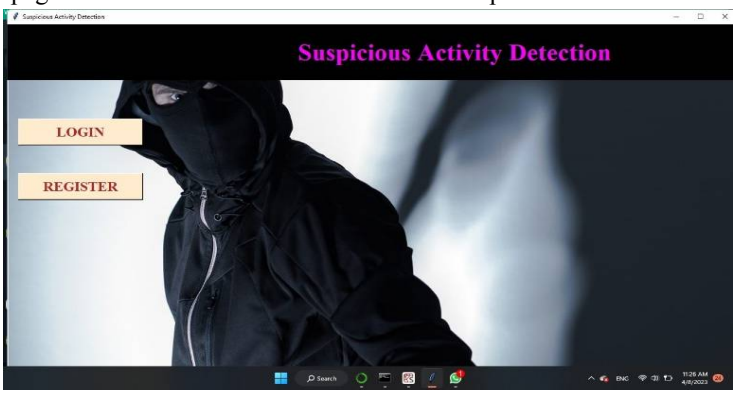


Fig 2. Main page

If there is a new user then he/she has to click on register button to get registered before using the system. They need to fill basic information.

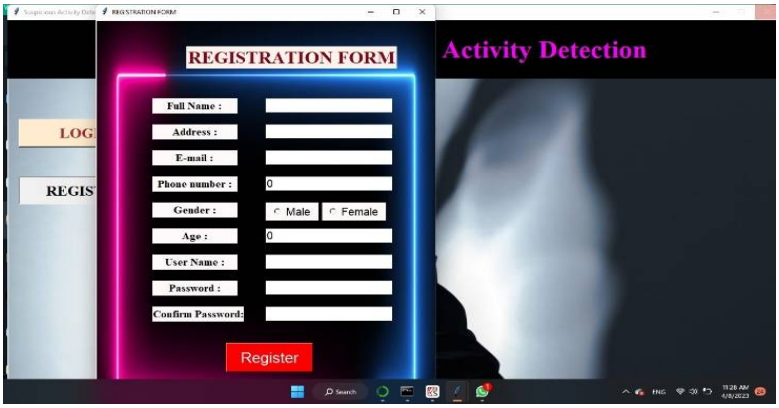


Fig 3. Registration Page

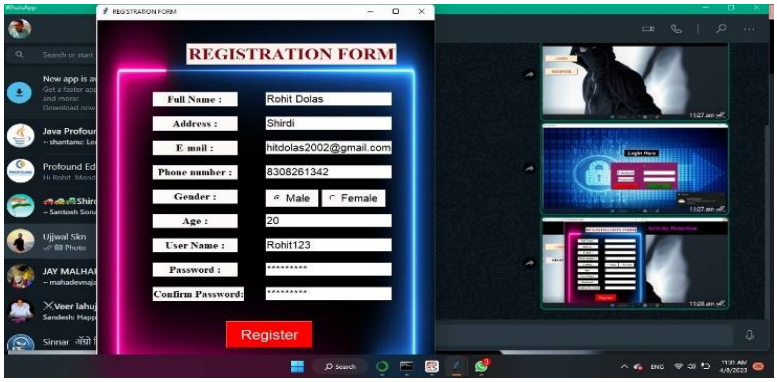


Fig 4. Registered Details

1) Once registered, users can access the Login page to sign in to the system.
2) The Login page prompts users to enter the username and password they provided during registration
3) This authentication process allows users to securely access the system's features and resources.



Fig 5. Login Page

After login we are directed to the main processing page where the processing of the provided video is done and the video is processed to tell if the suspicious activity is detected or not.



Fig 6. Master Page



Fig 7. Processing

In the last step an email is generated and sent to the linked device about the result of the processing.

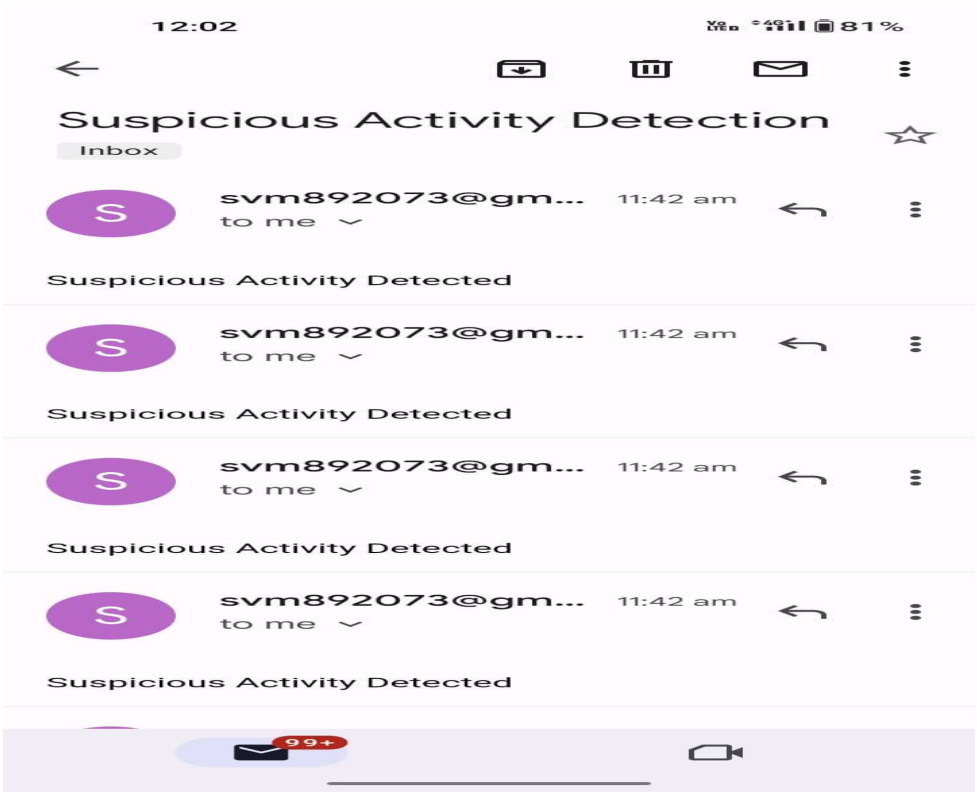


Fig 8. Result sent on Email

V. CONCLUSION

Human behaviour in the natural environment is complex and highly variable. In this paper, we formulate the suspicious behaviour detection of the security system. The accuracy achieved is about 95%. We found that YOLOv3 outperforms Faster R-CNN in terms of image recognition processing time. Current feature extraction methods provide accurate results only in controlled environments. Better feature extraction methods can be incorporated to improve results. However, due to the small amount of training data, there were still some discrepancies between test results and ground truth comparisons. Therefore, our future improvement work is to extend the training data set with suspicious videos of different activities and resolutions to achieve better detection and make the model more viable. You can also develop more sophisticated algorithms for real-time applications.

VI. ACKNOWLEDGMENT

I am grateful to Dr. M. S. Rohokale and Dr. Sarang Patil (Department of Computer Engineering at SKN Sinhgad Institute of Technology & Science, Lonavala) for their valuable guidance, help, cooperation, and encouragement.

I would like to extend my gratitude to SKN Sinhgad Institute of Technology & Science, Lonavala College for providing me with this opportunity to enhance my knowledge and skills in Machine Learning. I am also thankful to my parents and family members for their unwavering support, both morally and economically.

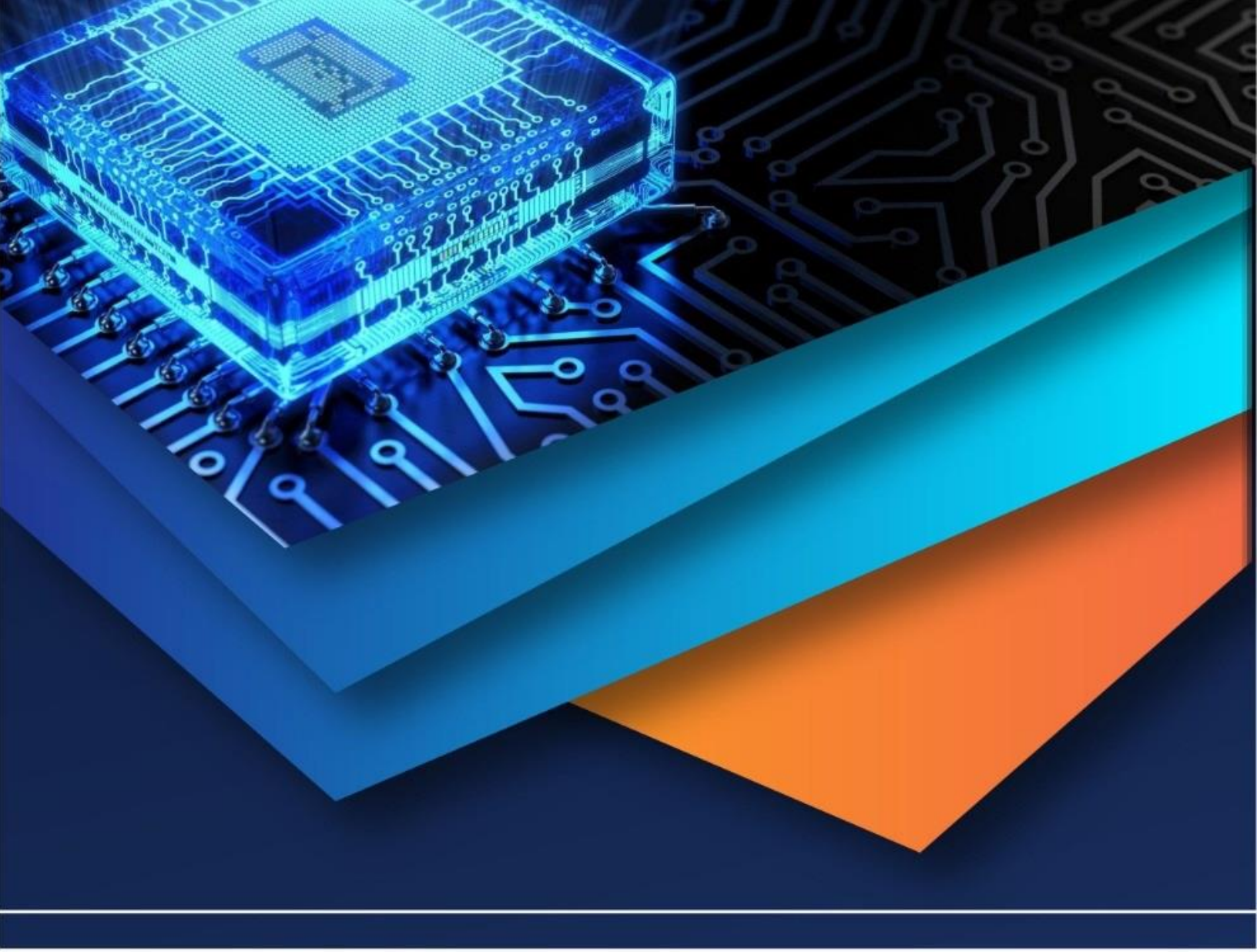
This acknowledgement would be incomplete without expressing my heartfelt thanks to everyone who has contributed directly or indirectly to this work. Any inadvertent omission is purely unintentional and does not reflect a lack of gratitude on my part.

REFERENCES

[1] S. Zaidi, B. Jagadeesh, K. V. Sudheesh and A. A. Audre, "Video Anomaly Detection and Classification for Human Activity Recognition," 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, 2017, pp. 544-548.

[2] M. Saab and J. Gotman, "A system to detect the onset of epileptic seizures in scalp EEG," Clinical Neurophysiology, vol. 116, no. 2, pp. 427–442,2005.

[3] Sandesh Patil and Kiran Talele "Suspicious Movement Detection and Tracking based on Color Histogram", 2015 International Conference Communication, Information & Computing Technology (ICCICT), Jan. 16-17.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)