WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Human Suspicious Activity Detection Using Artificial Intelligence

Mr. Mahendra M[1], Charitha V[2], Uday Kumar Rao B[3], Shireesha J[4], Swathi K[5], Vishnu Vardhan Gowd P[6], Vandana R[7]

[1]Head & Asst. Prof of Computer Science and Engineering, Sanskrithi School of Engineering, Andhra Pradesh
[2]Department of Computer Science and Engineering, Sanskrithi School of Engineering, Andhra Pradesh
[3]Department of Computer Science and Engineering, Sanskrithi School of Engineering, Andhra Pradesh
[4]Department of Computer Science and Engineering, Sanskrithi School of Engineering, Andhra Pradesh
[5]Department of Computer Science and Engineering, Sanskrithi School of Engineering, Andhra Pradesh
[6]Department of Computer Science and Engineering, Sanskrithi School of Engineering, Andhra Pradesh

ABSTRACT

An average of 380 million criminal activities is recording yearly in India. It is nearly impossible for humans to keep an eye on the surveillance cameras all the time. The most recent research aims to incorporate computer vision, image processing, and artificial intelligence into video surveillance applications.

This paper offers a deep learning approach for detecting suspicious behaviour. Real-time aggression and violent behaviour detection is the aim in order to separate abnormal behaviour from usual patterns. The algorithm shows which frame and portion of unexpected activity, which enables a quicker determination of whether that unusual activity is abnormal or suspicious.

KEYWORDS: criminal activities, surveillance cameras, computer vision, image processing, artificial intelligence, video surveillance, deep learning, suspicious behaviour, real-time, aggression, violent behaviour, abnormal, unusual activity.

I. INTRODUCTION

In this paper, we propose a deep learning approach for detecting suspicious behaviour in real-time. The aim of our approach is to accurately identify aggression and violent behaviour and separate it from usual patterns of behaviour. By identifying the frame and portion of unexpected activity, our algorithm enables a quicker determination of whether that unusual activity is abnormal or suspicious. The proposed approach can provide law enforcement agencies with an efficient tool to enhance public safety and mitigate criminal activities.

II. PROBLEM DEFINITION

Video surveillance systems must include activity detection in order to do activity-based analysis. Traditionally, CCTV camera video streams were analysed by human operators. These operators watch multiple displays simultaneously in search of any unexpected activity. This is a time-consuming and ineffective way to monitor. Finding timely and accurate activity data consequently becomes quite difficult. Because of this, humans require an automated process, or the right choice is provided by the suspicious behaviour detection system. Systems that use video to detect suspicious activity can either take the place or either supplement human operators in keeping an eye out for unusual activity. They receive a prompt and accurate response from the system.

III. OBJECTIVE

The objective is to develop a system that can analyse surveillance footage automatically. Designers will conduct a real-time analysis of the video feed to spot any suspicious activity, such as theft or robbery, monitor items with the help of installed CCTV cameras, and instantly identify any security policy and procedure violations. This system also aims to lower people's expenses by using cutting-edge technologies.

IV. LITERATURE SURVEY

[1] This paper briefs about, how robust the proposed violence detection system works in recognizing the scenes of violence from real time videos. Football hooliganism is the way of violence in sports defined as the conflict between the players or audience during the event. The proposed violence detection system analyses a stream of video frames from different sources to detect violence scenes. The video streams are converted into non-overlapping frames,

which are then processed by the Histogram of Oriented Gradients (HOG) algorithm in the Spark environment to extract features. The features are then used to train a Bidirectional Long Short-Term Memory (BDLSTM) network, which can recognize violence actions in real-time. The system alerts security forces if violence is detected, and stores recognized violence frames for future reference.

[2] The proposed system utilizes multiple machine learning models, including support vector machines (SVM), random forest, and extreme gradient boosting (XGBoost), to classify human activities as suspicious or non-suspicious. The system also uses an optical flow algorithm to extract features from video frames, which are then used as input to the machine learning models. The proposed system is evaluated on a publicly available dataset, and the results demonstrate that the ensemble approach achieves higher accuracy compared to using a single machine learning model. The paper concludes that the proposed system has potential for use in real-world surveillance applications.

[3]A key concern of any society today is providing safety to an individual. The main reason behind this concern is due to the constantly increasing activities causing threats, starting from deliberate ferocity to an injury caused through an accident. In the proposed system, for detecting anomalous behavior, the CNN i.e. convolution neural network have been used. For effectively classification of anomalous activities, it is essential to recognize the temporal data in the video. Recently, CNN is mostly used for extracting key features from each frame of the video. CNN is only the algorithm best suited for this purpose. For classifying the given input successful, it is necessary that the features get extracted from CNN, therefore CNN should be capable of knowing and extracting the needed features from the frame of videos.

[4] The system uses a training data set consisting of photos of people taken from different angles, with values generated from the images stored in a database along with the students' details. The video is converted into frames and preprocessed by converting to grayscale, removing noise with Gaussian blur, and detecting edges with the Canny edge detection algorithm. The Surf features approach is used to detect faces in the image. The output is compared with the database to identify the people and their activities, which are then checked for suspicious behavior. If suspicious behavior is detected, the system sends an alert message to concerned officials.

[5] The system consists of different phases, including video capture, video pre-processing, feature extraction, classification, and prediction. Deep learning networks like CNN and RNN are used for suspicious activity detection from video surveillance. The system uses the KTH dataset, the CAVIAR dataset, and YouTube videos for training suspicious behavior. The input videos are taken from various sources, and the pre-trained model used in the system is VGG-16. The system is capable of monitoring suspicious activities in a campus and alerts the security when any suspicious event occurs.

[6] YOLOv3 algorithm and the COCO dataset are used for object detection and training. The system can detect abnormal activity, crowd density, and suspicious objects in real-time for emergency dispatch and early threat detection. The importance of feature extraction in image processing is also highlighted, with YOLOv3 and Darknet-53 being used in the system's architecture. Accuracy and speed are evaluated using mean Average Precision and inference time.

[7] The authors use a deep convolutional neural network (CNN) architecture to learn features from the videos and classify the activities as suspicious or not. The CNN is trained on the dataset using transfer learning, where a pre-trained CNN is fine-tuned on the target dataset. The paper also proposes a system for detecting fights using motion features extracted from the video frames. A motion history image is computed for each frame, and motion vectors are extracted from the image. The authors use a support vector machine (SVM) classifier to detect fights based on the motion vectors.

[8] The main idea of the paper is to propose a system for detecting suspicious human activity in video surveillance applications using a hybrid deep learning approach that combines a convolutional neural network (CNN) and a Dynamic Bayesian neural network (DBNN). The proposed system first uses a CNN to extract relevant features from the input video frames, and then a DBNN is used to perform anomaly detection and classify the detected activity as suspicious or not. The system is evaluated using a publicly available dataset and achieves high accuracy in detecting suspicious activity.

V. PROPOSED SYSTEM

The main idea behind this proposed system is to create an automated system that can detect unusual activities in surveillance footage without the need for human intervention. The system uses a machine learning model trained on images of suspicious activities like people carrying guns or wearing masks, etc. The video footage is then analysed by the model by dividing it into frames to determine which frames contain unusual activities. The system uses OpenCV and Discriminative Deep Belief Network Algorithm to segment the video into frames, extract the background and foreground, and classify normal and abnormal activities. The system is trained with anomalies activities using CNN and can remember past experiences for future classification.

VI. IMPLEMENTATION

The goal of this project was to create an automated system that can detect unusual activities in surveillance footage without the need for human intervention. The system utilizes machine learning, video segmentation, and anomaly detection techniques to analyse video footage and identify frames that contain suspicious activities such as people carrying guns or wearing masks. The implementation of this system involved using OpenCV and the Discriminative Deep Belief Network Algorithm to segment the video into frames, extract the background and foreground, and classify normal and abnormal activities. The system was trained with a Convolutional Neural Network (CNN) on annotated datasets of anomaly activities for accurate detection.

The implementation of the system was done in Python, utilizing OpenCV, Deep Belief Network (DBN), and Convolutional Neural Network (CNN) libraries. The following steps were followed:

Dataset Preparation: An annotated dataset of surveillance footage with labelled normal and abnormal activities was collected for training the CNN model. The dataset was carefully curated to include a diverse range of anomaly activities, such as people carrying guns, loitering in restricted areas, or wearing masks.

Model Training: The CNN model was trained on the annotated dataset using a supervised learning approach. The dataset was split into training and validation sets, and the model was trained using backpropagation and stochastic gradient descent (SGD) optimization. The model was fine-tuned using hyperparameter tuning techniques to achieve high accuracy in anomaly detection.

Video Segmentation: The OpenCV library was used to segment the video into frames, and the Discriminative Deep Belief Network Algorithm was applied to extract the background and foreground from each frame. This helped in isolating the areas of interest and reducing noise in the subsequent anomaly detection process.

Anomaly Detection: The pre-trained CNN model was then used to classify the foreground frames as normal or abnormal. The model utilized learned patterns of suspicious activities to detect unusual activities in real-time.

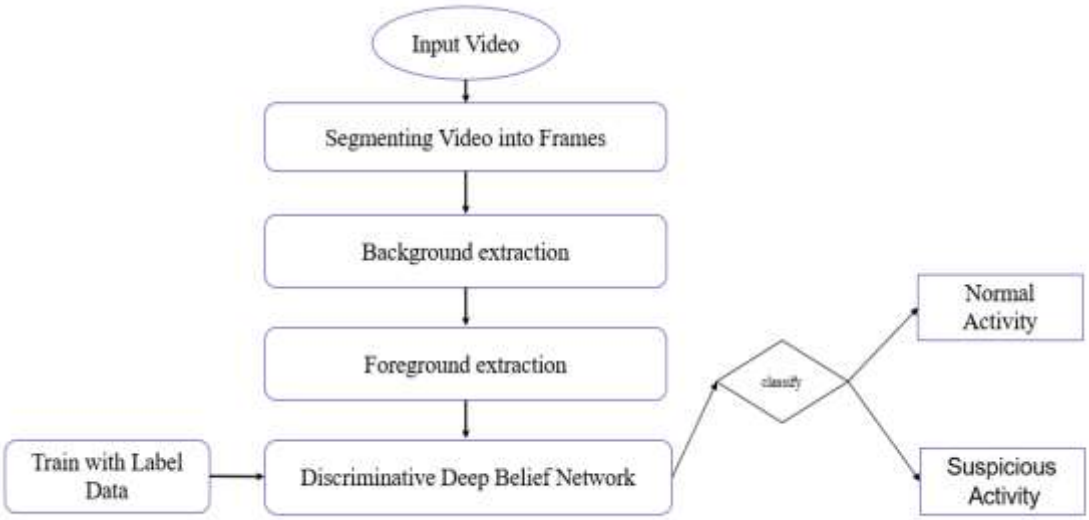


Fig: Flow Chart

Alert Generation: When abnormal activities were detected, alerts were generated in real-time, which could be sent to relevant stakeholders through notifications, alarms, or other forms of alerts, depending on the application requirements

VII. RESULTS

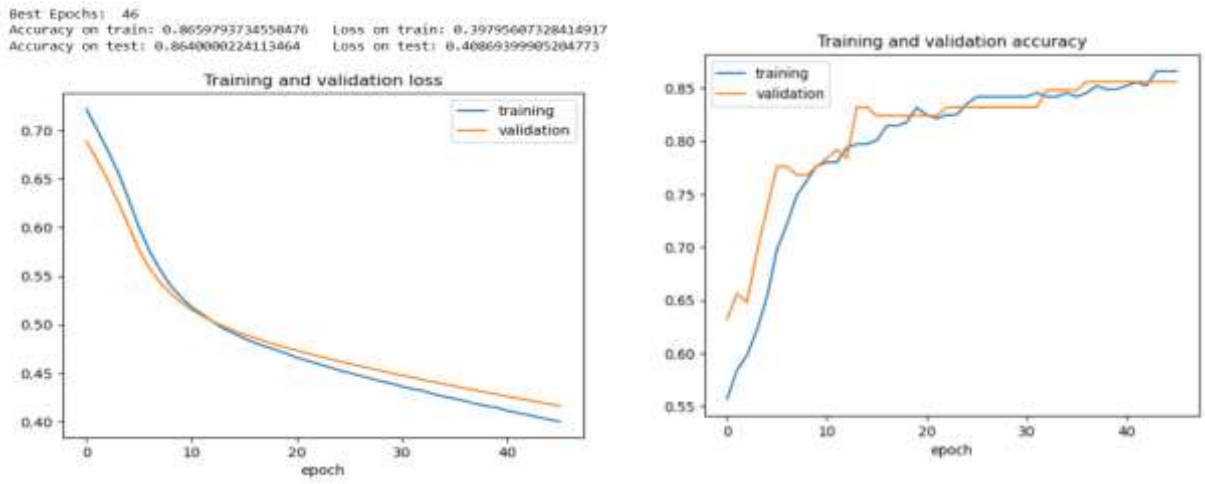
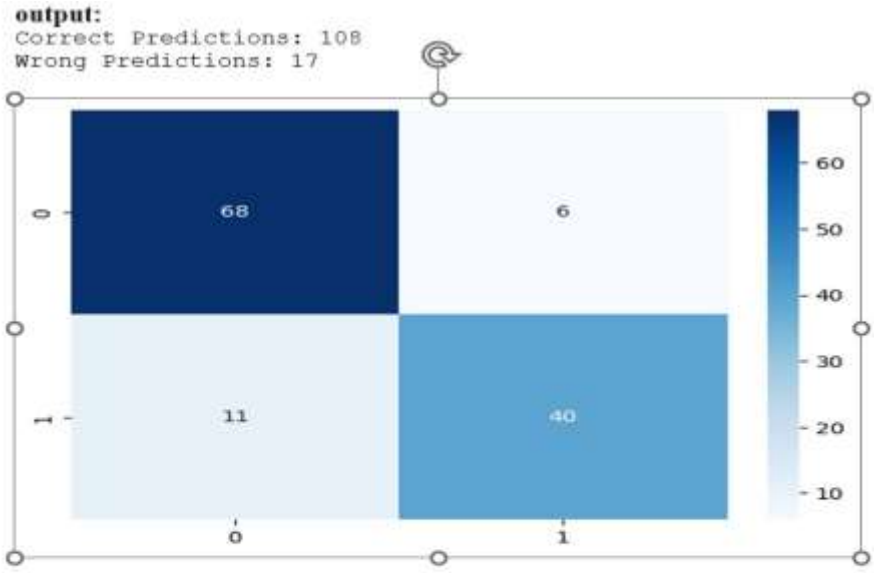


Fig: Training and Validation Accuracy, Training and Validation loss



	precision	recall	f1-score	support
unsuspicious	0.86	0.92	0.89	74
suspicious	0.87	0.78	0.82	51
accuracy			0.86	125
macro avg	0.87	0.85	0.86	125
weighted avg	0.86	0.86	0.86	125

Fig: Output Predictions

Fig: Before the Fighting Started (Detect as Unsuspicious Activity)

Fig: Before fighting (Detecting as a Unsuspicious Activity)

Fig: Detecting Fighting as a Suspicious Activity

Fig: Detecting Closing Camera as a Suspicious Activity

VIII. CONCLUSION

The research suggests employing a convolutional neural network for feature extraction and a discriminative deep belief network for action classification to detect suspicious behavior from surveillance video. By using a deep-learning-based model, the suggested approach achieves better categorization than earlier efforts. To begin, we divided video into frame segments and used CNN to extract features from the background and foreground. The output is then input into a trained DDBN, which classifies the recognized behaviors as normal or suspicious. The deep learning model guarantees more precision and fewer false positives.

IX. FUTURE SCOPE

- The current system uses a simple rule-based approach for detecting suspicious activity. However, by integrating with advanced machine learning algorithms, the system can become more accurate and efficient in detecting anomalies.
- The system can be enhanced to provide real-time monitoring of suspicious activity. This can be achieved by integrating with real-time data streaming technologies like Apache Kafka, Apache Flink, or Apache Spark.
- Currently, the system only monitors transactions on one channel (e.g., web-based transactions). However, by integrating with multiple channels like mobile applications, point-of-sale devices, and other systems, the system can become more comprehensive and effective in detecting fraud.
- The system can be improved by providing detailed reports on suspicious activities, including the types of activities, frequency, and other relevant details. This can help organizations to identify trends and patterns and take proactive measures to prevent fraud

X. REFERENCES

[1]. Dinesh Jackson Samuel R, Fenil E, Gunasekaran Manogaran, Vivekananda G.N, Thanjaivadivel T, Jeeva S, Ahilan A, "Real time violence detection framework for football stadium comprising of big data analysis and deep learning through bidirectional LSTM", The International Journal of Computer and Telecommunications Networking,2019

[2]. Aqil Shamnath, Meena Belwal, "Human Suspicious Activity Detection Using Ensemble Machine Learning Techniques", 2nd International Conference on Intelligent Technologies (CONIT), Publisher: IEEE, 18 August 2022

[3]. Tejashri Subhash Bora , Monika Dhananjay Rokade "Human Suspicious Activity Detection System Using CNN Model For Video Surveillance" IJARIIE-ISSN(O)-2395-4396, Vol-7 Issue-3 2021

[4]. Nandini. G , Dr. B. Mathivanan , Nantha Bala. R. S, Poornima. P, "Suspicious Human Activity Detection", International Journal of Advance Research and Development, Volume3, Issue4 – 2018.

[5]. Amrutha.C, Jyotsna.C, Amudha, J. (2020), "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video" 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA).

[6]. Shriya Akella, Priyanka Abhang, Vinit Agrharkar, Reena Sonkusare, (2020), "Crowd Density Analysis and Suspicious Activity Detection", 2020 IEEE International Conference for Innovation in Technology (INOCON)

[7]. Digambar Kauthkar, Snehal Pingle, G.H. Raisoni , Vijay Bansode, Pooja Idalkanthe, prof. Sunita Vani, "Suspicious Human Activity and Fight Detection using Deep Learning", International Journal of Innovative Science and Research Technology, Volume 7, Issue 6, June – 2022 .

[8]. Alavudeen Basha A, Parthasarathy P, Vivekanandan S, "Detection of Suspicious Human Activity based on CNN-DBNN Algorithm for Video Surveillance Applications", 2019 Innovations in Power and Advanced Computing Technology (i-PACT)

[9]. Pankaj Bhambri, Sachin Bagga, Dhanuka Priya, Harnoor Singh, Harleen Kaur Dhiman, "Suspicious Human Activity Detection System", IRO Journal of IoT in Social, Mobile, Analytics, and Cloud, Volume – 2, Issue – 4, December 2020

[10]. P. A. Dhulekar, Dr. S.T. Gandhe, NachiketSawale, Vikas Shinde, Sunil Khute, "Surveillance System for Detection of Suspicious Human Activities at War Field", International Conference on Advances in Communication and Computing Technology (ICACCT) Amrutvahini College of Engineering, Sangamner, Ahmednagar, India, 2018.