WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

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

# Intelligent Video Surveillance

***Vishruti Bharadwaj[1], Yatra Bharkhada[2], Ruchika Jamba3, Prof. Sanjay Ranveer[4]***

[1]Computer Engineering, Usha Mittal Institute of Technology,
[1]bharadwajvishruti@gmail.com, [2]ydbharkhada@gmail.com, [3]ruchija04@gmail.com, [4]su.ranveer@gmail.com

**ABSTRACT—**

Intelligent Video Surveillance (IVS) system designed for anomaly detection and monitoring of suspicious activities in video streams. The system utilizes a Convolutional Neural Network (CNN) algorithm for efficient and accurate detection of anomalies, such as fights and abuse, in CCTV footage. Upon detection, the system sends email alerts to the user, including snapshots from the CCTV feed highlighting the suspicious activity. Additionally, audio alerts are triggered to notify security personnel of the detected anomaly. The email alerts also include the location information (latitude, longitude, and address) of the CCTV camera, providing context for the incident. The system is capable of labeling anomalies detected for further analysis and reporting. Overall, this IVS system offers a comprehensive solution for proactive surveillance and response to security threats in various environments.

***Keywords*** **– Video Surveillance, Anomaly Detection, CCTV videos, computer vision, activity detection, object tracking, CNN, abmodel.h5, video label, mail alerts, audio alert, location track- ing.**

## I. Introduction

In light of the growing need for security in public spaces including train stations, airports, supermarkets, schools, and congested streets, surveillance cameras are employed to keep an eye on everyday activities. However, since abnormal occurrences only occur in 0.01% of cases and 99.9% of monitoring time is wasted, this method is labor-intensive and requires constant human supervision, making it a tedious procedure. Furthermore, a surveillance system generates a large amount of redundant video data that needs extra storage. To reduce human errors and storage costs, it is necessary to build an efficient automated surveillance system for detecting any strange behaviours that may lead to dangerous situations.

In recent years, there's been a growing interest in making surveil- lance systems better. Researchers are working hard to create surveil- lance systems that can spot strange behaviors, which could signal danger. This is important because it's part of a bigger discussion about keeping public places safe. However, even with all the progress, there's still a big problem: the current systems aren't very good at catching unusual behaviors. While some studies recognize the need for better systems, they haven't figured out how to make them work well. This study aims to fix that by suggesting the development of a more efficient surveillance system that uses advanced machine learning technology.

Intelligent Video Surveillance system with anomaly detection capabilities can greatly enhance security measures and provide a safer environment for various applications, including public safety, transportation, and commercial security. It increases the likelihood of spotting illegal behavior while decreasing the amount of man- hours required to keep an eye on these frequently intricate systems.

While initial setup costs may be involved, in the long run, surveillance systems can be more cost-effective than manual monitoring, as they can operate 24/7 without the need for constant human supervision.

Using computer vision and machine learning algorithms, the system analyses each frame of the video to detect anomalies such as fights, abuse, accidents, or fires. It utilizes CNNs to improve accuracy and reduce false positives also CNN can analyze spatial and temporal features in video frames, crucial for understanding activities and identifying abnormalities.

The system can provide valuable insights into patterns of behavior and potential vulnerabilities, which can be used for further analysis and improving security measures. Users can monitor video feeds and receive alerts from anywhere, providing flexibility and conve- nience in surveillance operations. The system integrates with email services (e.g., Gmail, Outlook) to send email alerts. Moreover, the mail includes compelling evidence, including location data(longitude, latitude, address) and CCTV snapshot. Simultaneously, the system plays an audio alert saying "Anomaly detected" to immediately alert the user.

## II. LITERATURE SURVEY

Searching and filtering recent articles on video surveillance using deep learning algorithms to analyze human actions was a crucial step in getting ready for the survey.

*A. Suspicious Activity Recognition in Video Surveillance Sys- tem [1]*

In this paper, the hierarchical approach is used to detect different suspicious activities such as loitering, fainting, unauthorized entry, etc. This approach is based on the motion features between the different objects. Semantic approach which applies the human under- standing of the activity. The object (bag) detection is done by the dual background approach using the Gaussian Mixture Model(GMM). Dataset used was CAVIAR (PETS 2004) and PETS 2006 with 84% Accuracy.

*B. Suspicious Activity Detection in Surveillance Footage [2]*

Breaking down complicated tasks and detecting sub-tasks that lead to potential crimes is one way to simplify an activity to be automated. We focus on two main potential leads to crimes which we attempt to detect through our models. With Faster R-CNN it achieved 90.35% on PETS 2006, MS-COCO dataset.

*C. Deep Learning Approach for Suspicious Activity Detection from Surveillance Video [3]*

To employ CCTV footage to continuously observe a campus environment, Identify any suspicious incidents, and promptly notify security personnel when such events are detected. In this CNN, LSTM and Twilio Library in Python for SMS Sending were used to achieve 87.15%.

*D. Abnormal Crowd Behavior Detection Using Motion Infor- mation Images and CNN [4]*

Existing approaches often struggle to accurately identify unusual crowd activities, necessitating the development of a more robust solution utilizing motion information images and convolutional neural networks to improve detection accuracy and reliability.CNN and Motion Information Image(MII) algorithm used on the UMN and PETS2009 to achieve accuracy 98.39%.

*E. Suspicious Activity Detection from Videos using YOLOv3 [5]*

So main motive is to create an automatic computerized system for human action recognition for suspicious movements that will be ro- bust and can work fast and accurately in every environment.YOLOv3 uses a CNN feature extractor named Darknet 53 on UMN Dataset achieving 93% accuracy.

## III. SYSTEM OVERVIEW

The proposed system will use footage obtained from CCTV cameras for monitoring activities and then send alert emails to the corresponding authority when any suspicious event occurs.

*A. System Architecture*

The architecture has different phases like video input, video surveillance, feature extraction, classification, and prediction. The general layout of the system architecture is shown in Fig.1.The system classifies the videos into three classes.

- Abuse, Assault, Arson, Arrest, Accident - Suspicious Class
- Walking - Normal Class
- Usual/Typical Car Movement on the road - Normal class

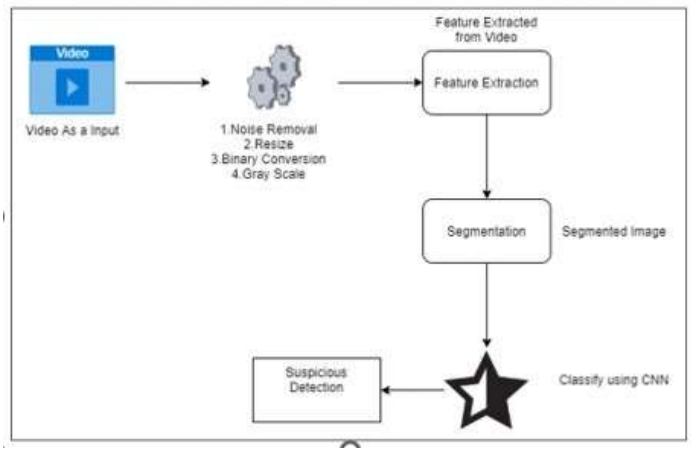


Fig. 1. System Architecture

*B. Dataset Description*

Anomaly detection has been extensively studied in many fields, especially in computer vision, to learn and understand activity recog- nition. The difficulty of this undertaking might increase dramatically because real-world situations are often complex. It is difficult to compile all of the abnormal incidents because there are infinity of them. The dataset is a standard dataset that has a collection of sequences representing various actions like arrest, fighting, abuse, accident, etc and each action class has multiple sequences. The whole dataset is manually labeled and separated into 80% for the training set and 20% for the testing set.

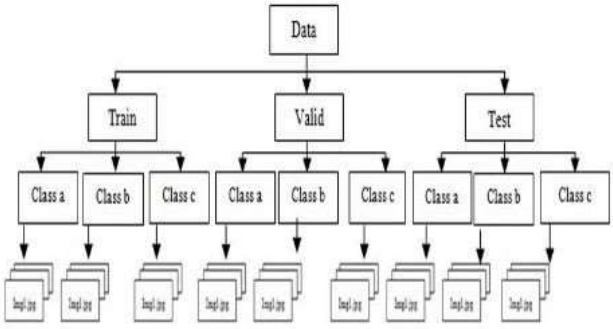


Fig. 2. Dataset Description

*C. Video Monitoring*

Our proposed system incorporates a deep learning network for the detection of suspicious activities in video surveillance. Utilizing deep learning architectures enhances accuracy, particularly when dealing with large datasets. Figure 1 provides a comprehensive overview of the system architecture.

The input videos are sourced from existing and newly created datasets. During processing, frames are extracted from these videos, organized into three labeled folders, and stored accordingly. The entire video is transformed into frames, saved as JPG images, and each frame is resized by 300% to align with the 2D CNN architecture. The testing video undergoes a similar process, with frames resized by 300% and stored in a designated folder. The video processing utilizes the OpenCV library in Python.

Subsequently, the image matrix and labels are shuffled using the shuffle function, and the data is split into training and testing sets. Normalization of pixel values to the range [0, 1] is executed by di- viding each pixel value by 255. Following this, a basic Convolutional Neural Network (CNN) model is constructed using the Keras library. The model comprises two convolutional layers employing Rectified Linear Unit (ReLU) activation, followed by flattening and a dense layer with softmax activation for binary classification.

Categorical cross-entropy loss and the Adam optimizer are used to compile the model.Subsequently, the CNN model is trained using the provided training data, incorporating a validation set and iterating through 10 epochs. The training accuracy of the model is computed based on predictions made during this training phase. Finally, the trained CNN model is saved to a file named ”abmodel.h5,” facilitating future use or deployment in various applications.

The system classifies videos as either suspicious (e.g., fighting, fire) or normal (e.g., walking, running). In the event of suspicious behavior, an email is sent to the registered user along with the location and CCTV snapshot.

## IV. RESULT ANALYSIS

The project aims to monitor suspicious activities at places like offices, roads, etc using CCTV footage and alert security when any suspicious event occurs. CNN was used to extract features from the frames in order to do this.

The steps for building the complete system are collecting video sequences from CCTV footage, extracting frames from videos, pro- cessing the images, and preparing of the training and testing sets from the datasets and executing them. In the case of suspicious activity, the system sends an email along with the CCTV snapshot and location inclusive of latitude, longitude, and address to the registered user.The system was built on an open-source platform using Python. Sending of emails is done by using SMTP.

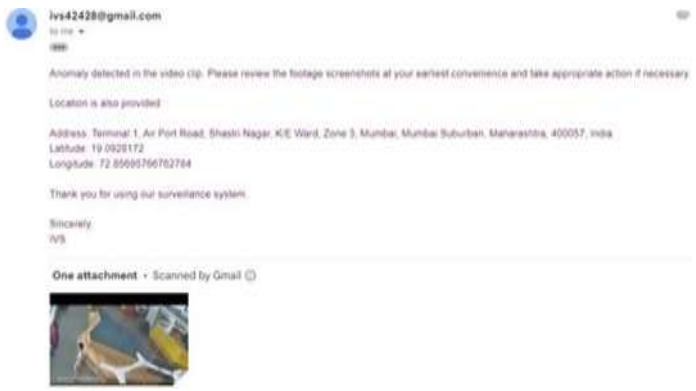


Fig. 3. Results


Fig. 4. Results

### *A. Training and Testing*

Frames are extracted from a diverse set of videos, sourced from a dedicated dataset, encompassing various instances of suspicious and normal behaviors. These videos are a compilation of CCTV footage capturing different scenarios from a viewpoint. The processing stage involves extracting frames from these videos. The core of our system relies on a trained model named abmodel.h5, a Convolutional Neural Network (CNN) that has been learned from this dataset to address our specific problem.

For testing, CCTV video clips from various situations are used, and these are converted into frames. These frames are then input into the trained model. The classifier utilizes the knowledge gained during training to categorize the videos as either exhibiting suspicious or normal behavior.

### *B. Results*

The initial epochs of the training phase yield a training accuracy exceeding 90%. To enhance model accuracy, one can consider increasing the number of videos in the dataset. Frames extracted from videos are consolidated into a single folder for testing purposes. The trained model categorizes frames as either suspicious (Abuse, Assault, Fighting, Fire, Accident) or normal (Walking, Usual/Typical Car Movement on the road). Upon detecting suspicious activity, the system triggers an email including a CCTV snapshot and lo- cation(longitude, latitude, address) to the registered user, achieving an overall accuracy of 95%.

## V. Conclusion

In conclusion, the Intelligent Video Surveillance system developed for anomaly detection in videos has proven to be a valuable tool for enhancing security and safety measures. By leveraging advanced algorithms, the system efficiently detects activities like fights, abuse, accidents, and fires, ensuring timely intervention. Upon detection, the system not only sends email alerts to the user but also plays an audio notification, enhancing the responsiveness of the monitoring process. The inclusion of the video's location as well as CCTV snapshots in the email provides further context, aiding in swift action. All things considered, this system is a major improvement in video surveillance technology, offering monitoring and alerts for enhanced security and safety.

## VI. FUTURE WORK

The upcoming work involves enhancing the intelligent video surveillance system by improving accuracy, efficiency, and effective- ness. We aim to address privacy concerns and ethical considerations while incorporating advanced technologies, machine learning, and real-time analytics. Possible extensions include adding features for detecting abnormalities like knives, guns, or suspicious objects. Integrating audio interfaces in an IVS system involves adding audio sensors or microphones to capture sounds. These sounds can then be analyzed alongside video feeds using audio recognition

algorithms. Detection of unusual audio events triggers alerts for further action, enhancing anomaly detection capabilities. For eg. a woman running and shouting for help. We also plan to implement 360-degree and panoramic cameras to detect abnormalities from all angles.

**References**

[1] Kamthe, U. M. and Patil, C. G., "Suspicious Activity Recog- nition in Video Surveillance System", pp. 1 - 6, 2018. [2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)].

[2] Loganathan, Sathyajit and Kariyawasam, Gayashan and Sumathipala, Prasanna, "Suspicious Activity Detection in Surveillance Footages", pp. 1-4, 2019. [2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)].

[3] Amrutha, C.V and Jyotsna, C. and Amudha, J., "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video", pp. 335-339, 2020. [2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)].

[4] Direkoglu, Cem, "Abnormal Crowd Behavior Detection Using Motion Information Images and Convolutional Neural Net- works", pp. 80408-80416, 2020.

[5] Bordoloi, Nipunjita and Talukdar, Anjan Kumar and Sarma, Kandarpa Kumar, "Suspicious Activity Detection from Videos using YOLOv3", pp. 1-5, 2020. [2020 IEEE 17th India Council International Conference (INDICON)].