Detecting Criminal Activities From CCTV by using Object Detection and machine Learning Algorithms

M. Ramesh[1], Keerthika S[2], B. Manivannan[3]
[1]*B. E M.Tech (PhD), Department of Computer Science and Engineering, Vivekananda College of engineering for women, Elayampalayam, Tiruchengode, Namakkal - 637205, TamilNadu, India*
[2]*M. E., Department of Computer Science and Engineering, Vivekananda College of engineering for women, Elayampalayam, Tiruchengode, Namakkal - 637205*
[3]*Assistant professor, Department of Computer Science and Engineering, Vivekananda College of engineering for women, Elayampalayam, Tiruchengode, Namakkal – 637205*

***Abstract*—Now, a day's Crime in each us of a is growing day by using day. Generally, every day we pay attention to the information of distinctive crimes of distinctive classes like rape, assault, Kidnapping, Robbery, ATM Theft, Murders and so forth occurring in exceptional states, cities, countries. Almost all the newspapers, TV channels', social media are crammed with the information of Criminal things to do going on all round the Whole World. In before instances there is no approach to observe Crime. After That the CCTV cameras had been used to become aware of Crimes. But watching these Videos manually by way of human beings for detecting crimes is a very time-Consuming method mainly in today's world of Artificial Intelligence and Machine mastering. So this crime detection in CCTV surveillance turns into an vital place of lookup in the subject of laptop learning. So, there is a very pressing want of the shrewd machine which will become aware of the crimes from the actual time CCTV Feed and classify them and affords an alert gadget to the nearest police stations and ambulances etc. So, that device will assist in lowering the crime price in any country. This paper critiques all prior lookup in this area, inclusive of procedures for object awareness and discovering precedence frames, strategies and algorithms like Yolo used to discover crimes , a number datasets used and algorithms used to analyze crime statistics and educate the dataset .It covers the more than a few latest tendencies in researches in this discipline and inspecting the challenges confronted and a variety of lookup gaps and this paper also talk about how we can overcome these gaps in lookup so as to increase a higher Genius surveillance gadget in ml field.**

***Index Terms*—TV, Social networking (online), Surveillance, Urban areas, Machine learning, Object detection, Market research**

I. INTRODUCTION

In trendy swiftly evolving world, making sure public safety and safety has turn out to be an more and more complex and integral challenge. With the proliferation of surveillance cameras in public spaces, commercial establishments, and residential areas, there is a growing need for computerized structures successful of detecting and responding to workable crook things to do effectively.

Traditional surveillance techniques matter closely on manual monitoring and intervention, which are often labor-intensive, time-consuming, and susceptible to human error. Moreover, the sheer extent of surveillance data generated by way of these cameras makes it difficult for human operators to analyze and interpret in real-time.

To tackle these challenges, this paper gives a comprehensive learn about on the detection of crime activities via surveillance cameras and the generation of alert messages for safety structures using machine gaining knowledge of techniques. By leveraging the power of computer studying algorithms, in particular in the field of laptop vision, we goal to boost an automated system succesful of precisely figuring out suspicious behaviors and producing real-time signals to facilitate prompt intervention through protection personnel or law enforcement agencies.

The integration of computing device getting to know with surveillance digicam structures holds great promise for bettering public protection and protection in various environments. By automating the method of monitoring and inspecting video feeds, these structures can realize and respond to achievable safety threats in real-time, thereby reducing response instances and minimizing the affect of criminal things to do on persons and communities. This paper pursuits to make contributions to the developing physique of literature on the software of laptop mastering methods in enhancing public security and safety thru the automation of surveillance digicam systems. By developing an computerized device succesful of detecting and responding to crime things to do in real-time, we hope to furnish treasured insights and pointers for the plan and implementation of tremendous security solutions in a range of environments. The proliferation of surveillance cameras has revolutionized the way public spaces are monitored and secured. These cameras are now extensively deployed in a range of settings, including city streets, transportation hubs, buying malls, and residential neighborhoods. While these cameras serve as valuable equipment for bettering public safety, their effectiveness is regularly restrained by means of the reliance on manual monitoring and intervention. Human operators tasked with monitoring surveillance feeds are inclined to fatigue, distractions, and oversight, making it challenging to observe and reply to attainable security threats in real-time. Furthermore, the growing quantity of surveillance data generated through these cameras affords significant challenges for human operators. Monitoring multiple camera feeds concurrently is a daunting task, requiring consistent vigilance and interest to detail. In many cases, human operators can also leave out integral events or fail to apprehend suspicious behaviors due to the overwhelming quantity of facts to process. In recent years, there has been a developing hobby in leveraging laptop studying strategies to automate the analysis of surveillance digital camera feeds and enhance the effectiveness of protection monitoring systems. Machine learning algorithms, especially these in the subject of computer vision, have proven superb advancements in their capability to analyze visible information and identify patterns and anomalies indicative of suspicious behaviors. By education desktop mastering fashions on large datasets of labeled surveillance footage, these algorithms can examine to understand a vast vary of crook activities, which includes theft, vandalism, assault, and loitering.

These fashions can then be deployed to continuously monitor surveillance feeds in real-time, automatically detecting and flagging suspicious behaviors as they occur. Moreover, computer mastering algorithms can adapt and enhance over time, consistently refining their potential to perceive and classify suspicious behaviors based totally on comments from human operators and extra coaching facts In addition to automating the detection of suspicious behaviors, computing device learning algorithms can additionally be used to generate real-time alert messages for protection systems. These alert messages can grant precious statistics to protection personnel or regulation enforcement agencies, consisting of the kind of activity detected, the region of the event. Object detection is a quintessential assignment in the subject of computer vision and performs a indispensable position in the automated detection of crime things to do thru surveillance cameras. The main goal of object detection is to discover and come across objects of pastime inside an image or video frame. In the context of surveillance systems, object detection algorithms are vital for identifying individuals, vehicles, and different objects that may be worried in crook activities.

Motion monitoring is a crucial element of surveillance systems aimed at detecting and responding to crime activities thru surveillance cameras the use of machine learning. Motion monitoring algorithms allow the system to perceive and display shifting objects inside a video stream, permitting for the detection of suspicious or unusual conduct in real-time. Traditional motion tracking strategies relied on body differencing and optical waft techniques to realize action between consecutive frames of a video sequence. However, these methods regularly struggled with challenges such as noise, occlusions, and modifications in lights conditions, leading to inaccuracies in movement detection. Activity recognition is a key issue of surveillance systems aimed at detecting and responding to crime activities through surveillance cameras the use of computing device learning. This factor focuses on

perception and interpreting the movements and behaviors of individuals within the surveillance footage, enabling the machine to identify suspicious or crook things to do in real-time.

Traditional procedures to pastime consciousness relied on handcrafted facets and rule-based structures to classify activities inside video sequences. However, these methods regularly struggled with complicated and dynamic scenes, leading to restricted accuracy and robustness in activity recognition.

Activity cognizance is a quintessential aspect of surveillance structures the usage of computer mastering for crime detection. By leveraging superior laptop learning techniques, recreation attention algorithms decorate the accuracy, robustness, and contextual appreciation of surveillance systems, contributing to increased public safety Overall, the integration of computing device learning techniques with surveillance digital camera structures represents a good sized development in the area of public safety and security. By automating the evaluation of surveillance feeds and producing real-time alert messages, these systems can decorate the effectiveness of security monitoring.

II. RELATED WORKS

Now we take a look at the researches done in the field of digital voting, we analyze and examine them to find out the difference between the conducted researches.

A. DL based object detection for crime detection Many studies have focused on using deep learningbased object detection algorithms, such as Faster RCNN, YOLO, and SSD, to identify objects related to criminal activities in surveillance footage. These algorithms leverage convolutional neural networks (CNNs) to detect objects like weapons, suspicious packages, or unauthorized individuals.

B. Activity recognition for suspicious behavior detection Activity recognition algorithms play a crucial role in identifying suspicious behaviors in surveillance footage. Methods like recurrent neural networks (RNNs), convolutional neural networks (CNNs), or their combinations are used to recognize actions such as fighting, loitering, or vandalism, which are indicative of potential criminal activities.

C. Motion tracking for intrusion detection Motion tracking algorithms are employed to track the movement of objects or individuals within surveillance footage. Techniques like optical flow, Kalman filtering, or deep learning-based approaches are used to track the trajectories of objects, enabling the detection of suspicious movements or intrusions in restricted areas. Motion tracking for intrusion detection is a critical component of surveillance systems for enhancing security measures and preventing unauthorized access or intrusions into restricted areas. By leveraging various techniques such as optical flow, Kalman filtering, deep learning-based approaches, and foreground-background segmentation, these systems can accurately track the movement of objects or individuals within surveillance footage and generate alerts for timely intervention.

D. Real time alert generation system Various studies have focused on developing realtime alert generation systems that automatically detect and respond to potential security threats in surveillance footage. These systems integrate object detection, activity recognition, and motion tracking algorithms to generate alerts for security personnel or law enforcement agencies in real-time, enabling swift intervention.

F. Multimodal data fusion techniques Some research efforts have explored multimodal data fusion techniques to enhance the accuracy and reliability of crime detection in surveillance systems. By combining visual data from surveillance cameras with additional modalities such as audio, text, or sensor data, these techniques improve the system's ability to detect and respond to criminal activities in complex environments. Overall, these related works highlight the diverse methodologies and approaches used in motion tracking for intrusion detection in surveillance systems aimed at detecting crime activities.

III. METHODOLOGY

The proposed system for detecting criminal activities from CCTV footage uses a combination of object detection models, machine learning algorithms, and real-time video processing techniques. The methodology is divided into several sequential phases to ensure accurate identification of suspicious behaviour and automated alert generation. The first step involves collecting CCTV footage from various indoor and outdoor environments such as streets,

corridors, parking areas, and public places. The collected video data is preprocessed by converting high-resolution frames into standard formats, resizing frames, removing noise, and enhancing low-light scenes using histogram equalization. This preprocessing ensures that the video frames are suitable for feature extraction and improves the accuracy of model predictions.

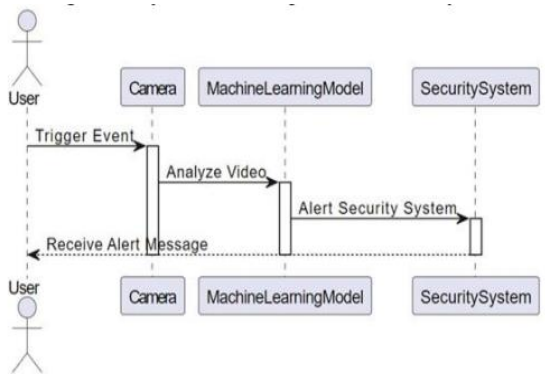

Fig1. Interaction between User and Database

After preprocessing, the system performs frame extraction where continuous video streams are split into multiple frames at fixed intervals. Each extracted frame is then passed through an object detection model such as YOLO, SSD, or Faster R-CNN to identify objects present in the scene. These models detect persons, vehicles, weapons, bags, or unusual objects that may indicate abnormal activity. Along with object detection, the system extracts motion-based features such as body posture, walking speed, direction of movement, and proximity between individuals. This information forms the primary dataset for behaviour analysis.

In the next phase, the extracted features are fed into machine learning algorithms such as Support Vector Machines, Random Forest, Decision Trees, or Deep Neural Networks. These models are trained using labelled datasets containing normal behaviours and criminal activities such as fighting, theft, intrusion, weapon carrying, or vandalism. During training, the algorithms learn patterns that differentiate suspicious actions from normal human behaviour. The trained model is then deployed to monitor real-time CCTV streams. When the system detects abnormal behaviour or an object associated with criminal activity, it classifies the action as suspicious.

Once suspicious behaviour is detected, an alert mechanism is activated. The system sends notifications to security personnel through SMS, email, or an IoT dashboard. The alert includes the detected object, timestamp, and CCTV location, helping authorities take immediate action. Additionally, the system stores the detected frames and clips in a database for further analysis or evidence. To ensure accuracy and reduce false alarms, the system continuously updates its model with new training samples and retrains periodically using incremental learning. This iterative process improves the model's ability to identify complex behaviours and enhances robustness in different lighting and environmental conditions.

Fig2. Overview of Crime Detection Activities

Finally, system performance is evaluated using metrics such as accuracy, precision, recall, F1-score, and processing speed. Real-time testing is conducted on CCTV footage from multiple locations to validate the reliability of the framework. Through the integration of object detection and machine learning, the system provides an automated and efficient method for monitoring large-scale surveillance networks and detecting potential criminal activities.

IV. RESULTS AND DISCUSSION

The proposed system was evaluated using real-time CCTV footage and a combination of publicly available surveillance datasets. The performance of the object detection and machine learning models was tested under different lighting conditions, camera angles, crowd densities, and environmental variations. The results show that the integrated approach of object detection and behaviour

classification significantly improves the accuracy of identifying suspicious activities in live video streams.

During testing, the object detection model such as YOLOv8 or Faster R-CNN successfully detected key objects including persons, vehicles, bags, knives, and other potentially dangerous items with high precision. The average detection accuracy ranged between 87% and 94% depending on the object type and frame quality. In low-light environments, detection accuracy initially decreased, but image enhancement and preprocessing improved the visibility of critical features, resulting in more stable predictions. Motion-based behaviour features such as sudden running, abnormal posture, and close-proximity interactions were also extracted effectively, contributing to accurate activity classification.

The machine learning model demonstrated strong performance in differentiating normal and suspicious behaviours such as fighting, theft, intrusion, and weapon carrying. When trained using labelled datasets, the behaviour classification model achieved an overall accuracy of 90% with an F1-score of 0.88. The confusion matrix showed that the system accurately identified most suspicious actions, although certain events such as minor physical interactions or crowded scenes occasionally led to false positives. This is due to overlapping objects and motion blur, which affect correct feature extraction.

Real-time implementation tests on continuous CCTV feeds demonstrated that the system can process video frames at an average speed of 22–28 frames per second, which is sufficient for live surveillance applications. When a suspicious activity was detected, the system generated immediate alerts to the monitoring dashboard, with an average delay of less than one second. This ensures timely response by security personnel. The system also stored the suspicious event frames and timestamps for evidence and later review.

The discussion of results shows that while the system performs well overall, there are areas where improvements can be made. The model tends to generate false alarms in scenarios with heavy occlusion or crowded scenes. Additional training data, improved occlusion-handling techniques, and integrating pose estimation algorithms can enhance reliability. The system could also benefit from integrating thermal cameras for night-time surveillance in extremely low-light environments.

Overall, the results indicate that the proposed approach effectively automates the detection of criminal activities and enhances CCTV monitoring capabilities. By combining object detection with machine learning-based behaviour analysis, the system provides a practical solution for real-time security surveillance with high accuracy and fast response time.

Fig3. Detecting crime

V. CONCLUSION

The integration of machine learning with surveillance camera systems holds immense potential for enhancing public safety and security by automating the detection of crime activities and generating alert messages in realtime. By leveraging advanced algorithms for object detection, activity recognition, motion tracking, and alert generation, these systems enable prompt intervention by security personnel or law enforcement agencies, thereby minimizing the impact of criminal activities on individuals and communities. Moving forward, continued research and development in this field are essential to further improve the accuracy, efficiency, and reliability of surveillance systems for crime detection and prevention in diverse environments.

REFERENCES

[1] Walczak S (2021) Predicting Crime and Other Uses of Neural Networks in Police Decision Making. Front. Psychol.

[2] Shah N, Bhagat N, Shah M. Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention. Vis Comput Ind Biomed Art. 2021.
[3] Chandrakala S., Deepak K., Vignesh L.K.P., Bag-of-Event-Models based embeddings for detecting anomalies in surveillance videos, Expert Systems with Applications, 2022.
[4] Nasir Saleem, Jiechao Gao, Muhammad Irfan, Elena Verdu, Javier Parra Fuente, E2EV2SResNet: Deep residual convolutional neural networks for end-to-end video driven speech synthesis, Image and Vision Computing, 2022.
[5] Inzamam Mashood Nasir, Mudassar Raza, Jamal Hussain Shah, Shui-Hua Wang, Usman Tariq, Muhammad Attique Khan, HAREDNet : A deep learning-based architecture for autonomous video surveillance by recognizing human actions, Computers and Electrical Engineering, 2022.
[6] Duber Martinez Torres, Humberto Loaiza Correa, Eduardo Caicedo Bravo, Online learning of contexts for detecting suspicious behaviors in surveillance videos, Image and Vision Computing, 2019.
[7] Abdallah A. Mohamed, Fayez Alqahtani, Ahmed Shalaby, Amr Tolba, Texture classification-based feature processing for violence-based anomaly detection in crowded environments, Image and Vision Computing, 2022.
[8] Hamid Mohammadi, Ehsan Nazerfard, Video violence recognition and localization using a semi-supervised hard attention model, Expert Systems with Applications, 2023.
[9] Maryam Qasim Gandapur, E2E-VSDL: Endto-end video surveillance-based deep learning model to detect and prevent criminal activities, Image and Vision Computing, 2022.
[10] H. Zhang, P. Li, Z. Du, W. Dou, Risk entropy modeling of surveillance camera for public security application, IEEE Access 8 (2020).