Detection of Crime Activities Using Machine Learning

Nisarga T N, Vaishnavi S V, Sukrutha B, Prof. Manoj Kumar H
Dept. Artificial Intelligence and Machine Learning, Bangalore Institute of Technology

Abstract - This research paper proposes a novel approach leveraging machine learning techniques for the automated detection of crime activities through surveillance camera feeds, coupled with the generation of real-time alert messages for security systems. The proposed system utilizes advanced computer vision algorithms to analyze live video streams from surveillance cameras, detecting anomalous behaviors and potential criminal activities. These algorithms are trained on large datasets of labeled video footage, enabling the model to learn and recognize patterns indicative of suspicious behavior such as trespassing, vandalism, theft, or violence. Upon detecting crime activity the system triggers alert message and sends alert message to security personal or law enforcement agencies.

***Keywords*— object detection, motion tracking and activity recognition**

I. INTRODUCTION

In today's rapidly evolving world, ensuring public safety and security has become an increasingly complex and critical challenge. With the proliferation of surveillance cameras in public spaces, commercial establishments, and residential areas, there is a growing need for automated systems capable of detecting and responding to potential criminal activities effectively. Traditional surveillance methods rely heavily on manual monitoring and intervention, which are often labor-intensive, time-consuming, and prone to human error. Moreover, the sheer volume of surveillance data generated by these cameras makes it challenging for human operators to analyze and interpret in real-time. To address these challenges, this paper presents a comprehensive study on the detection of crime activities through surveillance cameras and the generation of alert messages for security systems using machine learning techniques. By leveraging the power of machine learning algorithms, particularly in the field of computer vision, we aim to develop an automated system capable of accurately identifying suspicious behaviors and generating real-time alerts to facilitate prompt intervention by security personnel or law enforcement agencies.

The integration of machine learning with surveillance camera systems holds significant promise for enhancing public safety and security in various environments. By automating the process of monitoring and analyzing video feeds, these systems can detect and respond to potential security threats in real-time, thereby reducing response times and minimizing the impact of criminal activities on individuals and communities. This paper aims to contribute to the growing body of literature on the application of machine learning techniques in enhancing public safety and security through the automation of surveillance camera systems. By developing an automated system capable of detecting and responding to crime activities in real-time, we hope to provide valuable insights and recommendations for the design and implementation of effective security solutions in various environments. The proliferation of surveillance cameras has revolutionized the way public spaces are monitored and secured. These cameras are now widely deployed in a variety of settings, including city streets, transportation hubs, shopping malls, and residential neighborhoods. While these cameras serve as valuable tools for enhancing public safety, their effectiveness is often limited by the reliance on manual monitoring and intervention. Human operators tasked with monitoring surveillance feeds are susceptible to fatigue, distractions, and oversight, making it challenging to detect and respond to potential security threats in real-time.

Furthermore, the increasing volume of surveillance data generated by these cameras presents significant challenges for human operators. Monitoring multiple camera feeds simultaneously is a daunting task, requiring constant vigilance and attention to detail. In many cases, human operators may miss critical events or fail to recognize suspicious behaviors due to the overwhelming amount of information to process. In recent years, there has been a growing interest in leveraging machine learning techniques to automate the analysis of surveillance camera feeds and improve the effectiveness of security monitoring systems. Machine learning algorithms, particularly those in the field of computer vision, have shown remarkable advancements in their ability to analyze visual data and identify patterns and anomalies indicative of suspicious behaviors. By training machine learning models on large datasets of labeled surveillance footage, these algorithms can learn to recognize a wide range of

criminal activities, including theft, vandalism, assault, and loitering.

These models can then be deployed to continuously monitor surveillance feeds in real-time, automatically detecting and flagging suspicious behaviors as they occur. Moreover, machine learning algorithms can adapt and improve over time, continuously refining their ability to identify and classify suspicious behaviors based on feedback from human operators and additional training data In addition to automating the detection of suspicious behaviors, machine learning algorithms can also be used to generate real-time alert messages for security systems. These alert messages can provide valuable information to security personnel or law enforcement agencies, including the type of activity detected, the location of the event. Object detection is a fundamental task in the field of computer vision and plays a crucial role in the automated detection of crime activities through surveillance cameras. The primary objective of object detection is to identify and locate objects of interest within an image or video frame. In the context of surveillance systems, object detection algorithms are essential for identifying individuals, vehicles, and other objects that may be involved in criminal activities.

Motion tracking is a vital component of surveillance systems aimed at detecting and responding to crime activities through surveillance cameras using machine learning. Motion tracking algorithms enable the system to identify and monitor moving objects within a video stream, allowing for the detection of suspicious or unusual behavior in real-time. Traditional motion tracking techniques relied on frame differencing and optical flow methods to detect motion between consecutive frames of a video sequence. However, these methods often struggled with challenges such as noise, occlusions, and changes in lighting conditions, leading to inaccuracies in motion detection. Activity recognition is a key aspect of surveillance systems aimed at detecting and responding to crime activities through surveillance cameras using machine learning. This component focuses on understanding and interpreting the actions and behaviors of individuals within the surveillance footage, enabling the system to identify suspicious or criminal activities in real-time. Traditional approaches to activity recognition relied on handcrafted features and rule-based systems to classify activities within video sequences. However, these methods often struggled with complex and dynamic scenes, leading to limited accuracy and robustness in activity recognition.

Activity recognition is a critical component of surveillance systems using machine learning for crime detection. By leveraging advanced machine learning techniques, activity recognition algorithms enhance the accuracy, robustness, and contextual understanding of surveillance systems, contributing to improved public safety Overall, the integration of machine learning techniques with surveillance camera systems represents a significant advancement in the field of public safety and security. By automating the analysis of surveillance feeds and generating real-time alert messages, these systems can enhance the effectiveness of security monitoring.

II. RELATED WORK

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 learning-based object detection algorithms, such as Faster R-CNN, 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 real-time 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. PROBLEM STATEMENT

The Detection of crime activities through surveillance and sending message to security systems using Machine Learning models.

Traditional surveillance systems often rely on manual monitoring, leading to delays in detecting criminal activities. There is a need for an automated system using Machine Learning models to efficiently detect crime through surveillance and send real-time alerts to security systems for prompt intervention.

However, the conventional methods of crime detection and prevention through surveillance systems have become inadequate. Traditional surveillance systems often suffer from limitations such as reliance on human operators, lack of real-time analysis capabilities, and the inability to swiftly respond to emerging threats. As a result, there is a pressing need for a more advanced and automated approach to crime detection and prevention that leverages the power of Machine Learning (ML) models.

The problem at hand revolves around enhancing the effectiveness and efficiency of surveillance systems in identifying and responding to criminal activities in various environments, including public spaces, commercial establishments, and high-security areas. The primary challenges to be addressed include

Real-time Detection traditional surveillance systems are often reactive, requiring human intervention to identify and respond to criminal activities after they have occurred. There is a critical need for a system that can analyse surveillance data in real-time and promptly detect suspicious behaviour or incidents as they unfold

Automated Alerting once suspicious activity is detected, there is a requirement for an automated mechanism to send alerts to security systems or designated personnel for immediate response.

This includes integrating the surveillance system with existing security infrastructure to ensure seamless communication and coordination.

Adaptability and Scalability the solution must be adaptable to various surveillance environments and scalable to accommodate different types of criminal activities. It should be capable of detecting a wide range of behaviors and incidents, including theft, vandalism, loitering, and unauthorized access.

Accuracy and Reliability ML models used for crime detection must exhibit high accuracy and reliability to minimize false positives and negatives. The system should continuously learn and adapt to evolving patterns of criminal behavior, ensuring robust performance over time.

In conclusion, the challenge is to develop an advanced surveillance system powered by Machine Learning models that can effectively detect criminal activities in real-time, send automated alerts to security systems, and facilitate timely intervention by security personnel. This solution should address the aforementioned challenges while balancing considerations such as accuracy, reliability, adaptability, scalability, cost-effectiveness, privacy, and ethical considerations.

IV. SYSTEM MODEL

Building a system for the detection of crime activities through surveillance and sending messages to security systems using Machine Learning (ML) models involves several components a detailed explanation of how they function.

The digital voting system consists of three primary components:

- Data processing and analysis
- Machine learning models
- Integration and communication

The primary components of a system for the detection of crime activities through surveillance and sending messages to security systems using Machine Learning models are implemented in real-time to create a robust and responsive framework. Object detection, occurring during live surveillance, identifies and locates entities of interest. Simultaneously, activity recognition

models operate in real-time, discerning specific behaviors indicative of potential criminal actions. These components work seamlessly with the integration of security systems, providing a continuous flow of information and facilitating immediate responses to detected activities. The standardized message format and content, generated in real-time, convey essential details to security personnel, aiding in timely decision-making. Throughout the entire process, stringent security considerations are maintained, ensuring secure communication.

A. Overview

The detection of crime activities through surveillance and the subsequent communication of relevant information to security systems using Machine Learning (ML) models represents a cutting-edge approach in the field of public safety and security. This innovative system harnesses the power of advanced computer vision and pattern recognition techniques to analyze real-time surveillance data.

The process begins with the collection of diverse and annotated surveillance data, followed by meticulous preprocessing to ensure data quality. Object detection models, such as YOLO and Faster R-CNN, identify and localize entities within the footage. Concurrently, activity recognition models, often based on LSTM or 3D CNN architectures, discern specific behaviors associated

Criminal activities. Anomaly detection algorithms, such as auto encoders or one-class SVMs, enhance the system's ability to identify unusual patterns that may indicate potential threats.

The integration of ML models with security systems is a pivotal aspect, allowing for instantaneous communication and response. Real-time alerts, generated in standardized formats, are transmitted to security personnel, providing critical details such as the type of activity detected, timestamp, and location. The inclusion of visual evidence further aids in informed decision-making.

Security considerations remain paramount throughout the entire process, addressing privacy regulations and ethical standards to ensure the responsible use of surveillance technology. The continuous monitoring of system performance, coupled with a feedback loop for refinement, contributes to ongoing improvements and adaptability to emerging patterns of criminal behavior.

Overall, this comprehensive system amalgamates state-of-the-art ML techniques with effective communication strategies to enhance the efficiency and responsiveness of crime detection and prevention efforts in modern surveillance systems. Security considerations are paramount throughout the entire system development and implementation process. Striking a balance between effective crime detection and respecting privacy regulations and ethical standards is crucial.

In the Secure communication protocols and compliance mechanisms safeguard user privacy and maintain the integrity of the system. Continuous monitoring and a feedback loop contribute to the system's adaptability and improvement over time. Feedback from security personnel aids in refining the models and addressing emerging challenges, ensuring the system's relevance and efficacy in dynamic security environments. In conclusion, the integration of ML models into crime detection through surveillance and communication with security systems represents a cutting-edge and holistic approach to public safety.

The initial phase involves the meticulous collection of diverse data from surveillance cameras and sensors, subsequently annotated to facilitate supervised learning. The data undergoes rigorous preprocessing, encompassing tasks such as noise removal, data normalization, and feature extraction. By combining advanced analytical capabilities with real-time communication strategies, this system empowers security personnel to make informed decisions, ultimately contributing to more effective crime prevention and response efforts in contemporary surveillance landscapes.

B. Deep Convolution Networks (CNN)

Deep Convolutional Networks (CNNs) are instrumental in the field of surveillance and crime detection, designed with a specific purpose: to analyze visual data for features and patterns. These neural networks exhibit a hierarchical feature extraction process, allowing them to automatically learn intricate features from input visual data. In the context of surveillance, these layers progressively capture spatial patterns, such as the arrangement of objects or the trajectory of individuals engaged in suspicious activities. The convolutional layers within CNNs perform local feature learning by applying filters to small portions of the input data, facilitating the identification of relevant objects or activities within surveillance footage. Additionally, CNN architectures demonstrate translation invariance, enabling them to recognize patterns regardless of their position in the visual field. Pooling layers reduce spatial dimensions, providing abstraction for efficient processing of surveillance data in real-time scenarios.

register their vote and can use any address on the

blockchain to participate in voting. We will learn more about the reason for this later.

C. Integrated surveillance analysis

Integrated surveillance analysis represents a sophisticated and all-encompassing approach to monitoring and analyzing activities within a given environment. This methodology involves the integration of diverse surveillance components, including video analytics, object detection, activity recognition, and anomaly detection. Video analytics, often leveraging advanced machine learning models like Convolutional Neural Networks (CNNs), facilitates object detection, allowing the system to identify and track individuals, vehicles, or other objects of interest.

Activity recognition focuses on categorizing actions or behaviors captured in video sequences, providing a deeper understanding of unfolding events. Anomaly detection mechanisms are crucial for identifying unusual patterns or deviations from normal activities, serving as a key indicator of potential security threats.

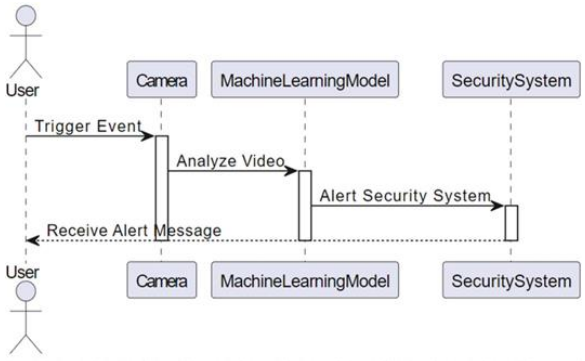

Fig1. Interaction between User and Database

To Real-time alerting mechanisms notify security personnel when specific criteria are met, conveying information about detected objects, recognized activities, or identified anomalies. Integrated surveillance analysis incorporates data fusion and correlation to provide a coherent and contextual understanding of the monitored environment. The system often includes adaptive learning mechanisms and a feedback loop for continuous improvement and adaptation to evolving patterns of behavior.

Security is a top priority, ensuring secure communication channels, compliance with privacy regulations, and seamless integration with existing security infrastructure. The insights generated by the integrated analysis serve as decision support for security operators, empowering them to make informed decisions and respond effectively to potential security incidents. Overall, integrated surveillance analysis plays a pivotal role in enhancing situational awareness, improving threat detection and enabling timely responses in diverse monitoring and law enforcement to industrial and critical infrastructure security. Integrated surveillance analysis stands at the forefront of advanced security systems, amalgamating a variety of cutting-edge technologies to create a comprehensive and responsive monitoring framework. This approach entails the orchestration of video analytics, object detection, activity recognition, and anomaly detection, providing a multi-layered system capable of understanding and responding to dynamic environmental conditions. Video analytics, often driven by sophisticated machine learning models like Convolutional Neural Networks (CNNs), enables precise object detection, allowing the system to identify, track, and analyze specific entities within the monitored area. Activity recognition further enriches the system's capabilities by categorizing observed actions, facilitating a nuanced interpretation of events and behaviors. Anomaly detection mechanisms enhance the system's alerting capabilities, identifying irregular patterns that may indicate potential security threats or unauthorized activities.

In real-time scenarios, the integrated system generates alerts, employing predefined criteria to notify security personnel promptly. These alerts not only include information about detected objects and recognized activities but also provide insights into identified anomalies.

Fig2. Overview of Crime Detection Activities

The integration of data fusion and correlation mechanisms ensures that information from various sources is harmoniously combined, enabling a holistic understanding of the monitored environment. Adaptive learning mechanisms embedded in the system continuously refine algorithms, adapting to evolving patterns of behavior and ensuring the system's adaptability over time. Security considerations are paramount, with the integrated surveillance analysis system ensuring secure communication channels, compliance with privacy regulations, and seamless integration with existing security infrastructure. The insights generated by this integrated analysis serve as valuable decision support for security operators, empowering them with actionable

information to make informed decisions and respond effectively to potential security incidents. In essence, integrated surveillance

analysis transcends traditional monitoring approaches, offering a sophisticated and proactive security solution that is crucial in applications ranging from public safety and law enforcement to industrial and critical infrastructure security.

The Extractor:

```
def preprocess_image(image):
    # Resize the image to (224, 224) as required by the model
    image = cv2.resize(image, (224, 224),
interpolation=cv2.INTER_AREA)
    image = np.asarray(image, dtype=np.float32).reshape(1, 224,
224, 3)
    image = (image / 127.5) - 1  # Normalize the image
    return image
```

Pseudo Code 1. Preprocessing and Extracting the frames

The multiprocessing module is employed to facilitate concurrent execution of tasks related to the extraction of frames from violent and non-violent video sources.

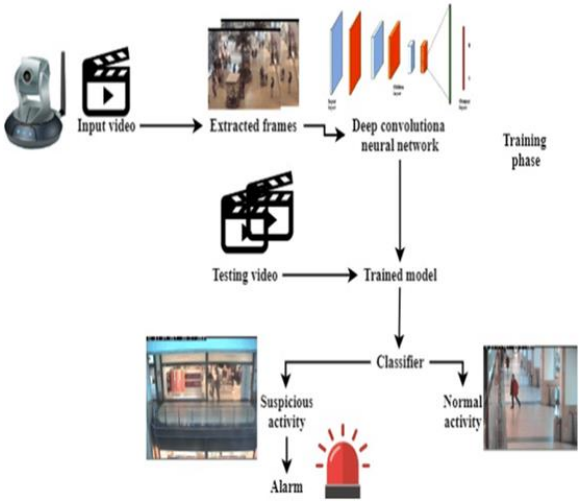

Fig3. The overview of sending alert message and identifying crime activities

Two processes, denoted as t1 and t2, are instantiated using the Process class from the multiprocessing module. Each process is assigned a specific target function, either thread_1 or thread_2, which are responsible for extracting frames from violent and non-violent video files, respectively. The start() method is then invoked on both processes, initiating their parallel execution. The subsequent use of join() ensures that the main program halts and waits for the completion of both processes, ensuring synchronization. Finally, the program prints "Complete" once both processes, corresponding to the extraction of violent and non-violent frames, have successfully concluded, indicating the overall completion of the task.

The multiprocessing:

```
def get_image_base64(plt):
    buffer = BytesIO()
    plt.savefig(buffer, format='png')
    buffer.seek(0)
    image_base64 = base64.b64encode(buffer.getvalue()).decode()
    plt.close()
    return image_base64

def send_email(fromaddr, toaddrs, subject, message):
    msg = f"From: {fromaddr}\r\nTo: {', '.join(toaddrs)}\r\nSubject:
{subject}\r\n\r\n{message}"
    server = smtplib.SMTP('localhost', 1025)  # Change this to your
SMTP server details
    server.sendmail(fromaddr, toaddrs, msg)
    server.quit()
```

Pseudo Code 2. Concurrently execute functions in separate process

D. Sending alert messages

Once suspicious activities are identified, the system generates standardized alert messages containing crucial details such as the type of behavior, timestamp, and location within the surveillance area. Visual evidence, including images or short video clips, is often included to enhance comprehension. These messages are transmitted through secure channels in real-time, facilitating prompt communication with security personnel. The alerting module acts as a decision support tool, providing valuable insights into potential security threats and contributing to the overall effectiveness of the surveillance system.

V. PERFORMANCE EVALUATION

The performance evaluation of a machine learning-based system for detecting crime activities through surveillance cameras and generating alert messages for security systems is crucial for assessing its effectiveness in real-world scenarios. This evaluation involves several key steps. Initially, a diverse dataset of surveillance footage containing various crime activities is collected and annotated. This dataset is then preprocessed to optimize model performance. Next, machine learning models such as Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs) are selected and trained on the annotated dataset.

Data Collection and Annotation: Collect a diverse dataset of surveillance camera footage containing various crime activities. Annotate the dataset with labels indicating the presence or absence of crime

activities at different timestamps.

Data Preprocessing: Preprocess the dataset to enhance model performance, which may include resizing, normalization, and augmentation.

Model Selection and Training: Choose appropriate machine learning models for video analysis, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), or their variants. Train the selected models on the annotated dataset using appropriate training techniques.

Model Evaluation: Evaluate the trained models using the defined metrics on a separate validation dataset to assess their generalization performance. Perform hyper-parameter tuning and model selection based on the validation results.

Response Time: The time taken to generate and deliver an alert message after detecting a crime activity.

False Alarm Rate: The proportion of false alerts generated compared to true crime activities.

Sensitivity: The proportion of true crime activities detected and alerted correctly.

Specificity: The proportion of non-criminal activities correctly identified as such.

VI. CONCLUSION AND FUTURE IMPROVEMENTS

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 real-time. 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.

A. Future improvements

The field of crime detection through surveillance cameras using machine learning will focus on enhancing object recognition, behavioral analysis, multimodal fusion, real-time anomaly detection, edge computing, privacy-preserving techniques, and adaptive learning.

1. Enhanced Object Recognition: Continuous advancements in machine learning algorithms can lead to more accurate and robust object recognition capabilities, enabling surveillance systems to identify a wider range of objects associated with criminal activities, such as weapons, suspicious packages, or specific behaviors indicative of criminal intent.
2. Behavioral Analysis: Integrating advanced behavioral analysis techniques into surveillance systems can enhance the detection of suspicious activities by analyzing patterns of behavior over time. This could involve developing algorithms to recognize subtle cues or anomalies in human behavior that may signal potential threats.
3. Multimodal Fusion: Leveraging multiple data modalities, such as visual, audio, and sensor data, can improve the overall effectiveness of surveillance systems. Integrating these modalities using multimodal fusion techniques can provide a more comprehensive understanding of the environment and enhance the system's ability to detect and respond to crime activities.

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, E2E-V2SResNet: 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: End-to-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).