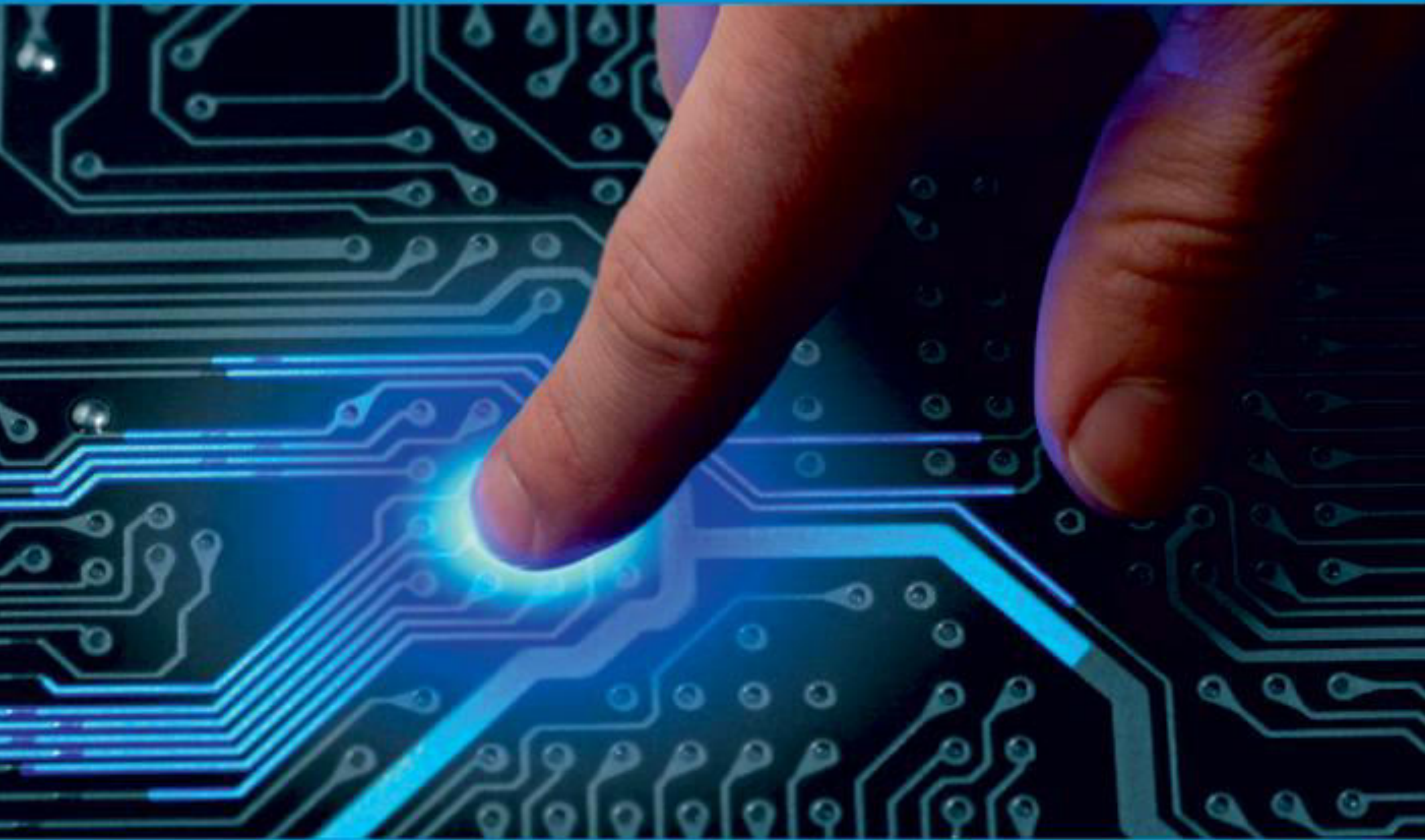
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Real-Time Crime Scene Analysis using Deep Learning to Enhance Smart City Surveillance

R.Abarna, D.Siva Senthil

Department of Computer Science and Engineering, Arunachala College of Engineering for Women, Manavilai, Vellichanthai, India

Department of Computer Science and Engineering, Arunachala College of Engineering for Women, Manavilai, Vellichanthai, India

ABSTRACT: With the rapid urbanization and growing complexity of modern cities, the need for efficient public safety mechanisms is more critical than ever. Traditional surveillance systems, dependent on human operators and passive monitoring, often fail to meet the demands of real-time threat detection and response. This work introduces a real-time crime scene analysis framework leveraging deep learning to enhance smart city surveillance systems. The framework integrates Convolutional Neural Networks (CNNs) for object detection and classification, and Recurrent Neural Networks (RNNs), specifically LSTMs, for analyzing temporal patterns to identify suspicious activities. Advanced computer vision techniques enable the system to detect and classify anomalies. By employing edge computing, the solution ensures low-latency real-time processing, while cloud architectures facilitate scalability for deployment across extensive surveillance networks. Additionally, facial recognition and object detection technologies are incorporated to support law enforcement in identifying individuals and tracking vehicles linked to criminal activities.Implemented using Python, the system achieves a classification accuracy of 99%, outperforming traditional methods.The system effectively identifies anomalies such as "Assault," "Robbery," and "Shooting" in real-time, as visualized in bounding box outputs. These results underscore the system's reliability and efficiency in real-time anomaly detection. The work demonstrates the potential of deep learning to revolutionize urban security systems by providing rapid, automated threat detection. This framework not only enhances public safety through proactive threat detection but also sets the phase for forthcoming innovations in AI-driven urban surveillance technologies.

KEYWORDS: Real-Time Crime Detection, Deep Learning Surveillance, Smart City Security, Anomaly Detection, Edge-Cloud Computing Integration.

I. INTRODUCTION

As a result of rapid urbanization, the populations are rapidly increasing and filling up the urban spaces, making them increasingly complex and congested[1]. Urban density, though rich with many benefits, has some serious problems, particularly in public safety and crimes control[2]. The more the people gathering in the urban areas, the more the crimes are rampant and diversified, and so is the growing demand for an efficient and effective surveillance system[3]. The former system of surveillance, which primarily comprises human eyes to observe this long territorial area, is overburdened with the volume and the rate at which city life occurs, a factor that would impede the proper observation of vast territories[4]. For such a reason, there is a rising demand for clever solutions for investigation, and it helps cities find ways to utilize advanced technologies so as to realize public safety in real-time[5].

Current surveillance systems fail in several areas to effectively assist authorities in managing public safety proactively[6]. Human-monitored systems have several glaring errors because of factors such as fatigue and oversight, and the time required to analyze and respond to surveillance footage often results in significant latency, delaying the response to critical situations[7]. But as far as resources are concerned, one major limitation that bars these systems from attaining total coverage in large urban areas is the trained personnel and infrastructure needed for monitoring[8]. Such deficiencies call for a high-technology automated real-time system capable of using deep learning to sense,

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

identify, and answer to potential dangers in real time[9], thus reducing dependency on human monitoring and promoting speed in response with accuracy in preventing urban crime[10][11].

Maintaining public safety in cities is becoming increasingly difficult as urbanization picks up speed[12]. Conventional surveillance systems, which mostly rely on human monitoring and static analysis of recorded material, are frequently insufficient[13]. Because deep learning makes it possible to gather and analyze video records in real time, it offers a chance to completely transform surveillance systems. This project investigates how deep learning may improve crime scene analysis, offering a more accurate and effective way to keep an eye on urban surroundings. Our goal is to make cities safer and give law enforcement the resources they need to successfully fight crime by incorporating smart technology into surveillance systems.

A. Key Contributions of the Proposed Framework

- The research proposes a robust approach for crime detection in surveillance footage by combining CNNs for spatial feature extraction and RNN networks for temporal anomaly detection. This dual approach ensures the accurate classification of crimes and the detection of unusual behaviors or movements over time, making it suitable for real-time security applications in smart cities.
- The research introduces an innovative edge-cloud computing architecture, where initial video processing is handled at the camera level. This setup enhances the system's ability to scale across urban environments while providing real-time alerts to law enforcement.
- The system integrates facial recognition technology to identify individuals of interest or known offenders, cross-referencing with a pre-existing database. This feature improves the security framework by enabling immediate identification and alerts, while also addressing privacy concerns and complying with data protection regulations such as GDPR.

B. Organization of the Paper

The paper is structured as, Section I gives an overview of the topic and work's objectives that are to be explored in this paper. Section II incorporates an extensive literature review, after which Section III would put forth the problem statement. The methodology is described in Section IV, and Section V is the results part of this paper, while Section VI would sum up the conclusion of the research.

II. RELATED WORKS

In an academic setting, Amrutha et al.[14] Employed a DL technique to recognize suspicious or normal conduct. If they anticipate suspicious action, they send an alarm message to the suitable authorities. It is common practice to monitor using successive frames that are taken from the video. The first step involves computing features from video frames, and the second step involves the classifier classifying the data as either normal or suspicious. In Bhatti et al.'s [15]work, weapons in CCTV footage were detected using deep learning models such as VGG16 and Inception-V3, focusing on the reduction of FP and FN. Besides YOLOv3 and YOLOv4, the authors used this test while the highest accuracy and precision were achieved by YOLOv4.

In the research by Shah et al.[16], machine learning together with computer vision is applied to improve crime detection and prevention. The analysis presented here summons up a faster and even accurate solution compared to the traditional ones. According to previous research work, predictive models are used so that the crimes predicted and even enhance strategies of enforcing law. Computer vision was also used for example, facial recognition and video analysis so that suspects can be identified or their suspicious activities could be tracked.

Maqsood et al.[17] applied deep learning-based techniques, mostly 3D convolutional networks (3D ConvNets), to recognize anomalous activities in surveillance videos with a focus mainly on the detection of different types of events except for just binary anomaly detection. Other works have demonstrated multiclass learning and spatial augmentation successfully improve deep learners' ability to generalize in anomaly recognition. Additionally, the authors indicate that fine-tuning a pre-trained model, 3D ConvNet amongst others, on the video dataset UCF Crime, achieved higher precision for recognizing the spatiotemporal features of anomalies.

© 2024 IJIRCCE | Volume 12, Issue 11, November 2024| DOI: 10.15680/IJIRCCE.2024.1211098

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. PROBLEM STATEMENT

Crime levels continue to grow, and populations are more crowded, therefore, complexity greater in urban areas. In such places, the traditional surveillance systems face more practical difficulty in being implemented and present outstanding challenges. Most of the conventional systems rely on static arrangements of cameras and are dependent on human participation in their day-to-day operations, meaning coverage will be limited, certain areas will be blind, and scope for many innocent errors due to drowsiness and inattention by humans[14]. Real-time processing of huge number of data hampers the crime prevention strategy, generally offering unnecessary delays and a rate of false positives. The above potential limitations will be overcome by this paper, which seeks to realize real-time crime scene analysis by leveraging deep learning-based frameworks. This framework integrated advanced computer vision techniques including convolutional and recurrent neural networks for trying to automate the detection, classification, and analysis of suspicious activities towards reducing their response times and improving public safety in smart cities.

IV. PROPOSED CNN FRAMEWORK FOR DETECTING FOGERY IMAGES

The proposed methodology for this work employs state-of-the-art deep learning techniques, CNN and RNN, for real-time crime-related incident detection and classification from raw data through surveillance feeds. A pre-processed version of the UCF Crime Dataset is used in order to prepare the data for model training. A CNN has been used in the system for the object's detection and also the classification of threats, such as weapon or anomalous activity, within a video frame. RNN, particularly LSTM networks, have been utilized in studying the temporal pattern and to identify any anomalies in behavior over time. The facial recognition technology cross-checks an existing database for increasing the identification capabilities of the system. It is an Edge-Cloud Computing framework, which is incorporated to make suitable placement of the computed processes in either edge devices on site that use real-time data processing for quick latency benefit, or in the cloud where remote computation is supported and used to adapt the model and scale up where necessary to achieve efficient and accurate crime detection across the urban environment. The methodology flow is depicted in Fig. 1.

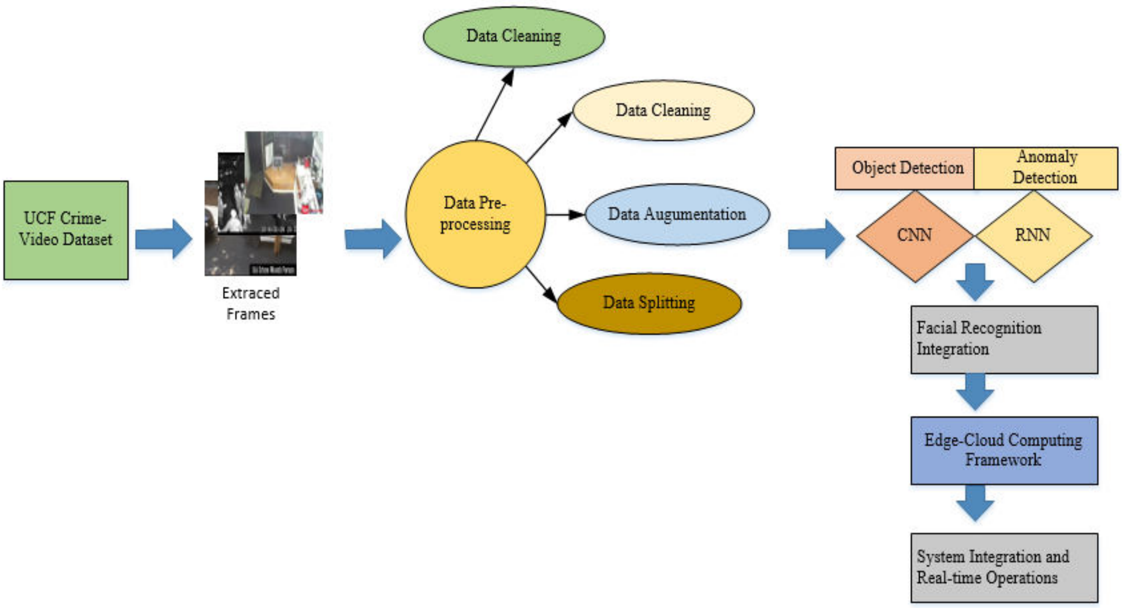


Fig. 1. Proposed Framework for Real-Time Crime Scene Analysis

A. Dataset Description

The UCF Crime Dataset is a video-based image dataset extracting images from real-world anomaly detection in surveillance footages, focusing on crime-related activities[18]. This dataset contains frames taken from every 10th frame of the videos in UCF Crime Dataset and resized each image into 64x64 pixels in the .png format. It cuts across

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

14 classes of incidents ranging from abuse, assault, robbery, shooting, vandalism, and road accidents, apart from normal, noncriminal activity. This dataset has resources for training and evaluation of deep learning models that help in the detection and classification of crimes in real-time surveillance videos, thus making it a good tool in advancing security systems in smart cities.

B. Dataset Pre-processing

The preprocessing of the UCF Crime Dataset starts with data cleaning, which should be absolutely sure that there is no missing or corrupted image and to have no duplicates. It then resized images to a standard 64x64 pixels, as the network requested an input size. In order to help neural networks train more effectively, pixel values were normalized to a range of [0,1] by dividing them by 255. To normalize the pixel values in a picture, remove the mean and divide the result by the standard deviation. For size increase in the dataset, data augmentation techniques like random rotation, flipping, cropping, and brightness/contrast adjustments are also applied so that the model can generalize better. Class labels, in this case, "Assault", "Robbery", etc., are encoded into numerical format using label encoding. The set is divided into sets for training, validation, and test, and this is done with stratified sampling, as a result, so that there is no bias toward the original class distribution; with such steps, the dataset will be structured well, thus making it easy to train models on it, optimized for better performance and generalization.

C. CNN for Object Detection and Classification

CNNs play a significant role in object detections and classifications in video surveillance. This is because CNNs automatically learn good features from large amounts of visual data through the recognition of patterns and details; hence, they are pretty efficient in identifying objects and distinguishing between incidents such as fights, burglaries, or vandalism happening within a frame of video. Due to these networks learning lots of efficient patterns, shapes, and structures in the images, they can detect objects of interest in cluttered or dynamically changing scenarios easily.

The CNN models are applied to analyze the real-time video streams and detect weapons, cars, or people. These objects are classified into the predefined categories: "person," "weapon," or "vehicle." In surveillance applications, this type of classification is crucial in recognizing potential threats - a person carrying a weapon or a suspiciously acting vehicle, to mention a few.

1. Real-Time Threat Detection with CNN

This makes CNN very effective for tasks that involve object detection and classification. For real-time threat detection, a CNN would process every frame of the video and extract features in the acknowledgment of potential threats such as weapons, abnormal movements, or unauthorized people. The architecture of a CNN, consisting of convolutional layers followed by pooling and fully connected layers, lets it recognize patterns like edges, textures, and parts of objects inside a frame. After being trained on labeled data-for example, different classes of crimes-the CNN then may classify incoming frames into specific categories, for example "assault," "burglary," or "suspicious movement."

For real-time crime scene analysis using CNNs, the key operation is the convolution operation, which is central to feature extraction in object detection tasks. The important equation for a convolutional layer in a CNN can be expressed as in Eqn. (1)

$$y_i = \sum_{j=1}^{k} x_{i+j} \cdot w_j + b \quad (1)$$

Where y_i is the output feature map, x_{i+j} is the input feature map, w_j is the filter.

This operation helps CNNs recognize features, such as edges, shapes, and textures, which are crucial for detecting objects like weapons or abnormal movements in real-time surveillance footage. The processing of a frame takes very short time over the CNN, permitting quick threats identification in the real-time surveillance. For instance, if the system would mark a weapon or a suspect who lingers or makes unusual movement, an alert signal can be produced in order to send an immediate response to this alarm; thus, CNN is very appropriate for speedy analysis in real-time, particularly where a fast action is required for public safety.

D. RNN for Anomaly Detection in Temporal Patterns

Contrary to CNNs with their strengths in the extraction of spatial features, RNNs are designed to analyze sequential data; hence they are ideal for understanding behaviors and activities over time. In the case of surveillance, RNNs appear to detect patterns of locomotion and interactions of people or objects as they cut across frames in a video. Video

© 2024 IJIRCCE | Volume 12, Issue 11, November 2024| DOI: 10.15680/IJIRCCE.2024.1211098

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

frames need to be processed in a sequence for LSTMs to remember key information from previous frames and so continue to maintain context which is why it is critical in detecting deviations in typical behavior over time. For example, the model may give an alert due to some anomalous behaviors such as a person standing at a given place for a long time or dissolving crowd rapidly. Which is likely suspicious behavior of potential criminal activity.The Eqn. (2) determines how the memory (cell state) is updated over time, allowing the network to remember or forget information from previous time steps.

$$C_t = f_t . C_{t-1} + i_t \widetilde{C_t} \tag{2}$$

WhereC_t, cells state at t,C_{t-1} is the earlier state of cell.f_t, is the output forget gate. i_t, the output of input gate.$\widetilde{C_t}$, is the candidate cells state.This equation allows the LSTM network to retain long-term dependencies, which is crucial for detecting anomalies based on sequential data (such as abnormal behavior over time in video surveillance).

Since the RNN is used in the analysis of the temporal pattern, the system can detect anomalous behaviors based on the flow of activity in the video instead of random events appearing in frames. This facility allows the system to flag anomalies that might never be accounted for by models only focused on spatial features. Monitoring these deviations early provides the system with an opportunity to alert and allow for faster response by law enforcement or security personnel, thereby improving overall public safety in real-time surveillance applications.

E. Facial Recognition Integration

The structure would include facial recognition technology to enhance its identification capabilities. The system may cross-check known offenders or individuals of interest against a pre-existing database of facial images to provide individual real-time identification. When a match is found, the system produces an alert that notifies law enforcement that an identified person is present in a restricted or sensitive area. However, ethical considerations regarding privacy are respected; it will not breach data protection laws, such as GDPR, and will respect the rights of individuals. Use cases of facial recognition are strictly limited and are specifically authorized to prevent misuse.

F. Edge-Cloud Computing Framework

Edge Computing: The first level of real-time processing on video data happens at camera sites through edge devices deployed there. Because the initial processing is local to the threat being detected and prompting for alerts without latency, edge computing narrows bandwidth usage through application of deep learning models on video streams, which happens only in these devices and not the entire data is sent to the cloud for further examination.

Cloud Infrastructure: This is important to the scalability of the system and to the ability to do really complicated operations in. It holds tremendous amounts of video, model weights, and training data. It does more complex computations such as model retraining and update for keeping the current most effective versions of the system. It also supports the aggregation of data from multiple cameras across different locations that can be analyzed uniformly.

G. System Integration and Real-time Operations

After deep learning models have been trained and deployed, the system starts running in real time to continuously monitor the entire urban environment. Implementing edge devices and cloud infrastructure translates into ease in scalability at several camera networks. There will be alerts and notifications for law enforcers in real time, which will comprise actionable insights into any detected threats. This further includes the updating of models periodically, based on new data, and retraining on detected anomalies.

V. RESULTS AND DISCUSSION

The results division assesses the performance of the implementation offered in this work with Python. This section offerings the results gained after applying the proposed deep learning model for a real-time analysis of the crime scene in the context of a smart city surveillance system. The model is evaluated based on several metrics. Performance metrics are reported using various techniques for evaluation, and the results are compared with existing systems to prove the efficiency of the model.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A. Sample Images

Fig. 2 showcases sample images from various crime classes, emphasizing the dataset's utility in real-time crime detection systems. These images represent every 10th frame from videos, covering 14 classes of events such as "Assault," "Robbery,""Stealing" and "Shooting."

Fig. 2. Sample Images- Representing Different Crime Classes.

B. Confusion Matrix

The matrix in Fig. 3indicates that the ability of the model across all categories of crime is very good, with very few misclassifications occurring and most errors being confined to adjacent classes, like for example "Assault" and "Robbery."

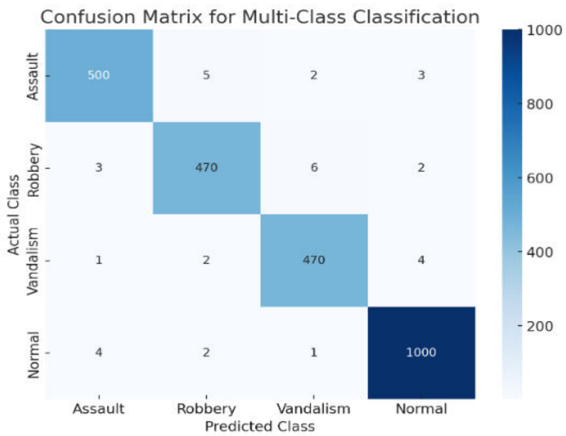


Fig. 3. Confusion Matrix

C. Anomaly Detection-Results

Fig. 4 shows the anomaly detection of the system with the manifestation in real-time surveillance footage - "Assault," "Robbery," "Stealing," and "Shooting" are correctly detected by the proposed model with bounding boxes. This shows that the model efficiently points out critical events, where timely interventions can occur.

Fig. 4. Anomaly Detection Results

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

D. Real-time Threat Detection Performance

Fig. 5 showcases real-time threat detection performance across four scenarios. It evaluates processing time, latency, and detection rate. While weapon detection has the highest processing time, all scenarios demonstrate high detection rates. Potential improvements include optimizing processing time and refining detection algorithms.

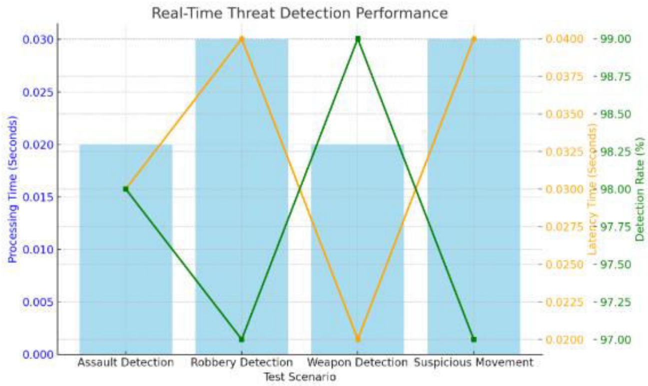


Fig. 5. Real-Time Detection Performance

E. Performance Comparison

The following Table 1 compares the performance of three classification models -DRNN, E-CNN, and the proposed framework-in terms of metrics.

TABLE 1: PERFORMANCE COMPARISON

Method	Accuracy	Precision	Recall	F1-Score
DRNN[19]	98%	96%	80%	78%
E-CNN[20]	97.05%	96.74%	96%	95.50%
Proposed Framework	99%	98.5%	98.2%	98.3%

The proposed framework outperforms both DRNN and E-CNN for all the measures by achieving the highest accuracy and attaining an F1-score of 98.3%. Although E-CNN shows very high precision at 96.74% and recall at 96%, the DRNN lags considerably behind at 80% recall and 78% F1-score, and that indicates the capability of the proposed method for overall performance enhancement.

F. Discussion

The proposed deep model results in the excellent real-time analysis of crime scene with an overall accuracy of 99%. Hence, the resultant would be the CNNs, especially when used along with anomaly detection, are very efficient in identification and classification of crime-related activities from surveillance footages. Thus, compared to the existing traditional machine learning like DRNN[19] and E-CNN[20], this proposed model allows for threat detection to thrive even more for smart city applications. Critical for the real-time performance of the system regarding urban safety is that it can recognize threats, such as perhaps weapons or abnormal movement, in milliseconds to immediately alert law enforcement. The combination of edge computing and cloud infrastructure gives the system scalability and fast response times that are very effective in the large-scale surveillance networks required for smart cities.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. CONCLUSION AND FUTURE WORKS

Deep learning-based real-time crime scene analysis system with exceptional performance at 99% accuracy level in identification and classification of crime-related activities. Because object detection employs CNN, possible threats related to weapons, suspicious movement, or abnormal behavior can be identified in real time. It will be an extremely useful tool in the process of improving smart city surveillance. Further and future research can extend the capabilities of the system from multimodal data like audio and thermal imaging, robustness under varied environmental conditions, to advanced AI techniques such as reinforcement learning to facilitate adaptive and predictive surveillance. This will further enhance the safety of urban areas and strengthen proactive crime prevention strategies.

REFERENCES

[1]Qasim et al., "Video anomaly detection system using deep convolutional and recurrent models," Results in Engineering, vol. 18, p. 101026, Jun. 2023, doi: 10.1016/j.rineng.2023.101026.

[2]Uganya et al., "Crime Scene Object Detection from Surveillance Video by using Tiny YOLO Algorithm." Accessed: Nov. 19, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10266136

[3]Muktho et al., "Design of a real-time crime monitoring system using deep learning techniques," Intelligent Systems with Applications, vol. 21, p. 200311, Mar. 2024, doi: 10.1016/j.iswa.2023.200311.

[4]A. Zappalà, L. Guarnera, V. Rinaldi, S. Livatino, and S. Battiato, "Enhancing Crime Scene Investigations through Virtual Reality and Deep Learning Techniques," Sep. 27, 2024, arXiv: arXiv:2409.18458. Accessed: Nov. 19, 2024. [Online]. Available: http://arxiv.org/abs/2409.18458

[5]K. J. Oguine, O. C. Oguine, and H. I. Bisallah, "YOLO v3: Visual and Real-Time Object Detection Model for Smart Surveillance Systems(3s)," Sep. 26, 2022, arXiv: arXiv:2209.12447. Accessed: Nov. 15, 2024. [Online]. Available: http://arxiv.org/abs/2209.12447

[6]M. Anderljung et al., "Frontier AI Regulation: Managing Emerging Risks to Public Safety," Nov. 07, 2023, arXiv: arXiv:2307.03718. Accessed: Nov. 15, 2024. [Online]. Available: http://arxiv.org/abs/2307.03718

[7]C.-S. Sung and J. Y. Park, "Design of an intelligent video surveillance system for crime prevention: applying deep learning technology," Multimed Tools Appl, vol. 80, no. 26, pp. 34297–34309, Nov. 2021, doi: 10.1007/s11042-021-10809-z.

[8]Sharma et al., "Crime Scene Analysis Using YOLOv5 Model." Accessed: Nov. 19, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10664101

[9]P. William, A. Shrivastava, N. Shunmuga Karpagam, T. A. Mohanaprakash, K. Tongkachok, and K. Kumar, "Crime Analysis Using Computer Vision Approach with Machine Learning," in Mobile Radio Communications and 5G Networks, Springer, Singapore, 2023, pp. 297–315. doi: 10.1007/978-981-19-7982-8_25.

[10]M. Boukabous and M. Azizi, "Image and video-based crime prediction using object detection and deep learning," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 3, Art. no. 3, Jun. 2023, doi: 10.11591/eei.v12i3.5157.

[11]Tiwari et al., "IoT Based Intrusion Detection System for Criminal Data Analysis in Deep Learning." Accessed: Nov. 19, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9751655

[12]D. Jalgaonkar, J. Gund, N. Patil, and M. Phadke, "Detecting Crime Scenes using ML," vol. 07, no. 05, 2020.

[13]S. Ahmed, M. T. Bhatti, M. G. Khan, B. Lövström, and M. Shahid, "Development and Optimization of Deep Learning Models for Weapon Detection in Surveillance Videos," Applied Sciences, vol. 12, no. 12, p. 5772, Jun. 2022, doi: 10.3390/app12125772.

[14]C. V. Amrutha, J. Chandrasekharan, and A. Joseph, Deep Learning Approach for Suspicious Activity Detection from Surveillance Video. 2020, p. 339. doi: 10.1109/ICIMIA48430.2020.9074920.

[15] M. T. Bhatti, M. G. Khan, M. Aslam, and M. J. Fiaz, "Weapon Detection in Real-Time CCTV Videos Using Deep Learning," IEEE Access, vol. 9, pp. 34366–34382, 2021, doi: 10.1109/ACCESS.2021.3059170.

[16]N. Shah, N. Bhagat, and M. Shah, "Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention," Vis. Comput. Ind. Biomed. Art, vol. 4, no. 1, p. 9, Apr. 2021, doi: 10.1186/s42492-021-00075-z.

[17]R. Maqsood, U. Bajwa, G. Saleem, R. H. Raza, and M. Anwar, "Anomaly Recognition from surveillance videos using 3D Convolutional Neural Networks," Jan. 04, 2021, arXiv: arXiv:2101.01073. Accessed: Nov. 15, 2024. [Online]. Available: http://arxiv.org/abs/2101.01073

[18]"UCF Crime Dataset." Accessed: Nov. 15, 2024. [Online]. Available: https://www.kaggle.com/datasets/odins0n/ucf-crime-dataset

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[19]Sahay et al., "A real time crime scene intelligent video surveillance systems in violence detection framework using deep learning techniques," Computers and Electrical Engineering, vol. 103, p. 108319, Oct. 2022, doi: 10.1016/j.compeleceng.2022.108319.

[20]Nandhini et al., "An Improved Crime Scene Detection System Based on Convolutional Neural Networks and Video Surveillance." Accessed: Nov. 15, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10179852