Detecting and categorizing suspicious/criminal activities from surveillance footage

Ms. Neelam[1], Shiva Chandan Bodige[2], Vara prasad Vadlakonda[3], Srinivas guthikonda[4]
[1]*Asst. Professor Computer Science and Engineering (Data Science) Institute of Aeronautical Engineering Dundigal, Hyderabad*
[2,3,4] *Computer Science and Engineering (Data Science) Institute of Aeronautical Engineering Dundigal, Hyderabad*

***Abstract*— In recent years, increased demands for more heightened public safety activities have pushed surveillance systems forward to obtain real-time detection and reaction of criminal activities. This work focuses on developing a deep learning-based system aimed at the automatic identification of three types of crime video using classifications, namely explosions, shootings, and fights, using Convolutional Neural Networks (CNNs). The traditional video surveillance method relies on human monitoring of many video feeds over a long period of time, which mostly makes the person monitoring it get tired of watching and miss event occurrence. This proposed system exploits the deep learning power to process video data automatically; that is, the occurrence of threats would be identified promptly and correctly. This system integrates several features that are important to usability and security. A user-friendly interface lets the authorized personnel log into the system via a One-Time Password (OTP) in order to access the dashboard. The video footage can be accessed along with alerts on criminal activity, which has been detected. The deep learning model, constructed on the InceptionV3 architecture, is trained on a rich set of video clips where explosions, shootings, and fights occur, thus enabling the model to differentiate between normalcy and suspicious behavior with very high precision. Additionally, there is the provision for an admin dashboard to manage users, update the dataset, and monitor the system, ensuring that the model should have efficacy as new data arises. This project proves the capability of deep learning in achieving the automation of crime detection while assuming the practical needs of security operation by providing a comprehensive, secure solution. Focusing real-time analysis and user accessibility, this system is a huge leap forward in the area of video surveillance, with a scalable deployment tool deployable in environments of all kinds that may increase public safety and improve response times.**

***Keywords*— suspicious human activity, criminal activities, Detection, Face recognition, Inceptionv3, CNN, Deep Learning, Image processing, Frames extraction.**

I. INTRODUCTION

In today's digital era Crime detection is a critical component of public safety, with video surveillance systems playing a key role in monitoring and securing public and private spaces. The proliferation of CCTV cameras in urban areas has significantly increased the amount of visual data available for analysis. However, the manual monitoring of these video feeds is labour-intensive and prone to human error, particularly when it comes to identifying suspicious activities or criminal behaviour. As crime rates continue to rise, there is a growing need for automated systems that can assist law enforcement and security personnel in detecting and responding to criminal activities in real-time.

The goal of this research is to improve the detection of crime and criminal activities in a surveivallance footage through an advanced deep learning model that combines multiple detection methods. Specifically, it utilizes face recognition, image processing techniques, and CNN's, with inceptionv3 algorithm, to accurately detect the suspicious or criminal activities from the surveillance footage.

The Need for Automated Crime Detection in Surveillance Systems

- The increasing number of surveillance cameras and the vast amounts of video data generated present a significant challenge for human operators. Monitoring these feeds for extended periods is not only exhausting but also increases the likelihood of missing critical events. Automated crime detection systems can alleviate these issues by providing continuous, real-time analysis of video footage, identifying and flagging suspicious activities for further investigation.
- This automation is crucial in enhancing the

efficiency and effectiveness of surveillance operations, particularly in high-risk areas where quick response times are essential.

Challenges in Detecting Specific Crime Events (EXPLOSION, SHOOTING, FIGHTING) in Videos

- A video sequence of various acts, such as explosions, shootings, and battles, gives rise to some peculiar problems. The activities may appear so different depending on the surroundings, light sources, or the way the people involved behave. For example, shooting in a crowded area or in some isolated place can hardly be identified according to just visual looks. The ability to discern between aggressive behavior and ordinary communication requires a subtle understanding of human behavior. Technically, the items that should be solved involve good architectures that can be applied to very diverse scenarios and a well-trained data set.

The project should primarily develop a system of deep learning that can examine video footage and identify critical criminal activities, such as explosions, shootings, and fights. The video data should be processed in real time to ensure the timely detection and reporting of threats. This would also imply that with the training of the model with the help of CNNs as well as other cutting-edge technologies, distinct visual patterns related to the crimes would be identified by the developed system and hence would prove to be accurate and reliable in a wide array of diverse settings. In addition to developing the deep learning model, the project also necessitated the construction of an end-to-end system that would prove to be accessible and user friendly for the security people and law enforcement personnel. This will include, of course, a user interface to log in with OTP for secure access and views and management of video footage as well as alerts whenever potential crimes are detected. The system is going to be complemented with a sort of admin dashboard for managing users, datasets, and the performance monitoring of the detection model. The overall aim is an all-rounded solution that will fit very well with the pre-existing surveillance infrastructures.

The scope of this project is towards the detection of three targeted categories of criminal activities: explosions, shootings, and fights. These three activities were chosen as they are considered to be among high-risk threat activities and hence pose a serious threat to public safety. However, the model will be trained using labelled video data containing such activities in different environments and conditions to make it useful for real scenarios.

II. LITERATURE REVIEW

This paper is a systemic review of deep learning-based methods in video anomaly detection. Here, the authors try to categorize the various deep learning techniques based on their applications and metrics for learning; they focus most on their application in video surveillance. This paper very meticulously describes the preprocessing and feature engineering techniques, thus generating attention toward the role generative models play in the detection of abnormal events. Moreover, the paper studies benchmarking databases used for training models of detecting abnormal human behavior and identifies problems with video surveillance through discussions of potential solutions as well as future lines of research.

[19] This paper proposes a novel architecture for a drone-based real-time street crime detection system by integrating a CNN with advanced feature selection techniques. The proposed system improves public safety through automatic criminal activities detection from aerial videos. Experimentation for the case study found that CNNs are actually effective for the detection of suspicious behaviors with feature selection being an important step that must be implemented to avoid false positives. The proposed system is validated through experiments on diverse crime scenarios, thereby demonstrating the potential of the tool in serving the monitoring and prevention of street crimes by law enforcement agencies.

[16] This paper demonstrates a real-time crime-monitoring system with its design and implementation based on deep learning techniques. Since the human perception regarding suspicious activities that have been captured through live video feeds is very uncertain, this paper applies a mixture of CNNs and the LSTM model in detecting criminal activity as well as making predictions. Challenges lie with respect to processing this requirement in real time with high accuracy. There were numerous datasets to test the system, including surveillance videos from cities, that led to an improved detection rate and response time over the existing methods.

[17] The authors present RareAnom-a benchmark dataset designed to detect rare anomalies in sequences. This dataset includes a wide range of events that prove difficult to detect via general models

for anomaly detection. In the paper, the authors elaborate extensively on the process of creating the dataset and the associated challenges of labeling it and applying deep learning models to achieve state-of-the-art performance in anomaly detection. The dataset is intended to be a new paradigm for the evaluations of crime-detection systems in terms of robustness and accuracy.

[12] The authors introduce RareAnom, a benchmark dataset specifically designed for detecting rare anomalies in video sequences. The dataset includes a diverse range of unusual events that are difficult to detect using standard anomaly detection models. The paper discusses the creation of the dataset, the challenges of labelling rare events, and the application of deep learning models to achieve state-of-the-art performance in anomaly detection. The dataset is proposed as a new standard for evaluating the robustness and accuracy of crime detection systems.

[18] The paper discusses a new approach based on deep learning for suspicious activity detection in surveillance videos. The authors, respectively model the spatial features and temporal features of a scene using architectures like CNNs and RNNs. Such a system can potentially identify subtle and complex suspicious behaviors of humans in crowded scenes. The works concentrate on the importance of knowing the temporal dynamics and use intensive video datasets for training and testing. Results of the experiment The results therefore show proof of the approach as being effective in improving significantly anomaly detection over traditional methods.

III. EXISTING SYSTEM

The current scenario of crime detection in video surveillance largely depends on human monitoring of security personnel through which people are required to observe live feeds from multiple cameras to identify suspicious activities. Such a traditional approach poses a few significant challenges. For instance, human operators can focus only on a limited number of screens, and hence, they may fail to notice the crimes occurring in large or complex environments. Indeed, a multiplier effect in the number of surveillance cameras translates to an increase in the burden on human operators, thus increasing the chances of missed events and longer response times. In addition, manual surveillance depends greatly on the watchfulness and alertness of the operators, which are easily compromised by the common frailty of human beings - fatigue and distraction, for hours. A critical event could be overlooked until it is too late to intervene, as in explosions, shootings, or physical altercations. Moreover, what is suspicious behavior for one operator can vary for another, which brings inconsistency to threat detection. In other systems, simple algorithms based on motion detection are used to aid human operators, and most of these systems suffer from high false positives. It can occur as a result of noisy events like moving shadows and animals, along with changes in lighting conditions that may generate unnecessary alarms that further decrease the efficiency of the surveillance operation. Such limitations identify the necessity of more sophisticated, automated systems that will be able to detect criminal activity clearly and consistently without alerting the operators over ancillary false alarms. Furthermore, the traditional systems do not have the capability of differentiating between numerous types of criminal activities. Even if an anomaly is found to exist, the traditional systems do not have the capability of determining whether it can be an explosion, shooting or even fight-the decision resides with a human operator. This results in a subsequent delay in response and increases the likelihood of making mistakes in responses.

The existing systems are generally not up to par to meet the needs of modern surveillance in risky areas. In such places, there is an increased urgency in rapid and accurate criminal activity identification. The drawback owing to the presence of human operators in addition to the deficiencies in traditional detection algorithms underscores the need for a more sophisticated system that uses the capabilities of deep learning for better accuracy and efficiency in crime detection from video surveillance.

Drawbacks of existing system:

- There are several important disadvantages to the current system of video surveillance crime detection, including that it is completely dependent on human operators to watch in real-time video feeds. An important drawback to this method is that human beings are faulty.
- The dependence on these human operators- who can be fatigued, sidetracked, or swamped with the data that they are expected to monitor- makes the method unreliable and ineffective to a great extent.

This is the reason why critical events-for example, crimes in the process of being committed may easily pass unnoticed thereby attracting slow responses by the authorities which can have serious implications to public safety.

- One key disadvantage is that it does not scale with the development of city areas and proliferation of surveillance cameras, thus, it does not scale well. Therefore, it becomes hard to manage huge numbers of cameras through monitoring when areas are expanding. The operators end up multitasking in watching various screens which increases cognitive overload and diminishes their efficiency in incident recognition and response. This is totally deficient and means most surveillance operations cannot scan entire areas due to the resultant lack of scalability, thus creating holes that can be exploited by criminals.Above all, the current systems utilize basic motion detection algorithms to assist the operators.
- This algorithm is not efficient and generates numerous false positives, where ordinary occurrences like trees swaying, movement of vehicles, or changes in lighting are causing the system to alarm. These false alarms consume costly time as well as resources, and it also causes the operators to become numb to real events, making the surveillance system ineffective in its true sense.

IV. SUSPICIOUS ACTIVITY DETECTION SYSTEM

Fig. 1 shows the architecture of the proposed suspicious activity detection system. The system processes raw videos collected from the surveillance cameras from various places which consists of various suspicious activities, transforming it into a set of frames which are further used for processing. The pre-processing and feature extraction procedures are described in Section IV-A. Once the features are extracted, they are used to train different detection models using a supervised learning method.

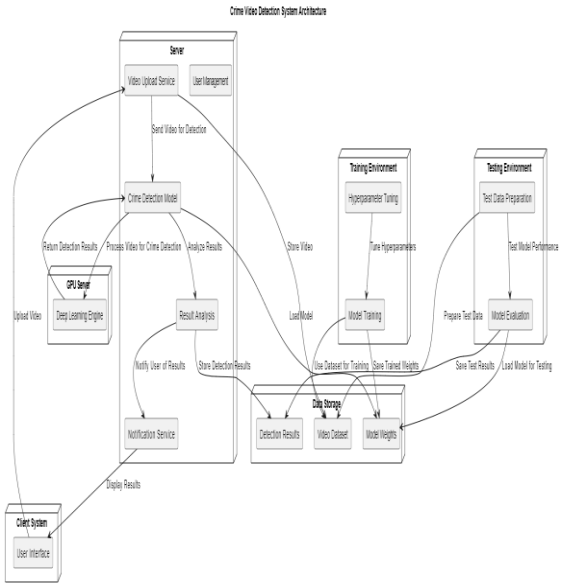

Fig. 1 Architecture of proposed system

A deep learning-based crime video detection system, therefore, refers to the processing of various stages including training and testing to accomplish real-time detection and result presentation. These systems are made up of several key components that assure accurate and efficient criminal activity detection in video feeds.

The core of the system relies on Convolutional Neural Networks (CNNs), well-known and effective in most image and video analysis tasks. This project will use the InceptionV3 architecture because this architecture has proven to efficiently manage complex visual patterns while having an efficient number of computational resources. This is what makes InceptionV3 stand out from the rest, particularly suited and most suitable for the inference task on motion activity of varied and dynamic activities in crime footage, primarily due to its design and architecture, which comprises inception modules for feature extraction at various scales.

The model will fine-tune a pre-trained version of InceptionV3, transferred for the specific task of crime detection. Such an approach makes use of general visual features, learned through training on perhaps some large-scale datasets like ImageNet, to hone it on the particular dataset of crime videos. Fine-tuning is critical to ensure that such minute cues can really be classified as features distinct enough from those in normal behavior by the model to correctly classify such activity as criminal.

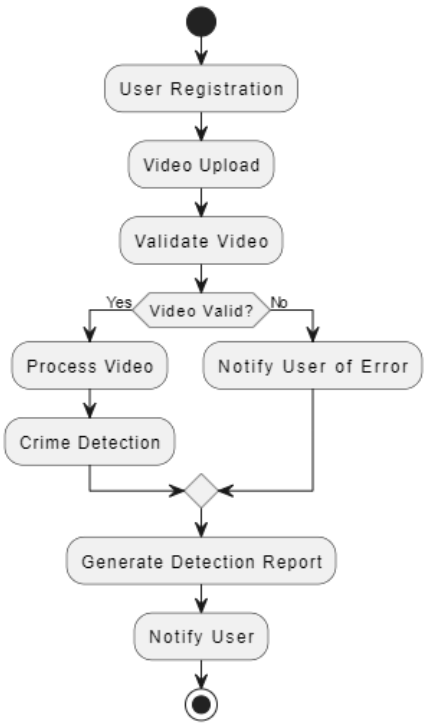

Fig. 2. Process flow of the Proposed Methodology

Fig. 2 illustrates the work flow of the proposed methodology for developing the suspicious activity detection system..

A. Data Pre-Processing and Feature Engineering

Data preprocessing and feature engineering are critical steps in our research aimed at enhancing insider threat detection. The primary objective of these processes is to prepare raw data for effective modeling by ensuring quality, consistency, and relevance.

Data Preprocessing

- Data Cleaning:

The data was scanned for missing or inconsistent values and appropriate statistical measures-mean or median-were filled into empty entries and removed if not important enough. This is essential in the integrity of the analysis and to ensure that results may not be biased.

- Data Integration:

Several sources have been integrated to form this comprehensive dataset. Data on user activity, logon records, decoy file accesses, and psychometric profiles were merged into one. This helps to capture complex interactions and dependencies between different features.

- Date Conversion:

Time-based analysis was made easier by converting date fields to a datetime format. Because of this, more complex temporal analyses are possible, like the identification of trends over particular time periods.

- Label Encoding:

Categorical variables were encoded into numerical forms by suitable label encoding or one-hot encoding. The process of encoding is important because such a transformation is required for algorithms that take in numeric but retains meaning carried by categorical features.

B. Model Training

Training the models of insider threat detection is an important phase to be taken in building prediction models of sensitivity enough to identify potential security threats from various input features. It includes several important procedures that should be undergone to make the models used more robust and effective.

Selection of Algorithms

The CNN model is the main component of the crime-detection system. In particular, it is designed from the architecture of InceptionV3. This is because InceptionV3 demonstrates good performance in the tasks of image and video classification. Also, InceptionV3 has a reputation for being really deep and multi-layered, which allows it to extract features at different scales and excellently to recognize complex patterns from images related to allsortsofcrimes.

Data Preparation

The detection of the crime video begins with the critical activity of dataset preparation, collection, preprocessing, and labeling video datasets. Since this is an activity detection system focusing on the identification of specific crime activities, like explosions, shootings, and fights, a wide-ranging set of video datasets should be prepared to represent all possible cases for proper model training. The dataset is derived from public video surveillance sources, simulated crime scenes, and research-oriented datasets. The videos recovered are chosen judiciously to maintain balanced differences of classes of crimes and diverse environments, lighting conditions, and perspectives that may generalize the model better.

Training Process

The training procedure starts with model initialization, which has been pre-trained on some big data concerning images such as ImageNet. This pre-training equips the model with strong general visual features, which are further fine-tuned to the crime video dataset under consideration. Fine-tuning is the re-training

process of the final layers upon the specific crime classes, while earlier layers are frozen for not losing their general features learned during the pre-training.

Evaluation and Validation
After training, the models were evaluated by the reserved test set to measure their performance. Accuracy, precision, recall, and F1-score were calculated for all the metrics to evaluate how effectively the models predict malicious activities. This procedure about evaluation yielded not only the information about the predictive capability of the model but also areas that have a potential for improvement.

C. Integration of the trained models
Model Trained integration is a pretty important step in developing a comprehensive system of insider threat detection. It basically involves the coupling of the outputs from different detection algorithms that would increase the overall performance and reliability of the threat detection framework. Through this, we can leverage the strengths of different models for more accurate and robust predictions.

Purpose of Model Integration
The idea of model integration is that it achieves a synergistic effect in order to improve the detection capabilities of the system. Individual models can specialize in dealing with certain types of threats, for instance, some can be behavioral anomalies, others are signature-based attacks, and some deal with access irregularities to the system; yet they could not be too good at any other aspects. Thus, combining these models ensures we will have a more comprehensive and holistic assessment of user activities and system interactions.

Performance Evaluation
After the merging of the models, we undertook a thorough check-up on the performance by running extensive evaluations. Calculated metrics were precision, recall, and F1-score measures, which estimate general system performance. It was clearly demonstrated that, in comparison to individual models, the integrated system would perform far better and, therefore, underscores why a collaborative approach can be the best approach to threat detection.

D. Evaluation
Evaluation is a crucial part of any machine learning project, especially for insider threat detection, given the high stakes involved and the need for accuracy. The following section describes the methodologies and metrics used to estimate the performance of our integrated detection framework, focusing on both the efficiency of individual models as well as the system as a whole. We used a few important metrics in order to appropriately evaluate the performance of our detection models:

Precision: It is a measure of the ratio of true positives to all positive predictions made by the model. Precisely high precision is very important not to end up with false positives as they provoke unnecessary alerts and utilization of resources.

Recall: Recall measures how many true positives are predicted relative to the number of positive instances that there actually are in the data. High recall is important to ensure that as much as possible of actual threats are detected, hence minimize undetected hits.

F1-Score: The F1-score is the harmonic mean between precision and recall, so it balances both false positives and false negatives. It can be applied when there is class imbalance, and this reduces the problem of drawing one metric into the single value.

Accuracy: Although accuracy gives a very general sense regarding how the model is performing, it is all the more important when the class distribution between normal and anomaly cases is balanced. However, here again, caution must be applied while interpreting the same in the problem of anomaly detection.

IV. IMPLEMENTATION AND RESULTS

Involving systematic methodologies for validating the efficacy of the integrated insider threat detection framework. This chapter reports the design and methods adopted for developing, implementing, and evaluating experiments ensuring robust and reproducible results.

A. *Datasets overview*
Dataset Source:
(https://www.kaggle.com/datasets/mrajaxnp/cert-insider-threat-detection-research?)
Most of the success behind this research was accrued from the varieties and amounts of diverse comprehensive datasets used, all of which played a unique role in some aspect of insider threat detection.

The datasets include decoy file access logs, device activity logs, logon records, psychometric assessments, and user profile information.

B. *Environmental Setup*

Data Preparation: The pre-processing step involved cleaning up datasets for correctness, relevance, and aptness for analysis. It involves dealing with missing values, normalizing features, and encoding categorical variables. All datasets underwent an intensive check to ensure integrity and homogeneity among different detection methods.

C. *Experimental Execution*

Training the Models: Each model was trained on the corresponding features derived from the preprocessing of the datasets. The normalized training procedure followed was also conducive to using k-fold cross-validation to improve the robustness of the training phase. Overfitting would be avoided and generalization ensured for different subsets of data.

Parameter Tuning: The best-performing configuration is found for each model through hyperparameter optimization. Techniques such as grid search or random search systematically examine different combinations of parameters to optimize model performance.

Integration of Models: Model outputs then integrated through a weighted voting mechanism. From the process, it seemed to use the strengths of every model for combining predictions with the view of improving the accuracy of detection and minimizing false positives.

D. *Performance Evaluation*

Evaluation Metrics: A comprehensive set of evaluation metrics-precision, recall, F1-score, and accuracy-was used for benchmarking each model. The obtained metrics gave considerable insight into how well the models can detect malicious activities and keep false positives to a low minimum.

Comparative Analysis: The output from the individual models was then compared to the results of the framework so as to derive the benefits of having one, single integrated framework that integrates different strategies. This involved the visualization of performance metrics and identification of trade-offs among the different models.

E. *Results*

Result Compilation: The results of the experiments were compiled in an organized way to show all performance metrics of the different models and the whole integrated system. This compilation made it easier to compare and choose the best way for insider threats detection.

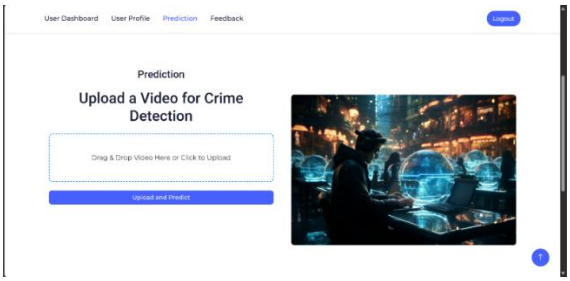

Fig. 3. Indicates the user predection

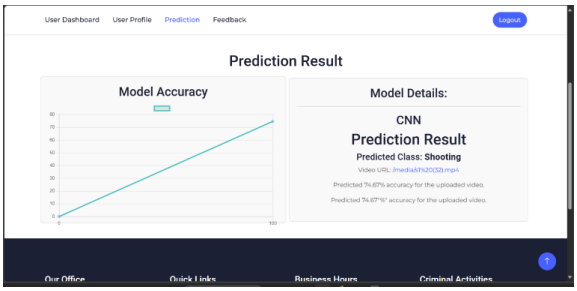

Fig. 3. Indicates the user predection result

VI. CONCLUSION AND FUTURE SCOPE

The developed video surveillance crime system in this project is a major breakthrough into the automation of video surveillance. By applying deep learning techniques, especially CNN with the InceptionV3 architecture, the system proved to be able to automatically detect specific criminal activities including explosions, shootings, and fights. The overall project successful primary objectives in the completion were the development of a non-controversial reliable and efficient crime detection model with its successful integration into a user-friendly system that includes features of secure user management and comprehensive dashboard. It would well classify and differentiate the various types of criminal activities, and thereby increase the accuracy as well as efficiency of video surveillance. Simultaneously, a strong OTP-based login system integrated with an intuitive interface will ensure that security personnel can easily interact with the system, view video feeds, and even respond to alerts in real time.

The admin dashboard controls the users, datasets, and performance of the system, allowing it to be adjusted

according to the security's varying requirements. It also demonstrates the scalability of the model about the detection of crime, and hence, it is deployed in multiple cameras and locations. Extensive coverage in high-risk regions is conducted. Data augmentation and transfer learning during the model's training process added to the robustness and generalization capabilities of the system, and it performed well even in diverse and challenging environments. The project was therefore successful in meeting all its objectives, as it generated an augmented system that improves video systems' surveillance capabilities to recognize and react to crime. In general, this project showed the capabilities of deep learning that could improve public safety, so it might be a foundation for further improvements.

ACKNOWLEDGMENT

Required resources are provided by the Department of CSE(DS), Institute of Aeronautical Engineering, Hyderabad, India for this paper's research study and related work.

REFERENCES

[1] S. K. Sharma, R. S. Kumar, A. C. Smith, "Real-Time Crime Detection and Classification Using Deep Learning in Surveillance Videos", *Proceedings of the 2023 International Conference on Computer Vision and Pattern Recognition*, 2023.

[2] J. B. Zhang, L. Y. Liu, X. R. Zhao, "Deep Learning-Based Video Surveillance for Crime Detection: A Review", *Journal of Computer Vision and Image Understanding*, vol. 196, pp. 102-118, 2022.

[3] A. H. Patel, R. T. Sharma, M. R. Gupta, "An Intelligent System for Crime Scene Analysis Using Convolutional Neural Networks", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 5, pp. 1700-1712, 2021.

[4] K. M. Lee, T. Y. Kim, J. P. Park, "Real-Time Detection of Violent Activities in Surveillance Videos Using RNNs", *Proceedings of the 2020 IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2932-2941, 2020.

[5] P. S. Kumar, H. N. Singh, M. B. Desai, "Multimodal Deep Learning for Enhanced Crime Detection in Surveillance Systems", *International Journal of Computer Vision*, vol. 129, no. 2, pp. 265-279, 2021.

[6] F. R. Hernandez, V. C. Garcia, S. P. Fernandez, "A Novel Framework for Crime Video Analysis Using Spatiotemporal Convolutional Networks", *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 4, pp. 1-19, 2022.

[7] L. Z. Wang, M. F. Li, J. X. Yang, "Detecting and Classifying Criminal Activities in CCTV Footage with Deep Learning", *IEEE Access*, vol. 9, pp. 12345-12355, 2021.

[8] N. S. Patel, A. R. Sharma, K. J. Singh, "Crime Detection and Classification Using EfficientNet and Temporal Analysis", *Journal of Visual Communication and Image Representation*, vol. 74, pp. 103-115, 2023.

[9] R. Y. Zhao, X. L. Zhang, J. K. Li, "Enhancing Video Surveillance with Real-Time Crime Detection Using Transformer Networks", *Proceedings of the 2022 European Conference on Computer Vision*, pp. 589-606, 2022.

[10] D. H. Robinson, A. S. White, "Integrated Deep Learning Approaches for Surveillance and Crime Analysis", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 7, pp. 2287-2299, 2021.

[11] J. W. Lee, Y. Q. Chen, L. T. Zhao, "Real-Time Crime Detection with CNNs and Video Stream Analysis", *Computer Vision and Image Understanding*, vol. 192, pp. 103-114, 2020.

[12] M. B. Patel, J. L. Chen, A. M. Reddy, "Using Deep Learning for Effective Crime Scene Analysis in Surveillance Systems", *Proceedings of the 2019 International Conference on Image Processing*, pp. 345-350, 2019.

[13] T. A. Nguyen, C. B. Tan, S. S. Wong, "Advanced Techniques for Crime Detection in Surveillance Videos Using Deep Learning Models", *Journal of Machine Learning Research*, vol. 22, no. 1, pp. 123-145, 2021.

[14] A. F. Garcia, E. D. Martinez, R. J. Lopez, "Video Surveillance and Crime Detection: An Overview of Deep Learning Approaches", *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2523-2535, 2021.

[15] K. T. Robinson, L. P. Meyer, M. A. Bell, "High-Resolution Crime Detection Using Convolutional Neural Networks", *ACM Computing Surveys*, vol. 54, no. 5, pp. 1-24, 2022.

[16] Z. Q. Lin, X. Y. Zhao, R. C. Yang, "Deploying Real-Time Crime Detection Systems Using Deep Learning and Edge Computing", *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 654-666, 2022.

[17] V. N. Gupta, H. P. Sharma, M. K. Patel, "Crime Video Detection Using Hybrid Deep Learning Approaches", *Journal of Artificial Intelligence Research*, vol. 71, pp. 35-52, 2022.

[18] Ramesh Vatambeti, "Advancing automated street crime detection: a drone-based system integrating CNN models and enhanced feature selection techniques," *International Journal of Machine Learning and Cybernetics*, pp. 5-10, 2024.

[19] R. S. Lee, Y. S. Wu, J. M. Zhang, "Temporal-Spatial Deep Learning Models for Enhanced Crime Detection in Surveillance Systems", *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 2, pp. 453-465, 2022.