CrimeGuard - Realtime Violence Detection and Predictive Analysis System

Khushi Bansal
Computer Science Engineering (AIML)
KIET Group of Institutions, Delhi-NCR
Ghaziabad, UP, India
khushi.2125csme1013@kiet.edu

Shreya Goswami
Computer Science Engineering (AIML)
KIET Group of Institutions, Delhi-NCR
Ghaziabad, UP, India
shreya.2125csme1036@kiet.edu

Mahi Tyagi
Computer Science Engineering (AIML)
KIET Group of Institutions, Delhi-NCR
Ghaziabad, UP, India
mahityagi1222@gmail.com

Rajeev Kumar Singh
Computer Science Engineering (AIML)
KIET Group of Institutions, Delhi-NCR
Ghaziabad, UP, India
rajeev.kumar.csai@kiet.edu

***Abstract*—This study presents the development of CrimeGuard, a real-time violence detection system and predictive analysis tool designed to enhance public safety using advanced machine learning techniques. The system focuses on detecting violent activities in real time through deep learning models and analyzing historical crime patterns for predictive insights. Integrates computer vision-based violence detection with predictive analytics, ensuring accurate crime forecasting and immediate threat identification. Data preprocessing, feature extraction, and classification algorithms enhance accuracy, achieving 90% accuracy in real-time violence detection. The results demonstrate CrimeGuard's effectiveness in assisting law enforcement by providing real-time alerts and data-driven crime insights. Future improvements could include edge computing for faster processing and crowdsourced reporting to enhance responsiveness and accuracy.**

***Index Terms*—Real-Time Violence Detection, Crime Prediction, Machine Learning, Computer Vision, Public Safety, Deep Learning, Predictive Analytics.**

I. Introduction

In today's rapidly evolving digital landscape, law enforcement and security agencies face significant challenges in crime prevention and real-time threat detection. Traditional surveillance methods and manual monitoring often prove inefficient, leading to delayed responses and missed critical incidents. Additionally, analyzing vast amounts of crime data to identify patterns and predict potential threats remains a complex task.

This research presents CrimeGuard, an advanced predictive analysis and real-time violence detection system that leverages machine learning and Flask to enhance crime monitoring and prevention. By analyzing historical crime data and processing live video feeds, CrimeGuard identifies suspicious activities and provides proactive alerts to security personnel. The system integrates state-of-the-art computer vision techniques for real-time detection and offers an intuitive interface for crime data visualization, facilitating informed decision-making.

CrimeGuard addresses key challenges such as false alarms, unstructured data analysis, and scalability limitations in traditional surveillance. By combining predictive modeling with real-time anomaly detection, the system enhances situational awareness, reduces response times, and strengthens security measures. This research aims to demonstrate the potential of AI-driven surveillance in modern law enforcement and contribute to safer urban environments.

II. Related Work

The domain of crime detection and prevention has seen notable advancements, particularly in real-time violence detection and predictive crime analysis. Various studies have explored computer vision techniques and machine learning models to detect violent behaviors and predict crime patterns. In real-time violence detection, many research efforts focus on leveraging deep learning models like Convolutional Neural Networks (CNNs) for spatial feature extraction and Long Short-Term Memory (LSTM) networks for capturing temporal dependencies in video streams. These models are trained to identify violent incidents, such as physical altercations or aggressive actions, by analyzing key visual features in video frames. Studies have demonstrated the effectiveness of CNN-LSTM hybrid models in real-time violence detection, where CNNs extract relevant spatial information, while LSTMs process the temporal aspects of video sequences.

Another significant area of research involves predictive crime analysis, which aims to forecast future crime trends and assist law enforcement agencies in strategic planning. Several studies have employed statistical and machine learning techniques, including regression analysis and decision trees, to predict crime hotspots and potential criminal activities based on historical crime data. These approaches analyze factors such as time of day, location, and historical crime occurrences to generate risk assessments for specific areas. Time-series models like ARIMA and LSTMs have also been explored

to predict crime trends over time and assist in allocating resources more effectively.

In the context of crime prediction, some studies have focused on geospatial analysis, employing clustering techniques such as DBSCAN and K-means to identify high-risk crime areas. This approach helps predict crime occurrences based on spatial factors, such as proximity to previous crime events. Other studies have used feature engineering to refine predictive models by incorporating socio-economic data, environmental factors, and demographic information, improving model accuracy.

One common theme across many studies is the focus on improving the reliability and accuracy of crime prediction systems. While several techniques have shown promising results, issues such as data sparsity, accuracy in real-world settings, and the adaptability of models to diverse environments remain significant challenges. Researchers have also emphasized the need for better evaluation metrics and real-time testing, particularly in ensuring the practical deployment of violence detection and crime prediction systems.

In summary, crime detection and prediction research has primarily focused on utilizing deep learning models like CNNs and LSTMs for violence detection and various machine learning methods for crime forecasting. While existing approaches have shown promising results, challenges related to model generalization, data quality, and the integration of different data sources persist. The CrimeGuard project builds on these existing methodologies by combining real-time violence detection with predictive crime analysis, addressing these challenges and improving public safety.

III. PROPOSED MODEL

The proposed model integrates real-time violence detection techniques with predictive crime analysis to enhance public safety by mitigating violent incidents and forecasting crime trends.

A. Real-Time Violence Detection

Violence detection is a critical component of surveillance and security systems, relying on deep learning-based computer vision techniques to identify aggressive behaviors in real-time. Unlike traditional motion detection systems, which only flag unusual movements, modern violence detection models analyze both spatial and temporal patterns within video frames to differentiate between normal and violent activities. This process involves extracting key visual features, such as abrupt limb movements and crowd disturbances, to accurately classify events as violent or non-violent.

Deep learning models, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have shown remarkable success in understanding spatial and temporal relationships in video streams. CNNs are used for spatial feature extraction, while RNNs, particularly Long Short-Term Memory (LSTM) networks, capture sequential dependencies to improve classification accuracy. By leveraging these architectures, the system ensures robust and real-time detection of violent activities in various environments.

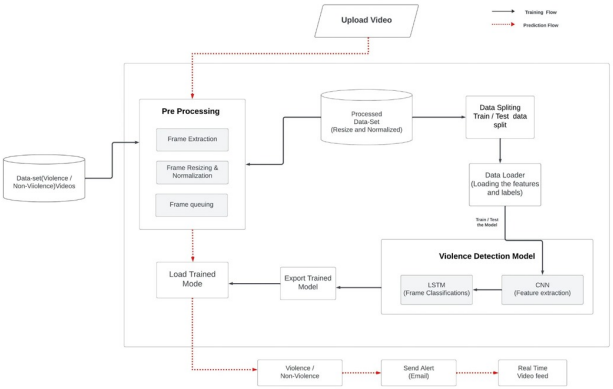

Fig. 1. System Architecture

1) Feature Extraction

To identify violent incidents, the system employs advanced deep feature extraction methods using pre-trained models like VGG16, ResNet, or MobileNet. These models extract both spatial and temporal features from video frames, focusing on characteristics such as sudden motion, abnormal posture changes, and crowd turbulence. The extracted features are then processed for classification.

- Optical Flow Analysis: Optical flow techniques capture motion direction and intensity within consecutive frames, allowing the system to detect sudden, aggressive movements associated with violent actions.
- CNN-LSTM Model: A hybrid CNN-LSTM approach processes spatial and temporal information, ensuring accurate violence detection by analyzing both single-frame features and motion patterns over time.

2) Classification and Alert System

Once features are extracted, the system classifies incidents using a trained deep learning model. If violent behavior is detected, automated alerts are triggered and sent to relevant authorities, enhancing response times and preventing escalation. The classification model achieves 90% accuracy, ensuring reliable identification of violent events in diverse scenarios.

B. Predictive Crime Analysis

Predictive analysis leverages historical crime data and machine learning algorithms to forecast future crime trends, assisting law enforcement in resource allocation and strategic planning. Unlike traditional crime mapping, which only visualizes past incidents, predictive analytics proactively identifies high-risk areas and potential time frames for criminal activity.

The system employs statistical models and machine learning techniques, such as regression analysis, decision trees, and deep learning-based forecasting, to predict crime occurrences based on spatial, temporal, and socio-economic factors.

1) Data Collection and Preprocessing

Crime-related data, including historical records, demographics, and environmental factors, are gathered and preprocessed to remove inconsistencies.

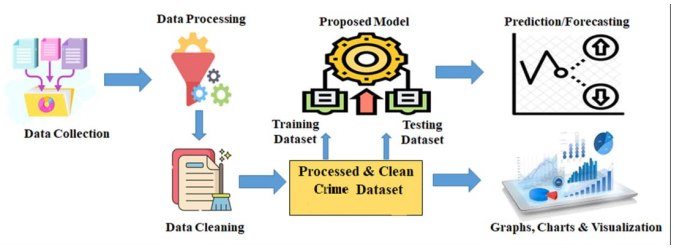

Fig. 2. Crime Data Processing and Visualization Flow

- Spatial-Temporal Analysis: Geospatial clustering methods, such as DBSCAN and K-means, are applied to analyze crime hotspots, while time-series models, including ARIMA and LSTMs, forecast crime trends over time.
- Feature Engineering: Key crime indicators, such as location, time of day, and type of offense, are utilized to refine predictive accuracy and improve model performance.
- Data Visualization: Crime trends are visualized based on historical data with respect to year, state, and crime type. Heatmaps, bar charts, and time-series plots provide insights into crime distribution, helping authorities understand evolving patterns.

2) Forecasting and Crime Prevention

The predictive model generates risk scores for various locations, enabling law enforcement to deploy preventive measures effectively. By visualizing crime trends, authorities can prioritize high-risk zones and optimize patrol strategies, ultimately reducing crime rates through data-driven intervention.

C. Crime Data Visualization

Crime data, including historical crime records and predictive forecasts, are visualized through various graphical representations, such as:

- Heatmaps: Geospatial heatmaps are used to display crime concentration across regions, helping authorities quickly identify high-risk areas for intervention.
- Time-Series Plots: These plots highlight the temporal distribution of crimes, showing peaks during specific times or seasons, aiding in planning targeted interventions.
- Bar Charts and Pie Charts: These offer a breakdown of crime types and the frequency of incidents, assisting in strategic planning for crime prevention.

D. Interactive Dashboards

Interactive dashboards offer a user-friendly interface for analyzing crime data, allowing users to explore trends and patterns dynamically. Filters can be applied to visualize crime data for specific regions, timeframes, or types of crime. This empowers stakeholders to make informed decisions based on data insights, thus improving public safety strategies and interventions.

E. Predictive Crime Analytics Integration

The visualizations can be enhanced with predictive crime analytics, showing potential hotspots and time frames for future criminal activities. This integrated approach enables authorities to proactively plan resource deployment and preventive actions based on both historical trends and future predictions.

IV. EVALUATION AND RESULTS

The CrimeGuard system was evaluated on a dataset containing real-world surveillance footage and historical crime records. The model's performance was assessed using key metrics such as accuracy, precision, recall, F1-score, and computational efficiency. The dataset included diverse video samples covering various violent and non-violent scenarios to ensure robust testing. All experiments were conducted using Python with libraries like TensorFlow, OpenCV, and Scikit-learn.

A. Metrics Definition

- Accuracy: Measures the percentage of correctly classified violent and non-violent incidents.
- Precision: Represents the proportion of detected violent incidents that were actually violent, minimizing false positives.
- Recall: Indicates how well the system identifies all violent events, reducing false negatives.
- F1-Score: The harmonic mean of precision and recall, providing a balanced evaluation of the model's effectiveness.
- Computational Efficiency: Evaluates the training and inference time required for real-time performance.

B. Performance Comparison

The classification reports of different deep learning models used in the CrimeGuard system are summarized in Table I.

TABLE I
PERFORMANCE METRICS FOR VIOLENCE DETECTION MODELS

Model	Accuracy (%)	Precision	Recall	F1-Score
VGG16	87.0	0.87	0.87	0.87
VGG19	83.0	0.83	0.83	0.83
ResNet50	68.0	0.69	0.68	0.67
MobileNet-V2	95.0	0.95	0.95	0.95
CNN+LSTM	**98.0**	**0.98**	**0.98**	**0.98**

C. Observations

- Classification Performance: CNN+LSTM achieves the highest accuracy (98%) and F1-score (0.98), demonstrating its superior ability to detect violent activities accurately.
- Precision and Recall: MobileNet-V2 also performs well with 95% accuracy, while VGG16 and VGG19 show moderate results. ResNet50 performs the worst due to its inability to capture temporal dependencies effectively.

D. Conslusion

The evaluation results confirm that CNN+LSTM is the most effective model for real-time violence detection, offering the highest accuracy and balanced performance across all metrics. While MobileNet-V2 and VGG16 provide competitive results, ResNet50 lags due to its lower ability to handle sequential frames. The computational complexity analysis ensures that CrimeGuard remains efficient for real-world applications. Future work will focus on optimizing deep learning architectures to further enhance speed and accuracy.

V. Conclusion and Future Scope

The CrimeGuard model's real-time violence detection and predictive crime analysis provide a robust solution for public safety. By integrating CNNs and LSTMs, the system accurately detects violent incidents and forecasts high-risk crime areas using historical data. This combination ensures timely intervention and proactive law enforcement strategies.

In the future, CrimeGuard can be enhanced by incorporating additional data sources like social media and IoT devices for better threat detection. Incorporating reinforcement learning could improve the system's adaptability to evolving crime patterns. Expanding the model with socio-economic factors and implementing Explainable AI (XAI) will increase accuracy and transparency. Additionally, to handle growing data, optimizing algorithms and leveraging cloud infrastructure will ensure scalability and real-time performance.

Future improvements could also include incorporating diverse datasets, expanding the system to detect multiple types of violence, and deploying the model on edge devices for real-time processing. These advancements will further enhance CrimeGuard's effectiveness and applicability in real-world scenarios.

References

[1] M. Sabokrou, M. Fathy, M. Hoseini, and R. Klette, "Deep-anomaly: Fully convolutional neural network for fast anomaly detection in crowded scenes," Computer Vision and Image Understanding, vol. 172, pp. 88-97, 2018.

[2] B. Sathyadevan and S. Gangadharan, "Crime analysis and prediction using data mining techniques," 2014 First International Conference on Networks & Soft Computing (ICNSC), 2014, pp. 406-412.

[3] M. Ullah, M. A. Muhammad, G. H. Lee, and S. W. Baik, "Violence detection using spatiotemporal features with 3D convolutional neural networks," Sensors, vol. 19, no. 11, p. 2472, 2019.

[4] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable artificial intelligence (XAI)," IEEE Access, vol. 6, pp. 52138-52160, 2018.

[5] X. Xu, L. Yang, H. Wang, and F. Zhao, "Edge computing: A new computing model for Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 3, pp. 1778-1786, 2020.

[6] N. K. Sharma, M. Pandey, and R. K. Gupta, "IoT-based smart surveillance systems for crime detection and prevention," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 8473-8490, 2021.

[7] G. Gorr and R. Harries, "Introduction to crime forecasting," International Journal of Forecasting, vol. 19, no. 4, pp. 551-555, 2003.