Avoid Crime Scenes Using Ai Based Security System

Vishal Nayakwadi[1], Manju Dalai[2]

[1]*Assistant Professor, Department of AI&DS, Zeal College of Engineering and Research,Pune (India)*

[2]*Student, Zeal College of Engineering and Research,Pune (India)*

***Abstract*—This review paper examines the application of AI-based security systems in preventing crime scenes by integrating advanced technologies such as machine learning, computer vision, and predictive analytics. It highlights how AI can enhance real-time surveillance, improve threat detection, and enable proactive crime prevention strategies. The paper discusses the key techniques used in AI-driven security systems, including facial recognition, object detection, and behavior analysis, which help in identifying potential criminal activities. Moreover, the review emphasizes the importance of predictive analytics, which utilizes historical crime data to forecast crime hotspots and trends, allowing law enforcement to deploy resources more effectively. AI systems can also reduce human error and increase the speed of decision-making, providing timely alerts for swift responses. Challenges such as privacy concerns, data security, and ethical implications are also addressed, with recommendations on how to mitigate these issues. The paper further explores the limitations of current AI technology, including false positives, biases, and the need for high-quality data. Finally, it discusses the future trends of AI in security systems, including the integration of advanced algorithms and the potential for AI to revolutionize law enforcement practices, ultimately contributing to safer communities.**

Index Terms*—Machine learning, C*omputer vision, Real-time surveillance, AI technology

I. INTRODUCTION

Crime prevention has always been a cornerstone of societal development, as communities strive to create safe environments for their citizens. However, as the complexity and frequency of crimes have evolved, traditional methods of ensuring security are no longer sufficient. Manual surveillance systems, static security protocols, and reactive crime response strategies often fall short in addressing modern security challenges. This gap necessitates the adoption of innovative technologies capable of providing proactive, scalable, and efficient crime prevention mechanisms. Among these technologies, Artificial Intelligence (AI) stands out as a transformative tool for reshaping how crimes are predicted, monitored, and prevented.

An AI-based security system uses advanced computational algorithms to analyze vast amounts of real-time data, detect anomalies, and predict potential threats. Unlike traditional systems that rely heavily on human intervention, AI systems operate with high precision and consistency, making them an indispensable asset in avoiding crime scenes. These systems integrate technologies such as machine learning, computer vision, and natural language processing to provide intelligent and automated crime prevention solutions. From identifying suspicious behavior to predicting high-crime areas, AI systems enable law enforcement agencies to take proactive measures, thus reducing the likelihood of crimes and enhancing public safety.

One of the defining features of AI-based security systems is their ability to monitor and process data continuously and in real-time. Surveillance cameras, IoT devices, and public databases generate immense volumes of information daily. Human operators often find it challenging to monitor this data effectively, leading to overlooked details and delayed responses. AI systems address this limitation by analyzing multiple data streams simultaneously, identifying unusual patterns, and triggering immediate alerts. For example, an AI-powered video surveillance system can recognize loitering in sensitive areas, detect unattended bags in public spaces, or identify individuals displaying aggressive behavior. These capabilities help mitigate potential threats before they escalate into crimes.

Another critical aspect of AI-based security systems is predictive analytics, which relies on historical crime data, social trends, and environmental factors to forecast where crimes are likely to occur. This functionality enables law enforcement agencies to deploy resources more efficiently, focusing on areas with the highest risk of criminal activity. For instance, predictive crime mapping can highlight specific neighborhoods prone to burglaries during certain times of the day, allowing police to increase patrols in those areas. By preemptively addressing potential crime hotspots, AI-based systems not only deter criminal activities but also foster a sense of security among the local population.

AI-based security systems also excel in tasks like facial recognition, license plate recognition, and object detection. These features are particularly useful in identifying known offenders, tracking vehicles involved in criminal activities, or detecting weapons in public places. Such capabilities enhance the accuracy of investigations and reduce the time required to resolve cases. Additionally, these systems can integrate with emergency response frameworks, automating the process of notifying law enforcement, medical services, or fire departments during critical incidents. This seamless coordination ensures faster response times and minimizes the impact of crimes or emergencies.

While the benefits of AI-based security systems are undeniable, their implementation is not without challenges. Privacy concerns are a major issue, as these systems rely heavily on data collection and surveillance. Citizens may feel uneasy about being constantly monitored, fearing misuse of their personal information. Furthermore, the potential for algorithmic bias in AI systems poses significant ethical questions. If not trained on diverse datasets, AI algorithms may inadvertently discriminate against certain groups, leading to unfair profiling or targeting. Addressing these concerns requires a balanced approach that ensures transparency, accountability, and adherence to legal and ethical standards. Policymakers, technologists, and law enforcement agencies must work collaboratively to establish guidelines that protect individual rights while leveraging AI's capabilities for public safety.

In conclusion, the application of AI in security systems marks a significant shift toward proactive crime prevention. By combining real-time analytics, predictive modeling, and intelligent automation, these systems provide an effective alternative to traditional security methods. Despite challenges related to privacy and ethics, the potential of AI-based security systems to revolutionize crime prevention is immense. This research paper delves into the design, implementation, and impact of such systems, with a focus on addressing technical limitations and ethical considerations. By harnessing the power of AI responsibly, society can move closer to achieving safer, more secure environments for everyone.

II. LITERATURE REVIEW

1. Forensic Science International: Digital Investigation is typically to present innovative research, methodologies, or case studies that advance the understanding and application of digital forensics in solving crimes. It aims to contribute to the field by addressing emerging challenges, improving techniques, or analyzing digital evidence effectively.
2. Image and video-based crime prediction using object detection and deep learning this paper is to develop a framework for predicting and analyzing crimes using image and video data by leveraging object detection and deep learning techniques. It aims to enhance public safety by automating crime detection and enabling proactive law enforcement measures through advanced computational models.
3. Current and emerging trends in the use of AI for community surveillance this paper is to explore current and emerging trends in the application of AI for community surveillance, focusing on its capabilities, challenges, and ethical considerations. It aims to provide insights into how AI-driven technologies can enhance public safety while addressing privacy and societal concerns.
4. Advancements in Crime Prevention and Detection: From Traditional Approaches to Artificial Intelligence Solutions is to examine the evolution of crime prevention and detection methods, transitioning from traditional approaches to modern AI-driven solutions. It aims to highlight the advancements, benefits, and challenges of integrating AI technologies into law enforcement and public safety strategies.
5. Design of a real-time crime monitoring system using deep learning techniques is to design a real-time crime monitoring system utilizing deep learning techniques to detect and analyze criminal activities efficiently. It aims to enhance situational awareness

and enable proactive responses through automated and intelligent surveillance.

6. London street crime analysis and prediction using crowdsourced dataset is to analyze and predict street crime in London using a crowdsourced dataset, leveraging data-driven techniques for actionable insights. It aims to support crime prevention efforts by identifying patterns, trends, and potential hotspots.

7. Using Information Technology for Comprehensive Analysis and Prediction in Forensic Evidence this paper is to explore the application of information technology for comprehensive analysis and prediction in forensic evidence. It aims to enhance accuracy, efficiency, and reliability in forensic investigations through advanced computational tools and predictive models.

8. IoT-Guard: Event-Driven Fog-Based Video Surveillance System for Real-Time Security Management is to develop IoT-Guard, a fog-based, event-driven video surveillance system for real-time security management. It aims to enhance surveillance efficiency by integrating IoT technologies with low-latency processing and intelligent event detection.

9. Designing and evaluation of a mixed reality system for crime scene investigation training: a hybrid approach is to design and evaluate a mixed reality system for training in crime scene investigation using a hybrid approach that combines virtual and physical elements. It aims to enhance the learning experience and skill development of trainees through immersive and interactive simulations.

10. An efficient image classification and segmentation method for crime investigation applications is to develop an efficient image classification and segmentation method tailored for crime investigation applications. It aims to improve the accuracy and speed of analyzing visual evidence, aiding law enforcement in solving crimes effectively.

Name of the paper	Year	objective	Methodology	Limitation
Forensic Science International: Digital Investigation	2024	To enhance the understanding of digital evidence collection, analysis, and interpretation,evaluate methodologies for digital forensic investigations.	Use of experimental setups to simulate cyber incidents or evidence analysis.Comparative analysis of forensic tools, algorithms, or techniques.	Limited scalability of proposed methods in large-scale or complex investigations.Challenges in replicating real-world cybercrime scenarios in experimental setups.
Image and video-based crime prediction using object detection and deep learning	2023	object detection and deep learning techniques to analyze images and videos for predicting potential criminal activities.	Data Collection, Preprocessing, Object Detection, Deep Learning Model, Evaluation, Real-time Implementation	Dataset Bias,False Positives/Negatives, Ethical Concerns, Scalability,Adaptability,Environmental Factors,Context Understanding
Current and emerging trends	2024	To identify current and future trends in AI-driven	Focus on diverse AI applications such as facial	Limited availability of comprehensive

in the use of AI for community surveillance		technologies used for public safety and monitoring.	recognition, behavior analysis, drone surveillance, and automated monitoring systems.	datasets to evaluate AI's effectiveness in diverse community surveillance scenarios.
Advancements in Crime Prevention and Detection: From Traditional Approaches to Artificial Intelligence Solutions	2024	How AI can revolutionize crime prevention and detection, transitioning from traditional, often reactive methods to proactive, data-driven approaches. Analyzing Traditional Methods,Exploring AI Solutions,Identifying Challenges	Observing and analyzing local crime prevention practices to understand the practical application and effectiveness of existing methods.	Limited access to comprehensive and high-quality data may affect the analysis of AI effectiveness in various crime scenarios. Bias in AI Models,Privacy Concerns,Legal and Ethical Challenges,Technological Barriers,Public Trust
Design of a real-time crime monitoring system using deep learning techniques	2024	Real-time crime monitoring system using deep learning techniques to detect and analyze criminal activities efficiently.	Employs deep learning techniques, such as convolutional neural networks (CNNs), for real-time analysis of video feeds to detect and classify criminal activities. It integrates these models with a monitoring system to provide instant alerts and enable timely law enforcement responses	The system may face challenges in handling diverse environmental conditions, data quality issues, and real-time processing constraints.
London street crime analysis and prediction using crowdsourced dataset	2024	analyze and predict London Street crime patterns using a crowdsourced dataset to identify trends and potential hotspots for crime prevention	utilizes a crowdsourced dataset to analyze street crime patterns in London, applying machine learning models to identify trends and predict potential crime hotspots. It combines data preprocessing, feature extraction, and predictive analytics to enhance crime prevention strategies	The reliability of predictions may be affected by the quality, completeness, and potential biases in the crowdsourced data.

Using Information Technology for Comprehensive Analysis and Prediction in Forensic Evidence	2024	Leverage information technology for comprehensive analysis and prediction in forensic evidence to enhance accuracy and efficiency in investigations	advanced information technology tools, such as data mining, machine learning, and statistical modeling, to analyze and predict forensic evidence. It integrates these technologies to enhance the accuracy and efficiency of forensic investigations through comprehensive data analysis.	Face challenges in integrating diverse data sources and ensuring the interpretability of complex predictive models.
Designing and evaluation of a mixed reality system for crime scene investigation training: a hybrid approach	2023	design and evaluate a mixed reality system combining virtual and physical elements to enhance training for crime scene investigations	mixed reality system that combines virtual simulations with physical environments for crime scene investigation training	system may require significant resources for implementation and might face challenges in replicating complex real-world scenarios accurately
An efficient image classification and segmentation method for crime investigation applications	2024	develop an efficient image classification and segmentation method to improve crime investigation applications by enhancing the analysis of visual evidence	It applies convolutional neural networks (CNNs) for feature extraction and object recognition, improving the accuracy of crime scene analysis.	struggle with processing images of low quality or those with complex, cluttered backgrounds, affecting classification accuracy
VD-Net: An Edge Vision-Based Surveillance System for Violence Detection	2024	develop VD-Net, an edge vision-based surveillance system for real-time violence detection to enhance public safety	VD-Net uses edge computing and deep learning models to process video feeds locally for real-time violence detection, reducing latency and bandwidth requirements. It employs convolutional neural networks (CNNs) to identify violent behaviors and trigger immediate alerts for security personnel.	face challenges with false positives and may be less effective in environments with low-resolution cameras or poor lighting conditions

III. PROPOSED SYSTEM

The proposed AI-based security system aims to prevent crime scenes by integrating advanced machine learning, computer vision, and predictive analytics technologies. The system would utilize real-time surveillance feeds from cameras, sensors, and IoT devices to continuously monitor public spaces and detect unusual or suspicious behaviors.

Key components of the proposed system include:

1. Real-time Video Surveillance**:** AI-powered cameras will analyze live video feeds using deep learning algorithms, such as convolutional neural networks (CNNs) for object detection, facial recognition, and behavior analysis to identify potential threats.
2. Predictive Analytics for Crime Prevention**:** By analyzing historical crime data and identifying patterns, the system will predict potential crime hotspots and times, allowing for targeted law enforcement interventions in high-risk areas.
3. Threat Detection and Alerts: The system will use machine learning models to detect aggressive or violent actions in real-time, such as physical altercations or vandalism, and generate immediate alerts for security personnel or law enforcement.
4. Automated Decision-Making and Response: The AI system will autonomously assess potential risks and initiate security responses, such as activating alarms, contacting law enforcement, or alerting nearby citizens via a mobile application.
5. Data Security and Privacy: The system will adhere to privacy guidelines and employ encryption and secure data storage protocols to protect sensitive information, ensuring compliance with data protection regulations.
6. Continuous Learning and Improvement: As the system gathers more data, it will improve its predictive capabilities through reinforcement learning and continuously adapt to new crime patterns and emerging threats.

The proposed system aims to create safer environments by reducing response times, preventing crimes before they occur, and supporting law enforcement with advanced tools for crime scene avoidance and prevention.

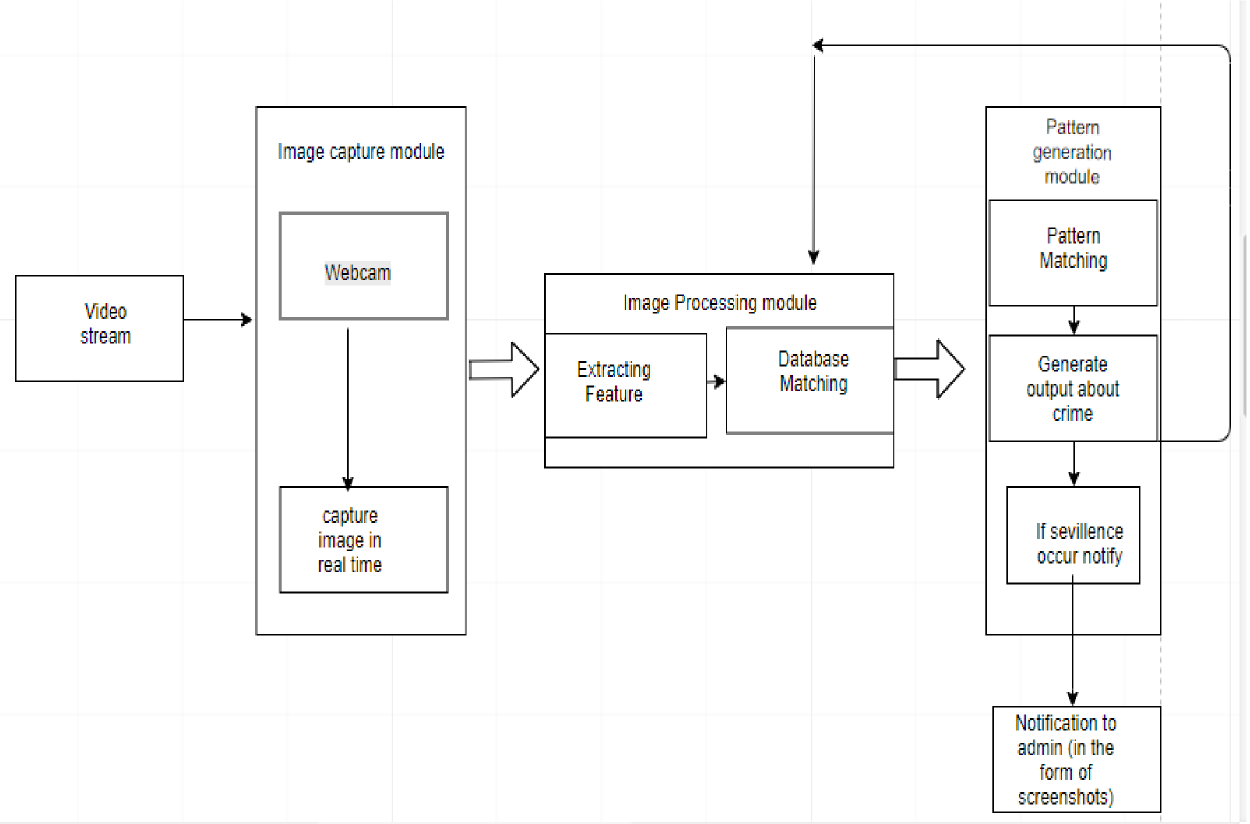
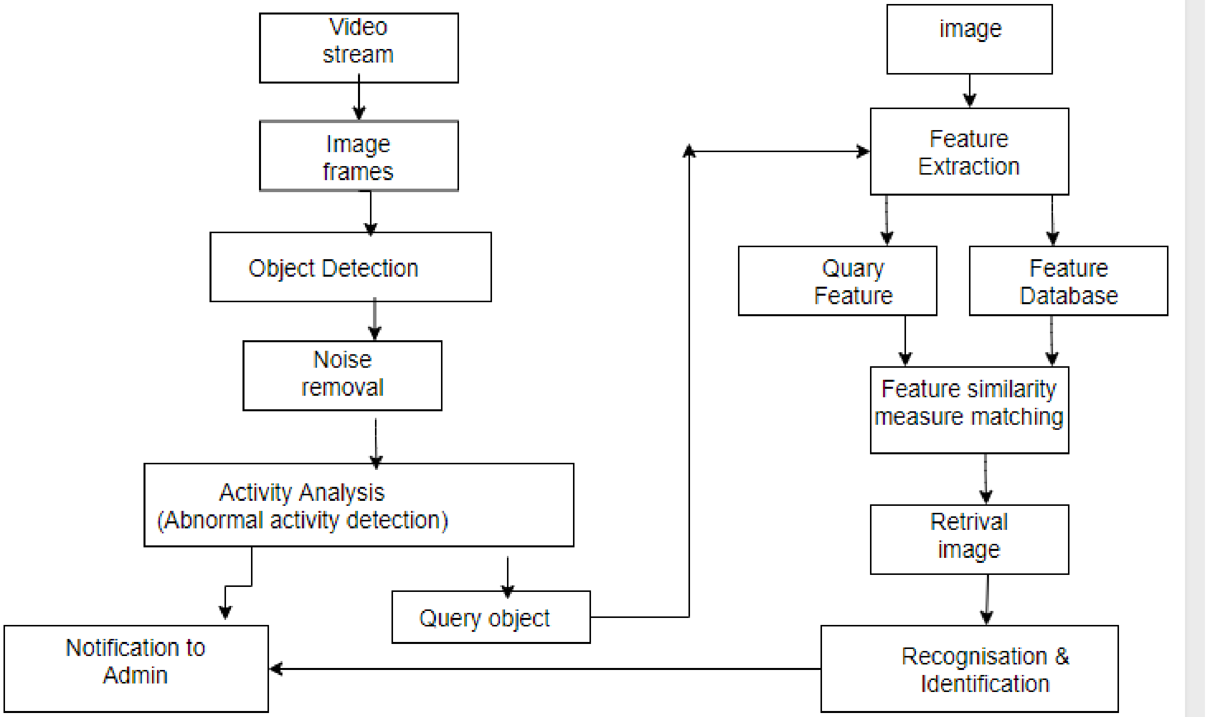

Video stream
Image capture module
Webcam
capture image in real time
Image Processing module
Extracting Feature
Database Matching
Pattern generation module
Pattern Matching
Generate output about crime
If sevillence occur notify
Notification to admin (in the form of screenshots)

Fig 1: System Architecture

Flow Chart

Fig 2: Flowchart



Datasets

A. Crime Data Datasets:

- UCI Crime Data: A comprehensive dataset of historical crime data, which can be used to predict crime hotspots and trends. This dataset includes information such as crime types, locations, and timestamps, which is useful for crime prediction models.
- Chicago Crime Data: A dataset from the City of Chicago containing details of reported incidents of crime, including types of crimes, locations, and times. This can be used to train predictive models and identify crime patterns.

B. Surveillance Video Datasets:

- ImageNet or COCO Dataset: For training object detection and recognition models, these general datasets provide labeled images of various objects, which can be extended to detect suspicious activities like aggression, theft, or vandalism.
- AVSS Surveillance Dataset: A dataset specifically for video surveillance, providing annotated video data to train AI systems for behavior recognition and violence detection in crowded environments.

C. Behavior and Activity Recognition Datasets:

- CASIA Human Action Dataset: A large-scale dataset containing videos of human activities that can be used to train AI models for recognizing suspicious behaviors, such as fights or thefts, in surveillance footage.
- Sports Activity Recognition Dataset: Though designed for sports applications, it can be used to detect abnormal behaviors in video feeds, such as aggressive physical interactions, which can be indicators of violent crime.

D. Facial Recognition Datasets:

- LFW (Labeled Faces in the Wild): This dataset contains labeled images of people for facial recognition, which can be used in conjunction with surveillance systems to identify persons of interest.
- FaceNet or VGGFace2: Datasets for training facial recognition models, useful for identifying individuals in public spaces and flagging known criminals or persons of interest.
- Smart City IoT Datasets: Data from sensors such as motion detectors, temperature sensors, or GPS tracking, which can help detect anomalies or

unusual behavior patterns in public spaces.

- MObiSense: A dataset for anomaly detection in urban environments, which could help in identifying unexpected events or behaviors that may signify criminal activity.

E. Crowdsourced Datasets:

- OpenStreetMap (OSM): This geographical data can be used to map out urban environments and identify areas with high crime rates or poorly lit streets, which may be more prone to criminal activities.
- Twitter Crime Datasets: Datasets that collect public social media data regarding criminal incidents, which can aid in monitoring real-time crime reports and support predictive analytics.

Tools and Techniques

1. Machine Learning and Deep Learning Frameworks

- TensorFlow / Keras / PyTorch: These popular deep learning frameworks enable the development of AI models, particularly for image recognition, object detection, and anomaly detection tasks. They are used for training models on large datasets and implementing real-time surveillance systems.
- Scikit-learn: A powerful library for implementing machine learning algorithms, such as classification, regression, and clustering, useful for crime prediction, trend analysis, and anomaly detection.

2. Computer Vision Techniques

- OpenCV: A widely used computer vision library for processing images and videos, applying algorithms for object detection, face recognition, and tracking. It is essential for analyzing video feeds in real-time surveillance systems.
- YOLO (You Only Look Once): An efficient and real-time object detection algorithm, ideal for detecting suspicious objects or behaviors (e.g., weapons, fights) in surveillance footage.
- DeepLabV3 (for Segmentation): A deep learning-based model for semantic image segmentation, which can be used to isolate regions of interest in crime scene images or videos for further analysis.

3. Predictive Analytics Tools

- ARIMA (AutoRegressive Integrated Moving Average): A time series forecasting model used for predicting crime patterns based on historical data, helping identify crime hotspots or high-risk periods.
- Random Forest and Decision Trees: These ensemble machine learning methods can be used to analyze and classify crime patterns based on various features such as location, time, and type of crime.
- K-means Clustering: A clustering algorithm to identify geographical areas or timeframes with high crime rates, which can assist in resource allocation and crime prevention.

4. Real-Time Data Processing and Edge Computing

- Edge Computing Frameworks (e.g., EdgeX Foundry): These frameworks allow real-time processing of video and sensor data at the edge (near the source), reducing latency and bandwidth requirements. This is crucial for quick response times in surveillance systems.
- NVIDIA Jetson (for Edge AI): A platform for implementing real-time AI applications on edge devices, enabling on-site processing of video feeds and sensor data to detect suspicious activities and send alerts without relying on cloud servers.

5. Facial Recognition and Biometric Systems

- OpenFace / FaceNet: These deep learning-based facial recognition models can be implemented to identify known criminals or individuals of interest in real-time surveillance footage.
- DeepFace: A Python library that wraps multiple facial recognition algorithms, making it easier to deploy in security systems for matching faces captured in surveillance videos to known criminal databases.

6. Natural Language Processing (NLP) for Social Media and News

- NLTK (Natural Language Toolkit): A library for processing text data, which can be used to analyze crowdsourced or social media data (e.g., tweets, news) for real-time crime alerts or public reports.
- GPT-3 / BERT: Advanced language models can help extract meaningful insights from unstructured text data, such as news reports or crime-related posts on social media, for predictive crime analysis.

7. **Data Visualization Tools**

- Tableau / Power BI: Visualization tools for representing crime trends, crime hotspots, and prediction outcomes in a user-friendly dashboard format, which can be useful for law enforcement and decision-makers.
- Gephi / QGIS: Geospatial analysis and visualization tools that help map crime data geographically, identify patterns, and display predicted crime hotspots for resource planning.

8. Cloud Computing and Big Data Solutions

- Amazon Web Services (AWS) / Microsoft Azure / Google Cloud Platform (GCP): Cloud platforms provide scalable storage and computing resources necessary for handling large datasets, training deep learning models, and implementing large-scale surveillance systems.
- Apache Spark / Hadoop: Big data tools that enable the processing and analysis of large crime data sets, allowing for more accurate crime prediction models and insights from diverse data sources (e.g., social media, surveillance footage).

9. IoT (Internet of Things) for Smart Surveillance

- IoT Sensors (motion, temperature, sound): Sensors integrated into the environment that collect real-time data on environmental changes and unusual activities. This data can be used to trigger alerts when suspicious activity is detected.
- MQTT Protocol: A lightweight messaging protocol for transmitting sensor data in real-time, often used in smart city infrastructure for monitoring and reporting crimes.

10. Security and Privacy Tools

- Blockchain for Data Integrity: Blockchain can be used to ensure the integrity and security of sensitive surveillance data, preventing tampering or unauthorized access.
- Homomorphic Encryption: A privacy-preserving encryption technique that allows data to be processed in its encrypted form, ensuring that sensitive personal information is not exposed during surveillance or data analysis.

11. Cloud-Based Collaboration Tools

- Slack / Microsoft Teams: Real-time communication and collaboration tools thatallow security personnel, law enforcement, and stakeholders to receive alerts and coordinate actions quickly.
- Geo-Alert Systems: Automated alert systems integrated with geographical mapping software to notify security personnel when a crime is predicted or detected in their proximity.

IV. PROPOSED METHODOLOGY

- Data Collection and Integration: Collect diverse data from surveillance cameras, IoT sensors, historical crime reports, and social media to create a comprehensive dataset for analysis.
- Preprocessing: Clean and preprocess the collected data by removing noise, normalizing data, and annotating relevant features, such as crime types, time, and location, for analysis.
- Real-Time Surveillance Analysis: Implement computer vision algorithms (e.g., YOLO, CNNs) to analyze video feeds for detecting suspicious activities like aggression, theft, or vandalism.
- Crime Prediction: Use machine learning algorithms (e.g., Random Forest, ARIMA) to analyze historical crime data and predict crime hotspots and trends, enabling proactive monitoring.
- Violence Detection: Apply deep learning techniques to detect violent behaviors in video footage, such as physical altercations or abnormal movements, using models trained on labeled crime data.
- Alert System and Decision Making: Trigger real-time alerts when suspicious activity or violence is detected, enabling rapid law enforcement responses or automated interventions.
- Continuous Learning: Continuously train the system on new data to improve its predictive accuracy, using reinforcement learning to adapt to evolving crime patterns.
- Privacy and Security: Ensure data privacy and compliance with regulations by employing secure data storage and encryption methods.Overview of Algorithms used.
- YOLO (You Only Look Once): An efficient, real-time object detection algorithm that detects objects and activities (e.g., weapons, physical altercations) in surveillance footage.
- Convolutional Neural Networks (CNNs): Used for object detection and image classification in

video feeds to identify suspicious behaviors, such as violence or theft.

- Random Forests and Decision Trees: Machine learning algorithms employed for crime prediction, analyzing historical data to classify crime types and forecast crime hotspots.
- Support Vector Machines (SVMs): Used for classifying suspicious events based on feature extraction from video and sensor data, distinguishing between normal and abnormal activities.
- K-means Clustering: A clustering algorithm used to identify crime hotspots by grouping geographical locations or times based on crime density.
- ARIMA (AutoRegressive Integrated Moving Average): A time-series forecasting model for predicting crime trends and forecasting future crime patterns based on historical data.
- Reinforcement Learning: Applied for continuous learning and adaptation of the system, allowing the model to evolve and improve crime prediction accuracy over time

V. SCOPE OF THE PROPOSED SYSTEM

Crime Prevention: The system aims to proactively predict and prevent crimes by analyzing historical data and real-time surveillance footage, enabling early detection of potential threats.

Real-Time Monitoring: By leveraging AI-driven algorithms for video analysis, facial recognition, and anomaly detection, the system provides continuous surveillance and immediate threat identification in public spaces.

Resource Optimization: The system helps law enforcement agencies optimize resource allocation by predicting crime hotspots and high-risk times, improving the efficiency of patrols and interventions.

Scalability: The system is designed to be scalable, allowing for integration with existing security infrastructure and expansion to larger urban areas or multiple public spaces.

Adaptability: Through continuous learning and reinforcement, the system adapts to evolving crime patterns and environmental changes, enhancing its long-term effectiveness.

VI. CONCLUSION

Avoid Crime Scenes Using AI-Based Security System is emphasizes the significant potential of AI technologies in enhancing public safety. By integrating machine learning, computer vision, and predictive analytics, the system can effectively detect, predict, and prevent crimes in real-time. It provides valuable tools for law enforcement to improve crime response times, optimize resources, and create safer environments. However, the paper also highlights the challenges of privacy concerns, data security, and the need for high-quality data to ensure accurate and ethical implementation. Overall, AI-based security systems represent a promising solution for modern crime prevention and public safety.

REFERENCES

[1] Md. Muktadir Mukto, Mahamudul Hasan, Md. Maiyaz Al Mahmud, Ikramul Haque, Md. Ahsan Ahmed, Taskeed Jabid, Md. Sawkat Ali, Mohammad Rifat Ahmmad Rashid, Mohammad Manzurul Islam, Maheen Islam. “*Design of a real-time crime monitoring system using deep learning techniques*”, ELSEVIER, 2024.

[2] Ahmed Yunus ∗, Jonathan Loo. “London street crime analysis and prediction using crowdsourced dataset”, ELSEVIER, 2024.

[3] Faris Kamil Hasan Mihna, , Mustafa Abdulfattah Habeeb, Abdalhusen Easa Al-saeedi, “Using Information Technology for Comprehensive Analysis and Prediction in Forensic Evidence” journals.mesopotamian.press,2024.

[4] Tanin Sultana, Khan A. Wahid, Senior Member,“IoT-Guard: Event-Driven Fog-Based Video Surveillance System for Real-Time Security Management” IEEE,2024.

[5] Meshal Albeedan · Hoshang Kolivanda, Ramy Hammady, “Designing and evaluation of a mixed reality system for crime scene investigation training: a hybrid approach” Virtual Reality, Springer 2024.

[6] Ahmed Sedik, Hoshang Kolivand, Meshal Albeedan, “*An efficient image classification and segmentation method for crime investigation applications*” Multimedia Tools and Applications, Springer 2024.

[7] Shweta Srivastava, Aditya Bisht, Neetu Narayan,"*Safety and Security in Smart Cities Using Artificial Intelligence-A Review*" IEEE,2024.

[8] Abdulsamad A. AL-Marghilani, "*Target Detection Algorithm in Crime Recognition Using Artificial Intelligence*" Tech Science Press,2021.

[9] Dipo Dunsin a, Mohamed C. Ghanem, Karim Ouazzane, Vassil Vassilev,"*A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response*" ELSEVIER,2024.

[10] Mohammed Boukabous, Mostafa Azizi,"*Image and video-based crime prediction using object detection and deep learning*" Bulletin of Electrical Engineering and Informatics (BEEI) 2023.

[11] Nelson Salgado, Jaime Meza, Monica Vaca-Cardenas, Leticia Vaca-Cardenas,"*Current and emerging trends in the use of AI for community surveillance*" EnPress,2024.

[12] Oghenevovwero Zion Apene, Nachamada Vachaku Blamah, Gilbert Imuetinyan Osaze Aimufua,"*Advancements in Crime Prevention and Detection: From Traditional Approaches to Artificial Intelligence Solutions*" AMO Publisher,2024.

[13] United Nations Office on Drugs and Crime, "Executive summary, World Drug Report," New Directions for Youth Development, vol. 2012, no.133, 2023. Available: https://www.oecd.org/innovation/inno/47164461.pdf%0Ahttp://www.ncbi.nlm.nih.gov/pubmed/22522447%0Ahttp://doi.wiley.com/10.1002/yd.20002

[14] D. Willmott, D. Hunt, D. Mojtahedi, Criminal Geography and Geographical Profiling within Police Investigations – A Brief Introduction, January, 2023.

[15] Oghenevovwero Zion Apene, Nachamada Vachaku Blamah, Gilbert Imuetinyan Osaze Aimufua, "*Advancements in Crime Prevention and Detection: From Traditional Approaches to Artificial Intelligence Solutions*" AMO Publisher,2024.

[16] F. Marcin, AI-Powered Surveillance: How Crime Prediction Algorithms are Changing Policing, 2023.Available: https://ts2.space/en/ai-powered-surveillance-how-crime-prediction-algorithms-are-changing-policing/

[17] H. Shah, S. Mishra, B. Dubey, D. Manikpurkar, "Criminal Investigation with the help of Face Recognition," International Journal of Engineering Research & Technology (IJERT), vol. 12, no. 4, pp. 351–355, 2023. DOI: 10.17577/IJERTV12IS040088

[18] S.A.H. Mohsan, M.A. Khan, F. Noor, I. Ullah, M.H. Alsharif, "Towards the Unmanned Aerial Vehicles (UAVs): A Comprehensive Review," Drones, vol. 6, no. 6, 2022. DOI: 10.3390/drones6060147

[19] Cao, C.; Wang, B.; Zhang, W.; Zeng, X.; Yan, X.; Feng, Z.; Liu, Y.; Wu, Z. An improved faster R-CNN for small object detection.IEEE Access 2019, 7, 106838–106846. [CrossRef]

[20] Al-Haija, Q.A.; Smadi, M.A.; Zein-Sabatto, S. Multi-class weather classification using ResNet-18 CNN for autonomous IoT and CPS applications. In Proceedings of the 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 16–18 December 2020; pp. 1586–1591.

[21] VGG16—Convolutional Network for Classification and Detection. Available online: https://neurohive.io/en/popular-networks/vgg16/ (accessed on 25 February 2024).

[22] Rajapakshe, C.; Balasooriya, S.; Dayarathna, H.; Ranaweera, N.; Walgampaya, N.; Pemadasa, N. Using cnns rnns and machine learning algorithms for real-time crime prediction. In Proceedings of the 2019 International Conference on Advancements in Computing (ICAC), Malabe, Sri Lanka, 5–6 December 2019; pp. 310–316.

[23] Alderliesten, K. Yolov3—Real-Time Object Detection. Available online: https://medium.com/analytics-vidhya/yolov3-real- time-object-detection-54e69037b6d0 (accessed on 25 February 2024).

[24] Chong, Y.S.; Tay, Y.H. Abnormal event detection in videos using spatiotemporal autoencoder. In Advances in Neural Networks-ISNN 2017, Proceedings of the 14th International Symposium, ISNN 2017, Sapporo, Hakodate, and Muroran, Hokkaido, Japan, 21–26 June 2017; Springer: Cham, Switzerland, 2017.

[25] Atrey, J.; Regunathan, R.; Rajasekaran, R. Real-

world application of face mask detection system using YOLOv6. Int. J. Crit. Infrastruct. 2023. [CrossRef]

[26] Sung, C.S.; Park, J.Y. Design of an intelligent video surveillance system for crime prevention: Applying deep learning technology. Multimed. Tools Appl. 2021, 80, 34297–34309.

[27] Jiang, B.; He, J.; Yang, S.; Fu, H.; Li, T.; Song, H.; He, D. Fusion of machine vision technology and AlexNet-CNNs deep learning network for the detection of postharvest apple pesticide residues. Artif. Intell. Agric. 2019, 1, 1–8.

[28] Forson, E. Understanding SSD Multibox—Real-Time Object Detection in Deep Learning. Available online: https://towardsdatascience.com/understanding-ssd-multibox-real-time-object-detection-in-deep-learning-495ef744fab (accessed on 25 February 2024).

[29] Inception V3 Model Architecture. Available online: https://iq.opengenus.org/inception-v3-model-architecture/ (accessed on 25 February 2024).

[30] Liu, K.; Zhu, M.; Fu, H.; Ma, H.; Chua, T.S. Enhancing anomaly detection in surveillance videos with transfer learning fromaction recognition. In Proceedings of the 28th ACM International Conference on Multimedia, Seattle, WA, USA, 12–16 October2020; pp. 4664–4668.