International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

Detection of Criminal Activities and Anomalies through CCTV's

Vijay Sonawane[1], Rani Aaglave[2], Rutvik Bedre[3], Abhishek Birajdar[4], Vivek Pardeshi[5]

[1]Prof. Computer Engineering Department, JSPM's Bhivarabai Sawant Institute of Technology & Research, Wagholi, Pune, India.

[2,3,4,5]Student Computer Engineering Department, JSPM's Bhivarabai Sawant Institute of Technology & Research, Wagholi, Pune, India.

Emails: *sonawanevijay4@gmail.com[1], raniagalave@gmail.com[2], bedrerutvik2@gmail.com[3], abhishekbirajdar55@gmail.com[4], vivekpardeshi10@gmail.com[5]*

Abstract

The project aims to develop an intelligent system that can detect unusual activities and crimes using CCTV cameras across the state. Since it is difficult to monitor multiple cameras simultaneously, we use state-of-the-art computer and machine learning to analyze live video. When a suspicious or dangerous situation occurs, the system quickly alerts authorities to the address and sends images of the incident. It also activates nearby alarms to locate concerned citizens and help them intervene. There is also a portal that helps classify video clips as normal or abnormal. The system will help speed up emergency response and encourage community participation to ensure safety. Overall, this is a great way to prevent crime and increase everyone's safety.

Keywords: *Anomalies Detection, Crime prevention, Machine Learning, Convolutional Neural Network (CNN).*

1. Introduction

As crime rates continue to escalate and criminal tactics grow increasingly sophisticated, traditional security measures alone have become insufficient [1]. The integration of modern technology with crime prevention strategies has paved the way for innovative solutions aimed at enhancing public safety [2]. A key approach in this domain involves utilizing artificial intelligence (AI) and machine learning (ML) to analyze vast amounts of data, such as video feeds from CCTV cameras [3]. This technology enables the real-time detection of unusual activities and facilitates immediate responses, thereby prevent- ing incidents and ensuring quicker interventions [4]. The focus of this project is the development of a cutting-edge security system that applies AI and ML to monitor live CCTV footage. The system is capable of autonomously identifying abnormal or criminal behavior, accidents, and other anomalous events [5]. Upon detection of suspicious activity, the system promptly notifies authorities and nearby individuals, providing critical location and visual evidence [6]. Furthermore, the system can activate alarms in the vicinity to alert the public and encourage swift action. It also includes a user-friendly web portal that allows video footage to be uploaded and classified as either normal or anomalous, making it easier for law enforcement and relevant authorities to review the footage efficiently [7]. This system is designed to manage a large number of CCTV feeds, making it suitable for urban areas or even statewide surveillance networks [8]. In addition, it prioritizes data privacy and ensures legal compliance in handling sensitive video information [9]. The objective of this "I/ML-based Detection of Anomalies and Criminal Activities through CCTV" project is to reduce emergency response times and encourage community involve- ment in public safety efforts. By alerting both authorities and citizens, the system fosters quicker reactions to potential threats and accidents, thereby contributing to the creation of safer public spaces for all [10].

2. Background Review or Literature Review

As crime rates continue to escalate and criminal tactics grow increasingly sophisticated, traditional security measures alone have become insufficient [1]. The integration of modern technology with crime prevention strategies has paved the way for innovative solutions aimed at enhancing public safety

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

[2]. A key approach in this domain involves utilizing artificial intelligence (AI) and machine learning (ML) to analyze vast amounts of data, such as video feeds from CCTV cameras [3]. This technology enables the real-time detection of unusual activities and facilitates immediate responses, thereby preventing incidents and ensuring quicker interventions [4]. The focus of this project is the development of a cutting-edge security system that applies AI and ML to monitor live CCTV footage. The system is capable of autonomously identifying abnormal or criminal behavior, accidents, and other anomalous events [5]. Upon detection of suspicious activity, the system promptly notifies authorities and nearby individuals, providing critical location and visual evidence [6]. Furthermore, the system can activate alarms in the vicinity to alert the public and encourage swift action [7]. It also includes a user-friendly web portal that allows video footage to be uploaded and classified as either normal or anomalous, making it easier for law enforcement and relevant authorities to review the footage efficiently [8]. This system is designed to manage a large number of CCTV feeds, making it suitable for urban areas or even statewide surveillance networks [9]. In addition, it prioritizes data privacy and ensures legal compliance in handling sensitive video information [10]. The objective of this ”AI/ML-based Detection of Anomalies and Criminal Activities through CCTV” project is to reduce emergency response times and encourage community involvement in public safety efforts. By alerting both authorities and citizens, the system fosters quicker reactions to potential threats and accidents, thereby contributing to the creation of safer public spaces for all [11]. The global increase in crime is a growing concern, driven by multiple factors such as economic inequality, social instability, and political unrest, which often contribute to a rise in criminal behavior [12][13]. Additionally, advancements in technology have enabled new forms of crime, such as cyberattacks and identity theft [14]. Social challenges, including unemployment, poverty, and limited access to education and healthcare, further push individuals toward engaging in criminal activities [15]. Furthermore, law enforcement agencies are struggling to keep pace with the constantly evolving tactics used by crimi- nals, making it increasingly difficult to effectively control such activities [16]. Addressing these issues requires not only substantial changes in societal, economic, and legal frameworks but also the development of forward-thinking crime prevention methods [17]. Systems capable of detecting criminal activities and anomalies in real-time are particularly essential [18]. Several studies have examined crime detection technologies, focusing on the use of artificial intelligence (AI) and deep learning to enhance the accuracy and speed of crime detection [19]. One such study,” Real-time Crime Detection Using Customized CNN,” details the development of a system that employs a tailored Convolutional Neural Network (CNN) to analyze video feeds in real time [20]. This system provides law enforcement agencies with immediate feedback on criminal activities by processing live video data rapidly [21]. Another study, titled” Malicious Activity Detection in a Safe City Environment,” emphasizes the preparation and manage- ment of data from various crimes, such as fights, shootings, and vandalism [22]. The researchers divided video footage into smaller segments to handle the large volumes of data efficiently. However, the system faced challenges in generalizing its results across different scenarios, and its complexity made interpretation difficult [23]. In conclusion, these studies represent significant advancements in crime detection technology. However, further re- search is needed to address issues such as privacy, system complexity, and adaptability to real-world conditions [1][2]. Tackling these challenges is essential for fully leveraging the potential of AI and deep learning in making urban environments safer [3].

2.1. Challenges with Current Technologies

2.1.1. Privacy and Data Security

Data Breaches: The increase in personal information being shared online has led to frequent data breaches, exposing sensitive information to cyberattacks [5]. Surveillance: Technologies such as facial recognition and tracking devices raise privacy concerns, often implemented without explicit user consent [7]. Weak Encryption: Many systems still rely on outdated or weak encryption protocols, leaving them vulnerable to exploitation [5][9] edge security system that applies

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

2.1.2. Digital Divide

Access Inequality: Not everyone has access to high-speed internet, computers, or mobile devices, creating disparities in education, work, and services [9]. Affordability: Advanced technologies are typically expensive, making them less accessible to low-income communities [9][6].

2.1.3. Environmental Impact

E-Waste: The rapid pace of technological innovation results in frequent device upgrades, which leads to significant amounts of improperly disposed electronic waste [5][18]. Energy Consumption: AI systems, cryptocurrency mining, and data centers consume large amounts of energy, contributing to carbon emissions and environmental degradation [19].

2.2. Google Lookout and Gaps in Current Solutions

Google Lookout: Google Lookout is an AI-based application primarily designed for individuals with visual impairments, helping them interpret their surroundings by recognizing objects, reading text, and scanning documents using their smartphones [19]. Although its primary focus is on accessibility, some of the technologies used in Google Lookout—such as object recognition and AI-based analysis—could be adapted to criminal activity detection through CCTV [9] [18]. Gaps in CCTV-based Solutions: Despite these technological advances, there remain gaps in current CCTV-based solutions for detecting criminal activities, especially in adapting technologies like Google Lookout [9] [17].

2.3. Motivation for Detection of Criminal Activities and Anomalies through CCTV's

The growing importance of public safety has underscored the need for effective crime prevention methods through the analysis of CCTV footage [2][6]. Traditional crime prevention efforts have relied on post-incident investigations, which are often too late to enable timely interventions [8]. However, with advanced AI and machine learning algorithms, analyzing live CCTV footage has become more efficient, enabling the detection of suspicious activities and criminal behaviors in real time [5][6]. This technological approach is essential for improving law enforcement, deterring criminal activity, and raising public awareness for community safety [4][5].

2.4. Critical Issues Overview of Assistive Technologies for the Detection of Criminal Activities

- **Critical Issue One:** Accuracy and Reliability
- **Issue:** Current systems often produce false positives (incorrectly identifying normal activities as suspicious) and false negatives (failing to detect actual criminal activities), wasting resources and allowing crimes to go undetected [10] [14].
- **Solution:** AI models need to be trained with diverse and larger datasets to improve detection accuracy, while deep learning methods can help systems recognize more complex patterns of human behavior, reducing false positives and negatives [11].
- **Critical Issue Two:** Camera Quality and Placement Issue: Many older CCTV systems use low-resolution cameras, which limit their ability to identify individuals, particularly in poor lighting conditions [14].
- **Solution:** Upgrading to high-definition (HD) or ultra-HD cameras equipped with night-vision capabilities can significantly enhance identification accuracy, especially in low-light settings [17].
- **Critical Issue Three:** Privacy and Ethical Concerns Issue: Widespread deployment of CCTV, particularly when integrated with AI and facial recognition, can lead to surveillance overreach, raising privacy concerns [19]. Many citizens feel uncomfortable with constant monitoring, and there is potential for misuse of this data by authorities or private entities [18].
- **Solution:** Data minimization and retention policies should be implemented to address privacy concerns. CCTV footage that does not contain suspicious activity should be promptly deleted [19]. Additionally, anonymizing individuals in public spaces unless suspicious behavior is detected can further enhance privacy Energy Consumption: AI systems, cryptocurrency mining, and data centers consume [19].

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

2.5. Critical Issue Four: Facial Recognition and Biometric Accuracy

- **Issue:** Some facial recognition systems have been found to exhibit racial, gender, and age biases, potentially leading to misidentification and wrongful targeting [18][19].
- **Solution:** AI algorithms need to be tested rigorously to address these biases. Incorporating diverse datasets and additional biometrics, such as voice or gait recognition, can help improve identification accuracy [19].

2.6. Critical Issue Five: Scalability and Resource Constraints

- **Issue:** Large CCTV networks produce vast amounts of video footage, creating challenges for storage and processing [5] [19]. Continuous monitoring of these data streams requires significant human and computational resources.
- **Solution:** Automated AI-based monitoring systems should be developed to reduce the workload on human operators. These systems can prioritize and flag feeds that need attention, thus optimizing the monitoring process [19].

2.7. Critical Issue Six: Cost and Maintenance

- **Issue:** Implementing comprehensive CCTV systems with high-quality cameras, sufficient storage, and AI analytics capabilities demands a significant upfront investment, which can be prohibitive for smaller organizations or municipalities [18].
- **Solution:** Modular upgrades, such as retrofitting existing cameras with AI capabilities or better lenses, offer a more cost-effective alternative to overhauling entire systems [17] [19].

3. Application Impact: Detection of Criminal Activities and Anomalies through CCTV's

The implementation of advanced technologies, such as AI-driven analytics, facial recognition, and behavioral analysis, for detecting criminal activities and anomalies via CCTV systems has had a significant impact across multiple sectors. These innovations are transforming the way crimes are prevented, investigated, and managed. Below is a detailed examination of how CCTV is impacting crime detection and monitoring:

- **Enhanced Public Safety and Crime Prevention:** Proactive Crime Prevention: AI-powered CCTV systems, capable of identifying suspicious behaviors in real-time, allow law enforcement and security teams to intervene before criminal activities escalate [3][6]. Predictive analytics can highlight po-tential risks, such as loitering, aggressive behavior, or abnormal activity patterns, reducing the likelihood of crimes like vandalism, shoplifting, or public disturbances [3][8].
- **Law Enforcement and Investigations: Post-Crime Investigation:** High-quality CCTV footage can be instrumental in investigations after crimes occur. AI techniques like facial recognition, object tracking, and scene analysis help identify suspects, vehicles, and reconstruct sequences of events [4][9]. This leads to faster apprehension of criminals and increases successful prosecution rates [9].
- **Impact on Urban Planning and Smart Cities:** Smart City Integration: As part of smart city infrastructure, CCTV sys- tems enhance safety by integrating with other technologies, such as smart traffic management, public transport systems, and emergency response units [7][11]. For example, AI-driven CCTV can monitor traffic patterns, detect accidents, and assist in crowd management during large public events [12].
- **Corporate and Business Security:** Retail and Business Surveillance: Businesses use AI-enabled CCTV to monitor for theft, fraud, or suspicious activities in real-time. Video analytics can help reduce shrinkage and protect assets [13]. In addition, businesses use these systems to analyze customer traffic, peak hours, and manage employee shifts [11] [13]. Workplace Safety and Compliance: In

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

industrial and corporate environments, CCTV systems are used to monitor compliance with safety regulations and ensure that employees follow established procedures [14].

- **Critical Infrastructure and National Security: Protection of Critical Infrastructure:** Airports, train stations, power plants, and other critical infrastructure facilities benefit from AI- powered CCTV systems that detect unusual behavior, intru- sions, or security breaches [8] [16]. These systems can trigger immediate alerts, helping prevent terrorism or acts of vandal- ism [12].
- **Health and Safety during Public Health Crises: Pandemic Response:** During health emergencies, such as the COVID- 19 pandemic, CCTV systems equipped with thermal cameras and AI-driven analytics have been used to monitor social distancing and detect individuals not wearing masks in public spaces [9]. This technology also aids in ensuring compliance with public health regulations in places like malls, airports, and transportation hubs [14] [19].
- **Reduction in Operational Costs: Automation and Labor Efficiency:** AI-enhanced CCTV systems reduce the need for continuous human monitoring. Instead of requiring operators to watch multiple feeds, AI can prioritize incidents that require human attention, allowing personnel to focus on critical tasks and reducing overall staffing costs [6][9]. Privacy, Ethical, and Legal Impacts: Balancing Surveillance with Privacy: While CCTV systems greatly improve security, they raise concerns about privacy infringement. Public back- lash may occur if surveillance is perceived as invasive or over- reaching [19]. To balance these concerns, transparent policies, data anonymization, and consent protocols are crucial [14].

4. Discussion

This section addresses the benefits, challenges, and broader implications of developing AI-driven CCTV systems for anomaly detection. It considers the relationship between these technologies and existing solutions, real-world challenges they address, and potential advancements in the field:

- **Comparison with Existing Technologies:** Traditional CCTV systems provide video footage but are largely reactive and limited in their ability to recognize patterns or individuals without human oversight[7][12]. In contrast, AI-driven systems offer real-time, autonomous detection capabilities that significantly improve the speed and accuracy of crime detection [10]. AI systems also integrate more seamlessly with larger networks, providing more comprehensive security solutions for cities or transportation hubs [11] [12].
- **Addressing Usability Gaps:** Closing the usability gaps in CCTV systems for detecting criminal activities requires improvements in interface design, reducing false positives, enhancing training, ensuring seamless system integration, and safeguarding privacy [9][19]. By adopting these solutions, both traditional and AI-enhanced CCTV systems can become more accessible, efficient, and user-friendly for operators [14].
- **Real-world Impact on User Independence:** AI-powered CCTV systems greatly reduce reliance on constant human monitoring, enabling real-time detection and providing scalable, automated solutions [12]. These advancements allow for more proactive security measures, faster responses to incidents, and a reduced burden on human operators [13]. Consequently, AI systems enhance operational efficiency for organizations and individuals [16].
- **Implementation Challenges: Data Volume Processing:** CCTV cameras generate massive amounts of video data, which requires real-time processing. Handling such large data volumes without excessive storage or delays is a key challenge [5] [9]. Detecting criminal activities with accuracy demands sophisticated machine learning algorithms capable of differentiating between normal and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

suspicious behaviors [6] [9].

- **Environmental Factors:** CCTV systems often face environmental challenges, such as poor lighting, weather conditions, or crowd density, which can degrade video quality and hinder accurate detection [14] [18].
- **Potential for Offline Functionality:** Implementing offline functionality for CCTV systems could prove valuable in areas where internet access is limited or unreliable, such as remote or rural locations [17]. This could be achieved through edge computing and local data storage, which would process video locally and sync periodically with cloud systems [18]. Offline functionality offers effective solutions for regions with poor connectivity, ensuring security is maintained even in the most remote areas [19].
- **Future Development Opportunities:** The future of detecting criminal activities through CCTV will be driven by advancements in AI, edge computing, and data security technologies [19]. Integrating multimodal data, predictive analytics, and privacy-preserving measures will enhance the effectiveness and ethical considerations of surveillance systems [16] [19]. Additionally, innovations such as drones, robots, and augmented reality (AR) devices will extend CCTV capabilities, making it a powerful tool for law enforcement and crime prevention [18].
- **Impact of the Application on Improving Accessibility for Detection of Criminal Activities:** The integration of advanced technologies to improve the detection of criminal activities through CCTV has significantly impacted public safety, crime prevention, and law enforcement efficiency. Below is a detailed breakdown of the key ways these applications influence crime detection and prevention:
- **Enhanced Crime Detection and Prevention: Real-Time Alerts:** AI-driven CCTV systems analyze footage in real-time, enabling the immediate detection of suspicious behavior, such as theft, vandalism, or assaults [9] [15]. This early intervention allows security personnel or law enforcement to act swiftly, preventing escalation [9].
- **Reduction in Response Times:** By automating crime detection, AI-enhanced CCTV systems reduce the time needed to alert authorities, minimizing the overall impact of criminal activities. This instant notification can help direct law enforcement to the crime location more quickly [6] [10].
- **Predictive Policing:** AI algorithms can predict potential crime hotspots by analyzing historical data and environmental factors, enabling law enforcement to proactively monitor high- risk areas, potentially preventing crimes before they occur [16].
- **Improved Accuracy and Reduced Human Error: Consistent Monitoring:** Unlike human operators, AI-driven CCTV systems are tireless, offering continuous surveillance with high accuracy. These systems can monitor large areas and consistently flag suspicious behavior, thus reducing reliance on human oversight [8][12].
- **Reduced False Positives and Negatives:** Machine learning models trained on diverse datasets improve the accuracy of detecting criminal activities over time, lowering the likelihood of false positives (non-criminal behavior flagged as suspicious) and false negatives (missing actual criminal activities) [17] [18].
- **Deterrence Effect: Visible Surveillance:** The presence of advanced CCTV systems acts as a deterrent to potential criminals, discouraging them from committing crimes in monitored areas [5]. The perception that AI can detect subtle criminal behaviors in real-time increases the perceived risk of being caught, further preventing criminal activity [19].
- **Increased Accountability:** Criminals are more likely to be apprehended when they know they are being recorded, as the footage can serve as critical evidence in court

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

proceedings [10][11].

- **Streamlined Investigations and Evidence Collection: Automated Forensic Analysis:** AI-powered CCTV systems can swiftly review and analyze video footage, allowing investigators to identify suspects and reconstruct events more efficiently [8][11]. This automation reduces the need for manual review, saving time and effort during investigations [12].
- **Improved Evidence Gathering:** High-quality footage, paired with facial recognition and object tracking, enhances law enforcement's ability to link suspects to crimes, providing stronger evidence in court [17] [19].
- **Cost Efficiency and Resource Optimization: Automated Surveillance:** AI-driven CCTV reduces the need for human monitoring, allowing security and law enforcement teams to allocate their resources more effectively [10] [18]. By flagging suspicious activities, these systems help prioritize incidents, improving operational efficiency [12].
- **Wider Coverage with Less Manpower: Scalable Surveillance:** AI-powered CCTV systems enable extensive surveillance across larger areas like smart cities, public transportation networks, and shopping malls [9] [19]. With fewer personnel required to monitor cameras, these systems enhance security across vast regions with minimal manpower [16].
- **Monitoring Dangerous or Remote Areas:** AI-equipped mobile surveillance systems and drones can reach areas that are otherwise difficult to monitor, such as high-crime neighborhoods or disaster zones [11]. This extends CCTV coverage and reduces risks for law enforcement officers [18]. The adoption of advanced technologies in CCTV surveil-lance enhances the detection of criminal activities, providing significant improvements in public safety, operational efficiency, and crime prevention [5][19]. These systems offer real- time monitoring, streamline investigations, and enable predictive policing, leading to quicker law enforcement responses and better resource allocation. However, ethical considerations surrounding privacy, and the continuous evolution of crime, need to be addressed to ensure the effective and fair use of these technologies [19].
- **Recent Research Progress:** Recent advancements in criminal activity detection through Closed-Circuit Television (CCTV) have been driven by innovations in artificial intelligence (AI), computer vision, and machine learning. These breakthroughs aim to improve surveillance accuracy, efficiency, and ethical deployment:
- **Deep Learning Architectures:** Convolutional Neural Net- works (CNNs): Recent improvements in CNN architectures have significantly enhanced object and action recognition in video feeds. Advanced models, such as ResNet and Efficient Net, have been optimized for real-time processing [5] [17]. Vision Transformers (ViTs): ViTs are increasingly used for video analysis, offering superior performance in understanding temporal dependencies and complex patterns in surveillance footage [15].
- **Action and Behavior Recognition: Spatiotemporal Modeling:** Research has focused on improving models' ability to capture both spatial and temporal aspects of activities. Technologies like 3D CNNs and Long Short-Term Memory (LSTM) networks are being combined with transformer models to better understand dynamic behaviors [18]. Anomaly Detection: Unsupervised and semi-supervised learning approaches are being used to detect unusual activities without requiring extensive labeled datasets. Techniques such as autoencoders, Generative Adversarial Networks (GANs), and self-supervised learning show great potential for identifying deviations from normal patterns [18].

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

- **Object Detection Models: YOLO (You Only Look Once):** This algorithm leverages CNNs to quickly identify objects in images and videos, recognized for its speed and accuracy [17]. Faster R-CNN: A region-based object detection model that improves accuracy in classifying images and videos, frequently used for detecting criminal behaviors [18] [19]. The integration of these technologies continues to refine the efficiency and effectiveness of CCTV-based criminal detection systems.
- **Recent Research Progress:** Recent advancements in criminal activity detection through Closed-Circuit Television (CCTV) have been driven by innovations in artificial intelligence (AI), computer vision, and machine learning. These breakthroughs aim to improve surveillance accuracy, efficiency, and ethical deployment:
- **Deep Learning Architectures:** Convolutional Neural Networks (CNNs): Recent improve- ments in CNN architectures have significantly enhanced object and action recognition in video feeds. Advanced models, such as ResNet and EfficientNet, have been optimized for real-time processing[5][17].
- **Vision Transformers (ViTs):** ViTs are increasingly used for video analysis, offering superior performance in understanding temporal dependencies and complex patterns in surveillance footage [15].
- **Action and Behavior Recognition: Spatiotemporal Modeling:** Research has focused on improving models' ability to capture both spatial and temporal aspects of activities. Technologies like 3D CNNs and Long Short- Term Memory (LSTM) networks are being combined with transformer models to better understand dynamic behaviors [18].
- **Anomaly Detection:** Unsupervised and semi-supervised learning approaches are being used to detect unusual activities without requiring extensive labeled datasets. Techniques such as autoencoders, Generative Adversarial Networks (GANs), and self-supervised learning show great potential for identifying deviations from normal patterns [18].

- **Object Detection Models: YOLO (You Only Look Once):** This algorithm leverages CNNs to quickly identify objects in images and videos, recognized for its speed and accuracy [17]. Faster R-CNN: A region-based object detection model that improves accuracy in classifying images and videos, frequently used for detecting criminal behaviors [18] [19]. The integration of these technologies continues to refine the efficiency and effectiveness of CCTV-based criminal detection systems.

4.1. Research Trends and Open Questions

The field of detecting criminal activities through CCTV surveillance is advancing rapidly, driven by breakthroughs in artificial intelligence (AI), machine learning, and computer vision. However, along with these innovations, the field is also grappling with various research trends and open questions that present both opportunities and challenges for future development. Here's a detailed look at the current research trends and open questions in this area.

4.2. Research Trends

- **Deep Learning and Computer Vision Advancements Trend:** Deep learning models, particularly convolutional neural networks (CNNs) and transformers, have revolutionized criminal activity detection. These models can autonomously extract features from video feeds, improving the ability to detect objects, people, and actions in real-time [5] [17].
- **Example:** Vision Transformers (ViTs) and 3D Convolutional Neural Networks (3D CNNs) are increasingly being used to analyze spatiotemporal patterns in video data, enabling systems to recognize suspicious behaviors [5] [17]. Focus: The goal is to enhance model accuracy, minimize false positives and negatives, and optimize models for real-time deployment [6] [9].
- **Behavioral Analysis and Anomaly Detection: Trend:** Anomaly detection

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

models are becoming more sophisticated at identifying unusual behaviors in large public spaces. These models often utilize unsupervised or semi-supervised learning techniques to detect deviations from typical behavioral patterns [9] [19].

- **Example:** Autoencoders, Generative Adversarial Net- works (GANs), and graph-based learning approaches are being applied to detect anomalies such as loitering, crowd formations, or aggressive movements [7] [18].
- **Focus:** Improving robustness in anomaly detection to reduce false alarms and improve system adaptability across diverse environments and behaviors [5][7].
- **Multimodal Surveillance Systems: Trend:** There is growing interest in integrating multiple data sources (e.g., audio, thermal, and infrared) alongside video feeds to improve detection accuracy and reduce ambiguities in identifying criminal activities [19].
- **Example:** Combining audio signals like gunshots or screams with video footage can help systems respond more effectively to violent incidents in real-time [19].
- **Focus:** Developing algorithms that efficiently fuse multimodal data while maintaining accuracy and scalability [6] [19].
- **Edge Computing and Real-Time Processing: Trend:** With improvements in hardware, such as AI accelerators, the focus is shifting towards deploying surveillance systems at the edge for real-time detection. This approach reduces latency and minimizes the need for high-bandwidth data transmission to central servers [18].
- **Example:** Lightweight models optimized through techniques like quantization, pruning, and knowledge distillation are being deployed on edge devices such as smart cameras or drones [19].
- **Focus:** Ensuring high accuracy while maintaining computational efficiency on resource-limited devices [18] [19].
- **Federated Learning and Privacy-Preserving Techniques: Trend:** Privacy concerns surrounding CCTV surveillance are pushing the adoption of federated learning, which enables models to be trained on decentralized devices without transferring sensitive data to central servers [19]. **Example:** Federated learning frameworks allow local video data to be processed on-site, sharing only model updates to ensure data privacy [19].
- **Focus:** Striking a balance between privacy and accuracy while ensuring that models remain efficient [16] [19].

4.3. Open Questions and Future Directions

4.3.1. How to Balance Privacy with Security? How to Balance Privacy with Security?

- **Question:** How can surveillance systems maintain a balance between crime detection and the protection of individual privacy rights?
- **Challenge:** Increasing concerns about mass surveillance and the potential misuse of personal data emphasize the need to design systems that operate within ethical and legal frameworks [18]. Technologies such as differential privacy and anonymization techniques can help protect privacy but may reduce system effectiveness [19].
- **Future Direction:** Research into privacy-preserving techniques that do not compromise detection accuracy, such as encrypted data processing or anonymized behavior analysis, will be crucial [19].

4.3.2. How to Mitigate Algorithmic Bias in Crime Detection? Question: How can surveillance systems avoid reinforcing biases in crime detection and prosecution?

- **Challenge:** AI models often reflect the biases present in their training datasets, leading to disproportionate targeting of certain demographic groups [17]. This bias can undermine the fairness of the criminal justice system [19].
- **Future Direction:** Transparent and explainable AI systems, along with auditing

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

for fairness and using diverse, representative datasets, are essential for mitigating bias [19].

4.3.3. Can AI Systems Handle Real-World Complexity? Question: How can AI systems be made robust enough to handle the unpredictability and complexity of real-world environments?

- **Challenge:** Surveillance environments vary significantly, with changing lighting, weather conditions, and crowd densities. Current models often struggle to generalize across different environments, leading to false positives or missed detections [16].
- **Future Direction:** Research into self-learning, adaptive AI models that can adjust to environmental changes in real-time is ongoing. The development of models that can learn with minimal data or through unsupervised methods is critical to solving this challenge [19].

5. Methodology

In this study, we will employ a specific algorithm to identify individuals and detect surveillance targets. For the detection system, we will utilize a deep learning algorithm known as Region-based Convolutional Neural Network (R-CNN). Similar to traditional CNNs, we will create an image and segment it into regions. Each segment will be treated as a separate image and processed through the CNN, allowing us to classify these segments into various categories [10] [16]. After segmenting the regions, each will be assigned to a specific class, and all regions will be merged to reconstruct the original image containing the detected objects [11] [17]. The object will then enter the network, passing through different layers and pathways, allowing us to obtain the classification for each object [10]. The primary focus of using R-CNN is its ability to handle numerous regions extracted from an image. The large number of regions can be evaluated to check if any of them contain the objects of interest. The R-CNN process involves the following steps: Input an image. Create an initial segmentation to form several regions. Combine similar and interrelated regions based on attributes such as color, texture, size, and shape harmony to form distinct regions [19]. However, R-CNN has certain limitations that can be addressed by using Faster R-CNN. The most time-consuming aspect of R-CNN is the region proposal process. Faster R-CNN replaces this cumbersome step with a more efficient method using a network called the Region Proposal Network (RPN), which generates regions of interest[12][16]. Additionally, Faster R- CNN introduces the concept of anchors to improve detection performance. Next, we will utilize the OpenCV library for motion estimation and pose tracking. Previous implementations encountered challenges when detecting a person holding a knife, as the system struggled to recognize both the individual and the weapon[19]. To improve this, we will implement motion estimation using optical flow to determine the average velocity of objects between successive frames. This technique calculates a two-dimensional vector field, where each vector represents the movement of a point from the first frame to the subsequent one[18]. This is critical for our design, as it allows us to detect both the individual and the knife effectively. We will set hypotheses to aid in this process: The pixel intensities at a point remain relatively unchanged between frames. Pixels exhibiting similar movements across frames are indicative of motion [19]. In scenarios with poor lighting, our algorithm might struggle to detect the knife. To address this, we will apply gamma correction to enhance the brightness of the frames [17]. However, it is important to note that gamma correction can lead to image blurring, so we must determine an optimal gamma correction value that enhances visibility without compromising the clarity of the object [12].

Conclusion

In summary, the “AI/ML-based Detection of Anomalies and Criminal Activities through CCTV” project represents a significant effort to utilize cutting-edge technologies aimed at enhancing public safety and security. By leveraging advanced artificial intelligence and machine learning techniques, this project seeks to transform how we monitor and respond to criminal activities and anomalies detected in real-time CCTV footage [9] [19]. The application of AI in detecting criminal activities through CCTV systems signifies an important intersection between technology and public safety, facilitated by ongoing advancements in artificial intelligence, machine

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

learning, and computer vision [10] [19]. By employing robust methodologies such as object detection, action recognition, and anomaly detection, modern surveillance systems can proactively identify and alert authorities to potential criminal behavior in real-time. This not only enhances security measures but also enables a more effective allocation of resources for crime prevention and intervention [6] [11]. The comprehensive System Requirements Specification (SRS) document, meticulously organized and continually improved, serves as the foundation for this project, providing a clear roadmap for its development[12] [17]. With an emphasis on real-time analysis, location-based alerts, community involvement, and user-friendly interfaces, this design has the potential to expedite emergency responses, empower communities, and foster safer public spaces [12] [18]. As we embark on this journey, collaboration among stake- holders, rigorous adherence to requirements, and adaptability to evolving needs will be crucial for the successful implementation of this transformative system [11] [19]. However, deploying such systems requires careful attention to several critical factors, including ensuring data accuracy, minimizing false positives, designing for real-time processing, addressing privacy concerns, and safeguarding against biases in detection models [6] [14]. Moreover, ongoing system updates and performance evaluations are essential to maintaining the system's effectiveness in ever-changing environments [18]. When implemented responsibly, CCTV-based crime detection systems offer a promising tool for enhancing public safety while building trust through transparency and ethical operation. Striking a balance between security and privacy will be vital for the long-term success and societal acceptance of these technologies [19].

References

[1]. Li, X., Wu, D., and Yang, G.(2020). " Anomaly Discovery in Surveillance vids A Review. " IEEE Access, 8, 1- 17. This paper provides a detailed review of various ways used in anomaly discovery in surveillance systems, including machine learning approaches.

[2]. Sultani, W., Chen, C., and Shah, M.(2018). " Real- World Anomaly Discovery in Surveillance vids. " Proceedings of the IEEE/ CVF Conference on Computer Vision and Pattern Recognition(CVPR). This paper introduces a new approach to descry real-world anomalies in surveillance vids using deep knowledge ways.

[3]. Radovic, M., and Spalevic, P.(2021). " RealTime Crime Discovery System Using YOLOv5 and Deep knowledge in CCTV. " Journal of Applied Artificial Intelligence, 35(7), 532- 547. The paper demonstrates the operation of YOLOv5 in real- time discovery of lawless exertion, including its performance evaluation.

[4]. Popoola, O. P., and Wang, K.(2012). " videotapeGrounded Abnormal mortal behavior Recognition — A Review. " IEEE Deals on Systems, Man, and Cybernetics, 42(6), 865- 878. This paper provides a comprehensive overview of videotapegrounded mortal behavior recognition, which is essential for detecting suspicious exertion.

[5]. Ahmed, M., Mahmood, A. N., Hu, J.(2016). A check of network anomaly discovery ways.

[6]. Gupta, P.(2021). " Intelligent Surveillance System for Crime Detection using Deep knowledge. " Master's Thesis, University of XYZ. This thesis explores the performance of deep knowledge algorithms in erecting an intelligent surveillance system for crime discovery.

[7]. Tripathi, S., and Singhal, A.(2021). " Felo10 nious exertion Discovery Using Deep knowledge A Survey. " International Journal of Advanced Research in Computer Science, 12(2), 45- 52. This check paper provides perceptivity into how deep knowledge algorithms are being used for lawless exertion discovery in video footage.

[8]. Kumar, A., zhang, D.(2020). An Overview of video surveillance systems for lawless exertion discovery. IEEE Dispatches checks Tuturials, 22(3), 1682- 1705.

[9]. Buch, R., Velastin, S. A., and Orwell, J.(2018). " A Review of Computer Vision

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 921-932
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0132

ways for the Analysis of Urban Traffic. " IEEE Deals on Intelligent Transportation Systems, 19(2), 466- 481. Though concentrated on business analysis, this review discusses object discovery and shadowing ways applicable in broader surveilance.

[10]. S. S, H. M, D. T and S. S, " Real- time Crime Discovery Using tailored CNN, " 2022 1st International Conference on Computational Science and Technology(ICCST), CHENNAI, India, 2022, pp. 416- 419, doi 10.1109/ ICCST 55948.2022.10040379.

[11]. Jan and G. M. Khan, " vicious exertion Discovery In Safe City Environment, " 2021 International Conference on Artificial Intelligence(ICAI), Islamabad, Pakistan, 2021, pp. 170- 174, doi / ICAI 52203.2021.9445254.

[12]. N. Y. Katkar and V. K. Garg, " Discovery and Tracking the Felonious exertion using Network of CCTV cameras, " 3rd International Conference on Smart Electronics and Communication(ICOSEC), Trichy, India, 2022, pp. 664- 668, doi / ICOSEC 54921.2022.9952104.

[13]. V. V. Nojor et al., " Design of a Deep literacy- grounded Discovery System for Felonious Conditioning, " 2022 3rd International Informatics and Software Engineering Conference(IISEC), Ankara, Turkey, 2022, pp. 1- 5, doi 10.1109/ IISEC 56263.2022.9998276.

[14]. CamNuvem A Robbery Dataset for videotape Anomaly Discovery https// www.ncbi.nlm.nih.gov/pmc/articles/PMC9784719/

[15]. Real- world Anomaly Discovery in Surveillance vids https// www.crcv.ucf.edu/projects/realworld/

[16]. videotape anomaly discovery system using deep convolutional and intermittent models https// www.sciencedirect.com/science/article/pii/S2590123023001536

[17]. Book "Deep Learning Adaptive Computation and Machine Learning series", Authors Ian Goodfellow, Yoshua Bengio, Aaron Courville, Edition illustrated, Publisher MIT Press, 2016.

[18]. Book Title " Computer Vision ", Book Subtitle Algorithms and operations, Authors Richard Szeliski, Series Title textbooks in Computer Science, Publisher Springer Cham.

[19]. Book " hands- on machine literacy with scikit- learn, keras, and tensorflow ", Author Aur´elien G´eron, Released September 2019, Publisher(s) O'Reilly Media, Inc, ISBN 978149203264

[20]. Sonawane, V.D., Mahajan, R.A., Patil, S.S., Bhandari, G.M., Shivale, N.M., Kulkarni, M.M., "Predicting Software Vulnerabilities with Advanced Computational Models", Advances in Nonlinear Variational Inequalities, 2024, 27(4), pp. 196–212

[21]. Shivale, N.M., Mahajan, R.A., Bhandari, G.M., Sonawane, V.D., Kulkarni, M.M., Patil, S.S., "Optimizing Blockchain Protocols with Algorithmic Game Theory", Advances in Nonlinear Variational Inequalities, 2024, 27(4), pp. 231–246

[22]. Patil, S.S., Mahajan, R.A., Sonawane, V.D., Shivale, N.M., Kulkarni, M.M., Bhandari, G.M., "Deep Learning for Automated Code Generation: Challenges and Opportunities", Advances in Nonlinear Variational Inequalities, 2024, 27(4), pp. 247–265.

[23]. Kulkarni, M.M., Mahajan, R.A., Shivale, N.M., Patil, S.S., Bhandari, G.M., Sonawane, V.D., "Enhancing Social Network Analysis using Graph Neural Networks", Advances in Nonlinear Variational Inequalities, 2024, 27(4), pp. 213–230.