

The Use of Artificial Intelligence in Early Detection of Security Threats through CCTV Systems

Literature Review

1. Propounding First Artificial Intelligence Approach for Predicting Robbery Behavior Potential in an Indoor Security Camera

This paper hypothesizes the use of AI in indicating the robbery possibility in indoor security cameras. The technique has three detection modules, such as head cover, crowd and loitering detection. The initial two modules are rooted in the retraining of the YOLOV5 model using a manually labeled dataset and loitering detection is performed using the DeepSORT algorithm. Final predictions on whether the robbery is possible are then carried out using a fuzzy inference machine. The research had an F1-score of 0.607 in identifying the robbery and this indicates the effectiveness of the research study. Nonetheless, the problem of varied angles of surveillance and low-end images is identified as an impediment to practical application. This study will provide a considerable contribution to the field of situational awareness enhancement in control centers and provide predictive services that may assist in preventing cases of robberies.

2. Big Data Enabled Real-Time Crowd Surveillance and Threat Detection Using Artificial Intelligence and Deep Learning

The survey explores the significance of AI and deep learning in real-time surveillance and threat detection of crowds. The issue of the labor-intensive human surveillance and the enhancement of the AI methodologies that enhance the detection of abnormal events are discussed in the paper. In the era of widespread use of surveillance cameras in the open and privacy areas, AI has become an important factor in improving security. The review of more than 150 articles identifies the multiple machine learning and deep learning algorithms that were applied to foretell the pattern of crimes. Although the paper provides in-depth information on the methods, it does not feature any practical reviews in various real-world situations, which is why more applied research

is required. Moreover, although the process of integrating IoT and computer vision is emphasized, additional research on their joint work in the field of work is needed.

3. Artificial Intelligence-Based Detection System of Critical Events for Road Security

This paper presents the Artificial Intelligence-powered Detection System of Road Security (ADEROS), which is aimed at improving the security and movement of traffic at problematic crossroads and railways crossings. The system integrates the process of detecting objects, computer vision and image processing to observe and analyze traffic. It identifies suspicious situations and dangerous situations in real-time, and uses the YOLOv4 deep neural network model to detect road participants, including vehicles and pedestrians. The system also checks the conditions of safety gadgets such as traffic lights and railway gates. Real-life application and experimental findings indicated better safety outcomes. Nevertheless, the prototype of the system currently available needs development further to be applied to large-scale usage and testing in a variety of traffic conditions. Although this is promising, the study is limited in the scope of applicability because it focuses on pilot projects.

4. Artificial Intelligence-Based Smart Security System Using Internet of Things for Smart Home Applications

The paper describes the creation of an AI-assisted smart security solution on the basis of IoT technology in smart homes. The system uses AI-based video processing methods including motion and face recognition to enhance home security. The paper examines different AI and IoT solutions, their applicability in video processing and smart home solutions. The findings indicate that the combination of AI and IoT improves the overall security system and provides real-time notification as well as better security control. Nevertheless, issues of system integration, real-time processing and device compatibility were also pointed out. The research indicates that the performance of the system can be optimized in the future to solve integration problems and enable the system to be more efficient in a smart home setting.

5. Artificial Intelligence in Video Surveillance Systems for Suspicious Activity Detection and Incident Response: A Systematic Review

This is a systematic review that examines how AI has helped to improve video surveillance systems to detect suspicious activity and respond to it in an incident. The article has analyzed 145 papers in databases such as Scopus and IEEE Xplore, with attention to such AI technologies as computer vision, edge computing, and deep learning. It marks the main tendencies of AI integration in surveillance and how the technologies enhance detection accuracy and efficiency. The ethical aspects of AI in surveillance are also discussed in the review as per the privacy issue. Although the study is very broad-based, it lacks empirical evidence of a real-life implementation, thus making it possible to state that additional research is required to confirm the usefulness of AI systems in various settings.

6. Integrated and Automated CCTV System: A Comprehensive Review of Current Challenges and Methods, Future Trends and Prospects for Emerging Electronics Engineering with AI Integration

In this conference paper, the systematic review of CCTV surveillance systems history exposes the overview of the developments of the conventional recording-based surveillance systems to the full-fledged and AI-enhanced intelligent surveillance systems. The research finds significant drawbacks on traditional CCTV system such as poor image quality, high false alarm rates, lack of flexibility and poor integration with other building management system. It talks about how new developments in the electronics engineering and artificial intelligence have been used to create automated CCTV systems that combine intelligent analytics, multi-sensor designs, networking solutions, and building controls. An analog, IP-based, and AI-enhanced CCTV systems are also compared in the paper, with the latter being superior to the former. In addition, it provides the trends of the future including edge computing, predictive analytics, and smart building integration. Nonetheless, being a review study it fails to provide empirical performance validation in actual working environments.

Commentary of Previous Studies

1. Technological Advancements and Strengths

- **Shift from Reactive to Predictive Surveillance:**

The majority of the studies show that the traditional systems of CCTV with the focus on recordings are replaced by AI-based predictive models that can identify the threat at an early stage, i. e. predict robbery behavior and detect a threatening event.

The execution of this involves deploying Deep Learning Models to enhance the existing QI procedures.

- **Integration of Deep Learning Models:**

Maximally advanced object detection algorithms (e.g., YOLO variants), trajectory tracking and behavioral analysis models have a substantial impact on detection accuracy and real-time performance.

- **Real-Time Monitoring and Automation:**

Some of these systems have automated decision-making systems, which decrease the use of human operators and increase situational awareness.

- **IoT and Smart Infrastructure Integration:**

Other works emphasize integration with IoT devices, smart homes, or intelligent transportation systems, which represents a general shift in favor of smart city ecosystems.

2. Methodological and Technical Limitations

- **Reliance on Controlled or Simulated Environments:**

Many studies confirm their systems in laboratory experiments, simulations or pilot implementations, and do not provide a generalization to real-world large-scale CCTV networks.

- **Limited Scalability Assessment:**

Little literature deals with the performance of their proposed systems to high data loads, multi-camera networks, or to other environmental conditions (lighting, weather, occlusion).

- **Performance Metrics Without Operational Context:**

Most of the papers are reporting F1-score, precision, accuracy, but little consideration is given to the computational cost, latency, long-term maintenance, and infrastructure constraints.

- **Narrow Threat Scope:**

Other models concentrate on a particular threat (e.g. robbery or road cases) without considering performance in a wide and dynamic security situation.

3. Ethical, Governance, and Deployment Gaps

- **Insufficient Privacy and Ethical Considerations:**

Technical studies tend to ignore the problem of data privacy, informed consent, transparency and the possibility of abuse of surveillance technologies.

- **Lack of Governance Framework Integration:**

Not many systems use regulatory compliance or AI governance models in their architectural design.

- **Cybersecurity Risks and Data Protection:**

Despite the sensitive nature of real time data that is carried out by surveillance systems, there is little discussion on the security of data transmission and storage as well as control over vulnerability.

- **Gap Between Innovation and Sustainable Deployment:**

New trends like edge computing and predictive analytics are suggested but effective models of deployment that are cost-effective, performant, and ethically responsible are still underdeveloped.

The literature reviewed affirms the dramatic ability of artificial intelligence to improve early detection of security threats using CCTV. Nevertheless, there is still a obvious disjunction between high accuracy experimental models and scalable, ethically controlled, real world implementation structures. The future research directions include a combination of large-scale validation, benchmark evaluation standards, the inclusion of ethical compliance, and hybrid edge-cloud systems in the future to guarantee sustainable and accountable AI-driven surveillance systems.

Summary of Previous Studies

No .	Study	Authors	Year	Research Type	AI Techniques Used	Key Contributions	Main Limitations
1	Propounding First AI Approach for Predicting Robbery Behavior Potential	Pouyan et al.	2023	Experimental	YOLOv5, DeepSORT, Fuzzy Inference	Early robbery behavior prediction using multi-module detection (head cover, crowd, loitering)	Sensitive to camera angle, low resolution, limited threat scope
2	Big Data Enabled Real-Time Crowd Surveillance and Threat Detection	Bhagat et al.	2024	Survey Review	Machine Learning, Deep Learning, Computer Vision	Comprehensive review of abnormal event detection and crime prediction methods	Lacks empirical validation and real-world performance comparison

3	ADEROS: AI-Based Detection System for Road Security	Kiac et al.	2023	Experimental / Pilot Deployment	YOLOv4, Object Detection, Computer Vision	Real-time detection of critical road events and smart traffic monitoring	Limited scalability testing, prototype-based implementation
4	AI-Based Smart Security System Using IoT for Smart Homes	Sabit	2025	Experimental	Face Recognition, Motion Detection, IoT Integration	Smart home AI surveillance with real-time alerts and automation	Integration complexity, hardware dependency
5	AI in Video Surveillance for Suspicious Activity Detection	Cabanillas - Carbonell et al.	2025	Systematic Review	Deep Learning, Edge Computing, Computer Vision	Comprehensive review of AI trends in surveillance aligned with SDG 16	Limited empirical validation, lacks deployment frameworks
6	Integrated and Automated CCTV System with AI Integration	Pistol et al.	2025	Review / Comparative Analysis	AI-Enhanced CCTV, Edge Computing, Predictive Analytics	Comparison of analog, IP, and AI-enhanced CCTV systems; future trends	No experimental validation, mostly conceptual analysis

References

- Pouyan, S., Charmi, M., Azarpeyvand, A., & Hassanpoor, H. (2023). Propounding first artificial intelligence approach for predicting robbery behavior potential in an indoor security camera. *IEEE Access*, 11, 1–15.
- Bhagat, S. N., Hanchate, D. B., & Bere, S. S. (2024). Big data enabled real-time crowd surveillance and threat detection using artificial intelligence and deep learning. *International Journal of Creative Research Thoughts (IJCRT)*, 12(5), 2320–2882.
- Kiac, M., Sikora, P., Malina, L., Martinasek, Z., & Srivastava, G. (2023). ADEROS: Artificial intelligence-based detection system of critical events for road security. *IEEE Systems Journal*, 17(4), 1–12.
- Sabit, H. (2025). Artificial intelligence-based smart security system using Internet of Things for smart home applications. *Electronics*, 14(3), 608.
- Cabanillas-Carbonell, M. A., Rivera, J. S., & Muñoz, J. S. (2025). Artificial intelligence in video surveillance systems for suspicious activity detection and incident response: A systematic review. *Advances in Science and Technology – Research Journal*, 19(3), 389–405.
- Pistol, N.-C., Alexandrescu, B., & Constantinescu, R.-C. (2025). Integrated and automated CCTV system: A comprehensive review of current challenges and methods, future trends and prospects for emerging electronics engineering with AI integration. In *Proceedings of the 2025 10th International Conference on Emerging Electronics Engineering*. IEEE.