

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

Prepared by

Mohammed faez Almania

List of Contents

Abstract	3
Chapter 1	3
Introduction	3
Background	5
Problem Statement	6
Research Objectives	8
Scope of the Study	9
Chapter 2	9
Literature Review	9
Commentary of Previous Studies	14
Chapter 3	17
Research Methodology	17
Expected Results	17
Gantt Chart (Timeline)	18
References	19

Abstract

This paper seeks to examine how artificial intelligence (AI) can be used to improve the early warning of security issues using CCTV surveillance systems. The growing dependence of video surveillance in other industries has rendered conventional surveillance systems ineffective because of the human factor and the escalating magnitude of the information produced by surveillance cameras. Thus, the use of AI technologies is now fundamental to enhance the efficiency and effectiveness of surveillance. The research uses the descriptive-analytical methodology of reviewing and analyzing the past literature connected to the usage of AI in video monitoring. It dwells upon major AI methods like machine learning, deep learning, and computer vision, which are applied in analyzing video data and identifying abnormal or suspicious actions in a real-time manner. The results demonstrate that AI-enhanced surveillance systems are capable of increasing the accuracy of detections and the speed of response and decreasing human error. Nevertheless, the paper also notes that there are also a number of challenges such as high costs of implementation, issues of data privacy, and system integration. The study finds that AI in CCTV systems can result in smarter, proactive, and efficient security solutions, and suggests additional research to overcome technical and ethical challenges to implement it in the real world.

Chapter 1

Introduction

Over the past few years, the vigorous development of surveillance tools has greatly reshaped contemporary security systems within the government and the corporate world. Video surveillance and especially Closed-Circuit Television (CCTV) has been an essential aspect in the surveillance of environments like transportation systems, smart cities, banks and homes. Nevertheless, old surveillance systems heavily depend on the human-based surveillance that is inefficient because of human factors, including fatigue, decreased attention, and the inability to observe various video streams in parallel (Şengönül et al., 2023).

As the number of surveillance cameras all over the world grows exponentially, the amount of video data generated is now too big to be analyzed effectively by humans. Anomaly detection (often referred to as detecting abnormal or suspicious activities) is a major challenge, given that these events are relatively infrequent and hard to predict and model (Şengönül et al., 2023). This means that a lot of critical occurrences can remain unnoticed or will not be detected timely and this can result in severe security issues.

Artificial Intelligence (AI) is a potent instrument to overcome these limitations to improve surveillance systems. By using AI methods, especially machine learning and deep learning, large-scale video data can be analyzed automatically, and systems can find patterns in it, detect anomalies, and determine suspicious behaviors in real-time. As an example, object detection, facial recognition, and behavior analysis can be used in AI-based surveillance systems to enhance the accuracy of threat detection and response time (Cadet et al., 2024).

Furthermore, the new AI-powered surveillance modules are being more and more oriented to work in real-time conditions, incorporating sophisticated data processing frameworks and edge computing devices to minimize delays and increase the effectiveness of decision-making. Such systems can receive numerous sources of data, such as video feeds and sensors, and provide a wide coverage of proactive threat detection (Cadet et al., 2024). Consequently, AI is transforming surveillance in the reactive model, which relies on the analysis of recorded videos, into a proactive and predictive paradigm, which is able to avert incidents before they happen.

Moreover, there are recent developments in computer vision algorithms including YOLO (You Only Look Once) which have greatly enhanced the speed and accuracy of criminal activity

detection in live video feeds. These technologies enable surveillance systems to detect threats like theft, intrusion, and unauthorized access with a high degree of accuracy and consequently, improve on the overall security and safety (Venkatesh et al., 2024).

Thus, this paper aims to explore the potential of artificial intelligence to help improve early warning of security threats by using CCTV surveillance systems, with a specific emphasis on the ability to provide real-time surveillance, the accuracy of detections, and the possibility of handling the practical issues related to the implementation of AI-based surveillance systems in the real world.

Background

The use of Artificial Intelligence has emerged as a key component of intelligent surveillance systems development, especially the area of anomaly detection in video streams. Anomalies refer to something that is not within the usual behavioral pattern and are usually rare and complex and can be hard to identify with traditional rule-based systems (Şengönül et al., 2023). This has given rise to the use of data-based AI techniques that are able to learn patterns based on large volumes of data and detect deviations automatically.

The techniques of machine learning and deep learning are very important in this case. The approaches allow systems to derive meaningful features of the video data, categorize objects and study behaviors across time. Particularly, deep learning models have been shown to be very effective in dealing with unstructured data like images and videos and, hence, they are applicable in surveillance tasks. Nevertheless, the issue of data accessibility persists due to the lack of abnormal events, which is hard to train and train on because they are rare and hard to recreate (Şengönül et al., 2023).

Besides that, AI-based surveillance systems frequently also support real-time data processing architectures to support the volume and speed of incoming data. Low-latency analysis is achieved with technologies like stream processing frameworks (e.g., Apache Kafka and Apache Flink), which process data more near its origin to reduce network congestion and enhanced response

times with edge computing (Cadet et al., 2024). These developments promote surveillance systems to work effectively in dynamic and large-scale settings.

The other significant observation of AI-based surveillance is that it is used in vital areas like banking and other security sensitive establishments. AI-powered intelligent surveillance cameras can be used to carry out more complex tasks like face recognition, access control, and intrusion detection. These systems may also be able to automatically detect unauthorized persons, issue alarms, and issue real-time notifications, which improves the security level and minimizes human intervention (Kumar et al., 2023).

More than that, the AI-based video surveillance systems utilize the advanced object detection algorithms to track the activities in real-time and precisely. Indicatively, using YOLO-based models enables systems to recognize and monitor objects in real-time, enabling quick identification of suspicious activities and taking timely measures (Venkatesh et al., 2024). This helps in forming safer environments, and contributes to proactive crime prevention measures.

In spite of these developments, there are a few challenges such as scalability, data privacy, system integration and cost of the computation. Hence, it is imperative to continue research on how to create more capable, efficient, and ethical AI-based surveillance systems that can be successfully used in practice.

Problem Statement

Video surveillance systems are now one of the most important means of ensuring security in the open areas, transport system, intelligent cities, and at individual premises. Conventional Closed-Circuit Television (CCTV) systems are mostly based on continuous recording and human being watching. Nonetheless, this method has a number of limitations, because human operators are likely to have fatigue, lack of concentration, and could not handle several video streams in a single instance. Consequently, suspicious acts or possible threats might not be noticed at all or on time to stop incidences.

According to recent research, it is expected that artificial intelligence (AI) plays an increasingly important role in enhancing the efficiency and effectiveness of surveillance systems. Computer

vision, deep learning, and object detection algorithms are AI techniques that can be used to analyze video streams and identify abnormal actions or suspicious events in real-time automatically. Indicatively, Pouyan et al. (2023) suggested an AI-powered system that foretells the characteristics of robbery in indoor areas through numerous detecting modules such as head cover identification, crowd recognition, and loitering determination. Their system also showed that AI models like YOLOv5 and DeepSORT would be practical in detecting suspicious activities but the results were influenced by other factors like camera angle and poor quality of captured images.

Correspondingly, Bhagat et al. (2024) focused on the significance of artificial intelligence and big data technologies when it comes to real-time surveillance of crowds and identification of threats. Their review indicated the potential to increase the detection rate of abnormal events in large scale surveillance settings using machine learning and deep learning models. The study, however, also indicated that most of the developed solutions have not been practically tested under real-world conditions and this limits the effectiveness when they are implemented in complex environment.

The application of AI-based systems in certain security situations is discussed in other studies. As an example, Kiac et al. (2023) have created the ADEROS system, where the computer vision and deep learning model are used to identify the most crucial events on the road traffic using the YOLOv4 model. Although the system proved to be more effective in terms of safety monitoring when it was tested in an experimental setting, its scalability and use in a wide range of environments have not been well-developed.

Moreover, AI surveillance systems are combined with Internet of Things (IoT) to improve the security of smart houses. Sabit (2025) suggested a smart security system that has AI capabilities and implements video processing methods including motion detection systems and face recognition to enhance surveillance and offer real-time notifications. The need to have a more automated and responsive system has been achieved, although issues concerning the integration of the systems and compatibility with hardware were noted.

Although these are the technological advancements, there are still a number of research gaps. Most of the currently available literature has addressed particular threat scenarios, as opposed to offering end-to-end systems that can identify multiple forms of suspicious behaviors in large scale surveillance networks. Besides, other papers note the performance metrics like accuracy or F1-score, but do not adequately cover the practical deployment problems like the scalability, computational cost, and the infrastructure requirements (Cabanillas-Carbonell et al., 2025; Pistol et al., 2025).

Thus, it is necessary to conduct additional research to explore the potential of utilizing the artificial intelligence methods in the CCTV surveillance systems to improve the timely identification of security-related threats and overcome the practical operational difficulties. This study will examine how AI-driven surveillance systems can be used and can help in the creation of smarter and more efficient security surveillance mechanisms.

Research Objectives

The primary aim of the study is

- to investigate how artificial intelligence can improve the process of early detection of any security threats using CCTV surveillance systems.

The objectives of this study are specific and they include:

- To determine the weaknesses of the conventional surveillance systems used in CCTV to identify suspicious behaviors and security threats.
- To study the use of artificial intelligence methods, such as computer vision and deep learning, in video surveillance.
- To examine available AI-based models of suspicious activity detection on CCTV footage.
- To determine how well the AI-enabled surveillance systems enhance real-time threat detection.
- To determine the technical and operational obstacles related to the implementation of the systems based on AI-driven CCTV in a real-life setting.

Scope of the Study

In this research, the author concentrates on how artificial intelligence can be used to enhance early identification of security threats by CCTV systems. It investigates AI methods including machine learning and computer vision to analyze video data on-the-fly. The research is confined to AI-driven video surveillance systems in such settings as community areas and intelligent systems. It further takes into consideration system performance and implementation issues, but does not produce a real system, rather based on analytical and literature-based methods.

Chapter 2

Literature Review

1. Propounding First Artificial Intelligence Approach for Predicting Robbery Behavior Potential in an Indoor Security Camera(Pouyan et al.,2023).

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(Bhagat et al.,2024)

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(Kiac et al.,2023).

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(Sabit,2025)

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(Cabanillas-Carbonell et al.,2025).

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(Pistol et al.,2025).

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.

7. An AI Powered Threat Detector for Banking Sector Using Intelligent Surveillance Cameras(Kumar et al.,2023)

This paper introduces an AI-powered surveillance platform tailored to the banking industry to improve the level of security and avoid unauthorized access. The system combines machine learning and image analysis methods to analyze surveillance video and locate individuals on the fly. It uses face recognition algorithms like Haar Cascade and LBPH to identify and authenticate authorized users and identify genuine face and fake images with help of eye movement detection.

The system can monitor restricted zones and send instantaneous notifications, in the form of alarms and email, in case of unauthorized access. Also, noise reduction methods are used in order to boost the quality of an image and also increase the accuracy of detection. The findings indicate that AI-assisted surveillance systems have a great potential to enhance security operations within the banking context by facilitating round-the-clock monitoring and quicker reaction to security threats.

Nonetheless, the research is quite narrow (banking sector) and thus cannot be generalized to different settings. Furthermore, the system is largely dependent on the accuracy of face recognition and controlled conditions, which can influence the performance in the real world when there is different lighting and quality of images.

8. AI-Powered Threat Detection in Surveillance Systems: A Real-Time Data Processing Framework(Cadet et al.,2024)

This proposed research is a detailed model on how surveillance systems can detect threats in real-time with the application of artificial intelligence. The framework combines machine learning and

deep learning models with real-time data processing technologies to process large quantities of data across various sources, such as video feeds, audio, and sensors.

The system employs the latest technologies including object detection, facial recognition, and anomaly detection to detect potential threats. It also includes stream processing software, such as Apache Kafka and Apache Flink, to provide low-latency processing, and edge computing to improve response time and network congestion.

The results indicate that AI combined with real time processing is a much more effective means to enhance the detection accuracy and system performance, particularly in the large scale application of AI to smart cities and critical infrastructure. Also, the framework enables the on-going training of models, which enables the system to respond to new and changing threats.

Although it has strengths, the research has challenges associated with the complexity of its system, infrastructure demands, and privacy of its data. In addition, real-life implementation of such frameworks consumes a lot of computational power and greater integration abilities.

9. Video Surveillance and Security Using Artificial Intelligence(Venkatesh et al.,2024)

The paper provides an AI-based video surveillance system with the YOLO algorithm used to detect and classify criminal behavior in real-time. The system is able to detect suspicious activities in real-time video feeds like theft and intrusion with a high rate and precision.

YOLO helps to make the process of object detection and tracking more efficient and provide the system with the ability to react promptly to possible threats. All findings demonstrate that AI-driven surveillance systems can be used to strengthen the security efforts by offering proactive surveillance and facilitating timely intervention that will also help prevent crimes.

Nonetheless, the system is as effective as the quality of the video input and the training data. Further, issues associated with environmental factors (e.g., lighting and occlusion) can affect detection accuracy in the field.

10. Exploring the Role of Artificial Intelligence in Enhancing Security Operations: A Systematic Review(Giarimpampa et al.,2025).

This systematic review focuses on how artificial intelligence can help enhance security operations in different fields. The article examines a vast amount of literature and points out that a considerable percentage of AI applications are dedicated to threat detection and surveillance.

The results indicate that AI technologies can help in enhancing efficiency, minimizing human error, and decreasing operational costs in security systems. Nevertheless, the research also notes that there are a number of limitations such as using non-explainable AI models, access to open-source tools is limited, and reliance on proprietary datasets.

Moreover, the study identifies issues of data quality, system integration, and explainability deficiency of AI models, which can impact trust and adoption in practice. The study suggests the need for more transparent and interpretable AI systems to enhance their effectiveness and acceptance.

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.

Chapter 3

Research Methodology

This research is a descriptive-analytical paper with a comparative analysis of the past literature to explore how artificial intelligence can be used to improve the detection of security threats at an early stage using CCTV surveillance systems. The study is based on the secondary data gathered by referring to peer-reviewed journals, conference papers, and other pertinent academic materials.

The approach is aimed at studying and comparing different AI-based methods of video surveillance, such as machine learning, deep learning, and computer vision. It looks into the application of these techniques in real-time detection of abnormal behaviors and suspicious activities.

Moreover, the paper assesses the performance of AI-based surveillance systems based on the key performance indicators found in the literature, including accuracy, response time, and detection efficiency. This analysis relies on the results of earlier empirical and experimental research, instead of business data gathering.

In addition, the paper recognizes the advantages and disabilities of the current AI models and discusses the technical and operational issues of their application, such as scalability, computing needs, and system integration.

Altogether, the given methodology guarantees a full-scale view of the research problem and contributes to meeting the study goals due to systematic analysis and the use of evidence-based assessment.

Expected Results

It is hoped that this research will show that artificial intelligence can play a huge role in enhancing the effectiveness and precision of CCTV surveillance systems. It is expected that the

findings will demonstrate that AI-based systems have the potential to increase the detection of threats in real-time and decrease the need to have human monitoring.

It is also anticipated that the study will shed light on the benefits of employing AI methods which include quicker response time, greater ability to detect abnormal behaviors, and less human error. Furthermore, it can indicate a number of difficulties, such as the high cost of implementation, data privacy, and technical restrictions.

In general, the findings should confirm the premise that making AI-based surveillance systems smarter will result in more proactive security solutions.

Gantt Chart (Timeline)

The study will be carried out within a certain period, which will be divided into several important stages. The initial stage involves stating the problem of the research and the literature review. The second step is to analyze the past research and come up with the conceptual framework.

The third step is concerned with the writing of the major chapters of the study, the methodology and discussion. Lastly, reviewing, editing and finalization of the research is the last step of the research.

Phase	Activity	Duration
Phase 1	Problem definition & literature review	Week 1–2
Phase 2	Analysis of previous studies	Week 3–4
Phase 3	Writing research chapters	Week 5–6
Phase 4	Review and final editing	Week 7

References

- 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.
- 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.
- Cadet, E., Osundare, O. S., Ekpobimi, H. O., Samira, Z., & Weldegeorgise, Y. W. (2024). AI-powered threat detection in surveillance systems: A real-time data processing framework. *Open Access Research Journal of Engineering and Technology*, 7(2), 31–45. <https://doi.org/10.53022/oarjet.2024.7.2.0057>
- Giarimpampa, D., Meier, R., Bissyandé, T. F., Lenders, V., & Klein, J. (2025). Exploring the role of artificial intelligence in enhancing security operations: A systematic review. *ACM Computing Surveys*, 58(3), Article 67, 1–38. <https://doi.org/10.1145/3747587>
- 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.
- Kumar, A. D., Raja, V. R., Mithun, P., Arikumar, K. S., Arthiya, A. P., & Bujitha, R. A. (2023). An AI powered threat detector for banking sector using intelligent surveillance cameras. In *Proceedings of the 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*. IEEE.
- 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.

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.

Sabit, H. (2025). Artificial intelligence-based smart security system using Internet of Things for smart home applications. *Electronics*, 14(3), 608.

Şengönül, E., Samet, R., Abu Al-Haija, Q., Alqahtani, A., Alturki, B., & Alsulami, A. A. (2023). An analysis of artificial intelligence techniques in surveillance video anomaly detection: A comprehensive survey. *Applied Sciences*, 13(8), 4956.
<https://doi.org/10.3390/app13084956>

Venkatesh, S., Akash, V., Hariharan, S., & Jayashri, J. (2024). Video surveillance and security using artificial intelligence. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, 4(4).