UDC 004.93

COMPUTER VISION TECHNOLOGY

Linnik M.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Perevyshko A.I. – Senior Lecturer at the Department of Foreign Languages

Annotation. This article explores the applications of computer vision (CV) technologies in security systems. It examines key implementations of CV, including video surveillance, facial recognition, access control and traffic monitoring. Special attention is given to the integration of machine learning methods to enhance the accuracy of security solutions. The conclusion discusses future development prospects.

Keywords: computer vision, security, facial recognition.

Introduction. Computer vision (CV) is a branch of computer science, which enables machines to interpret visual information. CV has gained significant importance in addressing contemporary security challenges. With its ability to analyze visual data in real-time, this technology has become a key component in such applications as threat detection, and access control, contributing to the protection of critical infrastructure, and private properties.

This article examines the diverse applications of computer vision in the security sphere, emphasizing its potential to address complex security issues effectively. Furthermore, the article will briefly explore how machine learning enhances CV capabilities, enabling the development of more accurate and adaptive security systems.

The main part. The implementation of computer vision technologies has significantly enhanced security capability in multiple domains. CV simplifies threat detection, reduces response times and improves the overall reliability of security infrastructure.

Modern surveillance systems incorporate computer vision algorithms to continuously monitor public and private spaces. As noted in «Computer Vision: Principles, Algorithms, Applications, Learning» by E.R. Davies [1], these systems now utilize deep learning-based approaches, that include motion detection with object classification, which distinguish humans from vehicles or animals. In addition, such algorithms can estimate crowd density, detect abnormal behavior, and identify potential threats such as unattended items or suspicious movement patterns. In the article by Thomas Watson it is pointed out modern systems can process video streams at 30-60 fps while maintaining over 95% detection accuracy [2]. The figure 1 below demonstrates objects recognition in the urban setting [5].

Figure 1– Segmentation of objects for detailed environmental analysis

Facial recognition technology has become a cornerstone of modern security infrastructure. Contemporary systems can use 3D facial mapping technologies to overcome lighting and viewing angle challenges. Sophisticated pattern recognition algorithms verify individual identities with increasing accuracy, that facilitates reliable access control in high-security facilities and border checkpoints. These technologies have made it possible to achieve a false alarm rate in less than 0.1% and enable the efficient operation of identification systems through «sophisticated background modeling and foreground object analysis» [1].

Furthermore, facial recognition is now widely used in mobile banking, airport security, and smart home systems, improving both convenience and protection.

Advanced video analytics enable real-time detection of unauthorized access attempts. This technology includes thermal imaging integration for continuous operation, AI-powered fence-line monitoring systems and predictive analytics for intrusion path forecasting. According to studies, such systems have significantly reduced false alarms compared to traditional motion sensors [3].

Computer vision applications in traffic surveillance include license plate recognition, accident detection, and congestion analysis. These systems contribute to enhanced road safety and more efficient traffic management in smart city environments. Moreover, CV-based technologies can detect traffic rule violations, monitor pedestrian flow, and optimize traffic light control in real time. For instance, in the picture below, E.R. Davis shows a simple procedure for locating license plates.

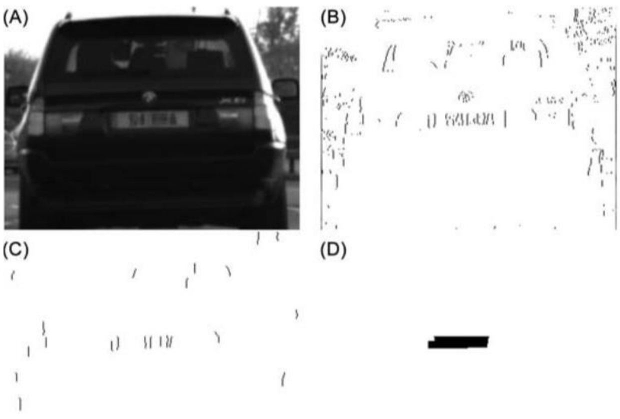

Figure 2 – The procedure of license plates recognition

The future of computer vision in security lies in its integration with emerging technologies such as the Internet of Things (IoT), 5G networks, and edge computing. These integrations can enable faster data processing, reduced latency, and more efficient security solutions. For example, smart cities and autonomous vehicles could benefit from CV-powered systems that provide real-time monitoring and decision-making capabilities. Another promising area is the development of explainable AI (XAI) for CV, which aims to create interpretable models that address bias, improve transparency, and build trust in AI-driven security systems [4].

Conclusion. While computer vision has already made significant contributions to the field of security, ongoing researches and innovations are crucial to overcoming its limitations and unlocking its full potential. By addressing technical, ethical, and regulatory challenges, CV can continue to evolve as a cornerstone of modern security systems, providing with safer and more secure societies.

References

1. *Davies, E.R. Computer Vision: Principles, Algorithms, Applications, Learning. Fifth Edition. Academic Press, 2018.*

2. *Achieving 95% Accuracy in an IT Asset Data Repository: There's No Magic Bullet [Electronic resource]. Mode of access: https://www.amitracks.com/wp-content/uploads/2012/05/AMI_RF_EdgeAchievingAccuracy1.pdf. Date of access: 16.03.2025.*

3. *Szeliski, R.Computer Vision Algorithms and Applications. Springer, 2022.*

4. *Favorskaya, M., Lakhmi C. Computer Vision in Control Systems-3. Springer, 2018.*

5. *Компьютерное зрение в 2024 году: Главные задачи и направления [Электронный ресурс]. Режим доступа: https://habr.com/ru/companies/otus/articles/810207/. Дата доступа: 14.03.2025.*