Baimukhamedov M.F.,
Doctor of Technical Sciences, professor,
bmf45@mail.ru[1]

Baimukhamedova A.M.,
senior lecturer, djanin50@gmail.co[2]

Boranbayev A.S.,
PhD, Professor,
askar.boranbayev@nu.edu.kz [3]

*Kostanay Social-Technical University
named after Z.Aldamzhar,
110000 Kostanay, ave. Koblandy Batyr, 27[1]*

*Gazi University
Turkiye, Emniyet Provincem, Bandirma st., 6/1[2]*

*Nazarbayev University,
010000 Astana, ave. Kabanbai Batyr, 53[3]*

APPLICATION OF ARTIFICIAL INTELLIGENCE IN SECURITY

Abstract. *Artificial intelligence is one of the key factors determining the future development of the security sector. To enhance the application of artificial intelligence in security and increase the level of automation, a more detailed study of the application of artificial intelligence in security is necessary so that software products in the security market can continually meet the new needs driven by social development. This article primarily examines the application of artificial intelligence technology in security. First, the level of development and stage of artificial intelligence in security are described. Second, the types of artificial intelligence technologies applied in security are presented. Third, the practical application of artificial intelligence in security is briefly discussed.*

Keywords: *artificial intelligence; security; biometrics; deep learning; machine learning, software products.*

Introduction

In recent years, the domestic security industry has maintained steady growth in market size, and its prospects are promising. Intelligent security is gradually becoming a focus for the transformation and modernization of the security industry, accounting for an increasing share of this trend. In terms of technology application, the application of artificial intelligence (AI) in security is primarily

related to facial and vehicle recognition, including biometric recognition technology, big data, and video structuring technology [1].

In terms of industry application, intelligent security currently has applications in public safety, transportation, finance, industry, construction, and other fields. In the transportation field, AI technology could be used in the future to analyze urban traffic flow in real time, adjust traffic light intervals, reduce vehicle waiting times, and so on, intelligently allocating resources to improve traffic efficiency. In construction, AI technology could be used for comprehensive building security and energy management, as well as for real-time monitoring of people, vehicles, and objects entering and exiting the building. Urban security is a cornerstone of urban development. As AI becomes increasingly diversified, it offers a valuable tool for addressing security challenges in urban management and operations, helping to create a healthy and safe urban environment.

Key artificial intelligence technologies in the field of security

With the development of artificial intelligence technology, it is constantly being integrated into modern security systems. The development of AI in the field of security is mainly driven by modifications to video structuring, biometrics, object recognition and big data analysis.

Video structuring

Video structuring is a fundamental prerequisite for biometrics and object recognition. In technical terms, it can be divided into three stages: detection, tracking and attribute extraction. During the detection process, the foreground object is extracted from the video, and then it is determined whether the foreground object is an effective target (people, vehicles, faces, etc.) or an unacceptable target (leaves, shadows, lights, etc.) [2].

The target tracking process involves continuously observing a specific target in a given environment and obtaining a high-quality image as a result of the entire tracking process. The target attribute extraction process involves identifying target attributes in the detected target image and assessing the visual characteristics of the target, such as gender, age, clothing, vehicle type, colour, and other attributes. The process of extracting object attributes is mainly based on feature extraction technology and deep learning network structure classification.

After that, artificial intelligence structures the video data, and the object recognition search speed will increase significantly. At the same time, deep intelligent analysis of structured data can perform a predictive function. In addition, structured video data takes up less memory space, which can effectively reduce the burden on information transmission and storage.

Biometrics

Biometric technology is a technology that uses physiological and behavioural characteristics inherent in the human body to identify individuals. With the development of science and technology, biometric technology has become an important means of identification or authentication technology. As an important branch of biometrics, facial recognition allows people to be identified in

the most natural and intuitive contactless way by users, and is also the most widely used technology in the field of public safety [3].

Currently, public safety agencies have the most pressing technical needs when working with people. In the field of real crime fighting, facial recognition can not only confirm identity, but also provide comparison, tracking, real-time detection, etc., helping the police to quickly identify a target in a crowd and achieve early warning of incidents.

Object recognition

Currently, in the field of security, a typical application of object recognition is vehicle recognition. With the help of a peripheral trigger and video call, an image of a vehicle can be obtained and the number plate automatically recognised.

Recognition of the characteristics of the vehicle's shape and license plate can not only determine the attributes of the vehicle, but also determine the attributes of the owner, related personal attributes, behavioural characteristics, and in combination with biometrics,create a three-dimensional prevention and control system.

In practical application, vehicle recognitioncan be sequentially compared with vehicle attributes, owner attributes, and other data for early warning of incidents involving vehicles with a high propensity for committing offences.

Checking passing vehicles at checkpoints allows vehicles to be filtered based on the creation of a large number of databases in order to quickly block target vehicles and reduce the workload on the relevant authorities.

Big data analytics technology

Big data analytics technology allows you to integrate massive amounts of unstructured and structured data, as well as analyse and calculate the attributes of this data. Big data technology provides powerful distributed computing and database management capabilities for AI, which is an important support for the analysis, prediction, and self-improvement of artificial intelligence [4]. The technology consists of three parts: big data management, large-scale distributed computing, and intelligent data analysis. Massive data management is used to collect and store comprehensive information from resources involved in the application of artificial intelligence and to accumulate data based on time. At the same time, valuable data can be generated through intelligent big data analysis, which can provide more effective data samples for deep learning.

Big data analysis technology can significantly reduce labour costs, increase efficiency, and even make it possible to solve some problems that cannot be done manually in some aspects.

For example, facial search, personnel database, ID card database search, duplicate personnel search using semantic description from video to search for a vehicle of a certain colour, number plate search, image search, video association and other applications.

Practical application of artificial intelligence in the field of security

Application of deep learning AI technology in the field of security Currently, the AI deep learning architecture network mainly includes an

autoencoder, a Boltzmann machine, and a convolutional neural network, the latter of which is similar to a biological neural network, has a smaller weight coefficient, and a lower model complexity. A deep convolutional neural network mainly includes three layers.

1) Input layer. Data collected by the device is then imported into the system.

2) Hidden layer. The hidden layer is divided into two layers: upper and lower layers. The upper layer is a fully connected layer, and the lower layer consists of a convolutional layer and a lower sampling layer alternately in pairs.

3) Output layer. The output layer can use logical data collection regression, SoftMax regression, or a support vector machine for image classification.

A convolutional neural network is a neural network that implements a 'local perception field' and 'weight distribution' using convolution. Based on the deep learning technology of artificial intelligence deep neural networks, monitoring equipment can automatically identify and evaluate the received image, independently process video content, and calculate a large amount of potentially useful information in the input data.

Application of AI video structuring technology in the field of security

Based on deep learning AI, intelligent video analysis technology, formed by establishing auxiliary technical measures, is AI video structuring technology. The technology has three main stages:

1) Target detection. The process of extracting foreground objects from image information and identifying them is called target detection 2) Target tracking. Target tracking is a kind of intelligent decision-making process that involves recording and capturing specific foreground targets, as well as certain key actions.

3) Target attribute extraction. The process of recognising, extracting, classifying and storing the visual characteristics of specific foreground objects is called object attribute extraction.

The above three steps combine deep learning AI, machine vision, data processing and other technologies to implement automatic search, evaluation and response functions in security technology.

A key link in the practical application of artificial intelligence in the field of security

From the perspective of various scenarios, the practical application of intelligent security can be analysed depending on the time of the event, the type of event, how to prevent the event, and how to reproduce the event process. Many events occur at night, while the colour palette of conventional cameras is black and white. Videos obtained from such cameras lose a lot of colour information and key details. Therefore, a 24-hour full-colour effect should be achieved. With the appropriate equipment, there is no need for external lighting compensation technology in dark or low-light monitoring conditions, which can also restore the perfect colour image.

A complete intelligent security product should have an audible and visual deterrent system to ensure that the system can actively use deterrence strategies to

prevent events from occurring when predicted. The warning system combines an audible alert, white light flashing, laser tracking, and other early intrusion warning modes. Traditional security systems rely heavily on humans. The most fundamental change is to turn retroactivity into advance warning, which will make the popularisation of intelligence inevitable.

AI can analyse the perimeter of the area and the behaviour of personnel, as well as respond flexibly to all kinds of intrusions, wandering, temporary stays, and so on.

Prospects for the development and trends in intelligent security in smart cities

The future trend in the development of intelligent security is mainly manifested in three aspects:

1) Providing monitoring systems with advanced computing capabilities, certain intelligent analysis functions, such as human image recognition, vehicle recognition and behaviour recognition, can be brought to the fore to implement a general AI security architecture. This not only meets the requirements of intelligent urban security applications, but also reduces the burden on network data transmission and dependence on data centres through computation to improve the intelligent efficiency of the entire network.

2) Human-machine collaboration and intelligent control.

Human-machine collaboration requires machine cognitive abilities based on human state modelling, human knowledge sharing capabilities, and global planning capabilities [5].

In the field of intellectual security, human-machine systems can play a role in remote emergency management, joint decision-making at accident sites, and work in areas inaccessible to humans.

For example, in critical situations, citizens can send distress signals to the video surveillance system using gestures.

3) Global cognitive intelligence. Big security data is a collection of data from multiple departments and systems at different points in time. The density of data values is very low, and the inability to perform global data analysis seriously limits its application. In the future, a key direction for the development of intellectual security will be to provide machine learning the ability to process large-scale, full-scale, and multi-source data [6] that cannot be processed by humans in real time, understand complex hidden laws, and, finally, formulate an optimal strategy that goes beyond local suboptimal decision-making by humans from a global perspective.

Conclusion

The level of artificial intelligence development in the field of security is changing rapidly. The first level is intelligent video surveillance terminal recognition technology, such as facial recognition and number plate recognition. The second level is intelligent security data analysis technology, which can automatically store data and analyse its essence. The third level is big data analysis and exploitation technology, which can model and analyse security patterns over a certain period of time, conduct in-depth analysis, and predict trends. In the future,

security products must be able to mimic human thinking [7], replace some human work, and create cross-platform networks for cooperation between different devices.

Intelligent security has entered the era of big data and artificial intelligence. Artificial intelligence, based on machine vision and deep learning technology, is widely used in public security control, traffic management, criminal investigation and other scenarios. In an environment without human intervention, a computer can automatically analyse the content of camera footage, including target detection, target segmentation extraction, target recognition, and target tracking. Working with massive heterogeneous data from multiple sources is a challenge that intelligent security must face. Currently, the public security system database accumulates a large amount of information on vehicles, personnel, social connections, and other data [8]. At the same time, city cameras, intelligent mobile terminals, and sensors constantly generate large amounts of social security data, which contains hidden information about city security.

REFERENCES
1. 'Decrypt' security view 'uncover' Analysis Centre. Huicong security network, 2016.
2. Luo Shixiong, Fu Shuangsheng. Discussion on the construction of intelligent PAAS platform integrating the advanced new technology. Technical Study, 2019. – pp. 25-26.
3. Zhang Jianxiong. Analysis of cloud computing market and development strategy of telecom operators // Telecommunication technology, 2016. – pp. 40-42.
4. Wu Shiwang. Research on the main technology and application prospect of artificial intelligence in the field of transportation. Communication design and Application, 2019, 26 (12), – pp. 132-133.
5. Kolesnikova G.I. Artificial intelligence: problems and prospects / G.I. Kolesnikova // Videonauka: online journal, 2018. – No. 2(10). – URL:
https://videonauka.ru/stati/44-novye-tekhnologii/190-iskusstvennyj-intellekt-problemy-i- perspektivy
6. Nikishova M.I. Prospects for the application of artificial intelligence technologies in corporate governance in the context of the transition to a digital economy // Management Sciences in the Modern World, 2018. – Vol. 1. – No. 1, – pp. 233–237.– URL: https://elibrary.ru/item.asp?id=35112711.
7. Slagle, J. Artificial Intelligence. – Moscow: Mir, 2016. – 320 p.
8. Teterkin M.A., Anisimov A.R., Tomilchenko L.R. Analysis of scenarios
for the use of virtualisation technology // Innovations and Investments, 2022. – No. 5. – Pp. 136–141. – EDN VLYKPT.

Баймухамедов М.Ф.,
техника ғылымдарының докторы, профессор,
bmf45@mail.ru[1]

Баймухамедова А.М.,
аға оқытушы, djanin50@gmail.co[2]

Боранбаев А.С.,
PhD докторы, профессор
askar.boranbayev@nu.edu.kz[3]

Академик З.Алдамжар атындағы
Қостанай әлеуметтік- техникалық
университеті,
110000 Қостанай қ., Қобыланды Батыр даңғылы, 27[1]

Гази университеті
Түркия, Емниет облысы, Бандырма көш., 6/1[2]

Назарбаев университеті,
010000 Астана, Қабанбай Батыр даңғылы, 53[3]

ҚАУІПСІЗДІК САЛАСЫНДА ЖАСАНДЫ ИНТЕЛЛЕКТТІ ҚОЛДАНУ

*   **Аңдатпа.** Жасанды интеллект қауіпсіздік саласының болашақ дамуын анықтайтын негізгі факторлардың бірі болып табылады. Қауіпсіздік саласында жасанды интеллектті қолдануды күшейту және автоматтандыру деңгейін арттыру үшін қауіпсіздік бағдарламалық өнімдері әлеуметтік дамудан туындаған жаңа қажеттіліктерді үнемі қанағаттандыра алатындай етіп, қауіпсіздік саласында жасанды интеллектті қолдануды егжей-тегжейлі зерттеу қажет. Бұл мақалада негізінен жасанды интеллект технологиясын қауіпсіздік саласында қолдану қарастырылады. Біріншіден, қауіпсіздік саласындағы жасанды интеллекттің даму деңгейі мен сатысы сипатталады. Екіншіден, қауіпсіздік саласында қолданылатын жасанды интеллект технологияларының түрлері ұсынылады. Үшіншіден, жасанды интеллекттің қауіпсіздік саласындағы практикалық қолданылуы қысқаша талқыланады.*
*   **Түйінді сөздер:** жасанды интеллект; қауіпсіздік; биометрия; терең оқыту; машиналық оқыту; бағдарламалық өнімдер.*

Баймухамедов М.Ф.,
доктор технических наук, профессор,
bmf45@mail.ru[1]

Баймухамедова А.М.,
старший преподаватель, djanin50@gmail.co[2]

Боранбаев А.С.,
доктор PhD, профессор
askar.boranbayev@nu.edu.kz[3]

*Костанайский социально-технический университет
имени академика З.Алдамжар,
110000 г.Костанай, пр-т. Кобыланды Батыра, 27[1]*

*Университет Гази
Турция, Провинция Эмниет, ул.Бандирма, 6/1[2]*

*Назарбаев университет,
010000 Астана, пр-т. Кабанбай Батыра, 53[3]*

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ БЕЗОПАСНОСТИ

***Аннотация.** Искусственный интеллект является одним из ключевых факторов, определяющих будущее развитие сферы безопасности. Чтобы усилить применение искусственного интеллекта в области безопасности и повысить уровень автоматизации, необходимо более подробное изучение схемы применения искусственного интеллекта в области безопасности, чтобы программные продукты на рынке безопасности могли постоянно удовлетворять новые потребности, вызванные социальным развитием. В данной статье в основном рассматривается применение технологии искусственного интеллекта в области безопасности.*

Прежде всего, описан уровень развития и стадия искусственного интеллекта в области безопасности. Во-вторых, представлены виды технологий искусственного интеллекта, применяемых в области безопасности. В-третьих, кратко излагается практическое применение искусственного интеллекта в области безопасности.

***Ключевые слова:** искусственный интеллект; безопасность; биометрия; глубокое обучение; машинное обучение, программные продукты.*