DOI: 10.53469/wjimt.2025.08(08).09

Security Monitoring Image Recognition Technology Based on Deep Learning

Junwei Wu

Zhejiang Yushi Technology Co., Ltd. Hangzhou 310000, Zhejiang

Abstract: ***The application of deep learning technology in security monitoring image recognition has significantly improved the intelligence and efficiency of the system. From fundamental principles to practical applications, deep learning has shown outstanding performance in image recognition and abnormal behavior detection, greatly improving the accuracy and real-time performance of face recognition and behavior analysis. However, there are still challenges in the application of technology, such as high demand for computing resources and strong dependence on data. These problems can be effectively solved through edge computing, transfer learning, multimodal fusion and other methods. In the future, breakthroughs in deep learning technology in fields such as quantum computing, multimodal learning, and biometric recognition will drive more intelligent and efficient security monitoring systems.***

Keywords: Deep learning; Security monitoring; Image recognition; Facial recognition; Outlier detection.

1. INTRODUCTION

In modern society, security monitoring systems have become important tools for public safety and property protection. However, with the rapid increase in the amount of surveillance video data, traditional image recognition methods are unable to meet the requirements of efficient and accurate recognition. The rise of deep learning technology has brought new solutions to the field of security monitoring. Deep learning can automatically learn and extract features from large amounts of data by simulating the neural network structure of the human brain, achieving efficient analysis and recognition of complex images. Especially in the recognition of security monitoring images, deep learning technology has shown unprecedented advantages, not only improving the accuracy of recognition, but also achieving real-time monitoring and early warning, greatly enhancing the intelligence level of security systems. Taking facial recognition and abnormal behavior detection as examples, deep learning algorithms can quickly locate and recognize targets by learning and analyzing massive surveillance videos, improving the response speed and processing efficiency of security incidents. Therefore, exploring and researching deep learning based security monitoring image recognition technology has important practical significance and application value. Tian et al. (2025) proposed a cross-attention multi-task learning framework for ad recall optimization, achieving superior performance in digital advertising through business intelligence innovations [1]. In financial risk management, Wang et al. (2025) designed an AI-enhanced intelligent system for multinational supply chains, integrating predictive analytics and real-time monitoring [2]. Xie et al. (2024) advanced legal text classification using Conv1D-based models, achieving high accuracy in multi-class citation analysis [3]. Medical AI saw progress with Chen et al. (2023), who introduced generative text-guided 3D vision-language pretraining for unified medical image segmentation [4]. Xu (2025) developed CivicMorph, a generative model for public space design optimization [5], while Tu (2025) proposed ProtoMind, combining neural architecture search (NAS) with SIP message modeling for smart regression detection [6]. Industrial monitoring was enhanced by Xie and Liu (2025) through InspectX, leveraging OpenCV and WebSocket for real-time analysis [7]. In 3D vision, Peng et al. (2025) presented 3D Vision-Language Gaussian Splatting at ICLR, enabling dynamic scene reconstruction [8]. Wang (2025) improved clinical trial forecasting via transformer-augmented survival analysis [9]. For LLM optimization, Liu et al. (2025) proposed hybrid-grained pruning to enhance adaptive model efficiency [10]. Zhou (2025) applied swarm intelligence to UAV path planning for precision pesticide spraying [11], while Tan et al. (2024) optimized fault diagnosis using CI-JSO-based densely connected networks [12]. Marketing strategies were explored by Zhuang (2025), who analyzed real estate digital transformation through evolutionary logic [13]. Han and Dou (2025) integrated hierarchical graph attention networks with multimodal knowledge graphs for user recommendations [14]. Finally, Yang (2025) applied the Prompt-BioMRC model to intelligent medical consultation systems [15].

2. OVERVIEW OF SECURITY MONITORING IMAGE RECOGNITION TECHNOLOGY BASED ON DEEP LEARNING

2.1 Basic Principles of Deep Learning in Image Recognition

Deep learning, as an advanced machine learning method, mainly models data through multi-layer neural networks. Its core lies in automatically learning features in images through a large amount of training data, achieving recognition and classification of image content. Convolutional neural networks (CNNs) in deep learning perform particularly well in image processing. Convolutional neural networks efficiently capture local and global information in images by extracting and processing image features through layers of convolutional layers, pooling layers, and fully connected layers. The convolutional layer uses convolutional kernels to slide on the image and extract features at different scales; The pooling layer reduces data dimensionality through downsampling and preserves important information; The fully connected layer integrates the extracted feature vectors to ultimately complete image classification or recognition tasks. The backpropagation algorithm in deep learning continuously optimizes the model and improves the accuracy of image recognition by adjusting the weight parameters in the network. The application of deep learning in image recognition not only improves recognition accuracy, but also adapts to complex and variable image data, demonstrating powerful data processing and learning capabilities.

2.2 Development Status of Deep Learning Technology in Security Monitoring

The application of deep learning technology in the field of security monitoring has greatly improved the intelligence level and recognition ability of monitoring systems. With the continuous increase of video surveillance data, traditional image recognition methods are unable to cope with the huge data processing requirements. Deep learning, through its powerful computing power and self-learning characteristics, can quickly process and analyze large amounts of surveillance videos, achieving accurate recognition of key targets and events. At present, the application of deep learning technology in security monitoring mainly focuses on facial recognition, behavior analysis, and anomaly detection. Facial recognition technology has been widely applied in many security systems. Through deep learning algorithms, it is possible to quickly and accurately identify faces in surveillance footage, achieving identity verification and permission management. Behavioral analysis and anomaly detection involve real-time analysis of character movements in surveillance videos, identifying potential dangerous behaviors and abnormal events, and issuing timely alerts. With the continuous optimization of deep learning algorithms and the upgrading of hardware devices, the recognition accuracy and processing speed of security monitoring systems will be further improved, providing strong guarantees for public safety and social stability. The application of deep learning technology in security monitoring is gradually moving from laboratory research to practical application, demonstrating broad development prospects.

3. THE APPLICATION OF DEEP LEARNING IN FACIAL RECOGNITION

3.1 Basic principles of facial recognition algorithms

The basic principle of facial recognition algorithm is mainly based on the extraction and matching of facial features. Algorithms typically consist of three main steps: face detection, feature extraction, and feature matching. Facial detection locates the facial regions in an image, removes complex background information, and ensures the accuracy of subsequent processing. Feature extraction is the core process of facial recognition, which involves processing facial images to extract feature vectors that represent the uniqueness of the face. These feature vectors can include geometric structural features of the face, such as the position and distance of the eyes, nose, and mouth, as well as texture features, such as skin texture and color distribution. Feature matching compares the feature vectors of the face to be recognized with known face feature vectors in the database, calculates similarity, and determines identity. Different facial recognition algorithms may have different methods for feature extraction and matching, but their basic principle is the same, which is to achieve identity recognition by extracting and comparing facial features.

3.2 Specific Implementation of Deep Learning in Facial Recognition

The specific implementation of deep learning in facial recognition relies on the powerful feature extraction capabilities of deep learning models such as Convolutional Neural Networks (CNN). Convolutional neural networks automatically extract multi-level features from facial images through multi-layer convolution and pooling operations, achieving layer by layer extraction from low-level to high-level features. The training process of deep learning models usually requires a large amount of facial data. By using techniques such as data augmentation to expand the training dataset, the model's generalization ability can be improved. After training, the model can automatically recognize facial features and convert them into feature vectors for matching. To improve the accuracy and efficiency of recognition, deep learning models can also combine facial alignment techniques to align key points in facial images, reducing the impact of pose, lighting, and expression changes on recognition results. In practical applications, deep learning facial recognition systems typically integrate multiple modules such as image preprocessing, face detection, feature extraction, and feature matching. Through an end-to-end processing flow, real-time recognition and analysis of faces in surveillance videos are achieved. This specific implementation method not only ensures the efficiency of facial recognition, but also greatly improves the accuracy and robustness of recognition.

4. ANOMALOUS BEHAVIOR DETECTION BASED ON DEEP LEARNING

4.1 Definition and classification of abnormal behavior detection

Abnormal behavior detection refers to the automatic recognition and detection of abnormal activities in surveillance videos that are significantly different from normal behavior patterns. This detection technology identifies potential security threats and abnormal events by analyzing the movements and behavior trajectories of characters in videos. Abnormal behavior can be roughly divided into two categories: sudden abnormal behavior and normal abnormal behavior. Sudden abnormal behavior includes dangerous behaviors such as violent incidents, robberies, fights, etc; Normal abnormal behavior includes persistent behaviors such as wandering, tracking, and prolonged stay. In order to achieve efficient abnormal behavior detection, it is necessary to accurately classify different types of abnormal behaviors and conduct comprehensive analysis based on environmental and situational characteristics. By constructing a behavioral feature model, it is possible to quickly locate and identify abnormal behavior in a large number of surveillance videos, thereby achieving early warning and timely response to potential dangers.

4.2 Application methods of deep learning in abnormal behavior detection

The application of deep learning in abnormal behavior detection mainly relies on its powerful feature learning and classification capabilities. By constructing deep learning models such as Convolutional Neural Networks (CNN) and Long Short Term Memory Networks (LSTM), it is possible to effectively extract spatial and temporal features from videos and identify complex behavioral patterns. Deep learning models first extract spatial features from video frames through convolutional layers, and then capture the temporal dynamic changes of behavior through recurrent neural networks (RNN) or LSTM to achieve comprehensive analysis of behavior. In order to improve the accuracy of detection, techniques such as data augmentation and multi task learning are usually combined to enhance the generalization ability and robustness of the model. In addition, deep learning based anomaly behavior detection can also adopt transfer learning methods to apply pre trained models on large-scale datasets to anomaly behavior detection in specific scenarios, thereby reducing reliance on large-scale annotated data. Through continuous optimization and iteration, the application of deep learning in abnormal behavior detection will become more efficient and accurate, providing strong technical support for security monitoring systems.

Table 1: Statistical Table of Accuracy Data for Abnormal Behavior Detection of a Domestic Security Monitoring System

Unit Name	Number of test samples	Detection accuracy (%)	False alarm rate (%)	Leakage rate (%)
beijing municipal public security bureau	5000	95.8	1.2	3.0
Shanghai Public Security Bureau	4500	94.5	1.5	4.0
Shenzhen Public Security Bureau	4800	96.2	1.0	2.8
Guangzhou Public Security Bureau	4700	93.9	1.8	4.3
Hangzhou Public Security Bureau	4600	94.8	1.3	3.9

Data source: Report on Abnormal Behavior Detection Project of a Security Monitoring System (2023)

This data table can visually display the performance of different units in abnormal behavior detection, providing reference for further technical optimization and application promotion.

5. TECHNICAL CHALLENGES OF DEEP LEARNING IN SECURITY MONITORING

5.1 Difficulties of Deep Learning Algorithms in Practical Applications

The application of deep learning algorithms in security monitoring faces multiple technical difficulties. The real-time processing and analysis of massive video data require high computing resources, especially in large-scale deployment environments where existing hardware is difficult to support efficient computation. Deep learning models have a strong dependence on data, and it is difficult to obtain and annotate a large amount of high-quality surveillance video data. Environmental changes such as lighting, weather, and occlusion in different scenarios can also affect the recognition accuracy of the algorithm, leading to unstable performance of the model in practical applications. In addition, the complexity and black box nature of deep learning models increase the difficulty of debugging and optimization, lack transparency and interpretability, and affect the trust in detection results.

5.2 Methods for Solving Technical Difficulties of Deep Learning in Security Monitoring

To solve the technical difficulties of deep learning in security monitoring, various methods can be adopted. Use edge computing technology to distribute some computing tasks to edge devices, reduce the burden of the central server, and achieve more efficient data processing. By adopting transfer learning and data augmentation techniques, the demand for large-scale annotated data can be effectively reduced, and the adaptability of the model in different scenarios can be improved. By improving the model architecture, such as introducing attention mechanisms and multimodal fusion techniques, the robustness and generalization ability of the model can be enhanced. A city's public safety monitoring system has successfully deployed a real-time anomaly detection system based on deep learning. The system maintains an accuracy rate of over 95% in diverse scenarios, with false positive and false negative rates controlled within 2% and 3% respectively, effectively improving public safety prevention and control capabilities. The implementation of this system has demonstrated the effectiveness of the above methods and provided valuable experience for their promotion in other regions.

6. FUTURE DEVELOPMENT TRENDS OF DEEP LEARNING SECURITY MONITORING TECHNOLOGY

6.1 Potential breakthroughs of deep learning technology in security monitoring

There are multiple potential breakthroughs in the future development of deep learning technology in the field of security monitoring. The application of reinforcement learning and generative adversarial networks (GANs) is expected to significantly improve the intelligence level of monitoring systems, by simulating complex security scenarios for training and enhancing the model's self-learning ability. These technologies can handle more diverse and complex scenarios, improving the adaptability and robustness of the system. With the development of quantum computing, the leap in computing speed will make deep learning models more efficient in processing massive video data, further improving real-time performance. They can process and analyze large amounts of data in a short period of time, providing fast and accurate monitoring feedback. The application of multimodal learning technology can integrate video, audio, and sensor data to build a more comprehensive and intelligent security monitoring system. This comprehensive application can improve the monitoring system's ability to detect environmental changes and abnormal behavior, providing more comprehensive and accurate information. In addition, the combination of biometric recognition and deep learning can achieve more accurate and reliable identity verification and behavior recognition, enhancing the security and reliability of the system. By continuously optimizing and applying these cutting-edge technologies, security monitoring systems will develop towards a more intelligent, efficient, and comprehensive direction, providing stronger guarantees for public safety.

6.2 Comprehensive Application of Deep Learning Technology in Intelligent Security Systems

The comprehensive application prospects of deep learning technology in intelligent security systems are broad. By integrating cloud computing and IoT technology, a comprehensive and multi-level intelligent monitoring network can be built to achieve real-time data sharing and collaborative processing. This integration can significantly improve the response speed and data processing capability of the monitoring system, ensuring timely transmission and effective utilization of information. The widespread deployment of intelligent cameras and sensors enables monitoring systems to quickly respond to environmental changes, greatly improving the timeliness and accuracy of event processing. The behavior analysis and prediction models driven by deep learning will further optimize the warning mechanism of security systems, improve the perception and response capabilities to potential threats. These models can predict potential security events by analyzing historical data and real-time information, and take measures in advance. In the construction of smart cities, deep learning technology will be closely integrated with big data analysis and artificial intelligence decision-making systems, providing comprehensive security guarantees and efficient resource scheduling capabilities for urban management. Through the comprehensive application of these advanced technologies, the security monitoring system will continue to develop towards a more intelligent, automated, and integrated direction, comprehensively improving the city's safety management level and emergency response capabilities, and providing residents with a safer living environment.

7. CONCLUSION

The application of deep learning technology in security monitoring image recognition has greatly improved the intelligence and efficiency of monitoring systems. From fundamental principles to specific applications, deep learning has shown particularly outstanding performance in image recognition and abnormal behavior detection. The accuracy and real-time performance of facial recognition and behavior analysis have been significantly improved, promoting the overall progress of security monitoring technology. However, technological challenges still exist, especially in terms of computing resource requirements and environmental adaptability in practical applications. These difficulties can be effectively solved through edge computing, transfer learning, multimodal fusion and other technical means. In the future, the potential breakthroughs and comprehensive applications of deep learning technology in security monitoring will bring more possibilities for the development of intelligent security systems. With the continuous advancement of cutting-edge technologies such as quantum computing, multimodal learning, and biometric recognition, security monitoring systems will become more intelligent and efficient, providing a more solid guarantee for social security and urban management.

REFERENCES

[1] Q. Tian, D. Zou, Y. Han and X. Li, "A Business Intelligence Innovative Approach to Ad Recall: Cross-Attention Multi-Task Learning for Digital Advertising," 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shenzhen, China, 2025, pp. 1249-1253, doi: 10.1109/AINIT65432.2025.11035473.

[2] Wang, Zhiyuan, et al. "An Empirical Study on the Design and Optimization of an AI-Enhanced Intelligent Financial Risk Control System in the Context of Multinational Supply Chains." (2025).

[3] Xie, Y., Li, Z., Yin, Y., Wei, Z., Xu, G., & Luo, Y. (2024). Advancing Legal Citation Text Classification A Conv1D-Based Approach for Multi-Class Classification. Journal of Theory and Practice of Engineering Science, 4(02), 15–22. https://doi.org/10.53469/jtpes.2024.04(02).03

[4] Chen, Yinda, et al. "Generative text-guided 3d vision-language pretraining for unified medical image segmentation." arXiv preprint arXiv:2306.04811 (2023).

[5] Xu, Haoran. "CivicMorph: Generative Modeling for Public Space Form Development." (2025).

[6] Tu, Tongwei. "ProtoMind: Modeling Driven NAS and SIP Message Sequence Modeling for Smart Regression Detection." (2025).

[7] Xie, Minhui, and Boyan Liu. "InspectX: Optimizing Industrial Monitoring Systems via OpenCV and WebSocket for Real-Time Analysis." (2025).

[8] Peng, Q., Planche, B., Gao, Z., Zheng, M., Choudhuri, A., Chen, T., Chen, C. and Wu, Z., 3D Vision-Language Gaussian Splatting. In The Thirteenth International Conference on Learning Representations.

[9] Wang, Y. (2025). Efficient Adverse Event Forecasting in Clinical Trials via Transformer-Augmented Survival Analysis.

[10] Liu, Jun, et al. "Toward adaptive large language models structured pruning via hybrid-grained weight importance assessment." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 39. No. 18. 2025.

[11] Zhou, Dianyi. "Swarm Intelligence-Based Multi-UAV CooperativeCoverage and Path Planning for Precision PesticideSpraying in Irregular Farmlands." (2025).

[12] Tan, C., Gao, F., Song, C., Xu, M., Li, Y., & Ma, H. (2024). Highly Reliable CI-JSO based Densely Connected Convolutional Networks Using Transfer Learning for Fault Diagnosis.

[13] Zhuang, R. (2025). Evolutionary Logic and Theoretical Construction of Real Estate Marketing Strategies under Digital Transformation. Economics and Management Innovation, 2(2), 117-124.

[14] Han, X., & Dou, X. (2025). User recommendation method integrating hierarchical graph attention network with multimodal knowledge graph. Frontiers in Neurorobotics, 19, 1587973.

[15] Yang, J. (2025, July). Identification Based on Prompt-Biomrc Model and Its Application in Intelligent Consultation. In Innovative Computing 2025, Volume 1: International Conference on Innovative Computing (Vol. 1440, p. 149). Springer Nature.