Application, Controversy and Governance of Artificial Intelligence Facial Recognition in Public Security

Jiaye Shen [1] and Jiale Zhan [2, *]

[1] Shanghai Nanyang Model Private School, 200333, China

[2] School of Electronic Information Engineering, Zhuhai College of Science and Technology, Guangdong, 519041, China

* Corresponding Author Email: 352019168@qq.com

Abstract. With the rapid development of artificial intelligence technology, facial recognition is more extensively applied in the field of public security as an efficient means of identity verification and surveillance. It brings convenience to crime prevention, suspect tracking and emergency response. However, the popularization of this technology has also sparked intense social disputes and governance challenges, mainly focusing on privacy infringement, data security, algorithmic bias, and potential abuse of power. Striking a balance between leveraging technological advantages and safeguarding citizens' rights has become a key issue. This study classifies, integrates and analyzes the application of artificial intelligence facial recognition in the field of public security by adopting a systematic literature review method. Findings indicate that while its use has expanded across various domains like crime prevention and border control, demonstrating notable efficiency gains, it simultaneously exposes problems such as lagging legal regulations, inconsistent technical standards, and a lack of ethical supervision. The core of the controversy lies in the conflict between technological power and fundamental civil rights. To foster the healthy development of artificial intelligence facial recognition in of public security, a comprehensive governance system integrating technical norms, legal constraints, and ethical guidance is essential.

Keywords: Artificial intelligence; Facial recognition; Public security.

1. Introduction

Nowadays, with the rapid development of artificial intelligence, big data and the Internet, the digital transformation of public security governance has become a global trend. Governments worldwide face the common challenges of pursuing more efficient and precise capabilities in social security prevention and control as well as crime combat. Among them, artificial intelligence facial recognition technology, as a cutting-edge biometric identification method, has rapidly moved from laboratories to public spaces due to its non-contact nature, speed, and capacity for processing large amounts of information simultaneously. It has thus become a key technological tool to strengthen public security and has attracted extensive attention and in-depth discussions from all sectors of society [1].

The application of artificial intelligence facial recognition in public security is characterized by diversification and deepening penetration. From the initial static photo comparison to the current identity recognition and tracking under real-time dynamic monitoring, its application scenarios have been widely embedded. Specifically, the technology is used for identifying visible and concealed firearms, recognizing and tracking criminal suspects, and matching with massive databases, significantly enhancing the efficiency of case-solving. It can also be applied to the surveillance and early warning of key areas, like airports and stations, enabling proactive prevention of potential threats. Alerts generated by low response times in weapon detection within less than 1.5 seconds and misconduct detection within 2.2 seconds ensure rapid intervention. Data augmentation techniques, including rotation, scaling, flipping and panning, enhance the generalization ability of the model, achieving an accuracy rate of 93.5% and a precision rate of 92.8%. They have good real-time performance and a low false alarm rate, and have the potential for practical deployment in public security systems [2]. It is used to locate missing persons and bring hope of reunion to countless

families [3]. In addition, it also demonstrates great potential in fields such as security for large-scale events and intelligent transportation management. Through the application of artificial intelligence, fingerprint and facial recognition technologies have been significantly improved. The wide use of the Internet of Things has brought security challenges and also created new opportunities for the application of biometric recognition in various applications. These applications undoubtedly demonstrate the positive aspects of technology for public safety and enhancing the efficiency of social governance, essentially using technology to compensate for human resource limitations and build a safer society that better protects its people.

The aim of this study is to comprehensively examine the current application status of artificial intelligence facial recognition technology in public security, deeply analyze the multiple controversies it provokes, and ultimately explore the construction of a comprehensive governance framework that can balance security, efficiency, ethics and rights, allowing people to enjoy a safe and relaxed life in an environment without feeling constantly being surveilled.

2. The Application and Controversy of Facial Recognition in Public Security

2.1. Deduction

The core algorithm of facial recognition technology is based on a Convolutional Neural Network (CNN). CNNs gradually extract features from the input face image through multi-layer convolution operations, moving from low-level features (like edges and textures) to high-level ones (such as facial organ combinations and overall contours) [4]. First, the convolutional layer performs local feature detection on the image, while the pooling layer reduces the feature dimension and retains key information. Then, the extracted features are integrated and mapped through the fully connected layer, which are finally compared with the existing facial feature templates in the database. When the matching degree exceeds the preset threshold, identity recognition can be completed. The DeepID series launched by Tang Xiaoou's team innovatively adopts a multi-region feature fusion strategy, extracting 160-dimensional compact features with a single model. The verification effect is optimized through a joint Bayesian algorithm, laying the foundation for subsequent efficient feature extraction solutions [5].

This algorithm possesses the ability to extract high-dimensional features and the advantage of fast parallel computing: on the one hand, it can accurately capture the subtle features of the human face, such as facial bone structure and skin texture, ensuring the accuracy of recognition. Among them, the Hybrid DeepID FaceNet (HyDeepIDF-Net) model is representative. This model integrates the advantages of DeepID-Net and FaceNet to address the problem in pedestrian recognition that "facial features are one of the core discriminative bases, but a single model is vulnerable to interference". The process first utilizes the Viola-Jone algorithm to accurately detect the faces in the key frames of the video. Then, the residual images of the input video faces and the queried faces are extracted through the Deep Residual Network (DRN). Finally, the semantic matching of the residual images is achieved based on HyDeepIDF-Net. With the capture ability of DeepID-Net for facial detail features and the expression ability of FaceNet for global facial features, the accuracy of cross-camera pedestrian recognition is improved. [6] On the other hand, with the parallel computing architecture of hardware such as GPU, the comparison of massive facial data can be completed within milliseconds. For instance, the CUDA parallel computing architecture can be used with GPUs to accelerate the Eigen face algorithm. Research has optimized key computational steps in both the training phase (calculating the mean, zero-mean, normalizing Eigen faces, etc.) and the testing phase (projecting onto Eigen face space, calculating Euclidean distance, etc.) of the Eigen face algorithm using different GPU parallelization acceleration methods. Experimental results show significant speed-up effects across all computational steps within a training dataset size range of 320-920 faces. This achievement has greatly enhanced the operational efficiency of the Eigen face algorithm in scenarios with large data volumes, providing the possibility for its wide application in real-time face recognition and other fields, and also offering an important reference for subsequent research on face

recognition algorithms in the direction of hardware acceleration. It is precisely based on such technical principles that facial recognition technology naturally meets the demands of the public security for "quickly identifying people's identities and enhancing the efficiency of public security prevention and control". [7] For instance, in crowded places like stations and airports, it can conduct real-time and rapid identity screening of massive flows of people, assisting the police in quickly identifying suspicious individuals.

2.2. Analysis

2.2.1 Privacy infringement

The application of facial recognition technology requires the collection of facial data as a prerequisite, but in some application scenarios, there is a problem of "overstepping" in data collection. For instance, in order to enhance security management, a certain community has installed facial recognition access control systems in all public areas and at the entrances of apartment buildings. These systems not only collect facial data from the residents but also record and store the facial information of visitors indiscriminately without clearly informing people the scope of data usage and the retention period. This "full coverage" collection model, which binds citizens' daily travel trajectories with facial information, excessively infringes upon citizens' privacy rights and violates the principle of "minimum necessity" in data collection. Against this backdrop, some studies have combined chaotic mapping, error-correcting codes and locally sensitive hashing to propose a novel face template protection scheme. This scheme uses two sets of parameters, namely the global key and the user key, to generate data containing the storage key and the biometric template. When generating the template, chaotic sequences are used to scramble the extracted feature vectors, destroying the correlations among different dimensions. The user key is processed through error correction codes to generate the storage key, which is used to recover the user key during authentication. By using local sensitive hashing based on random numbers to process permutation vectors, a biometric template is generated. The experimental results and theoretical analysis show that this scheme has both good accuracy and security, effectively resisting various attacks on face templates, providing strong support for the further reliable application of face recognition technology in the field of security. [8]

2.2.2 Data security

As sensitive personal information, the leakage of facial data may pose serious security risks. In 2023, a provincial public security monitoring platform suffered a cybersecurity protection vulnerability, resulting in the leakage of over 100,000 pieces of facial data records, including facial images, identity information, and corresponding travel trajectories. Some of the data was used by lawbreakers for illegal activities such as telecom fraud. The existence of such data security vulnerabilities makes facial recognition technology convenient for public security governance while also becoming a "loophole" for criminals to obtain sensitive information, exposing the shortcomings in security protection during data storage and transmission. This requires legal collaborative governance. In addition to the collaborative governance of laws, the optimization and innovation of the technology itself is also the key to balancing the application and risks of facial recognition. Currently, privacy and security solutions that combine deep learning with encryption algorithms demonstrate great potential: First, the FaceNet deep learning algorithm is utilized to extract facial features. This algorithm, leveraging the structural advantages of multi-layer convolutional neural networks, can efficiently and accurately capture the core feature points of the face, providing a high-quality feature foundation for subsequent recognition. Second, the introduction of the CKKS fully homomorphic encryption algorithm enables face recognition operations to be performed directly on encrypted data, technically preventing the exposure of original facial features in plaintext and safeguarding user privacy at the source [9].

2.2.3 Algorithmic Bias

Training data for facial recognition algorithms often suffers from sample imbalance, leading to varying recognition accuracy rates across different demographic groups. Research data from the

Massachusetts Institute of Technology in the United States shows that the misjudgment rate of mainstream facial recognition systems for dark-skinned women is 37% higher than that for light-skinned men; and the recognition accuracy for the elderly and children is also significantly lower than that for young and middle-aged groups. In public security applications, this algorithmic bias may lead to unfair treatment of minority groups, such as innocent people being wrongly identified as suspicious individuals, causing issues like unfair law enforcement. One study innovatively combines convolutional neural networks (CNNS) with remote photoplethysmography (rPPG) to propose a brand-new face authentication method. This method takes advantage of the powerful feature extraction capability of CNN to deeply mine the detailed features of face images. Meanwhile, it uses the vital signal-related information obtained by rPPG to assist in authentication, effectively improving the accuracy of recognition [10].

2.2.4 Abuse of power

Some regions have experienced unauthorized expansion of facial recognition application scope. For instance, a municipal public security bureau in one city installed facial recognition surveillance equipment on a large scale in public areas like main roads, shopping malls, and parks for daily monitoring of pedestrian flow and behavior analysis, without obtaining proper authorization procedures. This exceeded the necessary scope of public security governance, resulting in "undifferentiated monitoring" and indirectly infringing upon citizens' personal freedom and dignity.

2.3. Future Development Trends

Through the analysis of multiple application cases and controversial events, this study has reached the following interim results. Firstly, the application value of facial recognition technology in public security is significant. It can effectively improve governance efficiency and reduce law enforcement costs, making it an important tool for promoting intelligent governance of public security. Secondly, the core contradiction of the current application disputes is that the speed of technological development does not match the speed of legal regulation and the construction of technical fault-tolerant mechanisms. The manifests specifically in the ambiguous boundaries defined by law for data collection, use and storage, and the need for improvement in algorithm optimization and security protection technologies. Thirdly, the focus of the dispute lies in two major pain points: "blurred boundaries of rights" and "lack of risk prevention and control". That is, the boundaries between the demands of public security governance and citizens' rights, such as privacy rights and personal dignity have not been clearly defined, and risk prevention and control measures, such as data security protection and algorithm bias correction, have not been synchronized with the application of technology. The future development trend will be to adapt to compliance, follow the principle of "minimum necessity", provide multiple alternative verification methods, and optimize the algorithm to reduce recognition bias through diversified samples and fairness algorithms. Finally, there is the security upgrade to establish a full lifecycle encryption and traceability mechanism for data, and to strengthen risk prevention and control.

3. Conclusion

This research systematically analyzes the application logic, core value, and contentious points of artificial intelligence facial recognition in the field of public security. It clarifies its irreplaceable role as an intelligent governance tool in enhancing screening efficiency and aiding criminal investigation, while also revealing the primary contradiction between technological application and the asynchronous development of legal regulation and risk control, along with prominent issues like privacy infringement, data insecurity, and algorithmic bias. This study not only clarifies the boundary relationship between public security needs and the protection of citizens' rights, but also provides a targeted analytical framework for the standardized development of technological application. It holds great significance for promoting the transformation of the industry from "priority on efficiency" towards a model that "emphasizes both security and fairness." Looking ahead, with the continuous

improvement of legal systems and ongoing technological iteration, facial recognition technology, under the guarantee of the rule of law, will achieve more precise and secure applications. It will inject sustained momentum into building an intelligent and humane public security governance system, ultimately realizing a beneficial symbiosis between technological innovation and social welfare.

Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

References

[1] Ali I A, Aiswarya B, Ezedin B, Khaled S. AI-powered biometrics for Internet of Things security: A review and future vision. Journal of Information Security and Applications, 2024, 82: 103748.

[2] Arul S, Kavitha P. Real-time crime monitoring system using deep learning for weapon, behavior, and facial detection. International Journal on Smart Sensing and Intelligent Systems, 2025, 18(1): 20250051.

[3] Face recognition allows vagrants to go home early. Chinese Civil Affairs, 2018, (11): 55.

[4] Chen B, Jiang X G. Convolutional neural network is used for facial feature extraction [J]. Modern Electronic Technology, 2022, 45(18): 182-186.

[5] Li X L, Liu Z K, Yu N H, et al. A region-based dynamic block image retrieval method [J]. Journal of Circuits and Systems, 2002, (01): 47-51.

[6] Ghogale K N, Apare R S, Borhade R H. HyDeepIDF-Net: Hybrid Deep ID FaceNet for Person Re-Identification. Journal of Ambient Intelligence and Humanized Computing, 2025, 16(6-7): 1-34.

[7] Li F, Yan X, Zhang X Y. GPU-based feature face algorithm optimization research [J]. Computer Science, 2021, 48(04): 197-204.

[8] Liu J Y, Wang Y, Wang K, Liu Z. A face template protection scheme based on chaotic map, error correction code and locality sensitive hashing. Cybersecurity, 2025, 8(1): 84.

[9] Byeon H, Shabaz M, Surbakti H, Keshta I, Soni M, Bhatnagar V. Deep learning and encryption algorithms based model for enhancing biometric security for artificial intelligence era. Journal of Ambient Intelligence and Humanized Computing, 2024.

[10] Wu L W, Yang C. IoT device identity authentication method based on rPPG and CNN facial recognition . International Journal of Advanced Computer Science and Applications (IJACSA), 2024, 15(5).