Research Progress and Development Trends of Identity Authentication Technologies for Ordinary Users

Haochen Ma

{2023006133@link.tyut.edu.cn}

College of Software, Taiyuan University of Technology, Jinzhong, Shanxi, China

Abstract. In today's rapidly evolving information age, identity authentication for ordinary users is an inevitable and important part of the field of human-computer interaction. Although significant progress has been made in recent years, the balance between security and usability remains an issue that cannot be ignored in the identity authentication of ordinary users. This article reviews the current mainstream identity authentication schemes for ordinary users, mainly analyzing identity authentication technologies such as deep convolutional neural networks, radio frequency fingerprint recognition, and multimodal information fusion. The full text discusses the existing limitations and future feasible development of current ordinary user identity authentication from the perspectives of security and usability.

Keywords: Human-computer interaction; Identity authentication; Security; Usability.

1 Introduction

Identity authentication for ordinary users is widely present in various scenarios of social life, ranging from online account registration, financial transactions to offline hotel check-in procedures. This undoubtedly demonstrates the great demand for identity authentication of ordinary users in today's social life. How to enable users to conduct identity authentication more safely, more efficiently, and more comfortably is an issue that must be discussed in the field of human-computer interaction.

In the current field of human-computer interaction, the identity authentication of ordinary users generally exhibits diverse characteristics. New types of identity authentication methods such as facial recognition and multi-modal information authentication have emerged one after another. Different from the traditional username-password identity authentication model, innovative biometric identity authentication methods have the advantage of high convenience, but still face three major problems: malicious attacks, environmental factors, and privacy protection. The identity authentication security issues faced by ordinary users are partly due to the cumbersome design of identity authentication. The cumbersome security design and poor user experience make users tend to adopt less secure designs. Taking password-based identity authentication by users as an example, according to the report released by CompariTech at the

ICIAAI 2026, May 22-24, Singapore, Singapore

DOI 10.4108/eai.22-5-2026.2365113

end of 2025, "123456" has been the most dangerous password for many years, and among the 2 billion leaked passwords worldwide, 761,000 accounts are still using this password [1]; another part can be attributed to the contradiction between the increasing information theft technology and the insecure design of identity authentication. The attack methods of current ransomware are gradually shifting from encryption to data leakage; at the same time, the role of generative artificial intelligence GenAI in network attacks is increasingly prominent, and attackers use it to accelerate attacks and steal information. Based on this development, it is necessary to design more secure identity authentication algorithms to balance usability and security, to optimize user experience as much as possible while ensuring that user information security is a top priority in the design of identity authentication for ordinary users.

Based on the above background, this paper focuses on two aspects: security and usability. It reviews and assesses the current mainstream identity authentication schemes for ordinary users. The research content will mainly cover three typical authentication schemes based on deep convolutional neural networks, radio frequency fingerprint recognition, and multi-modal information fusion. By analyzing the performance of these three schemes in dealing with three major challenges: malicious attacks, environmental interference, and privacy protection, as well as the current research status of their integration with deep learning algorithms, this paper discusses the current limitations of the identity authentication schemes for ordinary users and the feasible development directions for the future, with the aim of providing theoretical references and practical inspirations for building a more secure and convenient next-generation human-computer interaction authentication system.

2 Identity authentication based on facial recognition

In the exploration of the usability of identity authentication schemes, facial recognition has been widely developed and applied due to its unique convenience. Compared with traditional password verification and emerging biometric authentication schemes such as voiceprint and fingerprint, facial recognition authentication has the advantages of low complexity, high user acceptance, and high support from existing equipment. This has led to its excellent performance in authentication payments during the payment process, authentication unlocking of smart devices, assessment and attendance tracking in government offices, and even in the criminal investigation and arrest systems.

The research on face recognition can be traced back to the 1950s. In the early days, face recognition was limited to the combination of manually designed feature recognition based on the relative geometric positions of the face, which could achieve a rough recognition of the face. However, it was greatly affected by environmental factors [2]. The real development of the security and accuracy of face recognition technology began with the addition of deep learning algorithms, which made it possible to accurately identify and authenticate faces with high precision. However, when it comes to changes in the objects being recognized, such as the deviation of posture, the change of lighting angle, and the recognition filtering of complex backgrounds, most traditional deep models still have considerable recognition deviations and instability. To a certain extent, this can be attributed to the fact that the existing deep models rely on fixed modeling and have relatively weak ability to match face recognition features in dynamic real environments [2].

The Convolutional Neural Network (CNN) is an efficient deep learning model that is widely applied in image processing for face recognition. Through repeated convolution and pooling operations, it can fully simulate the visual observation effect of humans [3]. Musab Coşkun et al. trained the CNN using standard face datasets and achieved a face recognition accuracy rate of over 97% [4]. The high-quality improvement brought by CNN technology to face recognition technology will continue to be deeply integrated with face recognition technology in the foreseeable future, leading to more accurate recognition results.

Although deep convolutional neural networks have significantly improved the security and accuracy of identity authentication based on facial recognition, they still face many problems: the increasing threat to data security and the challenge of privacy protection; face recognition spoofing attacks and personal privacy ransom attacks have raised higher requirements for the accuracy and security design of face recognition; in dynamic environments, how to better avoid the influence of environmental factors such as lighting, and how to more accurately capture the objects to be identified and authenticated in complex background environments, are all directions that the future face recognition algorithms need to develop and optimize.

3 Identity authentication based on radio frequency fingerprint recognition

3.1 Radio frequency fingerprint identification identity authentication technology

The identity authentication technology based on face recognition has effectively solved the problem of "who am I". However, a completely trustworthy scenario requires not only ensuring the credibility of the person but also the credibility of the device connection, which is also an important part of identity authentication. With the widespread use of wireless devices in people's daily lives, accurately and effectively identifying target wireless devices in complex network environments and resisting unknown security threats has greatly increased the necessity of research on identity authentication for wireless devices. To adapt to the rapid development of wireless devices, the identity authentication method based on radio frequency fingerprint recognition has been proposed and used.

Radio Frequency Fingerprinting (RFF) refers to a technology that uses the basic physical characteristics of signals, such as frequency and phase, as the core identification of the device's physical layer. By accurately capturing and identifying the signal characteristics, identity recognition and authentication can be achieved. There are always minor differences in the characteristics of signals between different devices. These physical features, like human fingerprints, have uniqueness and stability. Due to their difficulty to be forged and their high binding with hardware devices, it greatly increases the difficulty of deception attacks and has high security. It has great potential for development in the field of wireless device identity authentication.

In the early days, radio frequency fingerprint recognition adopted a single-model processing method, which was greatly affected by wireless communication noise. The main challenge faced by identity authentication based on radio frequency fingerprint recognition lies in how to improve the feature extraction and recognition capabilities of radio frequency fingerprints and enhance the accuracy of recognition. In recent years, with the development of deep learning

technology, new possibilities have been provided for the precise recognition of radio frequency fingerprints. Relevant research mainly focuses on the feature extraction and recognition authentication algorithms of radio frequency fingerprints.

For ordinary users, the identity authentication scheme based on radio frequency fingerprint recognition is widely applied in daily life: The connection of smart home devices places high demands on the security of device connections. The application of radio frequency fingerprint authentication fundamentally prevents illegal access to the home network and provides security for the home. In the fields of mobile payment and wireless communication, traditional authentication methods lack defense against man-in-the-middle attacks. Direct authentication between hardware and hardware ensures the legitimacy of both connected parties. In addition, the access to some key facilities, the connection of smart cars and user devices, and the use of wireless devices, the design of identity authentication based on radio frequency fingerprint recognition effectively protects users' privacy information and property security.

3.2 Current research status of radio frequency fingerprint recognition technology

Regarding the issue of improving the accuracy of radio frequency fingerprint recognition, Yang Kai proposed to adopt the multi-dimensional fingerprint extraction method (MDFR) to mitigate the problem of inaccurate recognition caused by the mutual influence between devices [5]. The core of the MDFR method lies in the introduction of three modules: the data generation module is used to prepare input data for the network model, and the module converts the received binary radio frequency signals into floating-point format. The received data is processed using the RSV method, and the data fragments are divided into I signal data, Q signal data, and mixed signal data. The feature extraction module extracts the three divided data fragments in multiple channels in parallel to capture the subtle differences in the signals and obtain the hardware features of the radio frequency signals. The fingerprint fusion module's task is to optimize the feature representation, organize and integrate the output of the upper-level signal channels, and finally combine the fully connected layer for identity recognition and authentication. The advantage of the MDFR method is that it has higher stability and accuracy compared to traditional radio frequency signal recognition schemes, enhancing the identity recognition and authentication capabilities of wireless devices.

In the optimization of radio frequency fingerprint recognition technology by integrating deep learning models, the Transformer model based on the self-attention mechanism has also been widely used. The research by Li Mingdian et al. utilized the Transformer to establish the global feature correlation of RF signals in the problem of drone identity recognition, solving the problem of long-distance signal recognition and making progress in the recognition of drone video transmission signals [6]; Li Kaiqiang constructed the RFF-CAT model by integrating convolutional neural networks and Transformer encoder to solve the resistance problem of traditional radio frequency fingerprint recognition technology in noisy environments, and improving the recognition accuracy and robustness of identity authentication technology based on radio frequency fingerprint recognition [7]. In the future, radio frequency fingerprint recognition technology will continue to integrate with deep learning algorithms, building an impenetrable barrier for the use of ordinary users' wireless devices.

4 Identity authentication based on multimodal information

Identity authentication based on biometric feature recognition has more significant advantages of being more convenient and secure. However, in the face of increasingly complex user experience demands and increasingly severe security threats, the single-modal identity authentication is revealing its inherent vulnerabilities: facial recognition authentication based on deep convolutional neural networks is ineffective in accurately recognizing faces in dynamic environments; voiceprint recognition authentication is highly sensitive to environmental noise. Therefore, the concept of multi-modal identity authentication has emerged. The identity recognition authentication based on multi-modal information pushes the original single and static authentication process to a diversified and dynamic one, making biometric feature recognition more resistant to environmental factors, and is the inevitable direction for the development of ordinary user identity authentication design.

The realization of multimodal identity authentication lies in the integration that occurs at three levels of the biometric system, specifically including the feature extraction layer for extracting and integrating biometric features, the matching layer for comparison and recognition, and the final decision layer [8]. The integration in the feature extraction layer mainly involves the extraction of biometric features and behavioral features. The former includes features such as fingerprints, faces, and irises that are distinctive and stable; the latter includes behavioral features of mouse usage, walking gait, and other features with strong personal characteristics. Multimodal identity authentication enhances robustness while also increasing the complexity of feature integration and the difficulty of system design. Therefore, the design of the integration strategy has become a research focus. That is, the quality of the integration strategy determines the accuracy of the biometric feature recognition results. From the perspective of where the integration occurs, the integration strategy can be classified into different forms such as the data layer, feature layer, and matching layer.

The fusion objects at the data layer are the raw data directly obtained by the devices, which are only for the single-modal biological feature data. Although the most genuine and complete data is retained as much as possible, without the extraction of data features, it also means a huge amount of data and severe interference from environmental factors. Beyond some aspects of face recognition and image detection, the application of data layer fusion is not widespread.

The fusion of feature layers has a high requirement for the matching degree between modalities and dimensions. The features of different modalities and dimensions often have high variability and difficulty. Hu Zhenghao et al. have conducted in-depth research on the audio-video fusion recognition of feature layers. They first used the sound training signal to construct a Gaussian mixture model to obtain speech feature information, then used wavelets for face recognition, processed the information using the PCA method to obtain face feature information, and finally obtained the mixed feature matrix by using the serial and parallel methods for the two feature matrices, effectively improving the noise resistance and recognition rate of identity recognition. The key to the fusion of feature layers lies in the complementary fusion of feature representations, reducing the influence on the recognition result caused by environmental factors on a single module [9].

The fusion flexibility of the matching layer is high, and it is easy to integrate existing single-module recognition systems. When the features obtained from different single modules are difficult to fuse, the matching layer fusion is often adopted. Li Xiuyan's research on the multimodal biometric information identity recognition and authentication of handback vein features, fingerprint features, and iris features chose the matching layer fusion. Mainly, the mean fusion recognition algorithm and the maximum and minimum value fusion recognition algorithm were used. In addition, the fusion algorithm based on the k-NN classifier and the Bayesian method also had good performance in the matching layer fusion. The modular and flexible characteristics of the matching layer also gave it engineering friendliness different from other layers. It is the preferred solution for a number of identity authentication project designs based on multimodal information [10].

5 Discussion and analysis

The article mainly introduces three types of identity authentication technologies: identity authentication based on facial recognition, identity authentication based on radio frequency fingerprint recognition, and identity authentication based on multi-modal information. Each of these authentication methods has its own characteristics, as shown in Table 1. In different application scenarios, they demonstrate unique advantages and corresponding limitations, and have different usage conditions in different fields.

Table 1. Comparison of Three Identity Authentication Methods.

Technical type	Core advantages	Main challenges	Usage scenarios/characteristics
Face recognition	Excellent user experience, convenience, and simple operation	Low accuracy in dynamic environments (lighting, occlusion); High privacy and security risks; High requirements for resisting adversarial deception attacks (such as AI imitation)	Daily consumer applications (phone unlocking, online payment)
Radio frequency fingerprint recognition	High security, difficult to counterfeit	Signals are interfered by noise in complex environments; Need to enhance anti-interference capabilities	Wireless network environment with high security requirements
Multimodal identity authentication	High reliability, providing safety redundancy	Large system computational load, complex algorithms, high cost, and difficult data management	Scenarios with high demands for security and stability

Deep learning models, as a current popular development trend, when actively integrated with identity authentication technology, can significantly enhance the accuracy and robustness of identity recognition, to a certain extent avoiding the influence of environmental factors on the results. The face recognition based on deep convolutional neural networks, the RFF-CAT model integrating convolutional neural networks and Transformer encoder in the field of radio frequency fingerprints, and the fusion strategies based on deep learning models in multimodal

information identity authentication, all have excellent performances in identity recognition and authentication.

Overall, long-term security threats and unstable environments have always been the limitations of current identity authentication technologies. How to strike a balance between the security and usability of identity authentication design, the complexity of algorithms, the user experience, and the information computing volume of the system are all key points that need to be considered at this stage. In the future, multi-modal fusion authentication methods may have better development prospects and will have good adaptability in fields such as finance and government affairs that have high standards for identity authentication; the development of secure algorithms and the protection of user privacy are also key points for optimizing the design of identity authentication.

6 Conclusion

In recent years, the speed of informatization in people's daily lives has been accelerating. Under the dual demands of information security and users' good experience, the necessity of designing identity authentication for ordinary users has become increasingly prominent. This article introduces the three current mainstream identity authentication methods: identity authentication based on facial recognition, identity authentication based on radio frequency fingerprint recognition, and identity authentication based on multi-modal information. It discusses and analyzes their current usability and security. With the development of deep learning algorithms, the identity recognition and authentication technology will be better integrated with deep learning models, providing a safer and more comfortable experience for ordinary users' identity authentication.

References

[1] Bischoff, P.: ‘Minecraft’, ‘qwerty’, and ‘India@123’ among 2025's most common passwords: report. Comparitech News. (2025). https://www.comparitech.com/news/

[2] Qi, R.: Design and Implementation of Password Management System Based on Face Detection and Recognition. Heilongjiang University. (2025)

[3] Song, F., Li, B.: Research on Face Recognition Algorithm Based on Deep Convolutional Neural Network. Information and Computer. pp. 10-12 (2025)

[4] Xu, S., Xu, S., Wang, Z., et al.: Face Recognition Algorithm Based on Convolutional Neural Network. Journal of Physics: Conference Series. pp. 022023 (2020)

[5] Yang, Z. K.: Research on Wireless Device Identity Recognition Based on Radio Frequency Fingerprint. Qingdao University. (2024)

[6] Li, M. D., Li, L. W., Shen, A. Z., et al.: UAV Fingerprint Recognition Based on Deep Learning. Radio Engineering. pp. 1835-1846 (2025)

[7] Li, K.: Research on Radio Frequency Fingerprint Recognition Technology Based on Deep Learning. Shandong Normal University. (2025)

[8] Wang, Y., Mu, Z. C., Xu, Z. G.: Progress Review of Multi-modal Biometric Recognition Technology. Computer Application and Software. pp. 31-34 (2009)

[9] Hu, Z. H., Zhai, H., Jiang, Z. Z., et al.: Research and Implementation of Identity Recognition Based on Multi-modal Feature Fusion. Ship Electronic Engineering. pp. 54-57, 134 (2021)
[10] Li, X.: Research on Multi-Biometric Identity Recognition Methods. Tianjin University. (2010)