

Advancements and Applications of Federated Learning in Biometric Recognition

Zhengliang Lyu^a

Computer Science and Technology, China University of Mining and Technology-Beijing, Beijing, China

Keywords: Federated Learning, Biometrics, Data Privacy Protection.


Abstract: The extensive use of biometric technologies has rendered the enhancement of model performance, while safeguarding user privacy, a significant concern. Federated learning, an emerging distributed machine learning technique, enhances model generalization and accuracy while safeguarding user privacy through collaborative training across several devices. This paper reviews the application progress of federated learning in the field of biometrics, and discusses its advantages in improving model performance and protecting user privacy, as well as the challenges and future development directions. Specifically, this paper first introduces different types of biometrics in the past and their disadvantages, the basic concepts and advantages of federated learning. It subsequently conducts a detailed analysis of the application of federated learning in biometrics, encompassing data diversity, real-time processing, and privacy protection. Then, this paper discusses the challenges faced by federated learning in biometrics, such as data leakage risk, high computing resource demand and uneven data distribution, and proposes optimization strategies such as edge cloud collaborative computing and distributed computing optimization. Finally, this article anticipates future advancements in federated learning within biometrics. The significance of this paper is to introduce the broad prospects of federated learning in the field of biometrics, and provide an effective method to protect user privacy for future research in biometrics

1 INTRODUCTION

Internet technologies and artificial intelligence have pushed society toward comprehensive Informatization and intelligence. This tendency has made it simpler to transfer personal information quickly, making people more aware of the need to protect their privacy. Recent advances in artificial intelligence have led to the widespread use of user privacy data for deep learning model analysis in recommendation, risk assessment, and identity authentication systems. These technologies collect a lot of user data, which researchers mine, analyze, and choose from. Despite its benefits, technology is a "double-edged sword," with large data analysis risks privacy data leaks. When assessing customer purchasing preferences on e-commerce platforms, insufficient data protection may expose purchase records and browsing histories. This may make targeted fraud easier for crooks. Corporations must also manage huge volumes of user identifying data.

Any data breach in identity authentication systems could have dire consequences for users. As a result, disclosing information violates user privacy and causes further problems, which increases demand for better privacy protection.

The fingerprint recognition technique is the best-known biometric recognition system. Early on in the 1990s of the 20th century, various businesses sought to fit fingerprint identification on mobile phones, Siemens exploited Bromba's technology, and created the first prototype mobile phone with fingerprint recognition in 1998. But using this technology calls for particular motions, which is a little uncomfortable. It is only in recent years that capacitive, optical and ultrasonic methods have begun to be widely used in fingerprint recognition. Capacitive fingerprint recognition is the most widely used capacitive fingerprint recognition solution. The fingerprint recognition sensor is combined with the subcutaneous electrolyte of the human body to form an electric field, and the unevenness of the fingerprint surface

^a <https://orcid.org/0009-0003-3569-8349>

will cause the voltage difference between the two to fluctuate in a certain amplitude. With this change, the accuracy of fingerprint recognition will be improved. Optical fingerprint recognition primarily illuminates fingerprints using an integrated light source, gathers reflected and refracted light, and subsequently directs this light through a prism to illuminate the target object. It analyzes the intensity and angle of the reflected light, generating a graph with multiple gray values, which is then compared against a pre-existing database for matching (Li, 2020).

Palmprint recognition is a biometric identification technology that offers better privacy protection features. The most important characteristic of palm prints is the features of the palm lines (Chen et al., 2019). The main lines are the most stable and clearest features among the palm prints, which can still be distinctly identified even in low-resolution and low-quality images. Huang et al. (Huang et al., 2008) proposed a method for palm print verification based on principal lines, using the Modified Finite Radon Transform (MFRAT) to extract the principal lines of the palm print. Experimental results demonstrate that the principal lines have strong distinguishability. Jia et al. (Jia et al., 2009) proposed a method for palm print retrieval based on principal lines, detecting a large number of key points on the three principal lines and using these key points for retrieval. Li et al. (Li et al., 2010) enhanced the quality of palm print images using grayscale adjustment and median filtering based on the characteristics of the main lines in the palm print. They then detected the palm lines based on diversity and contrast, refined the results using an improved Hilditch algorithm, and finally obtained a single-pixel palm print main line image using an edge tracing method. The iris, as a biometric feature of the human body, is difficult to replicate and has natural anti-counterfeiting properties; it remains stable throughout a person's life. In the early 1990s, Daugman first proposed algorithmic architecture for iris recognition systems (Daugman, 1993), and researcher John Daugman from Cambridge University pioneered the iris biometric identification system for human recognition (Daugman, 1998). Daugman designed the famous Integro-Differential Operator (IDO) to mark the contours of the iris. Firstly, preprocess the iris image to enhance contrast; then, use differential operators (such as the Sobel operator) to extract edge information and identify the contours of the iris. Next, apply integral operators to smooth the image and reduce noise impact; finally, extract feature points and label them. This method can effectively improve the accuracy and stability of iris recognition.

Although these biometric technologies are already in use, they have certain drawbacks: iris recognition is very accurate, but its widespread application is limited due to the high cost of establishing iris recognition systems. The process of fingerprint recognition often involves physical contact, making it easy to be stolen in public places. These technologies do not provide any form of comprehensive security protection for personal privacy.

The remainder of the chapter is organized as follows. Firstly, this study will introduce the method of federated learning-based biometrics recognition in Section 2. Then, in Section 3, the future prospects and future challenges in the field of federated learning-based biometrics recognition in general will be discussed. Finally, Section 4 summarizes the paper and gives the conclusions drawn from the discussion.

2 METHOD

2.1 Concept of Federated Learning

Problems with data privacy, user rights to use their data, and the presence of data silos led to the development of the federated learning idea. Federated learning is a subset of distributed training that ensures data is both invisible and accessible when training deep learning models. It does not need collecting all data on a single server. This method successfully protects the private information of users while simultaneously monitoring the model's progress in training. By utilizing federated learning, any person may process data locally and safely share model updates with other participants at the same time. This method protects data privacy while also doing away with the hazards connected to centralized data storage. Federated learning is a promising solution for striking a balance between data utilization and privacy protection, which will eventually benefit individuals and society.

2.2 Federated Learning-based Face Recognition

Federated learning, which keeps users' facial information local to improve model generalization while protecting privacy, has been introduced as a means of privacy protection in recent years due to the rapid development of facial recognition technology. Due to variables like device capabilities and data volume, the global optimized model that the federated learning central server obtains may not always be the local optimum for the participants. As such, getting a

local model that works for each user is just as important as taking into account the best global model. Federated Face Recognition (FedFace) (Aggarwal et al., 2021) was proposed by Aggarwal et al. as a framework for group face recognition model learning. Using the local data set, the client trains the model updates before uploading them to the server. FedFace uses federated learning to expand the data set size and improve the performance of the facial recognition model by leveraging the models that have been trained on facial images from various clients. However, this approach may also result in user privacy violations because it requires uploading each local model's class embedding matrix.

It was suggested by Meng et al. (Meng et al., 2022) to include differential privacy technology in the model update procedure. When mapping user facial features onto a hypersphere during the model aggregation process in traditional federated learning frameworks, feature overlap can occur. This reduces the recognition accuracy of the model. As a result, Meng et al. (Meng et al., 2022) shares an embedding matrix with other users using a de-identified form. The server sends users a class center matrix with noise perturbations from other users based on the assumption that the server is trustworthy. Both feature privacy and feature overlap are addressed by the differential privacy local clustering algorithm (DPLC).

Another problem with traditional federated learning methods is that it becomes hard to compute the negative loss that is used to distinguish between different categories because a single client only has access to data from one category and lacks category information from other clients (Zhang et al., 2022). This reduces the ability to distinguish between category vectors, prevents inter-class distances from growing, and consequently has an impact on the model's overall performance. This paper offers a novel solution to the previously mentioned problems, which enables each client to calculate the negative item loss without directly disclosing the category vector information to other clients. This is accomplished by creating a new, comprehensive category vector on the server side by combining all of the client-provided category vector data. The client can compute the negative loss based on this newly generated vector once it has been received. The privacy and security of the data are guaranteed by the way this new vector is made, which prevents it from being used to retrieve any original category of vector information from the client. This new fusion vector is referred to as the aggregated category vector in this article. This paper uses cosine similarity to calculate

the similarity of the aggregated category vectors after they are generated, so that the aggregated category vectors sent to the client cover a wider feature space. The degree of direction similarity between two vectors is measured using cosine similarity. The two vectors are more similar when the cosine value is closer to 1, which also indicates that the angle between them is closer to 0 degrees. Thus, the aggregated category vectors are sorted and the types of aggregated category vectors are chosen based on the computed cosine similarity values (Gao, 2024).

2.3 Fingerprint and Finger Vein Recognition

2.3.1 Fingerprint Recognition Algorithm

A novel fingerprint recognition algorithm, termed FedGFR, has been proposed to address the challenges of subpar raw data quality and equitable client selection in federated learning for fingerprint recognition. The comprehensive system architecture of FedGFR integrates numerous local models via federated learning to develop a universal recognizer while safeguarding user privacy on the client side. A client fair scheduling strategy has been proposed to achieve a more equitable distribution of accuracy among clients in a federated learning framework. Upon the arrival of new clients in the training set, it is essential to determine whether to incorporate them into the existing sample array, followed by the random overwriting of sample data at a designated position within the set. Clients develop their recognition models through a federated learning approach utilizing their local data. The server acquires model parameters from data proprietors and consolidates them, revising the global model parameters via the FedAvg algorithm within the federated server. The consolidated global model is subsequently prior to the commencement of the new iteration, equitably selecting the clients participating in each round until the model reaches convergence. Thus, privacy concerns associated with centralized learning in conventional machine learning techniques can be avoided (Wang, 2024).

2.3.2 Development of a Finger Vein Recognition Algorithm N-Model Personalized Federated Learning

In N-model-based personalized federated learning, a series of aggregation algorithms is performed for N clients at the central server, producing a distinct aggregation model for each client on the server. Upon

gathering the local models from all clients, the central server will execute various model aggregation algorithms for each client. Consequently, when the finger vein datasets exhibit significant heterogeneity, the algorithm proposed in this paper can produce tailored aggregation models for each client on the central server, thereby personalizing the local models and effectively accommodating the distribution of their local datasets (Lian, 2023).

3 DISCUSSIONS

3.1 Issues in Federated Learning-based Biometrics Recognition

Federated learning has great potential in development and application, but it also confronts tremendous obstacles as shown below.

3.1.1 Computing Power Issues

Although federated learning can effectively improve model performance by training multiple devices together while protecting the privacy of all parties, the computational power of today's mobile devices only allows for the implementation of algorithms with small computational loads, such as logistic regression, on the device side. This limits the deployment of mainstream neural networks that include feedback processes (Yao, 2021). At the same time, to protect user privacy, federated learning often employs techniques such as differential privacy and homomorphic encryption. While these technologies provide privacy protection, they also increase computational overhead and reduce training efficiency. For example, the PrivacyFace framework mentions that the Differential Privacy Clustering Algorithm (DPLC), although capable of protecting privacy, introduces additional computational overhead, increasing the complexity of model training. Therefore, the issue of high computational resource demands is particularly prominent when integrating facial recognition technology with federated learning.

3.1.2 Communication Issues

Firstly, palm print recognition models typically use deep learning methods, such as convolutional neural networks (CNNs), which contain a large number of parameters. In addition, the palm print image itself has a large amount of data, especially in high-resolution images. For example, a high-resolution

image of a palmprint may be several megabytes in size, while a typical deep learning model may contain millions of parameters. This large amount of data will occupy a large amount of network bandwidth during the transmission process, resulting in low communication efficiency, and federated learning requires frequent communication between the client and the server, which will bring a huge burden to the transmission network and greatly prolong the training time. So the communication requirements of the coordinator are high, as it often needs to wait for all participants to deliver their intermediary data before performing secure aggregation or other data processing. One of the issues that hinders the development of federated learning is how to improve the capacity and quality of communication channels (Konečný et al., 2017).

3.1.3 Security and Privacy Issues

Biometric data (such as fingerprints, faces, iris, palm prints, etc.) is highly sensitive personal information. Unlike traditional usernames and passwords, biometric data is unique and unchangeable. Once leaked, users will face serious privacy violations and security risks. In federated learning, biometric data needs to be transferred frequently between the client and the server. However, most of the current research in the relevant literature assumes that the participants and servers of federated learning are secure and trustworthy, but in practical applications, there is a possibility that the user-sensitive model parameter information obtained during the training process may be exposed to the server or a third party, for example, in an unstable network environment, data transmission errors may occur, resulting in packet loss or corruption. Attackers can exploit these errors to obtain data through replay attacks, among other things. During data transmission, attackers can also disguise themselves as legitimate communication nodes to intercept and tamper with data. This will cause privacy leakage and reduce the security of federated learning systems (Sun et al., 2022).

3.2 Future Prospects

Federated learning in open-world environments is a new research domain. Despite notable research advancements, some challenges need further investigation, which is currently quite limited.

Initially, to mitigate the demand for computing resources, two methodologies—edge cloud collaborative computing and distributed computing optimization—are proposed as effective strategies to

address the high demand for computing resources and the low communication efficiency encountered in the integration of biometric technology and federated learning. Edge-cloud collaborative computing enables the offloading of complicated computational activities to the cloud, alleviating the strain on edge devices and optimizing the utilization of high-performance computing resources in the cloud. By optimizing distributed computing, one may dynamically modify the computational tasks and communication frequency of each device, equilibrate the computational load among various devices, and diminish communication overhead. The integration of these two methodologies can markedly enhance the computational efficiency of federated learning in biometric applications.

The second is the need to improve communication efficiency. This problem mainly stems from the large amount of data in the recognition model of palmprint, iris and other features, the difficulty of transmission optimization, and the complex communication coordination between different devices. In order to solve this problem, the following strategies can be adopted: asynchronous communication and data deduplication technology can be used to improve communication efficiency; Leverage edge computing technology to reduce direct communication between devices. Through these methods, the communication efficiency of federated learning in biometric tasks can be significantly improved.

Finally, in order to address the risk of data breaches, a variety of measures can be taken, such as data encryption, secure transmission protocols and authentication etc. Through these measures, the data security and privacy protection level of federated learning in biometric tasks can be effectively improved.

4 CONCLUSIONS

This article presents three categories of biometrics, each associated with certain limitations. In order to address the limitations of biometric recognition in practice, it is possible to mitigate potential risks by integrating it with federated learning. However, federated learning continues to encounter challenges. While it can safeguard personal privacy under specific circumstances, challenges in data processing and inefficiency must yet be resolved. In conclusion, within the current framework prioritizing data ownership and privacy safeguards, federated learning possesses significant promise. However, several technological hurdles and integration advancements

must be resolved. This review aims to offer support and inspiration for research in federated learning-based biometrics recognition.

REFERENCES

- Aggarwal, D., Zhou, J., & Jain, A. K. 2021. Fedface: Collaborative learning of face recognition model. In 2021 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-8).
- Chen, X., Jia, W., Li, S., et al. 2019. Palmprint recognition method integrating global and local directional features (in Chinese). *Journal of Graphics*, 40(4), 671-680.
- Daugman, J. G. 1993. High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(11).
- Daugman, J. 1998. Recognizing people by their iris patterns. *Information Security Technical Report*, (1).
- Gao, M. 2024. Research on face detection and recognition method based on federated learning (in Chinese). Doctoral dissertation, Changchun University of Technology.
- Huang, D., Jia, W., & Zhang, D. 2008. Palmprint verification based on principal lines. *Pattern Recognition*, 41(4), 1316-1328.
- Jia, W., Zhu, Y., Liu, L., et al. 2009. Fast palmprint retrieval using principal lines. In 2009 IEEE International Conference on Systems, Man and Cybernetics (pp. 4118-4123). San Antonio: IEEE.
- Konečný, J., McMahan, H. B., Yu, F. X., et al. 2017. Federated learning: Strategies for improving communication efficiency [EB/OL].
- Li, C., Liu, F., & Zhang, Y. 2010. A principal palm-line extraction method for palmprint images based on diversity and contrast. In 2010 3rd International Congress on Image and Signal Processing (pp. 1772-1777). Yantai: IEEE.
- Li, M. 2020. Research on the current situation and development trend of fingerprint recognition technology (in Chinese). *Wireless Internet Technology*, 17(01), 158-159.
- Lian, F. 2023. Research on finger vein recognition based on personalized federated learning (in Chinese). Doctoral dissertation, South China University of Technology.
- Meng, Q., Zhou, F., Ren, H., et al. 2022. Improving federated learning face recognition via privacy-agnostic clusters. *arXiv preprint arXiv:2201.12467*.
- Sun, E., Zhang, H., He, R., et al. 2022. Mobile communication resource management based on federated learning: Methods, progress, and prospects (in Chinese). *Journal of Beijing University of Technology*, 48(07), 783-793.
- Wang, C., Lu, Y., & Shen, J. 2024. Federated learning fingerprint recognition algorithm for fairness (in Chinese). *Computer Science*, 51(S1), 1014-1022.
- Yao, J. J., & Ansari, N. 2021. Enhancing federated learning in fog-aided IoT by CPU frequency and wireless power

control. IEEE Internet of Things Journal, 8(5), 3438-3445.

Zhang, Y., Liu, L., & Cheng, J. 2022. Training method and device for face recognition model based on federated learning (in Chinese) [Patent]. Beijing: CN202111509411.X.

