


# The Advancements and Future Prospects of Federated Learning-Based Methods for Biometrics

Yifan Zhang <sup>a</sup>

*Artificial Intelligence, Beijing Normal University-Hong Kong Baptist University United International College,  
Zhuhai, China*

**Keywords:** Federated Learning, Biometrics, Privacy Preservation.


**Abstract:** Biometrics has gained great attention due to its effectiveness in security applications recently. Although Deep Learning (DL) has proven useful in biometrics, but it requires huge, high-quality datasets and raises privacy issues. Federated Learning (FL) provides a solution, which trains models on clients and sending updates to the global model without sharing sensitive information. This paper reviews recent advances in applying FL for biometrics, mainly focusing on its use in face recognition, iris recognition, palmprint recognition, and finger vein recognition. Some FL-based methods such as FedFace, FedGC, PrivacyFace, and other methods are introduced, and their contributions are discussed in this paper. These methods have greatly contributed to privacy preservation and model performance. Despite the great progress, there are still great challenges and limitations in handling model interpretability and applicability due to the non-independent and identically distributed (non-IID) data and model complexity. The future prospects include enhancing model interpretability through techniques such as SHapley Additive exPlanations (SHAP) and Local Interpretable Model-agnostic Explanations (LIME) and improving applicability by implementing transfer learning and domain adaptation. This paper provides suggestions and references for future research and concludes that FL provides a promising path forward for biometrics.

## 1 INTRODUCTION

Biometrics, the science and technology of analyzing biological data, is under significant attention as a rapidly evolving field. Because the conventional information-saving methods is facing great challenges as the technological innovation day by day, using biometrics as the password is gaining increasing popularity, which have the features of uniqueness and non-transferability, and show great effectiveness in device unlocking, identity verification, and other practical applications (Jain & Kumar, 2012). Biometrics is mainly divided into two categories. The first category is physiological characteristics, such as fingerprints, iris recognition, facial recognition, and the second category is behavioral characteristics, which include gait analysis and voice recognition. Nowadays, researchers found that the traditional method used in biometrics may not have satisfactory predictive accuracy due to some special scenarios; for instance, monozygotic twins

have a high degree of similarity in facial appearance (Srinivas et al., 2011). Thus, researchers turned their attention to Deep Learning (DL), for it has great ability in feature extraction and prediction, which match well with the requirements of the biometrics field (Minaee et al., 2023).

In recent years, Artificial Intelligence (AI) such as DL have been widely used in fields like biology, chemistry, and especially biometrics. As shown by Saeed et al. (Saeed et al., 2022), deep learning methods based on Convolutional Neural Network (CNN) model have achieved great progress on classifying cross-sensor fingerprints. Similarly, the use of Deep Learning techniques has proven effective in face recognition and identification, as indicated by the research of Teoh et al. (Teoh et al., 2021). However, the high demand for biological data when using deep learning requires considerable resources and complicated data collection processes. Some approaches have tried to solve the problem through data sharing, but it may lead to leakage problems.

<sup>a</sup> <https://orcid.org/0009-0000-2520-9036>

Therefore, this has led to increasing concerns about the potential risk of revealing some sensitive user information.

In this regard, researchers have considered the need to implement Federated Learning (FL) to biometrics to protect user privacy. FL allows the client to update the model locally and only exchange model parameters, offering a secure and collaborative framework without sharing private and sensitive data (Tomashenko et al., 2022). According to the work form Cheng et al. (Cheng et al., 2022), a fingerprint-based localization system has gained progress after introducing a FL-based localization algorithm named FedLoc-AC. Additionally, the work form Gupta et al. on iris database performed in Federated Learning with CNN also gained effective outcomes (Gupta et al., 2022). In the same vein, FL has also been used in behavioral characteristics such as fall detection and automatic speech recognition (ASR), demonstrating the adaptability of FL to privacy protection requirements (Qi et al., 2023; Mammen, 2021). Since FL can effectively train biometric models while addressing the problem of user privacy protection, and numerous works have been proposed recently, it is vital to conduct a comprehensive review of the application of FL to the field of biometrics.

The remainder of the paper is organized as follows. In Section 2, this paper will summarize how to combine FL with biometrics to train models and make predictions under various situations. Then in Section 3, this paper will discuss some issues and limitations that exist in recent works, in the meantime exploring the future directions of Federated Learning in biometrics. Finally, the whole paper will be summarized in Section 4.

## 2 METHODS

### 2.1 Preliminaries of Federated Learning

Federated Learning, as a decentralized machine learning method, enables the clients to train a global model without sharing their local data. The main idea is that the central server only needs to aggregate these updates from the client to improve the global model to achieve preserving data privacy by using distributed data sources.

The basic components of FL include clients, the central server, and the communications between them. Clients could be the node or the devices that storing the data, and the gradients, weights, and model changes are sent to the central server. A typical

FL workflow consists of three steps: local training, model aggregation, and global model updates. The whole process iterates from multiple communication rounds until the central server's global model converges.

### 2.2 Federated Learning in Face Recognition

#### 2.2.1 FedFace

Bai et al. proposed a new federated learning framework called FedFace to the problem of face recognition (Bai et al., 2021). The framework contains two new algorithms, Partially Federated Momentum (PFM) and Federated Validation (FV). PFM applies the estimated equivalent global momentum locally to obtain approximate centralized momentum to solve the client drift problem while protecting training efficiency. The FV algorithm dynamically searches for the best federated aggregation weights by testing the aggregated model, thus enhancing the ability of generalization. Through experiments, FedFace has better privacy preservation and performance compared to formal FL methods.

#### 2.2.2 FedGC

Niu and Deng proposed a new federated learning method called FedGC in the face recognition field (Niu et al., 2022). This method introduces a SoftMax regularizer and a gradient correction mechanism at the base of FL infrastructure to enhance privacy protection and model performance. The innovation of FedGC is that it ensures each client has their own private, fully connected layer, and by precisely injecting cross-client gradient terms, it effectively solves the privacy-preserving and model performance decline issues that may occur in traditional FL methods. Through experiments on popular datasets, the effectiveness of the FedGC has been demonstrated.

#### 2.2.3 PrivacyFace

A new federated learning method called PrivacyFace was proposed by the study carried out by Meng et al. to enhance the privacy protection in facial recognition (Meng et al., 2022). By combining the tradition FL with Differential Privacy (DP) techniques, the method improves the model performance. PrivacyFace innovates an algorithm called Differentially Private Local Clustering (DPLC) for generating privacy-agnostic clusters of class centres. This approach ensures that no specific information

can be learned, no matter in what condition. Additionally, the study used a consensus-aware facial recognition loss function that can learn more discriminative features. The framework is proven to be differentially private by mathematics while introducing a lightweight overhead and achieving performance improvements.

## 2.3 Federated Learning in Iris Recognition

### 2.3.1 FedAvg-based CNN

Gupta et al. (Gupta et al., 2022), in their paper, put forward a method on iris recognition based on federated learning to protect the user's data privacy. In this work, the researchers utilized the CNN model to extract features and used Softmax as an activation function to enhance the functionality of currently in use frameworks. In addition, this paper discussed the influence of the number of clients and the training sessions on the model's effectiveness. This approach improved the accuracy of the iris recognition model while avoiding the transmission of sensitive user data.

### 2.3.2 FedIris

Luo et al. introduced a new federated learning framework called FedIris to improve the accuracy and privacy protection of iris recognition (Luo et al., 2022). In this framework, researchers proposed a Fed-Triplet loss function based on iris templates instead of typical averaging Empirical Risk Minimization (ERM) to enhance the interpretability. Besides, by adjusting the Wasserstein Distance to reweighting aggregation and incorporating it into Fed-Triplet loss, the high distribution shifts between the clients by the negative transfer will be mitigated. Experiments on multiple public iris data verify that FedIris surpasses model-sharing FL methods.

## 2.4 Federated Learning in Palmprint

### 2.4.1 PSFed-Palm

The work from Yang et al. proposed a novel physics-driven spectrum-consistent federated learning method named PSFed-Palm for palmprint verification (Yang et al., 2024). The method uses the physical properties of different wavelength spectrums and partitions the client into two groups: short-wavelength and long-wavelength groups based on their spectrum types, then designs the corresponding anchor models and constrains the optimization

directions. Besides, the work designed a spectrum-consistent loss function to ensure the consistency between different spectral templates. In this situation, the model can prevent model drift and protect data privacy without sharing local data, showcasing its vast potential for palmprint verification.

## 2.5 Federated Learning in Finger Vein

### 2.5.1 FedFV

Lian et al. proposed a federated learning framework called FedFV for finger vein certification (Lian et al., 2023). Through the use of FedFV, each client can acquire information from all members of the federation without resulting in the leakage of templates. Furthermore, the work also proposes a personalized federated aggregation algorithm called FedWPR in order to solve the issue of non-IID data brought on by client diversity, therefore, to obtain the best performance for each client. In addition, FedFV performed well on different scenarios, as the first personalized federal finger vein authentication framework, will also serve as a point of reference for upcoming studies on biometric privacy protection.

### 2.5.2 fvPAD

Mu et al. proposed a novel federated learning method for finger vein presentation attack detection (fvPAD) (Mu et al., 2024). The work first applied FL in fvPAD by considering the data volume and computational power among different clients and divided the traditional FL clients into two categories: institutional clients and terminal clients. For institutional clients, the work designed a triplet training mode combined with FL to enhance the model's generalization. Meanwhile, the study introduced an unsupervised learning module for terminal clients to enable the fvPAD model to adopt local data distribution and optimize itself while using unlabelled data. Through extensive experiments, the results showed the advantage in accuracy and robustness, especially when dealing with data from diverse clients.

## 3 DISCUSSIONS

### 3.1 Challenges and Limitations

#### 3.1.1 Interpretability

Despite the significant contributions of FL to address biometric issues, there also raise questions about the

model's interpretability. Because FL is trained on each client and the training process is non-transparent, this will increase the complexity of comprehending the model. Besides, the data held by the client are difficult to be Independent Identically Distribution (IID), therefore leading to data heterogeneity, for which the model needs to be generalized over different data distributions; this also affects the interpretability of the model. In addition, FL, through the exchange of the model update to protect privacy instead of using raw biometric data, may still encapsulate sensitive information. Consequently, providing interpretability of the model without any divulge is particularly challenging.

### 3.1.2 Applicability

In addition to the challenges about the interpretability, the problem of applicability associated with FL also poses a great challenge. Due to the non-Independent and Identically Distributed (non-IID) characteristics, such as label distribution skew, feature distribution skew, and data quantity skew, the model may be impeded to converge under the condition that some clients are significantly different in distribution from other clients. Thus, the model of the client may overfit to the local data to adapt to the data distribution, which can conflict with the objectives of the global model. Therefore, handling non-IID data in federated learning scenarios is significant to deal with applicability issues.

## 3.2 Future prospects

To mitigate these issues, focusing on enhancing model interpretability and using transfer learning and domain adaptation are key objectives for future research.

Introducing some existing instruments is efficient to enhance model interpretability. For instance, Expert System (ES) can help with comprehending how biometric data is used to train and predict the FL model. Based on the knowledge from expert systems, constructing an explainable model becomes more feasible. Additionally, implementing a popular interpretive model SHapley Additive exPlanations (SHAP) into FL in biometrics can help to understand how each feature contributes to the predictions made by the model, thereby enhancing the model's interpretability. Moreover, using Local Interpretable Model-agnostic Explanations (LIME) can be another option. LIME can create interpretable models locally based on specific prediction instances, hence providing more intuitive explanations for the predictions made by federated learning models in

biometrics. In addition, some advanced interpretability methods can be also considered. For example, Qiu et al. proposed a dense registration-based approach for improving the interpretability during the fingerprint matching process (Qiu, 2024). Yin et al. focus on enhancing the interpretability of face recognition by proposing a novel approach that incorporates a spatial activation diversity loss (Yin, 2019). This method is designed to facilitate the learning of more structured and interpretable face representations.

The utilization of Transfer Learning (TL) and Domain Adaptation (DA) can also facilitate future research at FL in biometrics. TL allows models to leverage knowledge acquired from one dataset to enhance performance on another dataset. Because the biometric data are rare and expensive, TL shows its particular effort in biometrics when there are limited labelled data. Meanwhile, biometric features tend to have different distributions in different cultures and regions captured by different devices. Owing to Federated Learning based biometrics being an interdisciplinary field, researchers can improve the model's applicability across various devices and environments through domain adaptation.

The future improvement of federated learning in biometrics tends to focus on how to improve the applicability and interpretability without sacrificing user privacy. By combining interpretability techniques, transfer learning, and domain adaptation, advancements will be gained in pursuit of this goal.

## 4 CONCLUSION

This paper provided a comprehensively review and summarization about recent advances in biometrics using Federated Learning. This paper has introduced several FL-based methods such as FedFace, FedGC, and PrivacyFace for face recognition and other methods for various biometric subfields. The integration of FL has led to significant advancements, but it also presents new challenges that must be navigated. The future prospects of FL in biometrics are full of opportunities, some potential research directions include mitigating non-IID data challenges, enhancing model interpretability. As a rapidly evolving field, the federated learning paradigm's application in biometrics still have great gaps to fulfill, but it has a promising future which user biometric privacy is preserved and data utilization is maximized. This paper aims to provide valuable insights and reference for researchers to continue pushing the boundaries in this field.

## REFERENCES

- Bai, F., Wu, J., Shen, P., Li, S., & Zhou, S. 2021. Federated face recognition. arXiv preprint arXiv:2105.02501.
- Cheng, X., Ma, C., Li, J., Song, H., Shu, F., & Wang, J. 2022. Federated learning-based localization with heterogeneous fingerprint database. *IEEE Wireless Communications Letters*, 11(7), 1364-1368.
- Gupta, H., Rajput, T. K., Vyas, R., Vyas, O. P., & Puliafito, A. 2022. Biometric iris identifier recognition with privacy preserving phenomenon: A federated learning approach. In *International Conference on Neural Information Processing* (pp. 493-504). Singapore: Springer Nature Singapore.
- Jain, A. K., & Kumar, A. 2012. Biometric recognition: an overview. *Second generation biometrics: The ethical, legal and social context*, 49-79.
- Lian, F. Z., Huang, J. D., Liu, J. X., Chen, G., Zhao, J. H., & Kang, W. X. 2023. FedFV: A personalized federated learning framework for finger vein authentication. *Machine Intelligence Research*, 20(5), 683-696.
- Luo, Z., Wang, Y., Wang, Z., Sun, Z., & Tan, T. 2022. Fediris: Towards more accurate and privacy-preserving iris recognition via federated template communication. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 3357-3366).
- Mammen, P. M. 2021. Federated learning: Opportunities and challenges. arXiv preprint arXiv:2101.05428.
- Meng, Q., Zhou, F., Ren, H., Feng, T., Liu, G., & Lin, Y. 2022. Improving federated learning face recognition via privacy-agnostic clusters. arXiv preprint arXiv:2201.12467.
- Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. 2023. Biometrics recognition using deep learning: A survey. *Artificial Intelligence Review*, 56(8), 8647-8695.
- Mu, H., Guo, J., Liu, X., Han, C., & Sun, L. 2024. Federated finger vein presentation attack detection for various clients. *IET Computer Vision*.
- Niu, Y., & Deng, W. 2022. Federated learning for face recognition with gradient correction. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 36, No. 2, pp. 1999-2007).
- Qi, P., Chiaro, D., & Piccialli, F. 2023. FL-FD: Federated learning-based fall detection with multimodal data fusion. *Information fusion*, 99, 101890.
- Qiu, Y., Chen, H., Dong, X., Lin, Z., Liao, I. Y., Tistarelli, M., & Jin, Z. 2024. Ifvit: Interpretable fixed-length representation for fingerprint matching via vision transformer. arXiv preprint arXiv:2404.08237.
- Saeed, F., Hussain, M., & Aboalsamh, H. A. 2022. Automatic fingerprint classification using deep learning technology (DeepFKTNet). *Mathematics*, 10(8), 1285.
- Srinivas, N., Aggarwal, G., Flynn, P. J., & Bruegge, R. W. V. 2011. Facial marks as biometric signatures to distinguish between identical twins. In *CVPR 2011 WORKSHOPS* (pp. 106-113). IEEE.
- Teoh, K. H., Ismail, R. C., Naziri, S. Z. M., Hussin, R., Isa, M. N. M., & Basir, M. S. S. M. 2021. Face recognition and identification using deep learning approach. In *Journal of Physics: Conference Series* (Vol. 1755, No. 1, p. 012006). IOP Publishing.
- Tomashenko, N., Mdahaffar, S., Tommasi, M., Estève, Y., & Bonastre, J. F. 2022. Privacy attacks for automatic speech recognition acoustic models in a federated learning framework. In *ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 6972-6976). IEEE.
- Yang, Z., Teoh, A. B. J., Zhang, B., Leng, L., & Zhang, Y. 2024. Physics-Driven Spectrum-Consistent Federated Learning for Palmprint Verification. *International Journal of Computer Vision*, 1-16.
- Yin, B., Tran, L., Li, H., Shen, X., & Liu, X. 2019. Towards interpretable face recognition. In *Proceedings of the IEEE/CVF International Conference on Computer Vision* (pp. 9348-9357).