Federated Learning Applications in Fingerprint and Finger Vein Recognition

Yongchao Wang

Computer Science, University of California, Davis, 95618 California, U.S.

Abstract. Fingerprints and finger veins are widely used in security identification in many fields due to their uniqueness and identifiability. However, their privacy issues are often criticized. This article summarizes several approaches that combine federated learning with fingerprint and finger vein recognition to solve privacy issues. One of the frameworks for fingerprint recognition, Federated Learning-Fingerprint Recognition, uses sparse representation techniques such as the Discrete Cosine Transform for data preprocessing. The framework also references the ResNet18 model and reservoir sampling so that each client can participate in training fairly. As for finger vein recognition, the Federated Learning-based Finger Vein authentication framework allows clients to share model weights to solve the data island problem and divide client data into shared and personalized parts to ensure privacy. This paper also points out its challenges, such as poor interpretability and applicability, and provides optimization solutions. For example, the interpretability issue can be solved by implementing an expert system. The expert system uses its robust knowledge base and inference engine to track model behavior and derive reasonable explanations. Transfer learning can also eliminate the applicability issue. It transfers the knowledge gained from training clients with concentrated data to clients with sparse data. In summary, this article comprehensively reviews the methods of federated learning in fingerprint and finger vein, respectively, and discusses the shortcomings and prospects.

1 Introduction

Fingerprints and finger veins (F&FV) are not unfamiliar to people nowadays. Fingerprints are the impression of ridge patterns in people's fingertips, and finger veins are the blood vessels under people's skin of fingers. Everyone's F&FV are similar but never overlap and remain unchanged throughout life. Due to these unique properties, F&FV recognition is used in many security-related fields, from F&FV information comparison at customs to validation for unlocking mobile phones. In traditional F&FV recognition, the input fingerprint and finger veins match the stored F&FV templates and compare the detail points across them. However, the conventional method has some limitations. F&FV comparison is less reliable when the input becomes blurred. For example, if the verifier's finger becomes damp or injured, the F&FV taken will differ from the template, resulting in recognition failure. Due to this

Corresponding author: yowwang@ucdavis.edu

consideration, more reliable methods should be considered to deal with these situations, such as combining F&FV recognition with artificial intelligence algorithms.

Due to its high efficiency and precision, Artificial Intelligence (AI) has been adopted by more industries in recent years and has helped them achieve breakthroughs. AI has gradually replaced human doctors in disease diagnosis [1]. Subsets of AI, such as machine learning and deep learning, have become decision-support systems due to their continuous self-learning capabilities and accurate diagnosis at low cost. Similarly, AI is widely used in chemistry. AI performs data analysis tasks when large amounts of data are present [2]. Besides saving time, AI can also predict new experimental data by training on large learning data sets [3]. In biometric recognition, the emergence of AI has significantly improved it in various aspects. The Internet of Things (IoT), a distributed network system in which different devices can communicate, has been challenged by security due to its widespread use. Nevertheless, a Convolutional Neural Network, a model under machine learning, can accurately extract facial features and create unique templates for recognition in real-time systems such as surveillance and access control, improving the security of IoT [4]. Since F&FV and facial recognition share the same principles, the trend of using AI algorithms in F&FV recognition is gradually increasing. For example, the minutiae-based method in fingerprint recognition is usually combined with an artificial neural network (ANN) [5]. Training the ANN model with a back-propagation algorithm enhances the accuracy of recognition and better processes low-quality images. However, in recent years, some works have gradually realized the importance of privacy in F&FV recognition, such as security, healthcare, etc. Considering privacy issues, more and more people are integrating federated learning with F&FV recognition. For example, Federated Weighted Proportional Reduction (FedWPR) is a new algorithm that aims to handle the problem of independent and identically distributed (non-IID) data across clients and ensure better aggregation of model updates in a federated learning setting [6]. Due to the importance of F&FV recognition for security verification and the fact that many algorithms have been proposed and developed in recent years, it is necessary to summarize federated learning combined with F&FV recognition comprehensively.

The rest of this review's framework is divided into three parts. The second part describes the current methods of combining F&FV and federated learning, and the third and fourth parts discuss and conclude the article. For the method part, this paper will first introduce the overall process of federated learning and then demonstrate how the federated learning algorithm combines machine learning and deep learning to solve various problems in F&FV recognition. The discussion will present some of the challenges currently facing this field and propose future development directions. Finally, the conclusion will give an in-depth summary of the entire article.

2 Method

2.1 Preliminaries of federated learning

Federated learning, shown in Fig. 1, is a decentralized machine-learning approach. It consists of a central server and multiple clients, each of which is an individual smart device, such as a smartphone or IoT device. The principle of federated learning is to keep the data in the client and train the model locally in each client without transferring data to the central server. The central server will first send the training model to the available clients. Instead of equally splitting the data between clients, the data on each client is highly heterogeneous in either size or composition. The clients will then do the local update for a few iterations and return only the updated model weights to a central server. The server finally improves the global

model by aggregating the updates and doing the entire process again. Because each client does not share data, federated learning preserves good privacy.

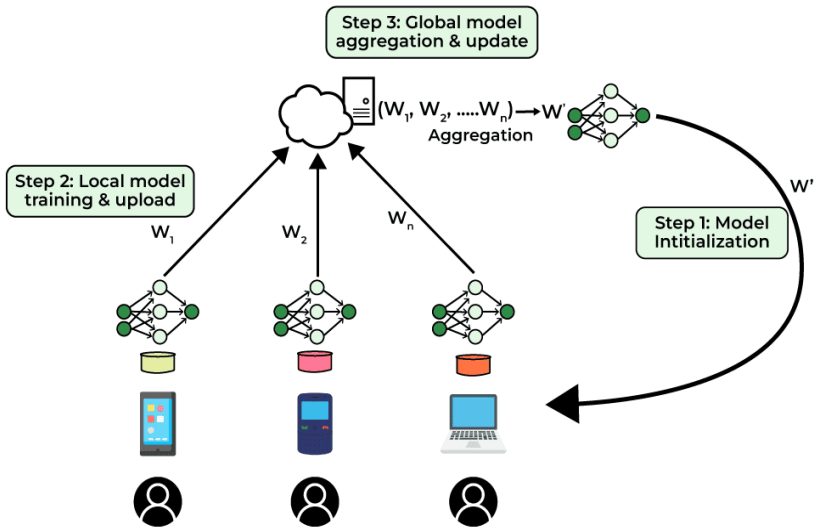

Fig. 1. The workflow of federated learning [7].

2.2 Federated learning-based fingerprint recognition

There are many ways to implement federated learning to protect privacy in fingerprint recognition. Federated Learning-Fingerprint Recognition (FedFR), a fingerprint recognition framework based on federated learning, solves privacy issues and enhances customer selection fairness and scalability [8]. Regarding data preprocessing, the study used sparse representation techniques, including Discrete Cosine Transform (DCT), K-SVD, and Orthogonal Matching Pursuit (OMP), to denoise the fingerprint images to improve image quality. Next, ResNet18 was selected as the model for local training for each client because of its superior accuracy and stability. To ensure fairness in client selection, the framework also introduced reservoir sampling, an algorithm that gives clients equal opportunities to participate in training to mitigate experimental bias. After the local model is trained, Federated Averaging (FedAvg) is used to aggregate the parameters of each client to ensure privacy by keeping data localized and only sharing model updates. Finally, the central server updates the global model by aggregating local model parameters, sending the updated model back to the client, and repeating the above steps until model convergence is achieved.

Furthermore, a dedicated framework is proposed to classify real and fake fingerprints while ensuring personal privacy. Each client in this framework uses an artificial neural network called a Convolutional Neural Network (CNN) [9]. The CNN model consists of convolutional layers, maximum pooling layers, and fully connected layers. They are trained locally on each client's dataset to ensure that biometric data never leaves the client's device. Following localized training, the model parameters are sent to a central server and aggregated using the FedAvg algorithm to form a global model. The server then sends the global model back to the clients for further training in an iterative process.

2.3 Federated learning-based finger vein recognition

In addition to its application in fingerprint recognition, federated learning has also made many contributions to vein recognition. For example, Federated Learning-based Finger Vein authentication framework (FedFV) aims to solve minor sample size problems and data diversity in finger vein authentication systems while ensuring customer privacy. Like most federated learning, this method involves training local models on each client's finger vein data without sharing the original data to prevent privacy leakage. Unlike this, FedFV allows clients to share learned knowledge through model parameters, alleviating the data island problem. The framework integrates the fed aggregation algorithm to ensure optimal performance by solving the non-IID data problem between clients. Among the clients, MobileNetV2 is adopted as the backbone model. It is divided into a shared part and a personalized part, where only the shared part is uploaded to the central server for aggregation, and the personalized part is retained locally.

Even though implementing FedFV effectively improves the accuracy and privacy of fingerprint recognition, more efficient client usage may still be needed. To further optimize the system, Personalized and Asynchronous Federated Learning for Finger Vein Recognition (PAFedFV) integrates asynchronous training to enhance client usage efficiency based on the FedFV framework [10]. It reduces the client's idle time by allowing clients to continue training their local models while waiting for the central server to update. In addition, the framework is enhanced by several tailored loss functions, such as Cross-Entropy and Cosine Similarity Loss, to extract finger vein features better and improve classification accuracy.

Another framework for federated learning in vein recognition is Dual-Decoupling Personalized Federated Learning for Finger Vein Recognition (DDP-FedFV) [11]. It protects privacy in finger vein recognition systems while addressing data heterogeneity. The framework applies a dual-decoupling mechanism in the model and separates domain-invariant features, which are generalizable information, from domain-specific features, which capture specific features in the client. Like FedFV, domain-invariant features are sent to the central server, while domain-specific features are retained in the local client to ensure data uniqueness. The framework introduces an aggregation method, Federated Personalization Weight Ratio Reduction (FedPWRR). This method calculates personalized aggregation weights based on the similarity of clients' data distribution and dataset size and tailors the global model for individual clients. Among them, MobileNetV3 is used as its backbone model and combined with SoftmaxLoss, CenterLoss, and reconstruction loss to extract and classify vein features accurately. Finally, DDP-FedFV aggregates domain-invariant features using FedAvg in the generalization phase, followed by personalized aggregation.

3 Discussion

3.1 Limitations and challenges

Although federated learning can benefit F&FV recognition, some potential challenges remain. In traditional F&FV recognition, researchers can see the reasons for recognition verification's success or failure because of its data transparency. With the support of these reasons, they can optimize the model. In contrast, although federated learning provides privacy, it also makes the entire process elusive because people can only access the weights instead of the original data. This reduction in interpretability prevents researchers from adjusting and improving the model through recognition analysis [12]. Additionally, the use of federated learning may result in a decrease in applicability. The data in F&FV recognition is highly personalized and varies from person to person. There is a probability that the model is trained

based on a specific group of people, which makes the model inapplicable to other groups. Individual differences or states, such as big and small or dry and wet fingers, will lead to data heterogeneity and non-IID problems. For federated learning, this may cause the convergence speed of its model to slow down, thereby reducing its overall performance. Another area for improvement besides model performance is efficiency. Since the computing power and storage space of F&FV recognition are usually limited, and federated learning sends the model and data to clients for local training, the training may strain the device when encountering complex models. This will result in reduced processing speed and increased energy consumption of the entire process.

3.2 Future prospects

However, the potential challenges mentioned above are not unsolvable. First, integrating expert systems into federated learning can effectively improve interpretability. An expert system is a computer program that solves a problem in a specialized domain using a knowledge base and an inference engine. This rule-based reasoning permits expert systems to follow and understand the behavior of models [13]. When applied to federated learning, expert systems permit full model transparency for any computations performed at either local or global levels. Based on its powerful features, expert systems can provide rule-based explanations of how a model makes decisions, solving the problem of interpretability.

Moreover, transfer learning, a machine learning technique, can solve the applicability problem. Transfer learning can transfer the knowledge gained from training on a task with a large amount of data to a task with sparse data, improving the performance of tasks with limited resources and reducing the need for retraining. In federated learning for F&FV recognition, transfer learning can be used in global models with extensive and diverse data. This method preserves the privacy of federated learning because only weights and features are transferred, and the transferred knowledge is used to perform local fine-tuning for each client, eliminating data heterogeneity and non-IID problems.

Finally, to optimize efficiency, researchers can add Sparse Ternary Compression (STC). A communication-efficient method meant to enhance federated learning, STC operates on the principle of sparsification and quantization. It applies sparsification to the model gradients and uses a ternary quantization scheme to transmit the remaining portion of the model gradient [14]. Applying STC to federated learning for F&FV recognition can overcome edge-device resource limitations. These devices only need to send and receive model updates in compressed form, alleviating the computation and the communication load. STC could enhance operational efficiency by lowering resource demand.

4 Conclusion

In this review, the paper investigated the federated learning framework for fingerprint and finger vein cognition to eliminate privacy risks. This article comprehensively summarizes some models in federated learning, such as FedFR and a dedicated framework in fingerprint and FedFV, PAFedFV, and DDP-FedFV in finger veins. Due to the unique properties of each method, they can be applied in different scenarios. For example, PAFedFV is more efficient under asynchronous conditions than FedFV, or DDP-FedFV is superior to the other two models in solving data heterogeneity. In addition, the article also points out the defects faced by the combination of federated learning with fingerprint and finger vein recognition. After discussion and analysis, it was found that federated learning has potential challenges regarding interpretability, applicability, and efficiency. In the future, federated learning can be integrated with expert systems, transfer learning, STC, and other methods to optimize the abovementioned problems.

References

1. S. Kaur, J. Singla, L. Nkenyereye, S. Jha, D. Prashar, G. P. Joshi, ... & S. R. Islam. Medical diagnostic systems using artificial intelligence (ai) algorithms: Principles and perspectives. IEEE Access, 8, 228049-228069 (2020).
2. R. C. Rial. AI in analytical chemistry: Advancements, challenges, and future directions. Talanta, 125949 (2024).
3. Z. J. Baum, X. Yu, P. Y. Ayala, Y. Zhao, S. P. Watkins, & Q. Zhou. Artificial intelligence in chemistry: current trends and future directions. Journal of Chemical Information and Modeling, 61(7), 3197-3212 (2021).
4. A. I. Awad, A. Babu, E. Barka, & K. Shuaib. AI-powered biometrics for Internet of Things security: A review and future vision. Journal of Information Security and Applications, 82, 103748 (2024).
5. N. A. A. Jabr. Pattern Recognition of Human Fingerprint Utilizing an Efficient Artificial Intelligence Algorithm. In International Conference on Signals, Machines, and Automation (pp. 569-578). Singapore: Springer Nature Singapore (2022, August).
6. F. Z. Lian, J. D. Huang, J. X. Liu, G. Chen, J. H. Zhao, & W. X. Kang. FedFV: A personalized federated learning framework for finger vein authentication. Machine Intelligence Research, 20(5), 683-696 (2023).
7. GeeksforGeeks. Collaborative Learning - Federated Learning (2024, March 20).
8. C. Wang, Y. Lu, & A. V. Vasilakos. Scalable Federated Learning for Fingerprint Recognition Algorithm. In 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 181-188). IEEE (2023, November).
9. A. Soni, M. Sandhya, & Y. S. Rao. Privacy Preserving Fingerprint Classification Using Federated Learning. In International Conference on Deep Learning, Artificial Intelligence and Robotics (pp. 71-80). Cham: Springer Nature Switzerland (2023, December).
10. H. Mu, J. Guo, C. Han, & L. Sun. PAFedFV: Personalized and Asynchronous Federated Learning for Finger Vein Recognition. arXiv preprint arXiv:2404.13237 (2024).
11. Z. Guo, J. Guo, Y. Huang, Y. Zhang, & H. Ren. DDP-FedFV: A Dual-Decoupling Personalized Federated Learning Framework for Finger Vein Recognition. Sensors (Basel, Switzerland), 24(15) (2024).
12. Y. Qiu, et al. Ifvit: Interpretable fixed-length representation for fingerprint matching via vision transformer. arXiv preprint arXiv:2404.08237 (2024).
13. B. G. Buchanan, & R. G. Smith. Fundamentals of expert systems. Annual review of computer science, 3(1), 23-58 (1988).
14. A. Khan, M. ten Thij, & A. Wilbik. Communication-efficient vertical federated learning. Algorithms, 15(8), 273 (2022).