

Federated Learning in Finger Biometrics: Opportunities and Challenges

Himani Bhardwaj¹, Akshay Juneja², Deepak Painuli³, Divya Mishra⁴, Priyanka Kumari⁵

^{1, 2, 3, 4}Department of Computer Science and Engineering, College of Smart Computing, COER University, Roorkee, Uttarakhand, 247667, India

⁵ECE Department, School of Engineering and Technology, CGC University, Mohall, Punjab, India

himanibhardwaj5606@gmail.com

akshay.j1207@gmail.com

prof.deepak.painuli@gmail.com

divya19aug@gmail.com

chaudharypriyanka01@gmail.com



This is an open-access article distributed under the terms of the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

In past decade, various architectures for fingerprint and finger vein biometric systems have been designed. They are utilized in various universities, organizations, and institutions. But there is an increase in number of forgeries due to lack of security in single biometric implementation across the globe. Therefore, the researchers have proposed different multi-modal architectures that utilize integration of fingerprint and finger vein identification, including federated learning, to preserve user privacy and security. The fingerprint data is processed using discrete cosine transform method. The deep learning architectures along with reservoir sampling are used to classify genuine and fake users. The federated learning is used to classify authenticate users to avoid data island problem. It permits to share model weights and divides user data into personalized and shared parts to ensure users' privacy. This paper highlights key challenges such as applicability and interpretability of optimization techniques. The interpretability is achieved using an expert system that uses its inference engine and knowledge base to identify the model's behavior that gives a reasonable explanation. This article discusses the limitations and challenges of federal learning with finger vein recognition and fingerprint.

Keywords – Biometrics, deep learning, federated learning, fingerprint recognition, finger vein recognition

1. Introduction

The terms related to finger biometric namely, fingerprint and finger vein (f&fv) are considered similar by public. The finger veins are a network of blood vessels hidden under the skin of an individual. On the other hand, fingerprints are the imprints of ridge patterns in an individual's fingertips. The f&fv of different persons appear similar, but they are unique and remain same throughout their life. Therefore, they are used in various areas of security and privacy. The

$f\&f\upsilon$ are used in different applications such as unlocking the smart phones to verify users' identity. As per the conventional techniques, the images of multiple $f\&f\upsilon$ are stored in the database as templates. The input image is matched with each template to identify the genuine users. However, in case of a finger injury or blurred image, the system fails to detect the individual. Therefore, AI based $f\&f\upsilon$ is needed to extract more relevant features and authentication of genuine users [1]. Deep learning and Machine learning are the subfields of AI that facilitate decision making process due to their characteristic of independent learning and self-improvement. They are used to perform diagnoses at cheap cost with high accuracy [2]. Further, a new test data is tested after training a large dataset [3]. Therefore, AI-based $f\&f\upsilon$ is the need of the hour. It performs self-learning to improve itself, and store new information with affecting the old data. In the domain of internet of things (IOT), authentication and security are a major challenge as many devices communicate and connect with each other over the internet. Therefore, this issue is mitigated using convolution neural network (CNN) to perform real time operations such as access restriction, monitoring, and authentication. It extracts characteristics from the biometric image of an individual and creates a template [4]. Although $f\&f\upsilon$ and facial based authentication works on the same principal, the applications of $f\&f\upsilon$ are increasing as they are highly reliable and secure as compared to facial identification.

The researchers utilized artificial neural network (ANN) to achieve fingerprint recognition using minutiae-based approach. ANN models use back propagation algorithm to ensure high precision to recognize and improve the distorted images. In recent years, the need of privacy and authentication gradually increases in different domains such as security and healthcare. Therefore, researchers have integrated federated learning and $f\&f\upsilon$ to improve privacy and security.

The major challenge is that the independent and identically distributed (non-IID) data across clients are handled by federated weighted proportional Reduction (fewer) that assures fine aggregation of federated learning model updates [5]. This paper focuses on the ongoing approaches of $f\&f\upsilon$.

The key contributions include:

- The generalized framework of federated learning technique is discussed.
- Existing modified federated learning techniques are discussed.
- Limitations and challenges of these techniques are presented.

Section 2 presents the existing methodologies related to federate learning in $f\&f\upsilon$ algorithms. It is followed by the optimization techniques and related challenges in Section 3. Finally, concluding remarks are presented in Section 4.

2. Background

This section presents the existing techniques on federated learning.

2.1. Preliminaries of federated learning

A decentralized machine learning technique is used in federated learning consists of multiple clients and central server including smart devices or IOT devices in its working environment. The data is trained and hold on to a local client model instead of directly transfer of data to the central server. Initially, the trained model is sent to the unoccupied client by the central server, followed by a non-uniform data splitting. The heterogeneous data is present at each client model that comprises the information. The first little iteration locally updates the performance of client model and returns the updated weights to the central server. The global improvement is performed at the central server and the complete process is repeated. The client models do not share the real data. It only sends the updated weights. Therefore, the federated learning framework preserves good privacy. The federated learning framework is shown in Fig.1. The summary of federated learning methodology is presented in Table 1.

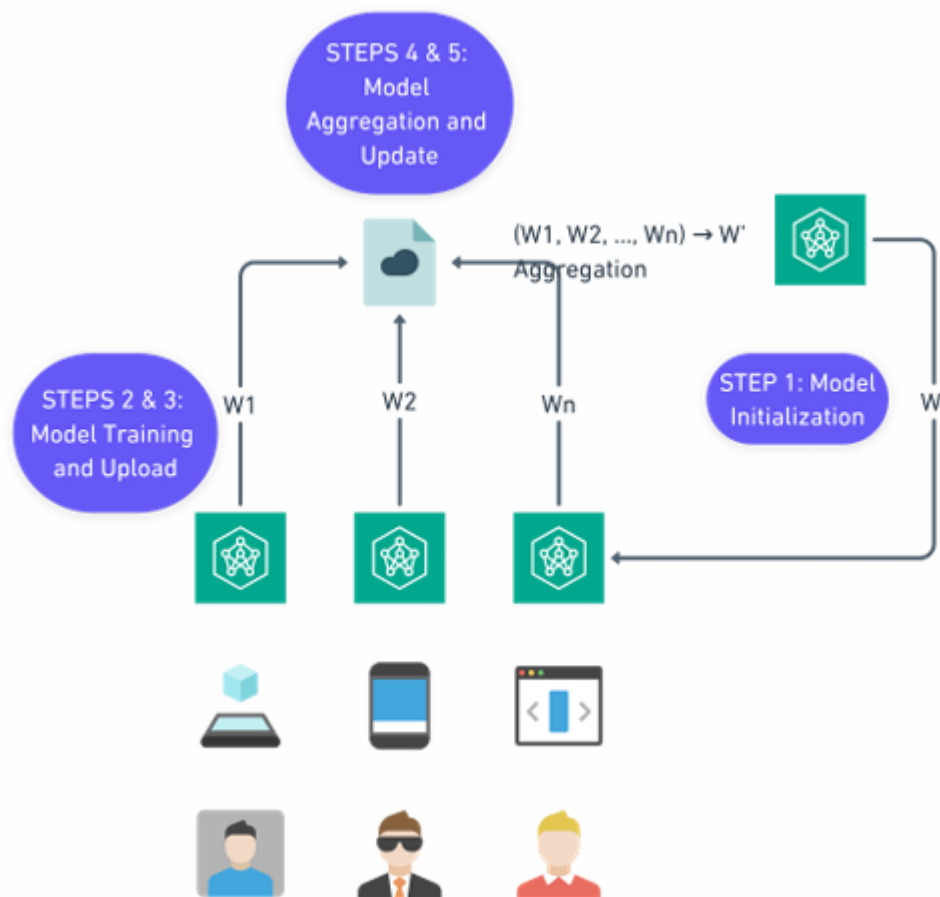


Figure 1 Framework of Federated Learning.

Table -1 Federated Learning Method Summary

Step	Description
1. Model Initialization	The central server creates a model and distributes it to all participating clients.
2. Local Training	Each client trains the model locally using its own private data to protect data privacy since raw data never leaves the device.
3. Upload Local Updates	After local training, clients submit the modified model weights or parameters to the central server.
4. Aggregation	The server combines all the incoming model updates to create a new global model.
5. Iteration	Steps 2 through 4 are repeated multiple times until the model converges to a stable state.

2.2. Existing Methodologies

There are several techniques that exist in the literature to solve the privacy issues, improve scalability, and achieve neutral behavior towards customer selection of $\mathbb{R}$ recognition [6]. These techniques include Sparse Representation, Discrete Cosine Transform (DCT), Orthogonal Matching Pursuit (OMP), and K-SVD in accordance with the data processing to obtain the improved image quality from distorted images. For instance, ResNet18 was used at client end for local training as it yields higher scalability and accuracy during client selection [7]. In another approach, a model was designed to provide each client uniform opportunity to reduce experimental bias, when local model training gets over. Therefore, the heterogeneous features from individual client model for model aggregation. A Federated Learning Averaging (Fedbag) is used to enhance the privacy as it shares the updated features and locally holds the real data. The global model is updated by the central server as it continuously follows the above process until the convergence is achieved. Moreover, to detect an artificial or real finger imprints, a dedicated framework designed using CNN is used by each client [8]. It ensures that biometric data is never erased from client devices. It is used locally at each client model and includes three major layers namely convolution layer, maximum pooling layer, and fully connected layer. The data is processed and aggregated at central server. Also, it globally updates the overall system and repeats the following process iteratively.

2.3. Modified Federated Learning Techniques

In [9], FedPWRR depicted a method for individual client as it calculates the Personalization Weight Ratio Reduction based on the similarity of clients. The data size and data distribution of these individual clients use a backbone model known as Mobilenet. It is combined with central loss, SoftMax loss, and reconstruct to fetch and label finger vein features accurately. The domain invariant features are obtained using FedAVG aggregates by DDP-FedFR followed by Personalized Aggregation.

3. Results And Discussion

This section presents different optimization techniques and related challenges.

3.1. Optimization techniques used in federated learning

There are several constraints present in the federated learning in $\mathcal{F}$ & $\mathcal{F}^*$ recognition such as applicability, communication overabundance, interpretability, data heterogeneity and transmission overhead. These issues are resolved using explainable artificial intelligence (XAI), that ensures model transparency and maintains data privacy at each level, i.e., local, hybrid or global level. The various federated learning techniques and their application levels are presented in Table 2.

Table -2 Techniques in Federated Learning and Their Application Levels

Technique	Level Applied	Use / Benefit
Differential Privacy	Local	Protects user data by adding noise before sending updates.
Personalized Federated Learning	Local	Improves accuracy by adapting model to each user.
Explainable AI (XAI)	Local	Explains predictions without sharing private data.
Expert System	Local / Global	Uses rule-based logic to explain model decisions.
Sparse Ternary Compression (STC)	Local	Reduces communication cost and device load.
Transfer Learning	From Global to Local	Applies learned knowledge to new, smaller tasks.
Robust Training / Encryption	Both	Protects against attacks and secures data transmission.

3.2. Limitations and Challenges

Although there are several advantages of federated learning in $\mathcal{F}$ & $\mathcal{F}^*$, it has various challenges as well. It comprises of the updated weights only. Therefore, it is difficult to modify and improve the system. In contrast with the traditional technique, the researchers access the recognition verification data including both successful and failed attempts that makes it comparatively easier to optimize the system [10, 11]. Moreover, if the training dataset may not include images of fingers with different sizes. Also, people with wet fingers are difficult to detect as it causes data heterogeneity and non-IID problems. The convergence speed of the model reduces, that affects the overall performance of a system. Furthermore, the $\mathcal{F}$ & $\mathcal{F}^*$ recognition system usually have limited memory and high computation cost. In federated learning, the process of sending data from the model to a client causes strain to the device capacity while containing the complex models. Therefore, to improve the interpretability of the model, an expert system is integrated with federated learning which is domain oriented. It utilized a computer system with a

knowledge base and inference engine. The expert system understands the model's behavior using rule-based reasoning. It provides full model transparency at both local and global level when federated learning is implemented [12]. Furthermore, the applicability issue is resolved using transfer learning. It eliminates the requirement of completely retraining the model. It improves the performance of task with limited resources and enables to transfer the knowledge gained from data rich task to task with limited data. It is implemented on global models with large and heterogeneous data by integrating it with federated learning for $\mathbb{R}$ and $\mathbb{C}$. Therefore, it protects the privacy of federated learning, as transferred information is used for tuning the hyper parameters. And updated weights are transferred [13]. In [14], a Sparse Ternary Compression is used to optimize the overall efficiency of the model. It operates on the rule of Quantization and Sparsification. A transmission efficient method is used to enhance the federated learning. It decreases the data in the model gradient by converting majority of the values to zero (scarification). In Ternary Quantization, only three possible values are used to send the rest of the data. The main advantage is to ingrate it with federated learning to conquer the Edge devices with limited resources. The small devices reduce load by transferring only compressed data and improves the computational efficiency and accuracy by reducing the resource demand.

4. Conclusion

Over the past decade, several biometric system architectures have been developed to enhance the reliability of fingerprint and finger vein recognition. However, there is an increase in forgeries that highlights the limitations of single-modal systems. Therefore, multi-modal approaches, i.e., $\mathbb{R}$ and $\mathbb{C}$ are utilized that are integrated with federated learning to improve the security and preserve user privacy. In this paper, the existing studies presenting fingerprint data processed using discrete cosine transform, and deep learning models coupled with reservoir sampling applied for user classification, are discussed. The federated learning is essential to resolve the data island problem as it enables the model weight sharing without affecting data privacy through personalized and shared partitions. Furthermore, interpretability challenges are addressed using expert systems that incorporate an inference engine and knowledge base. It provides the insights into the model's decision-making process. Finally, the challenges related to optimization applicability and interpretability is discussed. Therefore, the researchers must focus to enhance these areas to improve the robustness and transparency of federated biometric systems in future.

References

- [1] Hammed, M., Wane, M. A., Shakily, K. A., Shaba, H., & Bad El-Latin, A. A. (2024). Deep cancelable multibiometric finger vein and fingerprint authentication with non-negative matrix factorization. IEEE Access.
- [2] Alshardan, A., Kumar, A., Agamid, M., Mashie, M., Kalahari, S., Malherbe, A. A., & Alzahrani, Y. (2024). Multimodal biometric identification: leveraging convolution neural network (CNN) architectures and fusion techniques with fingerprint and finger vein data. Peer Computer Science, 10, e2440.
- [3] Kyeremeh, G. K., Abdul-Al, M., Awaji, R., Ali, N. T., & Abd-Alhameed, R. A. (2025). Fusion of Hand Biometrics for Border Control Involving Fingerprint and Finger Vein. IEEE Access.

- [4] Cadim, S. M., Paw, J. K. S., Take, Y. C., & Amen, S. (2024). Deep Learning Models for Biometric Recognition based on Face, Finger vein, Fingerprint, and Iris: A Survey. *Journal of Smart Internet of Tidings*, 2024(1), 117-157.
- [5] Wang, Y., 2025. Federated Learning Applications in Fingerprint and Finger Vein Recognition. In *ITM Web of Conferences* (Vol. 70, p. 01023). EDP Sciences.
- [6] Avenues, S. D., Sudharshan, B. S., Rishwanth, M., Suit, U., & Anita, G. (2025, June). Biometric Recognition using Fingerprint and Finger Vein. In *Proceedings of the International Conference on Materials, Energy, Environment & Manufacturing Sciences & Computational Intelligence and Smart Communication (MEEMS-CISC 2024)* (Vol. 269, p. 40). Springer Nature.
- [7] Wang, S., Sheen, Y., & Yang, W. (2024). Touch less Finger Vein and Fingerprint Verification via Exploiting Attention-Based Cross-Domain Fusion. *IEEE Transactions on Circuits and Systems for Video Technology*.
- [8] Juneau, A., Kumara, P., Bhatia, M., Tindal, H., Waxhaw, G., & Khan, P. (2024, December). Revival of Fingerprint Recognition-based Biometric Systems. In *2024 Eighth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 622-627). IEEE.
- [9] Gomez-Barrera, M. (2025). Finger vein. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 905-910). Cham: Springer Nature Switzerland.
- [10] Li, E., Yang, L., Wang, K., Wang, Y., & Yin, Y. (2025). Vein Pattern Based Partial Finger Vein Alignment and Recognition. *IEEE Transactions on Biometrics, Behavior, and Identity Science*.
- [11] Painful, D., Hardwar, S., & Chose, U. (2023). Optimized diagnosis of central nervous system (CNS) cancer using gene expression microarray & machine learning (ML) methods. *European Chemical Bulletin*, 12(10), 9757-9771.
- [12] Painful, D., Hardwar, S., & Chose, U. (2025). Efficient Feature Selection and Hyper parameter Tuning for Improved Speech Signal-Based Parkinson's Disease Diagnosis via Machine Learning Techniques. *Health Technology Assessment in Action*, 9(1).
- [13] NeeluJyoti, D. M. D. N. D., & Painful, A. D. (2018). Fuzzy Expert System to diagnose Psoriasis Disease. *International Journal of Computer Science and Information Security (IJCSIS)*, 16(9).
- [14] A. Sony, M. Sandy, & Y. S. Rae. 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).