ASEC 2025 Conference

The 6th International Electronic Conference on Applied Sciences

09–11 December 2025 | Online

MDPI

A Federated Learning Approach for Privacy-Preserving Automated Signature Verification

Haris Veraros, Fotios Zantalis, Stylianos Katsoulis, Elias Zois, Grigorios Koulouras*,

TelSiP Research Laboratory, Department of Electrical and Electronic Engineering, School of Engineering, University of West Attica, Ancient Olive Grove Campus, 250 Thivon Str., GR-12241 Athens, Greece

*** Corresponding author**

INTRODUCTION & AIM

The growing interconnectivity of digital systems has led to the massive collection and centralization of sensitive data, raising serious concerns about confidentiality and compliance with privacy regulations. Biometric authentication systems, such as Offline Signature Verification (OSV), are especially affected due to the personal nature of the data involved. To mitigate such concerns, Federated Learning [1] introduces:

- Distributed models training without exposing raw data
- Addresses privacy risks in OSV systems

In addition, Deep Learning models exhibit notable strengths and inherent limitations [2], such as:

- Strong performance in image-based recognition tasks
- Barriers of Robust training in data scarcity environments

METHODOLOGY

This work investigates privacy-preserving Writer-Dependent (WD) Offline Signature Verification (OSV) within an FL framework. To address limited biometric datasets, we explore complementary techniques [2], [3] such as:

- Data Augmentation
- Transfer Learning
- Knowledge Distillation
- Meta-Learning

Incorporating these approaches into FL pipelines can improve model generalization. The current implementation integrates the pre-trained CNN model into FL, leveraging the data augmentation as shown in Figure 1.

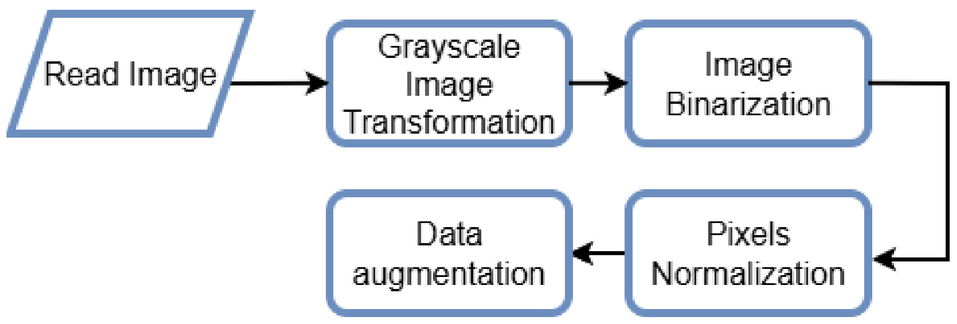

Fig. 1 - Federated Clients Image Pre-processing pipeline

RESULTS & DISCUSSION

Preliminary experiments suggest that combining FL with data scarcity mitigation strategies improves the robustness of signature verification systems. The data augmentation and transfer learning reduce overfitting and enhance classification performance, while knowledge distillation enables lighter yet accurate models suitable for distributed environments.

The proposed WD-OSV system (Figure 2) was trained and evaluated on the popular CEDAR signature dataset, on which an average Area Under Curve (AUC) of 88.93%, along with an average binary accuracy (ACC) of 80.12% are reported as preliminary results.

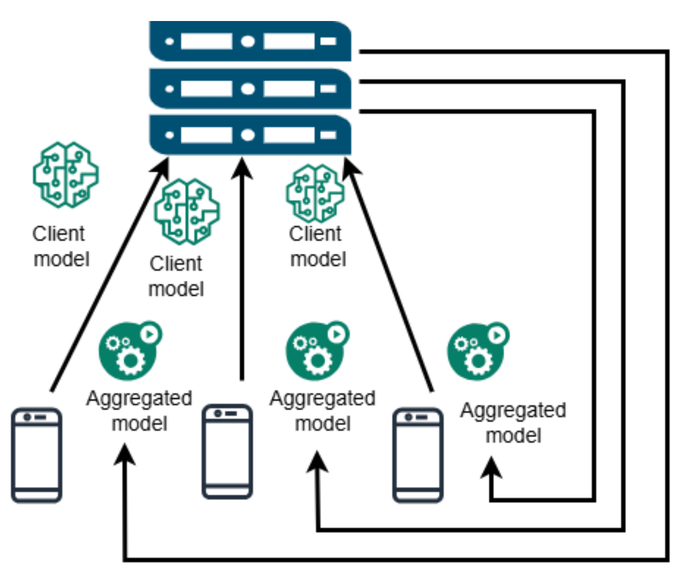

Fig. 2 - Federated Learning Diagram

CONCLUSION

FL offers a viable pathway to secure and effective biometric authentication by keeping sensitive data local. Incorporating advanced data efficiency strategies further strengthens the reliability of offline signature verification systems.

Beyond biometrics, the findings are extendable to healthcare applications, where privacy and data scarcity pose parallel challenges [4].

FUTURE WORK

Future research will focus on addressing the challenges of data scarcity in WD scenarios through the following directions:

- Advance synthetic data generation methods.
- Exploration of one/few shot learning methods.
- Federated Learning frameworks for improving clients' learning collaboration

REFERENCES

1. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial intelligence and statistics (pp. 1273-1282). PMLR. Link
2. Pandey, G. K., Raj, V., Agarwal, A., Dixit, M., Chauhan, S. S., & Srivastava, S. (2025, February). Offline Signature Verification: An Extensive Survey of Deep Learning Methods. In 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL) (pp. 892-898). IEEE. Link
3. Alzubaidi, L., Bai, J., Al-Sabaawi, A., Santamaría, J., Albahri, A. S., Al-Dabbagh, B. S. N., ... & Gu, Y. (2023). A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications. Journal of Big Data, 10(1), 46. Link
4. Upadhyay, A. K., & Bhandari, A. K. (2024). Advances in deep learning models for resolving medical image segmentation data scarcity problem: a topical review. Archives of Computational Methods in Engineering, 31(3), 1701-1719. Link