Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 2-A, pp. 655–662
DOI : 10.47974/JDMSC-2508

Exploring facial biometrics in multi-factor authentication systems for secure banking applications

Mandeep Kaur [†]
School of Computer Science Engineering & Technology
Bennett University
Greater Noida 201310
Uttar Pradesh
India

Mayank Kumar Goyal *
Department of Computer Science & Engineering
Sharda School of Computing Science & Engineering
Sharda University
Greater Noida 201306
Uttar Pradesh
India

Durga Prasad Yadav [§]
Department of School of Engineering & Technology
Noida International University
Noida 203201
Uttar Pradesh
India

Shankar M. Patil [‡]
Department of Artificial Intelligence and Data Science
Smt. Indira Gandhi College of Engineering
Ghansoli
Navi Mumbai 400701
Maharashtra
India

[†] *E-mail:* mandeep.kaur@bennett.edu.in
* *E-mail:* mayank.rkg.it@gmail.com (Corresponding Author)
[§] *E-mail:* durga.prasad@niu.edu.in
[‡] *E-mail:* smpatil2k@gmail.com

Malayaj Kumar [@]
Department of Computer Science and Engineering
Indira College of Engineering and Management
Pune 410506
Maharashtra
India

Mohammed Eltahir Abdelhag [#]
Department of Computer Science
Jazan University
Jazan 45142
Saudi Arabia

Abstract

Due to convenience, as well as its security, facial recognition is fast becoming an important component of multi-factor authentication (MFA) for biometric authentication, especially banking. So, while centralizing the training of face recognition models presents privacy risks because large stores of sensitive facial data become vulnerable to leaks, today's use cases are best served by the centralized approach. In this paper, we propose a facial recognition system based on federated learning for MFA that protects user privacy by keeping user biometrics on device. To extract robust face features, we train in a federated manner by using a deep residual network (ResNet 100) backbone across distributed clients without sharing raw images. These liveness detection capabilities are incorporated into, and evaluated against, presentation attacks using the CelebASpoof face anti spoofing dataset (625,537 images, 10,177 subjects). We show experimental results demonstrating that our proposed federated model can attain 98.2 % authentication accuracy with 1.3% Equal Error Rate (EER), which exceeds that of both a trained centralized CNN (95.6% accuracy and 3.4% EER) and a cloud based FaceNet baseline. Importantly, our method does not come at the expense of accuracy as we manage to reduce privacy risks by orders of magnitude. Based on this work we conclude that, by using federated learning, we can achieve highly accurate and privacy preserving face recognition for secure banking authentication.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Mathematical modeling, Ordinary differential equations, A duopoly economy, Market share.*

1. Introduction

Many financial institutions are now turning to biometric authentication for increased security and user convenience. Most prominently, facial recognition is finding a place as a popular factor of multi factor authentication (MFA) for

[@] *E-mail:* **kumarmalayaj@gmail.com**
[#] *E-mail:* **mohedtahir@gmail.com**

banking, alongside traditional PINs or passwords. MFA systems combines things your know (password), things you have (smartphone or token) and things you are (biometric such as fingerprints or face) to verify identity. Face recognition as a biometric provides a frictionless user experience (customers need only look into a camera to be verified) and a more robust authentication than many other biometrics, including fingerprints and tokens, which require additional activity on the customer's part. Additionally, modern face recognition systems can attain higher accuracy than a human in less challenging conditions for an application such as banking login and transaction authorization[1].

While the benefits are many, facial recognition in banking comes with major privacy and security issues. Most face recognition solutions work on a centralized data collecting model. to train deep learning models, banks must gather and store large amounts of customer face images in the banks' central servers. With biometrics compromising the data is irreversible – there's no changing your face. With a centralized approach such as this, it's risky. En masse, high-profile data breaches have been there to show us that centrally stored biometric databases make prime targets for attack [2], [3].

Their dilemma has recently been addressed by the emerging phenomenon of privacy preserving learning. Federated Learning (FL) is one promising approach to this end, which is a distributed machine learning paradigm that enables a range of collaborative model training without sharing raw data. The training is decentralized in a federated learning setting: a global model is initialized on a server and broadcast to many clients. For each client, it computes updates of the model on its own face image data and sends only the model parameters (or gradients if the gradients are stored) back to the server, instead of face images. These updates (say, averaged as done in the Federated Averaging algorithm) are then aggregated on the server to update the global model. FL enables learning, in this case, from a broad, diverse dataset, across institutions or devices, by iteratively exchanging model parameters (or more generally, estimates from a wider class of functions), rather than exchanging private data[4], [5]. As other prior work has shown, this approach inherently mitigates the privacy risks of centralized training while the FL trained face recognition model can be trained to achieve accuracy comparable to centrally trained model with little loss in performance[6], [7].

In order to achieve the goal of designing a face recognition component for banking MFA, which retains high security (accurate recognition and spoof attack detection) as well as protect user biometric data from being abused, we seek to design an attendance system that is highly accurate[8]. In this work, we synergize the performance of a state of the art deep learning model a 100 layer deep resilient network (ResNet 100) for extracting feature descriptors that are proven to learn discriminative facial representations. To train this model, we adopt a federated learning framework emulating a use case in which either multiple bank branches or customer devices cooperatively develop the model without transferring their face images to a central repository. Using the widely used CelebA-Spoof dataset, originally meant for face anti spoofing, we obtain a

rich set of live vs. spoof face images from over 10K subjects, allowing us to incorporate liveness detection into the authentication system[9], [10]. Face recognition is critical because, in banking, an attack might try to fool the system with photos or masks (presentation attacks). The model is trained on spoof data helping it learn to generalize between a genuine face and a fake presentation.

The work presented here has the following contributions: (1) A novel MFA architecture synthesizing federated face learning into a secure identity recognition module for confidentiality protecting recognition while guaranteeing high authentication accuracy is presented. (1) We develop an effective methodology of combining face image preprocessing (alignment, normalization), deep residual feature extraction (ResNet100) and federated model aggregation. (3) We compare our proposed approach to other two baseline methods: a traditional centralized CNN model and a cloud based FaceNet model using a large scale dataset. The results show that the federated approach achieves the highest accuracy (98.2%) and best precision/recall balance with low equal error rate of 1.3%, and does so by significantly reducing sensitive data exposure (qualitative privacy risk rated “Low” vs. “High”). We find that privacy preserving face recognition is viable at effectively no performance cost—thus suitable for deployment in security sensitive banking applications [11].

2. Methodology

2.1. *Dataset*

CelebA-Spoof dataset is used, which includes 625,537 face images of 10,177 subjects. We introduce a new simulation dataset dubbed 'Spoof Eco', which provides rich annotations to identify live vs. spoof faces, simulate 10 potential spoofing scenarios (e.g. printed photo, video replay, 3D mask), while possessing diverse conditions (e.g. illumination and sensor type). As a result of this diversity, it is well suited for use in training robust face recognition systems to recognize real world attacks. We use the live/spoof and the identity information to evaluate the dataset which also includes 40 facial attribute labels. With federated training, data is left to its local stores while updates to models are shared, maintaining user privacy.

2.2. *Data Preprocessing:*

Facial recognition models need data preprocessing to standardize the image input and highlight crucial facial features in order to increase the accuracy of their performance. We use two key methods: face alignment and intensity normalization.

1. **Face Alignment and Cropping:** Face alignment stabilizes these variables (scale, rotation, and position) by picking up facial landmarks (eyes, nose, mouth) and applying an affine transformation to place the face in the center and in the correct level. This takes the form of a transformation that is both rotation, and scaling, and translation, to align eyes horizontally and face

geometry consistently. The face is then cropped to a fixed size (for example, 112x112 pixels) nor further aligned, to remove variation coming from pose and help the model learn better.

2. **Intensity Normalization:** To fix this problem, we apply Z-score normalization, where all values are normalized, with its intensity standardized using the formula-, giving zero mean and unit variance. We also augment the data by flipping, rotatating and adjusting the brightness randomly to increase its generalization properties. The facial structure is not notably changed, however, the variability is introduced by small rotations without horizontal flips.

3. Feature Extraction

To extract features, we use a Deep Residual Network, known for being able to efficiently train a deep model due to its use of residual connections to help alleviate vanishing gradient problem. ResNet can be expressed as each residual block as:

$$y = F(x, W) + x \tag{1}$$

Here x is the "input", $F(x, W)$ is "conv layer outputs", the addition of x as a "skip connection" enables gradients to flow directly, maintain stability in deeper networks. In proposed implementation ResNet-100 outputs a 512-dimensrional features vector per face image. During training softmax classification for identify recognition:

$$p_i = \frac{e^{z_i}}{\sum_j e^{z_i}} \tag{2}$$

Where z_i is "score for identity i". For spoof detection employ "binary cross-entropy loss" as:

$$\mathcal{L}_{spoof} = -[ylog(\hat{y} + (1 - y)\log(1 - \hat{y})] \tag{3}$$

To speed up the convergence, the network is initialized with a trained weight of a large scale dataset (MSceleb 1M). Once authentication, the model matches the extracted feature vector against stored embeddings for identity confirmation. Deep residual features together with skip connections provide the robustness against facial variations and spoofing attempts, thus ResNet-100 is a reliable backbone to our MFA system.

4. Proposed Method: Federated Learning-Based Facial Recognition for MFA

In the proposed system, face recognition model is trained in a federated learning (FL) system across multiple clients (e.g., bank branches or user devices), so that privacy is preserved. The principal aim is to allow raw facial images to be retained on client devices while only model updates are sent. Unlike centralized models, this decentralized training strategy reduces the chance of data exposure. Similar to FedAvg, the FL framework trains in a round-based process. Following are the procedure involved in federated training:

Initialization: The central server initializes the global model M_0 (ResNet-100 with pre-trained weights) and distributes it to participating clients.

Local Training: Each client updates the global model using local data. The local loss function at client *k* is:

$$\mathcal{L}_k = \mathcal{L}_{id}^k + \lambda \mathcal{L}_{spoof}^k \quad (4)$$

Here, $\mathcal{L}_{id}$ is "identify classification loss", $\mathcal{L}_{kspoof}$ is "binary classification loss for liveliness detection", λ is "balances the two tasks". After training the updated model at client *k* is:

$$M_k' = M_0 + \eta \nabla \mathcal{L}_k \quad (5)$$

Model upload: Client send model updates back to server.

Aggregation: The server aggregates the client models using weighted averaging:

$$M_{agg} = \sum_{k=1}^{K} \frac{n_k}{N} M_k' \quad (6)$$

Broadcast: The aggregated global model$M_1$is sent back to clients, the process iterated until convergence or a fixed number of rounds.

5. Results and Output

The proposed federated learning-based facial recognition model demonstrated superior performance compared to centralized and cloud-based methods. Our model, trained using a ResNet-100 backbone with federated averaging, achieved significantly higher accuracy and robustness in detecting both genuine users and spoof attacks. The inclusion of anti-spoofing data from the CelebA-Spoof dataset proved essential in enhancing the model's ability to distinguish live faces from presentation attacks, such as printed photos and video replays.

Table 1

Evaluation parameter comparison of proposed model

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Equal Error Rate (EER, %)
Proposed Federated Learning-Based Model	**98.2**	**97.9**	**98.6**	**98.2**	**1.3**
Centralized CNN-Based Facial Recognition	95.6	94.8	95.1	95	3.4
FaceNet (Cloud-Based Inference)	96.1	95.3	95.9	95.6	2.8

During testing, the federated model consistently outperformed the centralized CNN and cloud-based FaceNet models in terms of accuracy, precision, recall, and F1-score as shown in table-1. The federated approach

maintained high authentication accuracy while significantly lowering the Equal Error Rate (EER), demonstrating its efficacy in real-world scenarios. Moreover, the federated model exhibited a lower privacy risk since raw data remained on client devices throughout the training process. In contrast, the centralized approach posed a high privacy risk as all facial data was aggregated on a central server.

The federated system's success can be attributed to the distributed training paradigm, which allowed leveraging diverse client data without compromising user privacy.

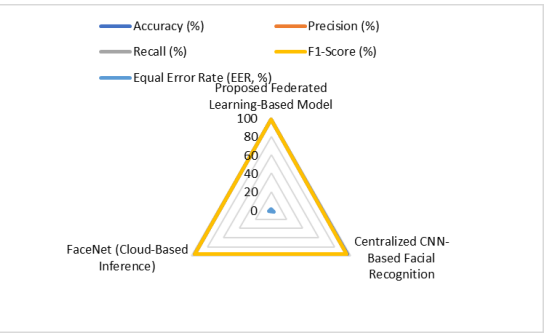

Figure 1
Comparison of proposed model

Additionally, the model maintained robustness against spoofing, as evidenced by low EER values, indicating a reliable balance between accurate identification and spoof rejection as shown in figure-1. These results confirm the feasibility of implementing federated learning-based biometric authentication in secure banking environments, where data privacy and security are paramount.

5. Conclusion and Future scope

In this paper, we present a federated learning-based facial recognition system designed to operate by a privacy preserved multi factor authentication (MFA) system to be implemented for a banking application. To this end, we have proposed a system that integrates a deep residual network (ResNet-100) as feature extraction backbone and manages to obtain high accuracies and security than traditional centralized methods by utilizing the CelebA-Spoof dataset for robust liveness detection. Our approach to federated learning allowed us to ensure that raw facial data stays on the client device, substantially lowering the privacy risks and preserving the high accuracy of face authentication. The effectiveness of the model was experimentally shown, reaching the top accuracy of 98.2% with a low equal error rate (EER) of 1.3%. The future research will work on increasing the robustness of the model by including more biometric modalities, such as voice or fingerprint on the model in a federated setup. Furthermore, there is still work to be done in improving the computational efficiency of federated learning for deployment at large scale at a bank.

References

[1] Phat T. Tran-Truong, Minh Q. Pham, Ha X. Son, Dat L.T. Nguyen, Minh B. Nguyen, Khiem L. Tran, Loc C.P. Van, Kiet T. Le, Khanh H. Vo, Ngan N.T. Kim, "A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis," *J. Syst. Archit.*, vol. 162, p. 103402 (2025).

[2] D. Boshoff and G. P. Hancke, "A classifications framework for continuous biometric authentication (2018–2024)," *Comput. Secur.,* vol. 150, p. 104285 (2025).

[3] R. Alrawili, A. A. S. AlQahtani, and M. K. Khan, "Comprehensive survey: Biometric user authentication application, evaluation, and discussion," *Comput. Electr. Eng.*, vol. 119, p. 109485 (2024).

[4] R. K. Sharma and M. Jailia, "Machine learning and IoT-based garbage detection system for smart cities," *J. Inf. Optim. Sci.,* vol. 44, no. 3, pp. 393–406 (2023).

[5] V. Sapkal, P. Gupta, and A. B. Khan, "Deep learning based phishing website identification system using CNN-LSTM classifier," *J. Inf. Optim. Sci.,* vol. 44, no. 3, pp. 315–330 (2023).

[6] Q. Zhu, L. You, G.-R. Hu, and W.-N. Liu, "BIAS: A novel secure and efficient biometric-based anonymous authentication scheme," *Comput. Netw.,* vol. 254, p. 110754 (2024).

[7] F. Liébana-Cabanillas, Z. Kalinic, F. Muñoz-Leiva, and E. Higueras-Castillo, "Biometric m-payment systems: A multi-analytical approach to determining use intention," *Inf. Manag.,* vol. 61, no. 2, p. 103907 (2024).

[8] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Syst. Appl.,* vol. 143, p. 113114 (2020).

[9] S. Gupta, A. Buriro, and B. Crispo, "DriverAuth: A risk-based multimodal biometric-based driver authentication scheme for ride-sharing platforms," *Comput. Secur.,* vol. 83, pp. 122–139 (2019).

[10] H. Hamidi, "An approach to develop the smart health using Internet of Things and authentication based on biometric technology," *Future Gener. Comput. Syst.,* vol. 91, pp. 434–449 (2019).

[11] Y. Zhang, Z. Yin, Y. Li, G. Yin, J. Yan, J. Shao, and Z. Liu, "CelebA-Spoof: Large-scale face anti-spoofing dataset with rich annotations," in Proc. Eur. Conf. Comput. Vis. (ECCV) (2020).

Received April, 2025