Federated Learning for Face Recognition via Intra-subject Self-supervised learning

Hansol Kim[1] Hoyeol Choi Youngjun Kwak[2] *

[1] Graduate School of Software Technology, Kookmin University, South Korea

[2] *Department of Electrical Engineering, KAIST, South Korea*

Introduction

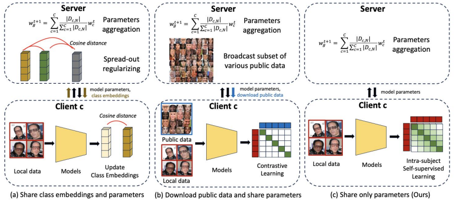

Figure 1: Pipelines of federated learning-based face recognition methods including our proposed method. (a) The server collects class embedding of client c (e.g. FedFace). (b) Client c continuously downloads public data from the server (e.g. FedFR). (c) Our proposed method(FedFS), client c performs intra-subject self-supervised learning without any additional work.

Definition

- In Environment of Federated Learning for Face Recognition, client have only own face datasets in their device.

Problem

- Previous methods use personal feature vector or public datasets.
- There are private issue and memory.

Contribution

- We propose FedFS, Federated Learning for personalized Face recognition via intra- subject Self-supervised learning framework. FedFS trains optimized facial features for each client and reduces intra-class variation by leveraging adaptive soft label con- struction utilizing dot product and intra-subject self-supervised learning employing cosine similarity while protecting users' data privacy.

- Regularization loss is proposed to prevent bias in the performance of personalized models. Through this, FedFS solves the problem of easily falling into overfitting when training only with personal data, and trains indirectly generalized facial features.

Experiments

Pre-trained model	FL method	DigiFace-1M		VGGFace		Pre-trained model	FL method	DigiFace-1M		VGGFace	
		AUROC	%	AUROC	%			AUROC	%	AUROC	%
MobileFaceNet	-	0.8248	-	0.8921	-	PocketNet	-	0.9128	-	0.9806	-
	FedFace	0.5001	-60.6%	0.5488	-61.51%		FedFace	0.4998	-54.7%	0.5865	-59.8%
	FedFR	0.8270	+0.2%	0.9477	+6.2%		FedFR	0.9637	+5.5%	0.9875	+0.7%
	FedFS(Ours)	**0.9629**	**+16.7%**	**0.9794**	**+9.7%**		**FedFS(Ours)**	**0.9794**	**+7.2%**	**0.9934**	**+1.3%**
GhostFaceNets	-	0.9612	-	0.9885	-	MobileNetV2	-	0.9339	-	0.9645	-
	FedFace	0.5106	-53.1%	0.5905	-59.7%		FedFace	0.5055	-54.1%	0.5542	-57.4%
	FedFR	0.9644	+0.3%	0.9929	+0.4%		FedFR	0.9588	+2.6%	0.9876	+2.3%
	FedFS(Ours)	**0.9944**	**+3.4%**	**0.9943**	**+0.5%**		**FedFS(Ours)**	**0.9647**	**+3.3%**	**0.9922**	**+2.8%**

Table 1: AUROC of various federated learning methods on DigiFace-1M and VGGFace. Each method uses MobileFaceNet, PocketNet, GhostFaceNet, and MobileNetV2 as a pre-trained model to measure AUROC and the AUROC increase/decrease rate compared to the pre-trained model.

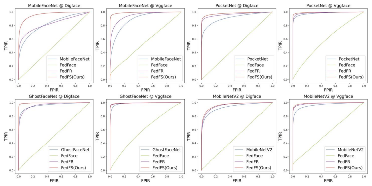

Figure 3: Each graph represents the ROC curve against the pre-trained model @ benchmark and the ROC curve against federated learning methods using the pre-trained model.

Methods

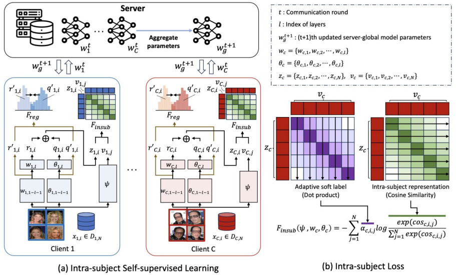

Figure 2: (a) is an overview of our proposed training process and (b) is the detailed process of intra-subject loss. The global model outputs two vectors and the personalized model also outputs two vectors. Using each output, we calculate regularization loss and create a z_c vector. Intra-subject loss is measured using the z_c vector and the output vector of the pre-trained model.

Regularization loss

$$F_{reg}(w_c,\theta_c) = 1 - \frac{r'_{c,i} \cdot q'_{c,i}}{||r'_{c,i}||_2 \cdot ||q'_{c,i}||_2}$$

Total loss

$$F_{total}(\psi, w_c, \theta_c) = \lambda * F_{insub}(\psi, w_c, \theta_c) + (1-\lambda) * F_{reg}(w_c, \theta_c)$$

Definition

$$r_{c,i} = \phi_c(x_{c,i}, w_c), \quad q_{c,i} = \phi_c(x_{c,i}, \theta_c), \quad v_{c,i} = \xi(x_{c,i}, \psi), \quad z_{c,i} = r_{c,i} \oplus q_{c,i}$$

Cosine similarity between personal face data

$$cos_{c,i,j} = 1 - \frac{z_{c,i} \cdot v_{c,j}}{||z_{c,i}||_2 \cdot ||v_{c,j}||_2}$$

Adaptive soft label

$$ass_{c,i,j} = z_{c,i} \cdot v_{c,j}, \quad ASS_{c,i,j} \in \{ass_{c,1,j}, \dots, ass_{c,i,j}\}$$

$$\beta_{c,i,j} \begin{cases} ass_{c,i,j} * \gamma, & \text{if } y_{c,j} = 1 \\ ass_{c,i,j}, & \text{else if } \star \\ 0, & \text{otherwise} \end{cases}$$

$$\alpha_{c,i,j} = \left(\frac{exp(\beta_{c,i,j})}{\sum_{i=1}^{N} exp(\beta_{c,i,j})}\right)^T$$

Intra-subject loss

$$F_{insub}(\psi, w_c, \theta_c) = -\sum_{j=1}^{N} \alpha_{c,i,j} log \frac{exp(cos_{c,i,j})}{\sum_{j=1}^{N} exp(cos_{c,i,j})}$$

* Corresponding author