UNIVERSITY of HOUSTON
CULLEN COLLEGE of ENGINEERING

ANTS LAB

Federated Learning of User verification Models Without Sharing Embeddings

Hossein Hosseini, Hyunsin Park, Sungrack Yun, Christos Louizos, Joseph Soriaga, Max Welling

ICML 21

Presented by Huai-an Su

Outline

- Background & Motivation
- FedUV method design
- Implementation
- Results
- Conclusion

Background & Motivation

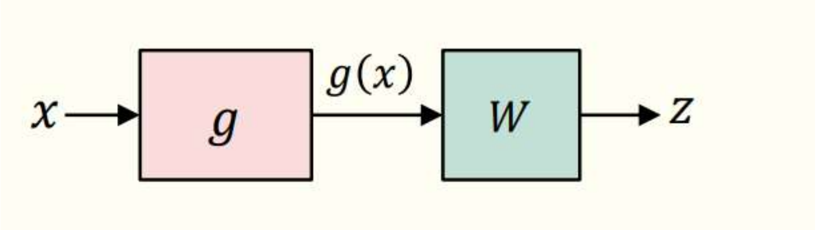
- User verification models have multiple forms of modalities
- Face, voice, fingerprint
- Used on mobile devices for unlocking or specific services

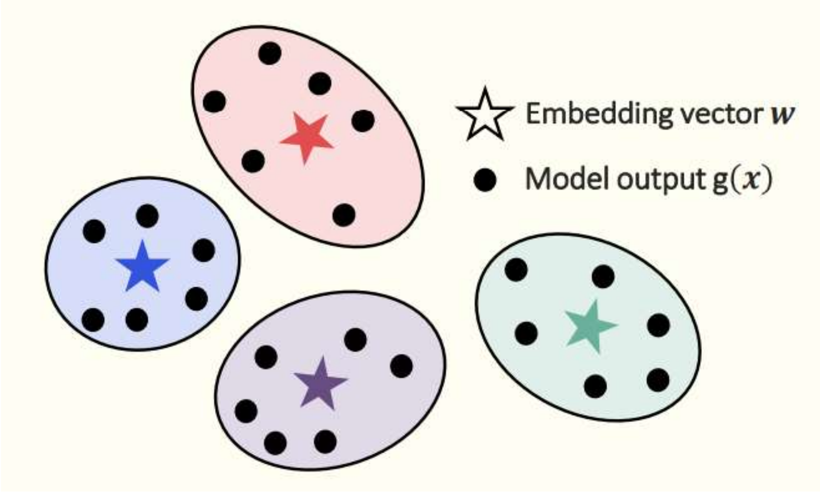
ANTS LAB

UNIVERSITY of HOUSTON
CULLEN COLLEGE of ENGINEERING

Background & Motivation

- User verification models: embedding-based classifier
- The embedding of data should be close to its user and away from other users





Background & Motivation

- How to train UV model: calculating loss function

  1) positive loss: minimize distance of g(x) to embedding vector of corresponding user

  2) negative loss: maximize distance of other users

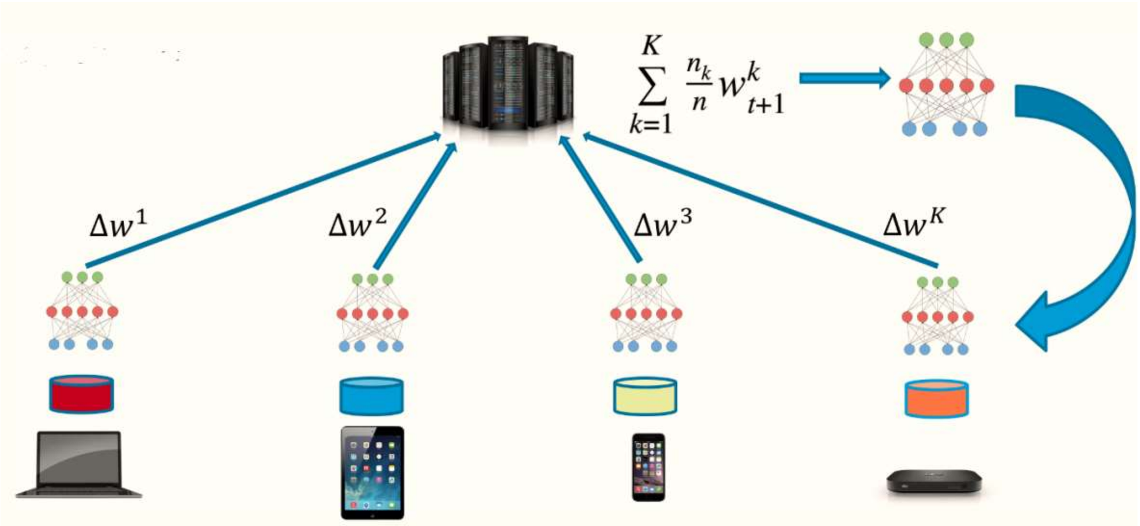
$$\ell = l_{\text{pos}} + \lambda l_{\text{neg}}$$

$$l_{\text{pos}} = d(g(x), w_y)$$

$$l_{\text{neg}} = -\min_{u \neq y} d(g(x), w_u)$$

Background & Motivation

- What we need: data for training and embedding vector
- Data collection encounters privacy issue
- Solution: Federated learning



Background & Motivation

- Embedding vector cannot be shared with other users
- Hence, cannot calculate negative loss
- Training with only positive loss will collapse all embeddings

$$\ell = l_{\text{pos}} + \cancel{\lambda l_{\text{neg}}}$$

FedUV method design

- Contribution: User verification without sharing the embedding vectors
- Comparable performance with existing approaches
- Using Error-correcting codes (ECC) as secret vectors

ANTS LAB

UNIVERSITY of HOUSTON
CULLEN COLLEGE of ENGINEERING

FedUV method design

- Definition of loss function
- Let W be a set of c vectors, v_u be the secret vector for user u
- Try to make the negative loss be negligible

- Original loss function: $\ell(x, y; g, w) = d(g(x), w_y) - \lambda \min_{u \neq y} d(g(x), w_u)$
- **FedUV** loss function: $\ell(x, y; g, w) = d(g(x), W^T v_y) - \lambda \min_{u \neq y} d(g(x), W^T v_u)$

ANTS LAB

UNIVERSITY of HOUSTON
CULLEN COLLEGE of ENGINEERING

FedUV method design

$$\begin{cases} \ell_{\text{pos}} = \max(0, 1 - \frac{1}{c} v_y^T W g_\theta(x)), \\ \ell_{\text{neg}} = \max_{u \neq y} \frac{1}{c} v_u^T W g_\theta(x). \end{cases}$$

Lemma 1. *Assume* $\|W g_\theta(x)\| = \sqrt{c}$ *and* $v_y \in \{-1, 1\}^c$. *For* ℓ_{pos} *defined in (4), we have* $\ell_{\text{pos}} = 0$ *if and only if* $W g_\theta(x) = v_y$.

Proof. Let $z = W g_\theta(x)$. The term $\ell_{\text{pos}} = 0$ is equivalent to $\frac{1}{c} v_y^T z \geq 1$. We have $\frac{1}{c} v_y^T z \leq \frac{1}{c} \|v_y\| \|z\| = 1$ and the equality holds if and only if $z = \alpha v_y, \forall \alpha > 0$. Since $\|z\| = \|v_y\| = \sqrt{c}$, then $\alpha = 1$ and, hence, we have $\ell_{\text{pos}} = 0$ if and only if $z = v_y$.

FedUV method design

- Error correcting codes (ECCs)
- Techniques that enable restoring sequences from noise
- Designed to maximize the minimum Hamming distance between distinct codewords

FedUV method design

Theorem 1. *Assume* $\|Wg_\theta(x)\| = \sqrt{c}$ *and* $v_y \in \{-1, 1\}^c$. *Assume* v_u*'s are chosen from ECC codewords. For* ℓ_{pos} *and* ℓ_{neg} *defined in (4), minimizing* ℓ_{pos} *also minimizes* ℓ_{neg}.

Proof. Since $v_u \in \{-1, 1\}^c$, the Hamming distance between v_{u_1} and v_{u_2} is defined as

$$\begin{aligned}\Delta_{u_1,u_2} &= \frac{1}{4}\|v_{u_1} - v_{u_2}\|^2 \\ &= \frac{1}{4}(\|v_{u_1}\|^2 + \|v_{u_2}\|^2 - 2v_{u_1}^T v_{u_2}) \\ &= \frac{c}{2}(1 - \frac{1}{c}v_{u_1}^T v_{u_2}).\end{aligned}$$

FedUV method design

- To wrap it up
- According to lemma 1:

$$\ell_{\text{neg}} = \max_{u \neq y} \frac{1}{c} v_u^T v_y$$

- According to Theorem 1:
- ECCs minimize: $\max_{u_1 \neq u_2} \frac{1}{c} v_{u_1}^T v_{u_2}$

- Negative loss is at its minimum when:

1) Positive loss = 0
2) v_u are chosen from ECC codewords

ANTS LAB

UNIVERSITY of HOUSTON
CULLEN COLLEGE of ENGINEERING

FedUV method design

- What we established: minimizing positive loss also minimizes negative loss
- Hence, no need to calculate negative loss
- Next: how to construct the secret codewords?

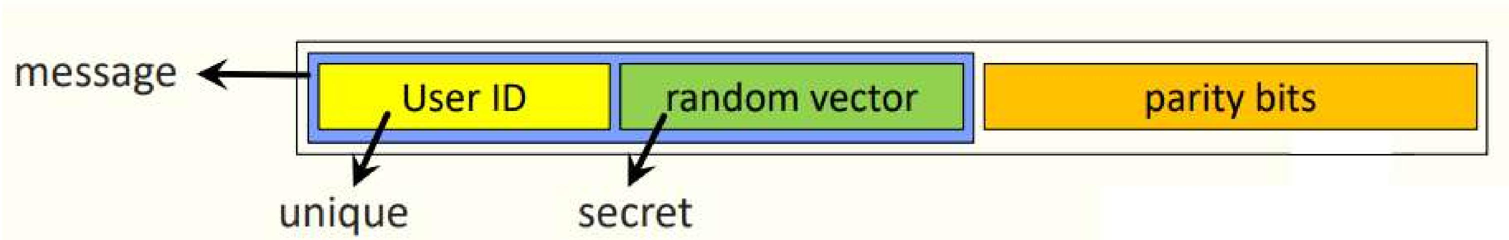
ANTS LAB Ai

UNIVERSITY of HOUSTON
CULLEN COLLEGE of ENGINEERING

FedUV method design

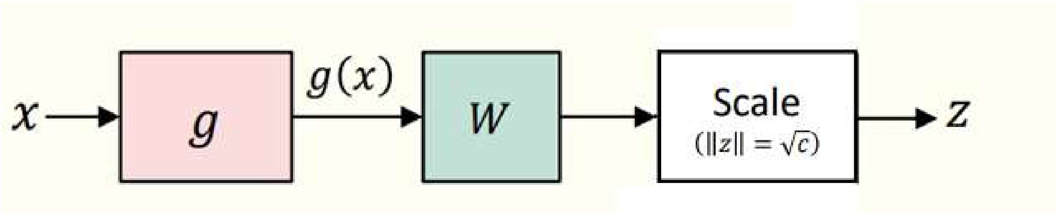
- Structure of secret codewords

1) Unique binary vector representing user ID
2) Random binary vector chosen by the user



FedUV method design

- Model structure of FedUV



- Loss function: $\ell_{\text{pos}} = \max(0, 1 - \frac{1}{c} v_y^T \sigma(W g_\theta(x)))$

- Verification: $\frac{1}{c} v_y^T \sigma(W g_\theta(x')) \underset{\texttt{reject}}{\overset{\texttt{accept}}{\gtrless}} \tau,$

Implementation

- Datasets

  VoxCeleb: text-independent speaker identification

  CelebA: over 20000 facial images for training

  MNIST-UV: handwriting identification
- Setting

  1000 users, BCH coding for generating codeword
- Baseline

  softmax, FedAwS

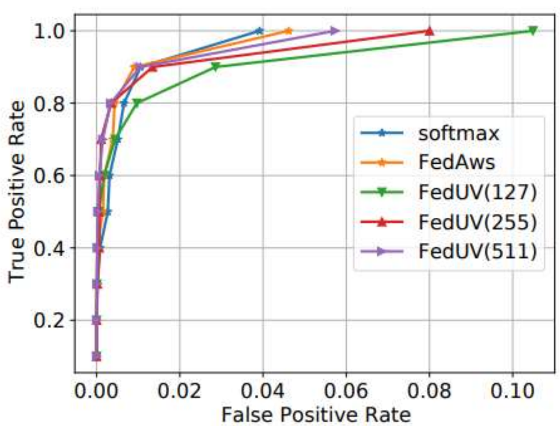
ANTS LAB

UNIVERSITY of HOUSTON
CULLEN COLLEGE of ENGINEERING

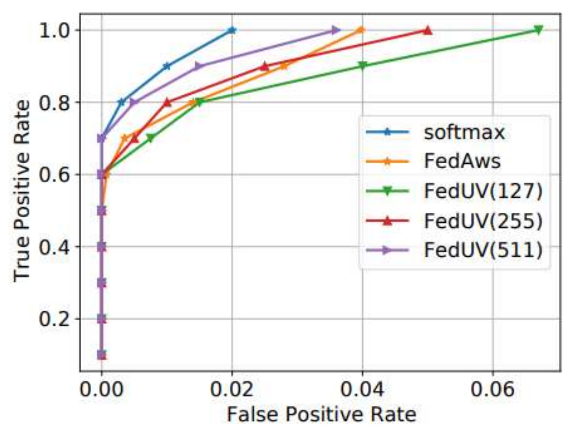
Results

- Verification performance

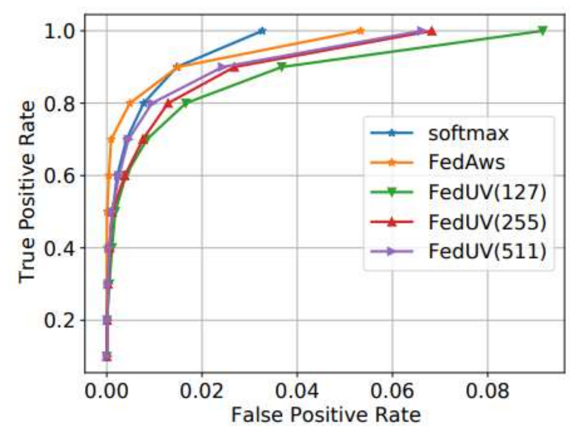
VoxCeleb dataset



CelebA dataset

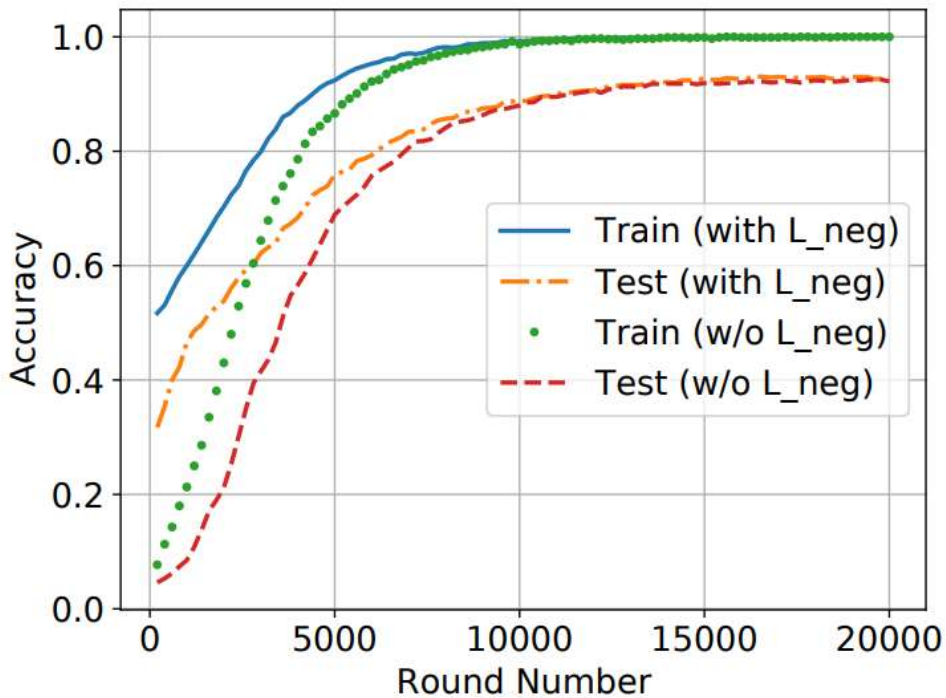


MNIST-UV dataset



Results

- Performance with or without negative loss



Conclusion

- FedUV: framework for training user verification models in FL setup
- Perform the training without sharing embeddings
- On par with existing approaches
- Showing results from variety of modalities

ANTS LAB

UNIVERSITY of HOUSTON
CULLEN COLLEGE of ENGINEERING


THANK YOU
UNIVERSITY of HOUSTON | ENGINEERING