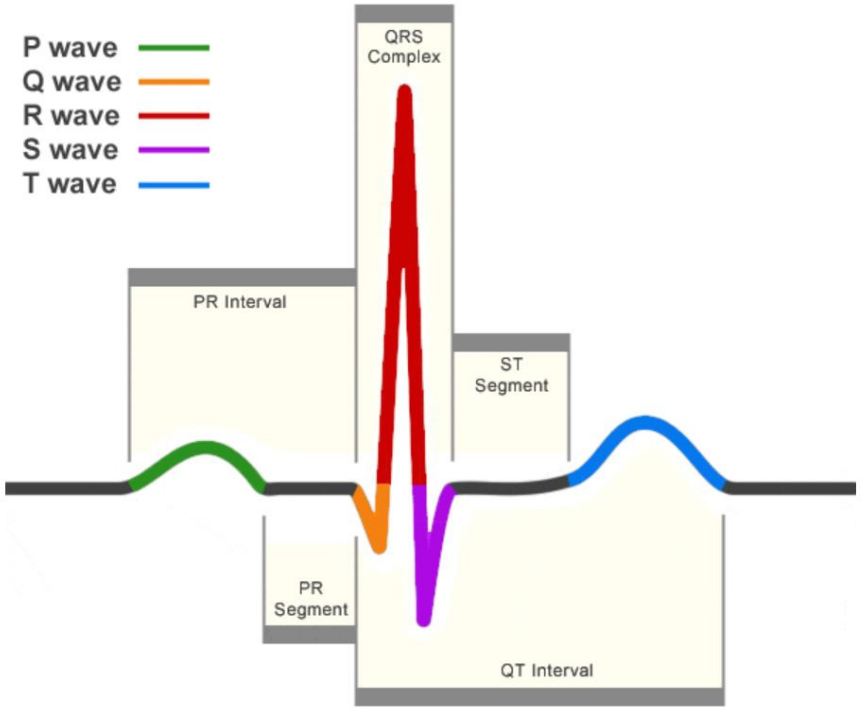
Paper Review

필수 reference 논문 리뷰

221014

202245235 김예진

ECG(electrocardiogram)



- P : 동방결절에서 전류 신호가 발생하고, 이것이 심방을 극성화 시키면서 판막의 심근이 수축
- P-Q : 전류 신호가 심장을 자극하지 않는 휴지기
- QRS Complex : 방실 결절이 전류신호를 놓아주면(Q), 심실이 즉시 극성화되었다(R)가 곧바로 비극성화(S)
- S-T : S와 T의 사이이며 전류 신호가 심장을 자극하지 않는 휴지기
- T : 심실이 다시 약하게 극성화 되었다가 다시 비극성화 되면서 심실과 심실 판막의 심근이 동시에 이완

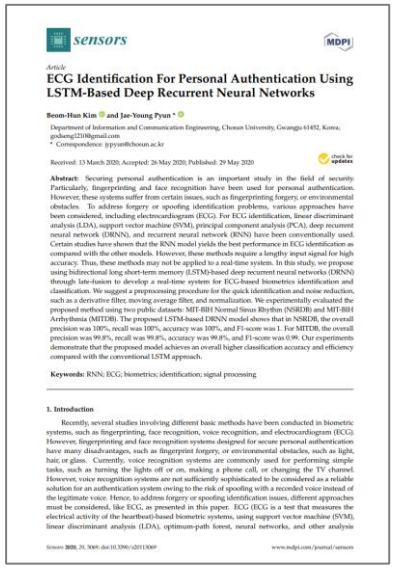
✓ 심장의 위치, 크기 및 전기 생리학적 요인 등에 의해 개인 고유의 특성을 가져 개인 간의 구별이 뚜렷함

✓ 위변조가 어렵기 때문에 보안 측면에서도 강점을 가짐

✓ 살아있는 모든 사람에게서 측정이 가능하며 시간이 많이 지나도 심전도의 파형이 크게 변하지 않아 등록을 자주 해주지 않아도 됨

Reference 1

ECG Identification For Personal Authentication Using LSTM-Based Deep Recurrent Neural Networks


sensors

MDPI

Article

ECG Identification For Personal Authentication Using LSTM-Based Deep Recurrent Neural Networks

Beom-Hun Kim and Jae-Young Pyun *

Department of Information and Communication Engineering, Chosun University, Gwangju 61452, Korea; godseng1210@gmail.com

* Correspondence: jypyun@chosun.ac.kr

Received: 13 March 2020; Accepted: 26 May 2020; Published: 29 May 2020

check for updates

Abstract: Securing personal authentication is an important study in the field of security. Particularly, fingerprinting and face recognition have been used for personal authentication. However, these systems suffer from certain issues, such as fingerprinting forgery, or environmental obstacles. To address forgery or spoofing identification problems, various approaches have been considered, including electrocardiogram (ECG). For ECG identification, linear discriminant analysis (LDA), support vector machine (SVM), principal component analysis (PCA), deep recurrent neural network (DRNN), and recurrent neural network (RNN) have been conventionally used. Certain studies have shown that the RNN model yields the best performance in ECG identification as compared with the other models. However, these methods require a lengthy input signal for high accuracy. Thus, these methods may not be applied to a real-time system. In this study, we propose using bidirectional long short-term memory (LSTM)-based deep recurrent neural networks (DRNN) through late-fusion to develop a real-time system for ECG-based biometrics identification and classification. We suggest a preprocessing procedure for the quick identification and noise reduction, such as a derivative filter, moving average filter, and normalization. We experimentally evaluated the proposed method using two public datasets: MIT-BIH Normal Sinus Rhythm (NSRDB) and MIT-BIH Arrhythmia (MITDB). The proposed LSTM-based DRNN model shows that in NSRDB, the overall precision was 100%, recall was 100%, accuracy was 100%, and F1-score was 1. For MITDB, the overall precision was 99.8%, recall was 99.8%, accuracy was 99.8%, and F1-score was 0.99. Our experiments demonstrate that the proposed model achieves an overall higher classification accuracy and efficiency compared with the conventional LSTM approach.

Keywords: RNN; ECG; biometrics; identification; signal processing

1. Introduction

Recently, several studies involving different basic methods have been conducted in biometric systems, such as fingerprinting, face recognition, voice recognition, and electrocardiogram (ECG). However, fingerprinting and face recognition systems designed for secure personal authentication have many disadvantages, such as fingerprint forgery, or environmental obstacles, such as light, hair, or glass. Currently, voice recognition systems are commonly used for performing simple tasks, such as turning the lights off or on, making a phone call, or changing the TV channel. However, voice recognition systems are not sufficiently sophisticated to be considered as a reliable solution for an authentication system owing to the risk of spoofing with a recorded voice instead of the legitimate voice. Hence, to address forgery or spoofing identification issues, different approaches must be considered, like ECG, as presented in this paper. ECG (ECG is a test that measures the electrical activity of the heartbeat)-based biometric systems, using support vector machine (SVM), linear discriminant analysis (LDA), optimum-path forest, neural networks, and other analysis

- 최근 지문, 얼굴 인식, 음성 인식 및 심전도(ECG)와 같은 생체 인식 시스템에서 다양한 기본 방법을 포함하는 여러 연구가 수행

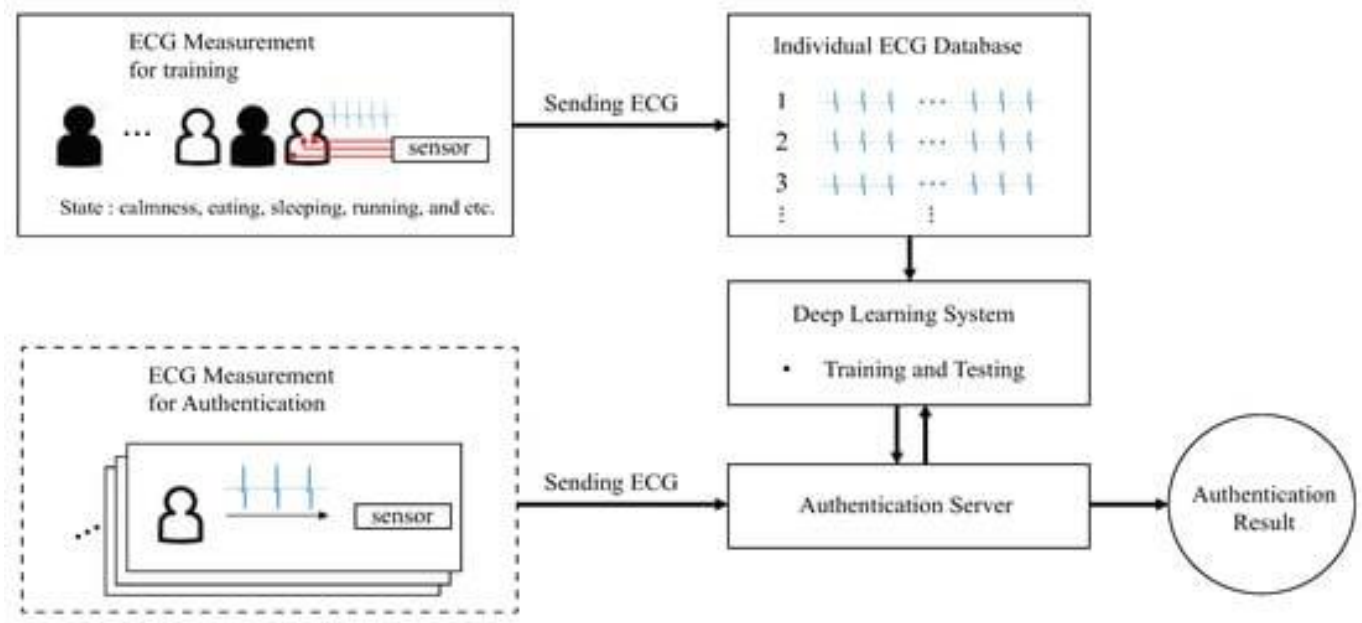
  - 지문 및 얼굴 인식 시스템은 지문 위조, 빛, 머리카락, 유리 등의 환경적 장애물과 같은 많은 단점 존재
  - 음성 인식 시스템은 일반적으로 조명을 끄거나 켜거나, 전화를 걸거나, TV 채널을 변경하는 것과 같은 간단한 작업을 수행하는데 사용
  - 위조 또는 위장 식별 문제를 해결하기 위해 이 백서에 나와 있는 것처럼 ECG와 같은 다양한 접근 방식을 고려해야함

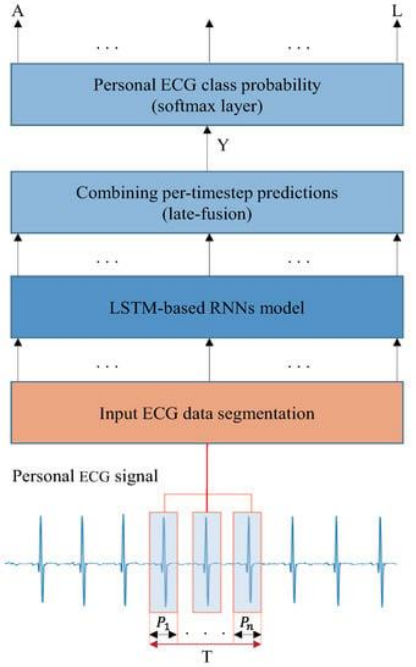
Kim, Beom-Hun, and Jae-Young Pyun. "ECG identification for personal authentication using LSTM-based deep recurrent neural networks." *Sensors* 20.11 (2020): 3069.

Reference 1

ECG Identification For Personal Authentication Using LSTM-Based Deep Recurrent Neural Networks

- 특징 추출, 시간 주기로 분할, R-피크 감지를 사용한 분할, 짧은 길이의 ECG 신호 그룹화를 포함한 전처리
  - MIT-BIH Normal Sinus Rhythm(NSRDB) MIT-BIH Arrhythmia (MITDB) 데이터 사용
  - ECG 기록을 신호 구성 요소 중 P 주기로 분할하여 사용





Kim, Beom-Hun, and Jae-Young Pyun. "ECG identification for personal authentication using LSTM-based deep recurrent neural networks." *Sensors* 20.11 (2020): 3069.

Reference 1

ECG Identification For Personal Authentication Using LSTM-Based Deep Recurrent Neural Networks

- ECG 분류를 위한 새로운 LSTM 기반 DRNN 아키텍처 사용
  - 입력 시퀀스 길이에 따른 식별 정확도 영향을 평가함
  - 제안된 모델은 최신 방법에 비해 시퀀스가 더 짧을 때 더 나은 성능을 보임
  - 빠른 결과가 필요한 실시간 개인 ECG 식별 시스템에 유용
  - 제안된 LSTM 기반 모델이 기존의 RNN 모델 보다 더 나은 성능을 보임

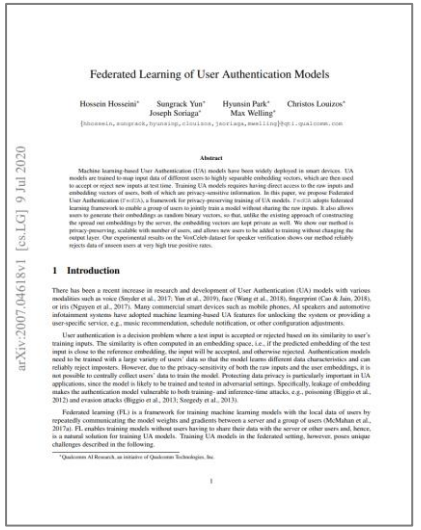
Methods	Dataset	Input Sequence Length (Number of Beats)	Overall Accuracy (%)
Proposed model	MITDB	3	99.73
		9	99.80
H. M. Lynn et al. [15]	MITDB	3	97.60
		9	98.40
R. Salloum et al. [26]	MITDB	3	98.20
		9	100
Q. Zhang et al. [19]	MITDB	1	91.10
X. Zhang [49]	MITDB	8	97.80
		12	98.9
Ö. Yildirim [50]	MITDB	5	99.39

- Depth, Number of hidden layer, data length를 조정하며 실험
  - NSRDB : 정밀도 100%, 재현율 100%, 정확도 100%, F1-score 1
  - MITDB : 정밀도 99.8%, 재현율 99.8% , 정확도 99.8%, F1-score 0.99

Kim, Beom-Hun, and Jae-Young Pyun. "ECG identification for personal authentication using LSTM-based deep recurrent neural networks." *Sensors* 20.11 (2020): 3069.

Reference 2

Federated Learning of User Authentication Models


Federated Learning of User Authentication Models

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

{hsseini, sungrack, hyunsinp, clouizos, jsoriaga, mwelling}@qti.qualcomm.com

Abstract

Machine learning-based User Authentication (UA) models have been widely deployed in smart devices. UA models are trained to map input data of different users to highly separable embedding vectors, which are then used to accept or reject new inputs at test time. Training UA models requires having direct access to the raw inputs and embedding vectors of users, both of which are privacy-sensitive information. In this paper, we propose Federated User Authentication (FedUA), a framework for privacy-preserving training of UA models. FedUA adopts federated learning framework to enable a group of users to jointly train a model without sharing the raw inputs. It also allows users to generate their embeddings as random binary vectors, so that, unlike the existing approach of constructing the spread out embeddings by the server, the embedding vectors are kept private as well. We show our method is privacy-preserving, scalable with number of users, and allows new users to be added to training without changing the output layer. Our experimental results on the VoxCeleb dataset for speaker verification shows our method reliably rejects data of unseen users at very high true positive rates.

1 Introduction

There has been a recent increase in research and development of User Authentication (UA) models with various modalities such as voice (Snyder et al., 2017; Yun et al., 2019), face (Wang et al., 2018), fingerprint (Cao & Jain, 2018), or iris (Nguyen et al., 2017). Many commercial smart devices such as mobile phones, AI speakers and automotive infotainment systems have adopted machine learning-based UA features for unlocking the system or providing a user-specific service, e.g., music recommendation, schedule notification, or other configuration adjustments.

User authentication is a decision problem where a test input is accepted or rejected based on its similarity to user's training inputs. The similarity is often computed in an embedding space, i.e., if the predicted embedding of the test input is close to the reference embedding, the input will be accepted, and otherwise rejected. Authentication models need to be trained with a large variety of users' data so that the model learns different data characteristics and can reliably reject imposters. However, due to the privacy-sensitivity of both the raw inputs and the user embeddings, it is not possible to centrally collect users' data to train the model. Protecting data privacy is particularly important in UA applications, since the model is likely to be trained and tested in adversarial settings. Specifically, leakage of embedding makes the authentication model vulnerable to both training- and inference-time attacks, e.g., poisoning (Biggio et al., 2012) and evasion attacks (Biggio et al., 2013; Szegedy et al., 2013).

Federated learning (FL) is a framework for training machine learning models with the local data of users by repeatedly communicating the model weights and gradients between a server and a group of users (McMahan et al., 2017a). FL enables training models without users having to share their data with the server or other users and, hence, is a natural solution for training UA models. Training UA models in the federated setting, however, poses unique challenges described in the following.

*Qualcomm AI Research, an initiative of Qualcomm Technologies, Inc.

- 사용자 인증 모델의 개인정보 보호를 위한 연합학습 제안
  - 공유하지 않고 모델을 공동으로 훈련할 수 있는 학습 프레임 워크로 임베딩 벡터 또한 비공개로 진행
  - 개인정보 보호, 사용자 수에 따른 확장 가능, 새 사용자 추가 가능의 이점이 있음
  - VoxCeleb 데이터 세트(Nagrani et al., 2017) 사용하여 실험 진행
    (화자 식별을 위한 대규모 음성파일 데이터 셋)

- 각각 원시 입력 및 임베딩 벡터의 개인 정보를 보호하기 위해 연합 학습 및 랜덤 이진 임베딩 사용

- 사용자 수에 따라 확장 가능하며 일반적으로 FL 설정에서 수행되는 통신을 제외하고 사용자 간 또는 사용자와 서버 간의 조정이 필요하지 않음을 증명

Hosseini, Hossein, et al. "Federated learning of user authentication models." *arXiv preprint arXiv:2007.04618* (2020).

Reference 2

Federated Learning of User Authentication Models

- 다양한 데이터 특성을 학습하고 사용자를 안정적으로 인증할 수 있도록 인증 모델은 다양한 사용자 데이터로 학습되어야 함
  - 화자 인식 모델은 높은 정확도로 사기꾼을 거부할 수 있도록 다양한 연령, 성별, 억양 등을 가진 사용자의 음성 데이터 학습이 필요

- 데이터 개인 정보 보호는 모델이 적대적인 환경에서 훈련되고 테스트될 가능성이 있는 UA(User Authentication) 애플리케이션에서 특히 중요
  - 원시 입력과 임베딩 벡터 모두 민감한 정보로 간주되어 공격에 취약해짐
  - 따라서, 임베딩 벡터도 비공개로 유지

Hosseini, Hossein, et al. "Federated learning of user authentication models." *arXiv preprint arXiv:2007.04618* (2020).

Reference 2

Federated Learning of User Authentication Models

- FL의 단점
  - 사용자의 임베딩 벡터는 미리 정의되지 않음
  - 모델 가중치와 기울기는 서버와 사용자 간에 여러 번 통신해야 함
  - 훈련 및 추론은 일반적으로 리소스가 제한된 로컬 장치에서 수행됨

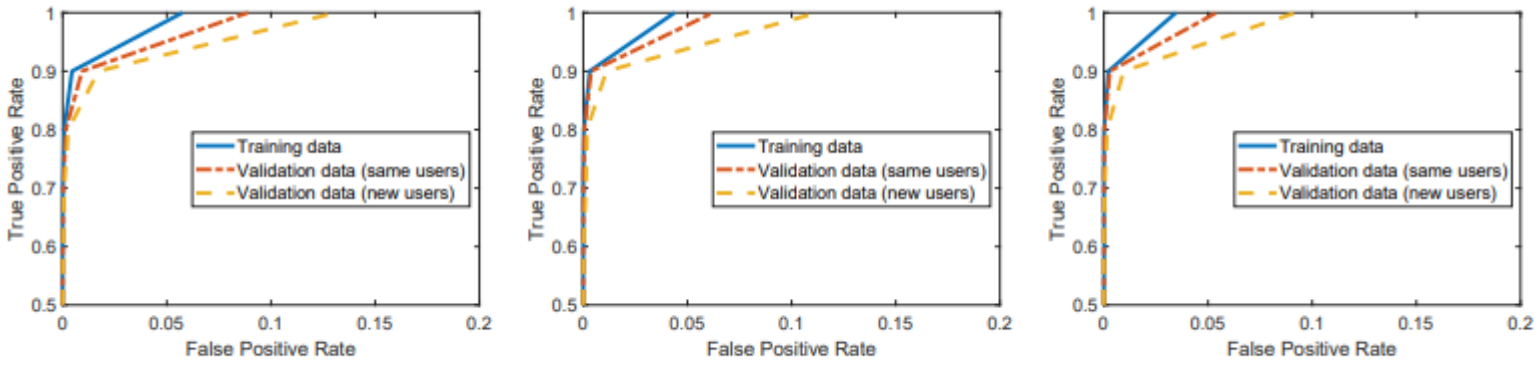
⇒ **UA 모델 학습을 위한 FL 프레임워크를 채택**

  - 사용자는 훈련 전에 생성된 임의의 임베딩 벡터로 모델을 훈련
  - 개인 정보를 보호하고 임베딩 벡터 간에 높은 수준의 분리성을 제공

Hosseini, Hossein, et al. "Federated learning of user authentication models." *arXiv preprint arXiv:2007.04618* (2020).

Reference 2

Federated Learning of User Authentication Models



(a) $n_e = 128$ (b) $n_e = 256$ (c) $n_e = 512$

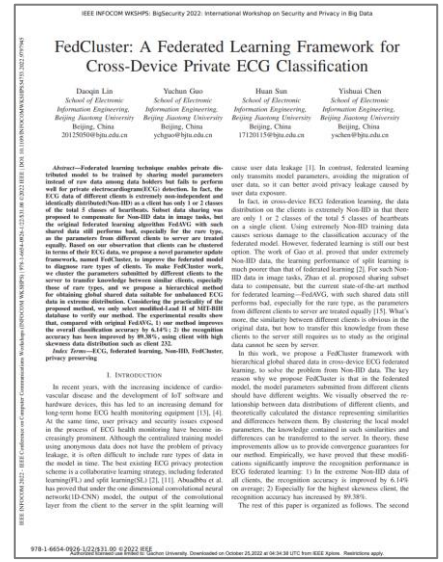
- 모든 경우에 매우 낮은 FPR(False Positive Rate)에서 높은 TPR(True Positive Rate)을 달성
- TPR=80%에서 ne(임베딩 벡터 길이) = 128, 256 및 512에 대해 신규 사용자 데이터에서 FPR=0.27%, 0.18%, 0.16% 달성

  - 화자 검증 데이터 세트에 대한 실험 결과는 제안된 방법이 매우 높은 TPR로 보이지 않는 사용자의 데이터를 안정적으로 거부함을 보여줌

Hosseini, Hossein, et al. "Federated learning of user authentication models." *arXiv preprint arXiv:2007.04618* (2020).

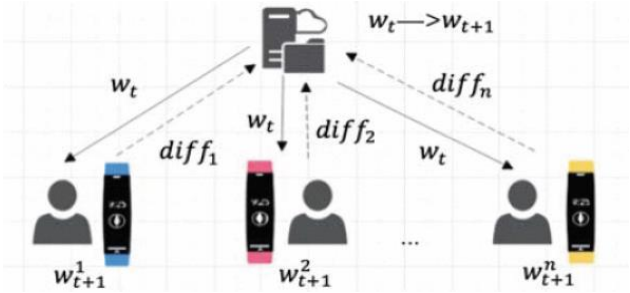
Reference 3

FedCluster: A Federated Learning Framework for Cross-Device Private ECG Classification



- 계층적 글로벌 공유 데이터를 사용하는 연합 메커니즘 Fedcluster를 제안
  - 연합학습으로 모델 매개변수만 전송하여 사용자 데이터 노출로 인한 개인정보 유출 위험 감소
  - MIT BIH Arrhythmia database 사용하여 총 5개 (N,S,V,F,Q) 클래스로 분류
  - 1D CNN 분류 모델 사용

- 각 클라이언트가 로컬 데이터에 대한 교육을 마친 후 모델 매개변수가 차등 방식으로 서버에 전송
  - 서버는 먼저 수신된 모델 매개변수를 클러스터링 하여 모델 매개변수의 업데이트된 결과를 클래스 내에서 먼저 평균화한 다음 클래스 간 평균화
  - 매개변수의 차이 값만 전송되므로 통신 효율성을 크게 향상



Lin, Daoqin, et al. "FedCluster: A Federated Learning Framework for Cross-Device Private ECG Classification." *IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2022.

Reference 3

FedCluster: A Federated Learning Framework for Cross-Device Private ECG Classification

Algorithm 1 FedCluster

Input: ECG data x & initial model parameters w_t.

Output: Updated model parameters w_{t+1}.

Server:

1: send w_t to each client.

2: recieve differential parameters of all clients:

$$(diff_1, diff_2, \ldots, diff_n)$$

3: Using kmeans to cluster differential parameters of all clients:

$$\text{diff}_{i,C_k} = F_1(diff_1, diff_2, \ldots, diff_n)$$

where, i denotes the client index, and function F_1 denotes kmeans function.

4: update model parameters:

$$w_{t+1} = \frac{\sum_k \text{diff}_{i,C_k}}{L(C_k) * K}$$

where, $L(C_k)$ represents that the number of clients belong to type k, K denotes the total number of all types.

Client i:

1: initialize the model.

2: load model parameters w_t.

3: train model to update parameters: w_{t+1}

4: send $diff_i$ to server: $diff_i = w_{t+1}^i - w_t$

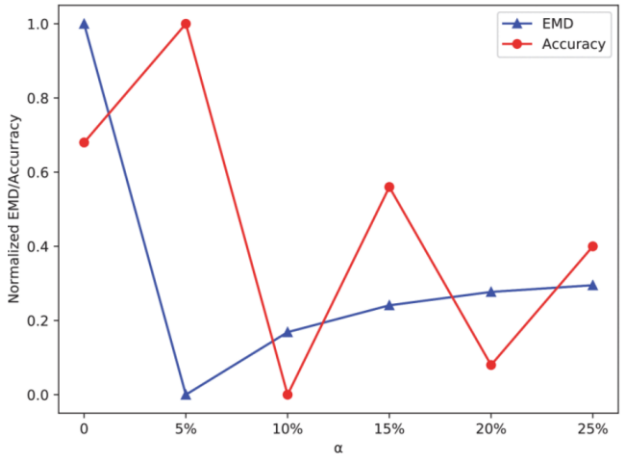
1. 각 클라이언트에 초기모델 매개변수 전달
2. 모든 클라이언트의 매개변수 수신
3. K-means를 사용하여 모든 클라이언트의 매개변수 Clustering
4. 모델 매개변수 업데이트

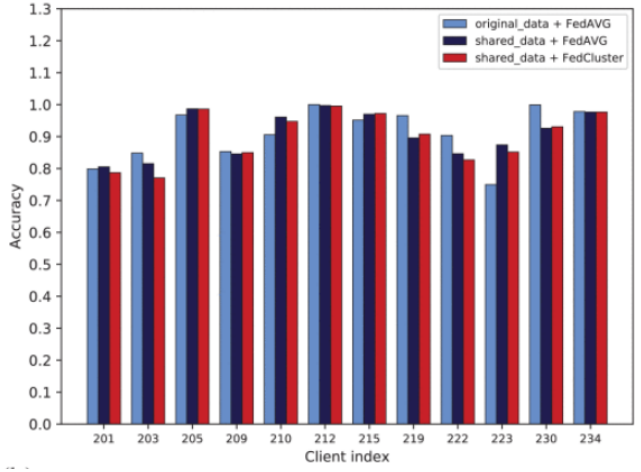
- 서로 다른 클라이언트의 데이터 분포 사이의 관계를 시각적 관찰 및 유사점과 차이점을 나타내는 거리를 이론적으로 계산
- 글로벌 공유 데이터를 생성하는 계층적 방법을 제안
- 각 클라이언트에 대해 서버에 다른 가중치를 제공하기 위해 새로운 프레임워크인 FedCluster를 제안

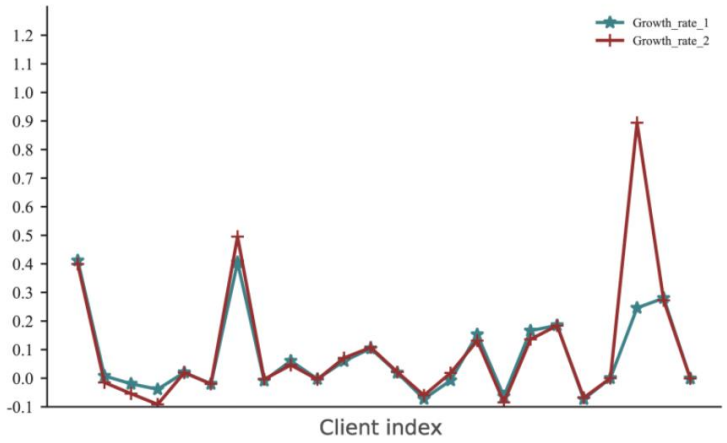
Lin, Daoqin, et al. "FedCluster: A Federated Learning Framework for Cross-Device Private ECG Classification." *IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2022.

Reference 3

FedCluster: A Federated Learning Framework for Cross-Device Private ECG Classification







- FedCluster 프레임워크를 채택한 후 FedAVG와 비교하여 모든 클라이언트의 전체 인식 정확도가 89.09%에서 89.26%로 향상
  - 왜도가 높은 클라이언트의 경우 분류 정확도가 52% 크게 향상

- Convolutional Layer와 2개의 Full Connected Layer로 구성된 모델을 이용하여 정확도 96.94% 달성

Lin, Daoqin, et al. "FedCluster: A Federated Learning Framework for Cross-Device Private ECG Classification." *IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2022.

감사합니다

Email: najin2445@gachon.ac.kr