지속적인 모델 최적화를 위한 연합 학습 효율화 전략

김영수 [1], 유헌창 [2]
[1] 고려대학교 SW/AI 융합대학원 석사과정
[2] 고려대학교 정보대학 컴퓨터학과 교수

zll11@korea.ac.kr, yuhc@korea.ac.kr,

For continuous model optimization Federated learning efficiency strategy

Youngsu Kim[1], Heonchang Yu[2]
[1]Dept. of SW/AI, Korea University
[2]Dept. of Computer Science and Engineering, Korea University

요 약

본 논문에서는 지속적으로 최적화된 인공지능 모델을 적용하기 위한 방안으로 연합 학습(Federated Learning)을 활용한 접근법을 제시한다. 최근 다양한 산업 분야에서 인공지능 활용에 대한 필요성이 증가하고 있다. 금융과 같은 일부 산업은 강력한 보안, 높은 정확도, 규제 준수, 실시간 대응이 요구됨과 동시에 정적 시스템 환경 특성으로 적용된 인공지능 모델의 최적화가 어렵다.

이러한 환경적 한계 해결을 위하여, 연합 학습을 통한 모델의 최적화 방안을 제안한다. 연합 학습은 데이터 프라이버시를 유지하면서 모델의 지속적 최적화를 제공이 가능한 강력한 아키텍처이다. 그러나 연합 학습은 클라이언트와 중앙 서버의 반복적인 통신과 학습으로, 불필요한 자원에 대한 소요가 요구된다. 이러한 연합 학습의 단점 극복을 위하여, 주요도 높은 클라이언트의 선정 및 클라이언트와 중앙 서버의 조기 중단(early stopping) 전략을 통한 지속적, 효율적 최적화가 가능한 연합 학습 모델의 운영 전략을 제시한다.

1. 서론

다양한 산업에서 신규 도입되는 서비스뿐 아니라, 기존에 제공되던 서비스의 고도화를 위한 방안으로 인공지능 모델이 적극 활용되고 있다. 금융분야에서 또한 인공지능을 활용한 서비스가 활발하게 이용되고 있으며, 대표적으로는 신분증 OCR, 이상 거래 탐지, 위 · 변조 탐지 등에 사용된다. 최근 금융감독원 지침으로 안면 인식 시스템을 도입한 비대면 서비스의 본인인증 강화 방안이 권고됨에 따라, 금융사에서는 딥러닝을 활용한 안면 인증 솔루션을 도입하여 고객서비스를 시행하였으나 낮은 정확도, 안면 인식 오류로 고객의 불편으로 이어지기도 했다.

금융과 같은 특수한 산업분야에서는 정적인 시스템 환경과, 개인정보 노출에 대한 위험, 각종 규제 등의 특징이 존재한다. 이러한 환경 속에서 인공지능 모델의 유동적인 최적화를 적용하는데 많은 제약이 존재한다. 이러한 제약에 대한 극복을 위해, 분산 저장된 데이터를 직접 공유하지 않고 서로 협력하여 인공지능 모델을 학습, 최적화 할 수 있는 분산 학습 기법인 연합 학습을 활용할 수 있다. 다만 연합 학습은 통신 오버헤드, 클라이언트 간 데이터 불균형, 지연시간 등의 한계가 존재한다. 이러한 연합 학습의 한계 극복을 위하여, 주요 클라이언트 선택 및 클라이언트, 중앙 서버의 조기 중단(Early Stopping) 전략을 제시하여 개선된 연합 학습 모델을 제안하여 극복하고자 한다.

2. 관련 연구

2.1 기존 연구 분석

[5]연합 학습이 2017 년 처음 알려진 이후, 다양한 분야에서 활용되며 연구되고 있는 분야이다. 특히 데이터 프라이버시와 모델 효율성을 중심으로 급격히 발전하고 있다. [1. 2] 통신비용 절감을 위하여 데이터 압축 및 전송 최적화 방법을 제시하는 연구나, 구조화된 업데이트를 통해 필수적이고, 중요 정보만을 전

송함으로써 효율적인 통신을 가능하도록 하는 연구도 지속되고 있다. 이러한 연구들을 통해 불필요한 데이터 전송을 줄이고, 학습에 필요한 핵심 정보의 전송에 집중 가능하도록 한다. [2]최근에는 연합 학습 모델의 조기 중단 전략 방안으로 추가적인 훈련이 더 나은 결과를 제시하지 못할 때 훈련을 조기 중단하여 계산 자원 및 통신 요구사항을 줄이는 연구가 진행되고 있다.

2.2 연합 학습 효율화 전략

2.2.1 주요 클라이언트 선택

각 로컬에서 학습을 마친 클라이언트들로부터 매개변수(Parameter)를 수집하여 중앙 서버 업데이트 시 매개변수 수집을 위한 통신 부하 및 중앙 서버 업데이트를 위한 컴퓨팅 자원 부하가 발생한다. 특히 손실 함수가 수렴에 가까운 경우, 대부분의 클라이언트와 중앙 서버 간 차이가 크지 않아 모든 클라이언트로부터 매개변수를 수집하는 과정은 학습 진행의 이점보다, 과정을 진행하는 부하로 인한 손실이 크다. 그렇기 때문에, 클라이언트를 선택할 때 모든 클라이언트가 아닌 주요한 클라이언트의 선정을 목표로 하였다. 주요한 클라이언트란, 서버와 클라이언트의 매개변수의 유사도가 작은 클라이언트를 의미한다. 유사도 값이 작은 클라이언트는 중앙 서버의 매개변수를 많이 업데이트 시킬 수 클라이언트이며, 유사도의 차이가 큰 절반의 클라이언트만 선택하도록 중앙 서버의 매개변수 업데이트 과정에 설정하였다.

2.2.2 클라이언트의 조기 중단

클라이언트와 중앙 서버가 충분히 유사할 경우, 중앙 서버의 매개변수를 전달받아 클라이언트를 업데이트 하는 과정은 연산 자원을 낭비한다. 불필요한 자원낭비 방지하기 위한 조기 중단을 구현하기 위해, 중앙 서버와 클라이언트의 차이가 설정한 임계 값 이하로 충분히 작은 경우 중앙 서버의 매개변수를 클라이언트로 전달하는 과정이 이루어지지 않도록 하였다. 불필요한 매개변수 전송 자원 및 클라이언트 연산 컴퓨팅 자원 사용이 감소된다.

2.2.3 중앙 서버의 조기 중단

중앙 서버는 연합 학습의 전체 과정의 모니터링이 가능하기 때문에, 조건에 따른 전체 학습과정의 조기 중단 메커니즘 실행이 가능하다. 중앙 서버의 조기 중단을 위해 클라이언트로부터 매개변수를 업데이트 받아 진동 감지(oscillation detection)를 사용하여 조기 중단을 실행하였다. 구체적으로는 업데이트 쌍의 50% 이상의 음의 코사인 유사도를 보일 때 조기 중단 메커니즘을 활성화 했다. 조기 중단 기동 시점에는 중앙 서버의 매개변수 업데이트가 서로 상반되는 방향으로 진행되며, 모델이 지역 최저점 사이를 오가고 있음을 의미한다. 이는 충분히 수렴하여 성능 발전이 없거나, 성능의 변화가 불안정할 때 추가적인 훈련이 리소스 낭비일 수 있기 때문에, 비효율적인 훈련을 조기에 중단시켜 컴퓨팅 자원 리소스와 통신 비용을 절약 및 모델의 과 적합(overfitting)을 방지한다.

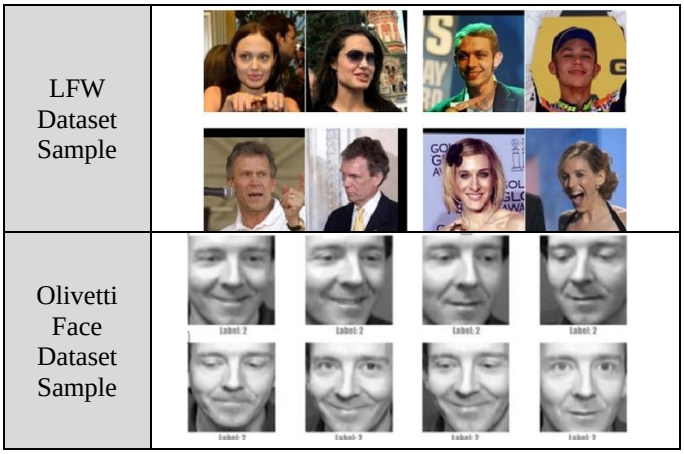
3. 안면 인증을 위한 모델, 데이터 셋 선정 및 실험

3.1 실험 모델 선정

최근 금융기관에 도입 된 안면 인증 모델을 예시로 활용하기 위해 샴 네트워크(Siamese Neural Networks)를 이용한 안면 인증 모델로 연합 학습을 진행하였다. 매개변수와 구조가 같은 인공신경망에 2 개의 안면 이미지를 각각 넣어 출력을 비교하는 방식으로 얼굴 인식의 결과를 도출하였다. 새로운 사람의 안면 이미지를 타겟 이미지와 다른 사람의 안면 이미지와 비교하여 유클리드 거리를 구하는 대조 손실(Contrastive Loss)함수를 이용하여, 같은 클래스의 이미지 쌍은 서로 가깝게, 다른 이미지 쌍은 서로 멀리 떨어지도록 학습하였다.

3.2 데이터 셋 선정

실제 환경에서는 클라이언트 별 데이터 셋의 불균형이나 품질의 차이가 존재한다. 그러한 상황을 재현하기 위해 LFW(Labeled Faces in the Wild)과 Olivetti 얼굴 데이터 셋(Olivetti Dataset for the faces)을 혼용하여 사용하였다. (그림 1)은 각 데이터 셋의 일부이다. LFW 데이터 셋은 자연환경에서 촬영된 칼라 이미지로 다양한 조명, 포즈, 표정을 포함한다. Olivetti 얼굴 데이터 셋은 AT&T 에서 제공하는 데이터셋으로 40 명의 사람들로부터 총 400 개의 64x64 픽셀 크기의 흑백 얼굴 이미지로 구성된다. 사람의 얼굴 사진은 다양한 각도, 표정, 조명 조건에서 촬영되었다.



(그림 1) 안면 데이터 샘플

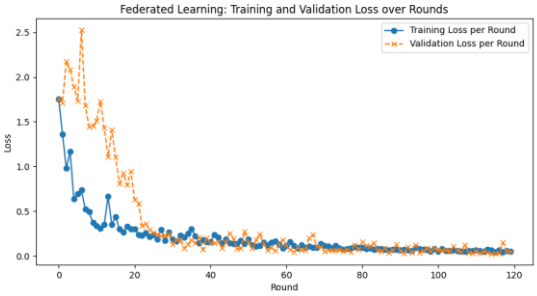
(그림 1) 샘플데이터를 통하여, LFW 데이터 셋에서는 다양한 배경과 색상, 크기나 노이즈의 포함여부 등 실제 인증 환경과 유사함을 볼 수 있으며, Olivetti 얼굴 데이터 셋은 별도의 배경이 없는 동일 환경에서의 흑백의 안면데이터임을 확인했다.

3.3 안면 인증 실험 및 결과

3.3.1 Baseline 구현

동일한 샴 네트워크 구조의 중앙 서버와 8 개의 클라이언트로 안면 인증 네트워크를 구성하여 연합 학습을 진행하였다. 중앙 서버에서 학습이 끝난 클라이언트의 매개변수를 전달한 후, 모든 클라이언트의 매개변수 평균을 계산하여 중앙 서버의 매개변수 업데

이트를 반복한다. 중앙 서버의 매개변수 업데이트 시 과 적합이 발생하여 validation loss 값이 증가하거나, 혹은 손실 변화가 임계 값 보다 작은지 여부로 성능 개선을 검증하여, 연속적으로 5 회 이상 성능개선이 없는 경우를 조기 중단 조건으로 설정하여 추가적인 학습을 중단했다.



(그림 2) 중앙 서버의 손실 함수 그래프

(그림 2)는 baseline 연합 학습 모델을 이용하여 안면 인증 모델의 손실 함수 그래프이다. 연합 학습의 성능 개선 여부를 비교하기 위해, 학습 완료 후 중앙 서버의 손실 값, 클라이언트 별 매개변수 업데이트 횟수, 중앙 서버의 학습 횟수를 10 회 학습을 진행한 결과의 평균을 계산했다.

<표 1> Baseline 실험 결과

성능 평가 수치 평균	결과
전체 클라이언트의 학습 횟수	826
중앙 서버 업데이트 횟수	103.25
검증 손실	0.1181

8 개의 클라이언트로 진행한 결과로서, 중앙 서버의 한번 학습 시 클라이언트의 학습 횟수 8.019 번으로 약 8 배 정도의 학습 횟수 차이가 있다. <표 1>의 결과를 이용하여 이 후의 연합 학습 효율화 전략이 유의미한 결과 여부의 기준으로 활용했다.

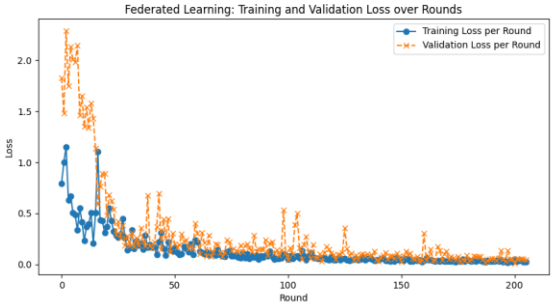
3.3.2 클라이언트 선택

주요도 높은 클라이언트를 선별하여 중앙 서버의 매개변수 업데이트에 이용했다. 주요도 기준은 중앙 서버의 매개변수를 더 많이 업데이트 시킬 수 있는 클라이언트로 정의했다. 즉, 중앙 서버와 가장 다른 매개변수를 가진 클라이언트를 사용했다. 구체적인 방법으로는 클라이언트 모델과 중앙 서버 모델의 매개변수를 각각 추출하여, 유클리드 거리(Euclidean distance) 값으로 계산 된 거리의 차이가 큰 상위 절반의 클라이언트를 선택하여 중앙 서버 학습에 활용했다.

<표 2> 클라이언트 선택 전략 실험 결과

성능 평가 수치 평균	결과
전체 클라이언트의 학습 횟수	454
중앙 서버 업데이트 횟수	114
검증 손실	0.00396

<표 2>의 실험 결과 중앙 서버의 학습 횟수에는 유의미한 차이가 없다. 그러나 중앙 서버의 학습 횟수 대비 전체 클라이언트의 학습 횟수를 비교해 보면, 중앙 서버의 학습 한번 당 클라이언트는 3.982 번의 학습이 진행되었다. <표 1>의 결과와 비교해보면, 중앙 서버 학습 한번 당 클라이언트의 학습 횟수가 약 절반의 수준으로 줄어드는 유의미한 결과를 나타낸다. 클라이언트, 중앙 서버의 연산 및 매개변수를 주고받는 통신 부하가 절반 수준의 감소를 의미한다. 특징적인 부분은 (그림 8)과 같이, 글로벌 모델의 손실그래프의 수렴과정에서 검증 그래프가 산발적으로 높아지는 현상이 있다. 이는 업데이트 폭이 큰 클라이언트들을 선택하여 수집하는 과정에서 발생한 현상이다.



(그림 3) 클라이언트 선택 전략 적용 손실 함수 그래프

검증과정에서 산발적으로 손실 값이 높아지는 현상은, 클라이언트의 매개변수를 수집하는 과정에서 중앙 모델과 많은 차이를 보이는 클라이언트로 인해 발생하며, 이러한 현상을 방지하기 위한 메커니즘을 추가 할 경우, 중앙 서버의 더 빠른 조기 중단이 기대된다.

3.3.3 클라이언트의 조기 중단

중앙 서버에서 전달받은 매개변수가 클라이언트의 매개변수와 설정 임계 값 보다 차이가 작은 경우, 이미 클라이언트에서 충분히 중앙 서버와 유사함으로 판단하여 매개변수를 업데이트 하지 않도록 설정했다. 중앙 서버와 클라이언트의 유사도는 코사인 유사도를 통해 계산하여 <표 3>의 결과를 보였다.

<표 3> 클라이언트 조기 중단 실험 결과

성능 평가 수치 평균	결과
전체 클라이언트의 학습 횟수	698.8
중앙 서버 업데이트 횟수	128.6
검증 손실	0.06895

<표 3>의 실험 결과를 통해 3.3.2 클라이언트 선택 전략과 유사한 결과를 나타낸다. 중앙 서버의 학습 한번 당 클라이언트의 학습 횟수는 5.453 번으로, 3.3.1 baseline 의 결과인 8.019 보다 감소 된 유의미한 결과이다. 클라이언트 내에서 불필요한 추가 학습을 진행하지 않으며, 컴퓨팅 자원의 낭비를 방지한다.

3.3.4 중앙 서버 조기 중단

중앙 서버에서 클라이언트로부터 업데이트 받은 각 매개변수를 모니터링하여 코사인 유사도를 측정하였다. 업데이트 받은 클라이언트의 매개변수 중에서 절반이상의 코사인 유사도가 음수인 경우, 중앙 서버 모델이 수렴하기 보다, 진동하고 있다고 판단하여 조기 중단 메커니즘을 활성화했다.

<표 4> 중앙 서버 조기 중단 실험 결과

성능 평가 수치 평균	결과
전체 클라이언트의 학습 횟수	956
중앙 서버 업데이트 횟수	117
검증 손실	0.1046

그러나 <표 4>의 실험 결과는 3.3.1 의 <표 1> 실험 결과와 비교해 보았을 때, 중앙 서버 및 클라이언트의 학습 횟수나, 검증 손실 값에 유의미한 차이가 없다. 이는 3.3.1 baseline 연합 학습에서 제공되고 있는 조기 중단 전략이 선행되기 때문에 진동 감지 조건을 만족시키지 못하고 baseline 연합 학습의 조기 중단 전략이 적용 됨을 의미한다.

4. 결론

연합 학습 과정을 더 빠르고 비용 효율적으로 만들어, 모델의 정확성과 자원 소비 간의 균형을 맞추기 위한 방법을 제시하고 실험하였다. Baseline 연합 학습 기반의 안면 인증 모델을 구현하고, 3 가지 전략을 접목하여 연합 학습의 효율성 향상 방안을 실험하였다. 각각의 실험 결론은 다음과 같다.

중앙 서버 업데이트 시 전체 클라이언트를 이용하지 않고, 주요도 높은 절반의 클라이언트만 활용하도록 하였을 때, 중앙 서버의 학습 횟수에는 변화가 없었으나, 전체 클라이언트 모델의 학습 횟수의 합은 절반의 수준으로 줄어드는 유의미한 결과를 얻었다. 이를 통해 중앙 서버의 학습 횟수 증가 없이, 주요도 큰 절반의 클라이언트 업데이트만으로 중앙 서버 모델 학습이 가능하며, 이를 통한 자원 절약이 가능함을 실험을 통해 증명하였다.

또한 중앙 서버와 클라이언트의 매개변수에 대한 유사도 검증을 통해 충분히 유사한 경우 클라이언트 업데이트를 수행하지 않는 클라이언트 조기 중단 전략을 통해, 불필요한 전송 및 연산 과정을 감소시킴으로써 리소스 낭비를 방지할 수 있다.

진동 감지를 통한 중앙 서버의 조기 중단 전략은 중앙 서버의 학습 횟수를 감소시켜줄 수 있을 것이라는 예상과 달리 유의미한 변화를 도출하지 못했다. 중앙 서버의 매개변수가 수렴하는 과정에서 절반이상 클라이언트의 코사인 유사도가 음수가 될 정도의 차이를 나타내기 이전 종료되는 것으로 추측된다. Baseline 연합 학습 모델에 별도의 조기 중단 전략이 없는 조건에서 실험이 진행되었다면, 진동 감지를 통한 조기 중단이 유의미한 결과를 보일 수 있을 것이다.

연합 학습 효율화를 위한 3 가지 전략이 적절히 혼재되어 사용 시 각각의 전략 시너지를 더할 수 있을 것이다. 또한 이러한 효율화 전략을 통해 금융 산업과 같이 제한된 환경의 다양한 산업에서, 인공지능 모델의 고도화 및 효율화 방안으로서 많은 활용이 될 것이라 기대한다.

참고문헌

[1] Jakub Konečný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, Dave Bacon, “Federated Learning: Strategies for Improving Communication Efficiency”, ICLR, 10, 2018

[2] Ziru Niu, Hai Dong “FLrce: Resource-Efficient Federated Learning with Early-Stopping Strategy”, IEEE TRANSACTIONS ON MOBILE COMPUTING, 15, 2024

[3] Moming Duan, Duo Liu, Xinyuan Ji, Renping Liu, Liang Liang, Xianzhang Chen, Yujuan Tan “FedGroup: Efficient Clustered Federated Learning via Decomposed Data-Driven Measure”, IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking, 10, 2021

[4] Gregory Koch, Richard Zemel, Ruslan Salakhutdinov “Siamese Neural Networks for One-shot Image Recognition”, ICML deep learning workshop, 2015

[5] H. Brendan McMahan Eider Moore Daniel Ramage Seth Hampson Blaise Aguera y Arcas, “Communication-Efficient Learning of Deep Networks from Decentralized Data”, Proceedings of the 20 th International Conference on Artificial Intelligence and Statistics, 11, 2017