연합 학습 환경에서 통합되고 강인한 다중 작업 학습 기법

안킷 쿠마 싱 [1], 최수빈 [2], 최봉준 [3]
[1] 숭실대학교 컴퓨터학과 박사과정
[2] 숭실대학교 컴퓨터학과 석사과정
[3] 숭실대학교 컴퓨터학과 교수

ankit@soongsil.ac.kr, schoi@soongsil.ac.kr, davidchoi@soongsil.ac.kr

Learning Unified and Robust Representations across Various Tasks within a Federated Learning Environment

Ankit Kumar Singh[1], Subeen Choi[1], Bong Jun Choi[1]
[1]School of Computer Science and Engineering, Soongsil University

요 약

현대의 머신러닝 환경에서는 특히 모바일 컴퓨팅 및 사물 인터넷(IoT)의 애플리케이션 영역에서 개인 정보를 보호하고 효율적이며 확장 가능한 모델에 대한 관심이 높아지고 있다. 본 연구는 연합 학습(FL)과 자기지도 학습(self-supervised learning)을 결합하여 이질적(heterogeneous)인 분산 자원에서 레이블이 없는 데이터를 활용하면서 사용자의 개인 정보를 보호하는 새로운 프레임워크를 소개한다. 이 프레임워크의 핵심은 SimCLR 과 같은 자기지도 학습 기법으로 학습된 공유 인코더로, 입력 데이터에서 고수준 특성을 추출하도록 설계되었다. 또한 이 구조를 통해 주석(annotation)이 없는 방대한 데이터셋을 활용하여 모델 성능을 향상시키고, 여러 개의 격리된 모델이 필요하지 않아 리소스를 크게 최적화할 수 있는 가능성을 확인했다. 본 연구를 통해 생성된 모델은 중앙 집중 방식(CL)이면서 자기지도학습으로 학습되지 않은 기존 모델과 비교하여 전체 평균 정확도가 14.488% 향상됐다.

1. 서론

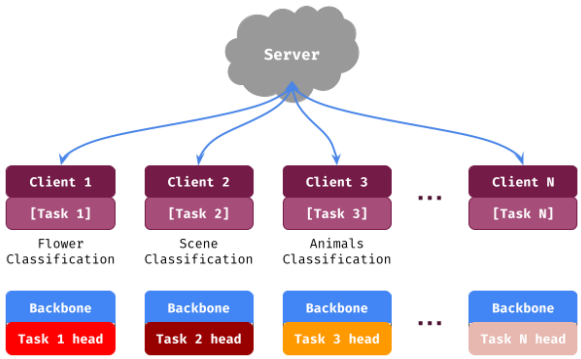
머신러닝은 다양한 분야에 혁신을 가져와 지능적이고 강력한 애플리케이션으로 변화시키고 있다. 머신러닝 모델은 더 나은 패턴과 특성 간의 관계를 도출하기 위해 충분한 양의 데이터를 필요로 한다. 모바일 및 사물 인터넷(IoT) 디바이스의 머신러닝 도입은 데이터 수집, 처리 및 활용 방식을 변화시켜 다양한 애플리케이션에 걸쳐 혁신을 주도하고 있다. 주변 디바이스들은 사용자 단말에서 중앙 서버로 데이터를 수집, 처리 및 공유하는데 사용되며, 일부는 충분한 데이터를 가진 사용자 단말에서 모델을 학습시키기도 한다. 그러나 이러한 발전은 데이터 프라이버시 문제, 주석이 없는 데이터의 효율적 사용 문제, 그리고 특정 작업에 특화된 모델(task-specific models)의 학습에 따른 계산 부담과 같은 몇 가지 중요한 과제들을 야기했다. 개인화된 경험을 위한 사용자 데이터 활용과 개인 정보 보호 사이의 균형잡힌 절충안은 머신러닝 커뮤니티의 핵심적인 관심사가 됐다.

연합 학습[1]은 많은 디바이스에서 분산된 모델 학습을 가능하게 하여 클라이언트 측에서 민감한 데이터를 로컬로 유지함으로써 강력한 솔루션으로 부상하고 있다. 모바일 컴퓨팅과 IoT 디바이스와 같이 말단의 다양한 클라이언트는 방대한 양의 데이터를 생성하고 있다. 이러한 데이터 생성은 데이터 이질성과 연합 학습 환경 내에서 레이블이 지정되지 않은 데이터 통합으로 인해 일반적인 연합학습 환경에서 문제를 야기한다. 실제 환경에서 데이터 레이블링은 많은 시간을 요구하기 때문에 클라이언트가 꺼려하는 어려운 작업이다. 자기 지도 학습(SSL)[2] 기술은 명시적인 레이블 없이도 주석이 없는 데이터의 의미 있는 표현(representation)을 더 잘 활용한다. 마찬가지로 연합 학습은 데이터 공유에 대해 우려하는 클라이언트를 위한 안전한 협업 학습 플랫폼을 제공한다. 또한 강력한 개인 정보 보호를 보장하기 위해 자기 지도

학습이 포함된 연합학습은 말단에서 개인 정보를 보호하는 머신 러닝 모델 학습의 새로운 가능성을 활용할 수 있는 시너지를 제공한다.

본 연구에서는 연합학습을 자기 지도 학습 공유 인코더 아키텍처와 통합하여 레이블이 없는 데이터에서 높은 수준의 특징(feature)을 추출할 수 있는 새로운 접근 방식을 제안한다. 또한 공유 인코더에 특정 작업을 위한 헤드(task-specific heads)를 추가함으로써 다양한 머신러닝 작업을 처리하는 동시에 사용자의 개인정보를 보호하고 계산 리소스를 최적화하는 확장 가능한 모듈식 솔루션을 제안한다. 따라서 본 연구는 모델의 효율성과 확장성을 향상시킬 뿐만 아니라 개인정보를 보호하는 머신러닝 기술에 대한 담론을 발전시키는 프레임워크를 제공함으로써 급성장하고 있는 연합 학습 및 자기 지도 학습 분야에 기여하고자 한다.

2. 연구 제안



(그림 1) 이질적 클라이언트 연합 환경에서의 자기 지도 학습 협업 머신 러닝 구조.

본 연구에서는 연합 학습 환경에서 공유 백본 모델을 활용하는 것이 미치는 영향을 평가하기 위해 그림 1과 같이 동일한 연합 학습 환경 설정 내에서 레이블이 없는 데이터에 대해 자기 지도 학습으로 사전 학습된 백본이 있는 시나리오와 없는 시나리오를 비교했다. 실험 프레임워크는 데이터 세트에 따라 다양한 클라이언트 작업을 반영하도록 설계되었다. Client_1은 꽃 분류를 위해 “flower102” 데이터 세트[4]를 사용했고, Client_2는 장면 분류를 위해 “intel scene” 데이터 세트[5]를 사용했다. 각각의 데이터 세트는 레이블이 있는 데이터 세트와 레이블이 없는 데이터 세트로 나누었으며, 데이터의 75%는 레이블이 없는 세트, 나머지 25%는 레이블이 있는 세트로 구성했다. 표 1은 특정 작업별 클라이언트 데이터 세트에서 레이블링된 샘플과 레이블링되지 않은 샘플의 분포를 보여준다. 본 연구는 공유 백본의 학습에만 레이블링되지 않은 데이터를 활용했으며, 각 클라이언트의 레이블링된 샘플에 대해 학습된 모델을 평가했다. 반대로, 특정 작업을 위한 헤드에서는 레이블링된 데이터는 학습 세트, 레이블링되지 않은 데이터는 평가 세트로 사용된다. 공유 백본은 작업 헤드를 위한 선형 레이어로 보완된 ResNet50 아키텍처[3]를 기반으로 한다. 시각적 표현을 학습하기 위한 자기 지도 학습 방법에는 대조 학습의 방법론 중 하나인 SimClr[2]가 사용되었다.

<표 1> 데이터 세트별 레이블링 여부에 따른 샘플 수

Flower102 (Client_1)		Intel scene (Client_2)	
Unlabeled	Labeled	Unlabeled	Labeled
6142	2047	12776	4258

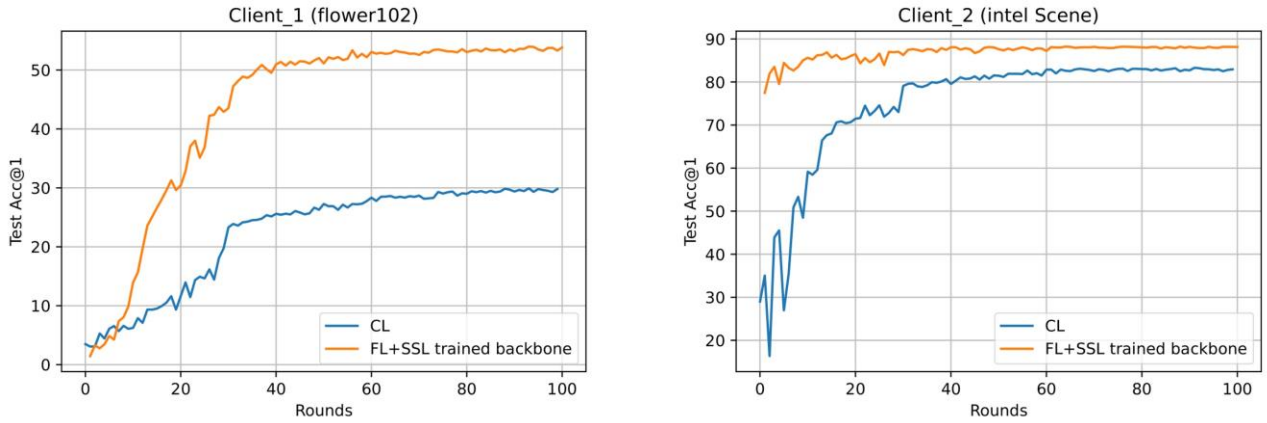
본 연구에서는 2 단계 연합 학습 구조를 사용한다. 먼저 공유 백본을 학습한 뒤, 사전 학습된 공유 백본의 존재 여부와 관계없이 작업 모델을 학습한다. 각 과정에서 클라이언트는 서버로부터 공유 백본 모델을 수신하고 로컬 데이터 세트에서 학습한 다음 서버에 업데이트를 제공한다. 그 후 서버는 FedAvg[1] 알고리즘을 사용하여 업데이트를 집계하고, 업데이트된 집계 가중치를 클라이언트에 재분배한다.

3. 성능 평가

<표 2> 클라이언트별 평가 정확도

method	Flower102 (Acc@1)	Intel Scene (Acc@1)
CL	29.926	83.288
FL + SSL trained backbone	**53.971**	**88.219**

본 연구에는 기존의 중앙 집중형 환경(CL)과 연합 학습(FL) 환경 모두에서 제안된 방법의 효과를 평가하기 위해 일련의 실험을 수행하였다. 특히 자기 지도 학습 백본을 활용한 경우의 모델 성능을 백본의 없을 때의 성능과 비교했다. 해당 실험을 통해 자기 지도 학습을 통해 사전에 학습된 공유 백본을 활용하면 시각적 표현이 보다 일반화되어 다양한 작업의 정확도가 향상된다는 결과를 얻었다. 표 2는 실험의 결과로 확인된 자세한 성능 개선 사항을 나타낸다. Client_1은 꽃 분류 작업에서 정확도가 24.045%로 크게 향상되었다. 이에 비해 Client_2는 장면 분류 작업의 정확도가 4.931% 향상되었다.



(그림 2) 중앙 집중형 방식과 SSL 로 훈련된 백본을 사용한 연합학습의 테스트 정확도 비교

결과적으로 자기 지도 학습 백본을 사용한 연합 학습 모델은 기존의 중앙 집중형 방식 모델에 비해 평균 14.488%의 성능 향상을 보여주었다. 또한 자기 지도 학습으로 사전 훈련된 모델은 성능이 더 우수할 뿐만 아니라 훨씬 적은 수의 훈련 라운드에서 정확도가 수렴에 도달하는 것을 확인하였다. 이러한 경향은 그림 2 에서도 명확하게 확인할 수 있다.

4. 결론

위에서 제안된 방법론은 컴퓨팅 리소스를 최적화하면서 클라이언트의 풍부한 라벨링되지 않은 데이터를 활용하는 것을 목표로 한다. 이는 연합 학습 프레임워크 내에서 레이블이 없는 데이터에 대해 공유 백본 모델을 학습시킨 다음 특정 작업 헤드를 백본에 연결하고, 이후 제한된 레이블 데이터 샘플 세트를 사용하여 특정 백본 매개변수의 최소한의 재학습과 함께 이러한 작업 헤드를 학습시킴으로써 달성할 수 있다. 이러한 전략을 사용한 결과, 중앙 집중형 환경(CL)의 자기 지도 학습 백본을 사용하지 않은 기존 방식과 비교하여 Client_1의 경우 24.045%, Client_2의 경우 4.931%, 전체 평균 14.488%의 성능 향상이 이루어졌다. 이 방법은 클라이언트의 데이터 세트와 작업의 다양성을 고려하고 각 클라이언트의 데이터 샘플이 다른 클라이언트의 데이터 샘플과 크게 다를 수 있음을 고려함으로써 공유 백본 모델의 일반화 기능을 향상시킨다. 향후 추가적인 조사와 실험을 진행하여 데이터 이질성 문제를 해결하고, 모든 클라이언트별 작업에서 성능을 향상시켜 보다 일반화된 백본 모델을 개발할 계획이다.

사사문구

본 성과는 과학기술정보통신부의 재원으로 한국연구재단의 지원을 받아 수행된 연구이며(NRF-2022R1A2C4001270), 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2020-0-01602).

참고문헌

[1] Brendan McMahan, et al. "Communication-efficient learning of deep networks from decentralized data", Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 2017, 1273-1282.

[2] Chen, Ting, et al. "A simple framework for contrastive learning of visual representations", Proceedings of the IEEE conference on computer vision and pattern recognition, 2020, 1597-1607.

[3] He, Kaiming, et al. "Deep residual learning for image recognition", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, 770-778.

[4] Nilsback, Maria-Elena, and Andrew Zisserman. "Automated flower classification over a large number of classes." 2008 Sixth Indian conference on computer vision, graphics & image processing. IEEE, 2008. (https://www.robots.ox.ac.uk/~vgg/data/flowers/102/)

[5] Puneet Bansal, "Intel Image Classification.", Kaggle, Jun 2019, https://www.kaggle.com/datasets/puneet6060/intel-image-classification, accessed: Apr 2024.