연합학습과 Image accessment

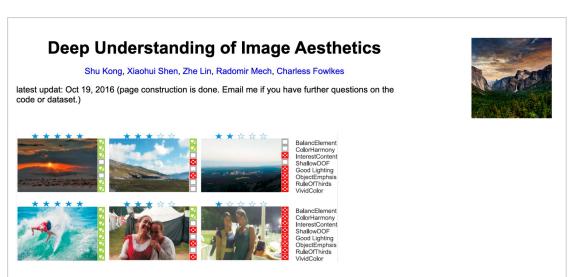
Project: Image Aesthetic Assessment



AADB dataset

Project. Image Aesthetic Assessment by GAN

데이터: <Image Aesthetic Assessment Assisted by Attributes through Adversarial Learning> 논문에 쓰인 AADB dataset 이용



https://www.ics.uci.edu/~skong2/ae sthetics.html

Project 참고 논문

제목: <Image Aesthetic Assessment Assisted by Attributes through Adversarial Learning, 2019>

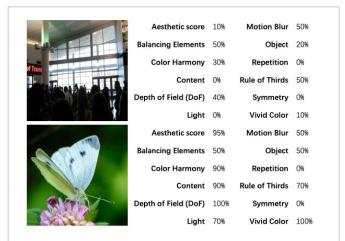
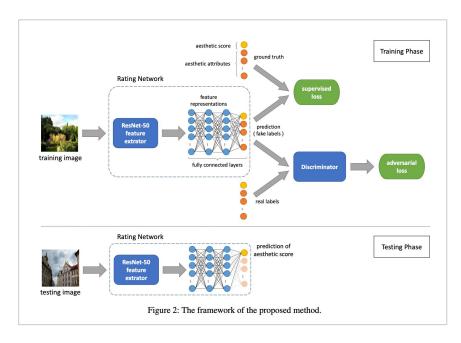


Figure 1: Two examples of aesthetic images (upper: low aesthetics; lower: high aesthetics) with respect to eleven assessment attributes. The ratings of the aesthetic score and attributes are written as percentage for convenience.



예측결과

예측값	점수
0.173746	0.2
0.79069746	0.9
0.3458445	0.35
0.36657217	0.45
0.39773205	0.4
0.7662744	0.75
0.42369613	0.5
0.33643967	0.35
0.5873672	0.5
0.33634272	0.417
0.26790738	0.6
0.59256893	0.55
0.41443825	0.45
0.6174326	0.65
0.6793358	0.65
0.68811	0.7
0.48442963	0.35
0.24432424	0.2
0.8867989	0.9
0.48421514	0.5
0.3106196	0.3



점수: 0.5

예측치: 0.4236913

→ **100**개의 이미지에 점수에 대한 <mark>평균 예측 오차값은</mark> 0.00572533

→ 비교적 점수를 잘 예측 하고 있는 것을 알 수 있다

Real-World Image Datasets for Federated Learning

Jiahuan Luo^{1*}, Xueyang Wu^{2*}, Yun Luo^{2,3}, Yunfeng Huang^{4*}, Yang Liu^{5†}, Aubu Huang⁵, Qiang Yang^{2,5}

¹South China University of Technology, China ²Hong Kong University of Science and Technology, Hong Kong SAR, China ³Extreme Vision Co. Ltd., Shenzhen, China ⁴Shenzhen University, China ⁵WeBank Co. Ltd., Shenzhen, China

 $seluojiahuan@mail.scut.edu.cn, \{xwuba, yluoav\}@cse.ust.hk, huangyunfeng2017@email.szu.edu.cn \\ \{yangliu, stevenhuang\}@webank.com, qyang@cse.ust.hk$

Abstract

Federated learning is a new machine learning paradigm which allows data parties to build machine learning models collaboratively while keeping their data secure and private. While research efforts on federated learning have been growing tremendously in the past two years, most existing works still depend on pre-existing public datasets and artificial partitions to simulate data federations due to the lack of high-quality labeled data generated from real-world edge applications. Consequently, advances on benchmark and model evaluations for federated learning have been lagging behind. In this paper, we introduce a real-world image dataset. The dataset contains more than 900 images generated from 26 street cameras and 7 object categories annotated with detailed bounding box. The data distribution is non-IID and unbalanced, reflecting the characteristic real-world federated learning scenarios. Based on this dataset, we implemented two mainstream object detection algorithms (YOLO and Faster R-CNN) and provided an extensive benchmark on model performance, efficiency, and communication in a federated learning setting. Both the dataset and algorithms are made publicly available1.



Figure 1: Examples taken from Street Dataset. The green bounding boxes represent the target objects.

greatly improved in the past few decades [Ren et al., 2017; Redmon and Farhadi, 2018a; Zhao et al., 2018]. A traditional object detection approach requires collecting and centralizing a large amount of annotated image data. Image annotation is very expensive despite crowd-sourcing innovations, especially in areas where professional expertise is required, such

제목: Real-World Image Datasets for Federated Learning

- 데이터셋은 26개의 도로 카메라와 7개의 객체 범주에서 생성된 900개 이상의 이미지로 구성
- 데이터 분포는 비 IID 이며, 불균형하게 되어 있고 실제 세계의 Federated learning 시나리오를 반영
- 이 데이터셋을 기반으로 YOLO와
 Faster R-CNN 두 가지 주요 객체 감지 알고리즘 구현
- Federated learning 환경에서 모델 성능, 효율성 및 통신에 대한 포괄적인 벤치마크 제공

Datasets

Table 2: Detailed distribution of the object labels in the training set of Street-5 Dataset and Street-20 Dataset

Street-5	Images/Client		Frequency/Client			
Dataset	total	mean	stdev	total	mean	stdev
Basket	127	25.40	15.08	165	33.00	22.20
Carton	133	26.60	27.94	215	43.00	55.13
Chair	369	73.80	59.36	494	98.80	87.60
Electro -mobile	257	51.40	45.23	510	102.00	105.27
Gastank	71	14.20	26.42	106	21.20	36.19
Sunshade	255	51.00	31.89	413	82.60	56.02
Table	73	14.60	29.20	102	20.40	40.80

Street-20	Images/Client		Frequency/Client			
Dataset	total	mean	stdev	total	mean	stdev
Basket	127	6.35	11.06	165	8.25	14.93
Carton	133	6.65	12.03	215	10.75	26.23
Chair	369	18.45	17.70	494	24.70	28.54
Electro -mobile	257	12.85	14.81	510	25.50	37.55
Gastank	71	3.55	11.14	106	5.30	16.63
Sunshade	255	12.75	19.14	413	20.65	37.87
Table	73	3.65	13.06	102	5.10	19.26

- 데이터셋은 26개의 도로 카메라와 7개의 객체 범주에서 생성된 900개 이상의 이미지로 구성
- 카메라의 지리적 정보에 따라 **Street** 데이터셋을 분할
- 총 26개의 도로 모니터링 비디오가 있지만,
 일부 카메라는 매우 적은 이미지를 가지고 있음
- 총 956개의 이미지로 구성된 전체 데이터셋을 80% (765개 이미지)의 학습용 데이터와 20% (191개 이미지)의 테스트용 데이터로 분할
- 테스트 세트는 매우 적은 이미지를 가진 6개 카메라의 이미지와 다른 20개 카메라에서 랜덤하게 샘플링된 이미지로 구성되어 있음
- 이렇게 데이터셋을 분할함으로써 테스트 세트는 기존 카메라의 이미지를 통해 예측 가능성을 평가하고, 본적 없는 카메라의 이미지를 통해 일반화 능력을 공동으로 평가 할 수 있음

Experiment

Algorithm 1 Pseudo FedAvg

Input: N client parties $\{c_k\}_{k=1..N}$, total rounds T, and Server side S;

Output: Aggregated Model w

 \mathcal{S} initializes federated model parameters, and saves as checkpoint. Client parties $\{c_k\}_{k=1..N}$ load the checkpoints.

```
for t=1,...,T do

for k=1,...,N do

w_k=w^{(t)}
each client \{c_k\} do local training:

for i=0,1,...,M_k do

(M_k \text{ is the number of data batches b in the client } c_k)
client \{c_k\} computes gradients \nabla \ell(w_k,b_i)
update with w_k=w_k-\eta\nabla\ell(w_k,b_i)
end for
save w_k results to checkpoints.
end for

\mathcal{S} loads checkpoints and get averaged model with w^{(t)}=\frac{1}{N}\sum_{k=1}^N w_k
end for
return w^{(T)}
```

- 이 논문에서는 FederatedAveraging (FedAvg) 알고리즘 [McMahan et al., 2016]을 기반으로 하는 프레임워크를 구현
- 데이터 분할과 페더레이티드 러닝 설정의 영향을 조사하기 위해, 서버-클라이언트 통신 프레임워크 (SocketIO와 같은)를 체크포인트 저장 및 복원으로 대체하여 가상의 FedAvg 알고리즘으로 수정
- FedAvg 알고리즘에는 세 가지 주요 매개변수가 있습니다: C는 각 라운드에서 학습에 참여하는 클라이언트의 수, E는 각 클라이언트가 로컬 데이터셋을 사용하여 수행하는 횟수, B는 클라이언트 업데이트에 사용되는 미니배치 크기
- FedAvg 알고리즘의 경우, 각 라운드에서 R 비율의 클라이언트를 선택하고 이러한 클라이언트가 보유한 모든 데이터에 대한 손실의 그라디언트를 계산
- 따라서 이 알고리즘에서 R은 전역 배치 크기를 제어하며, R = 1은 전체 배치 경사하강법에 해당
- 더 좋은 결과를 얻기 위해, 저희는 R = 1로 고정하여 서버가 학습에 참여하는 모든 클라이언트의 업데이트를 기다리도록 설정

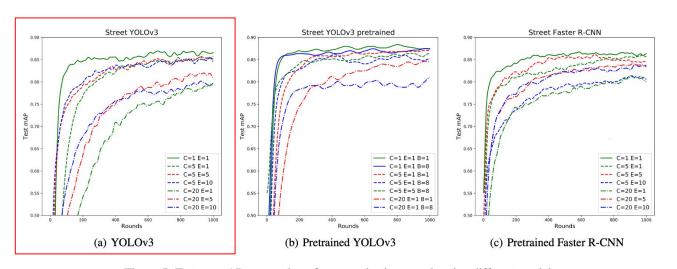


Figure 5: Test set mAP vs. number of communication rounds using different models

- Figure 5(a)는 사전 학습 모델 없이 YOLOv3의 테스트 세트 mAP를 보여줍니다
- 지리적 위치에 따라 데이터가 다섯 부분으로 분할되며, 각 클라이언트 당 계산량을 늘리기 위해 **E(epoch)**를 증가
- 지역 epoch E를 증가시키는 것이 효과적임을 알 수 있다.
- Figure 5(a)는 라운드마다 더 많은 지역 SGD 업데이트를 추가하고 결과 모델을 평균화함으로써 훈련 절차 초반에 더 높은 mAP에 도달할 수 있음을 보여줍니다.

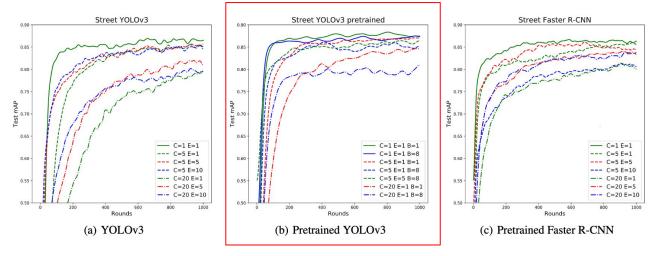


Figure 5: Test set mAP vs. number of communication rounds using different models

- ImageNet 사전 학습은 최첨단 결과를 개선하는 데 중요한 역할을 했음. 사전 학습의 중요성 때문에, 이 논문에서는 사전 학습된 모델을 사용하여 추가 실험을 진행
- Figure 5(b)는 사전 학습된 모델 가중치로 초기화하는 것이 특히 각 클라이언트에 사진이 적은 Street-20 데이터셋을 포함하여 유의미하고 안정적인 개선을 가져온다는 것을 보여줌
- Figure 5(b)는 각 클라이언트의 배치 크기의 영향을 보여줍니다.
- 각 클라이언트의 배치 크기를 증가시켜도 효과가 크지 않습니다. 이는 각 클라이언트의 사진 수가 적기 때문일 것으로 추측됩니다.
- 특히 Street-20 데이터셋에서는 각 클라이언트에 수십 개의 사진만 포함되어 있기 때문에, 더 큰 배치 크기는 심지어 성능이 떨어지게 할 수 있음

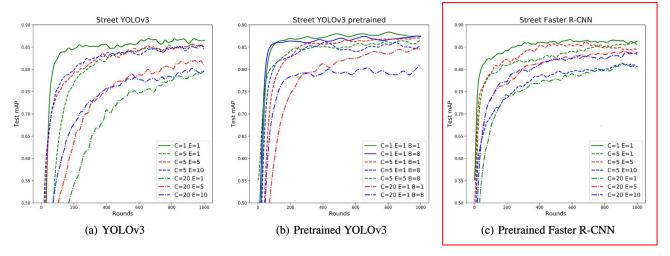


Figure 5: Test set mAP vs. number of communication rounds using different models

- 객체 탐지에 대한 원 스테이지 접근 방법 외에도, 우리의 벤치마크로서 인기있는 두 스테이지 접근 방법인 Faster R-CNN을 포함하고 있음
- Figure 5(c)는 사전 학습된 VGG-16 백본 네트워크를 사용한 Faster R-CNN의 성능을 보고
- Faster R-CNN의 경우 C = 5, E = 1, FedAvg 모델은 결국 중앙 집중식 학습과 거의 동일한 성능을 달성
- C = 5, E = 5, FedAvg 모델은 400 라운드 이후에 상당한 mAP를 달성
- 사전 학습 모델로 훈련하는 것은 더 빠른 수렴을 보여줌
- C = 5일 때, 작은 지역 epoch가 더 좋은 성능을 나타냄

- C: 각 라운드에서 학습에 참여하는 클라이언트의 수,
- E: 각 클라이언트가 로컬 데이터셋을 사용하여 수행하는 횟수
- · B: 클라이언트 업데이트에 사용되는 미니배치 크기



This CVPR 2021 paper is the Open Access version, provided by the Computer Vision Foundation.

Except for this watermark, it is identical to the accepted version;
the final published version of the proceedings is available on IEEE Xplore.

Model-Contrastive Federated Learning

Qinbin Li National University of Singapore Bingsheng He National University of Singapore Dawn Song UC Berkeley

qinbin@comp.nus.edu.sg

hebs@comp.nus.edu.sq

dawnsong@berkeley.edu

Abstract

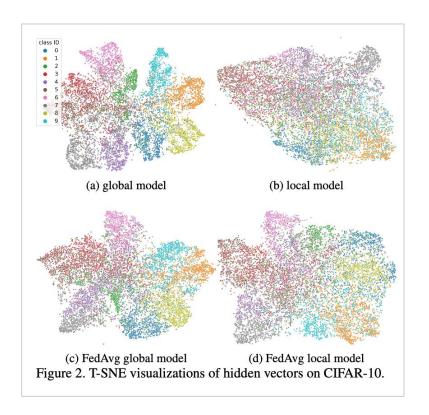
Federated learning enables multiple parties to collaboratively train a machine learning model without communicating their local data. A key challenge in federated learning is to handle the heterogeneity of local data distribution across parties. Although many studies have been proposed to address this challenge, we find that they fail to achieve high performance in image datasets with deep learning models. In this paper, we propose MOON: modelcontrastive federated learning. MOON is a simple and effective federated learning framework. The key idea of MOON is to utilize the similarity between model representations to correct the local training of individual parties. i.e., conducting contrastive learning in model-level. Our extensive experiments show that MOON significantly outperforms the other state-of-the-art federated learning algorithms on various image classification tasks.

A key challenge in federated learning is the heterogeneity of data distribution on different parties [20]. The data can be non-identically distributed among the parties in many real-world applications, which can degrade the performance of federated learning [22, 29, 24]. When each party updates its local model, its local objective may be far from the global objective. Thus, the averaged global model is away from the global optima. There have been some studies trying to address the non-IID issue in the local training phase [28, 22]. FedProx [28] directly limits the local updates by ℓ_2 -norm distance, while SCAFFOLD [22] corrects the local updates via variance reduction [19]. However, as we show in the experiments (see Section 4), these approaches fail to achieve good performance on image datasets with deep learning models, which can be as bad as FedAvg.

In this work, we address the non-IID issue from a novel perspective based on an intuitive observation: the global model trained on a whole dataset is able to learn a bet-

- 피더레이티드 러닝은 로컬 데이터를 공유하지 않고 여러 당사자가 협력하여 기계 학습 모델을 훈련할 수 있는 방법을 제공함
- 피더레이티드 러닝에서의 주요 도전 과제는 당사자 간의 로컬 데이터 분포의 이질성을 처리하는 것이다.이에 대해 다양한 연구가 제안되었지만, 딥러닝 모델을 사용하는 이미지 데이터셋에서는 높은 성능을 달성하기 어렵다는 문제점이 있음
- 본 논문에서는 MOON(모델 대비적 피더레이티드 러닝)을 제안한다. MOON은 간단하고 효과적인 피더레이티드 러닝 프레임워크
- MOON의 핵심 아이디어는 모델 표현 간의 유사성을 활용하여 개별 당사자의 로컬 훈련을 보정하는 것인데, 이는 모델 수준에서 대비적 학습(contrastive learning)을 수행하는 것
- 광범위한 실험 결과 MOON이 다양한 이미지 분류 작업에서 다른 최신 피더레이티드 러닝 알고리즘보다 현저히 우수한 성능을 보여줌

Motivation



- MOON은 직관적인 아이디어에 기반하고 있습니다: 전체 데이터셋으로 훈련된 모델은 편향된 하위 집합에서 훈련된 모델보다 더 나은 특성 표현을 추출할 수 있다. 예를 들어, 개와 고양이 이미지로 훈련된 모델에서는 훈련 중에 전혀 존재하지 않는 새와 개구리를 구별할 수 있는 특성을 기대할 수 없다.
- 이 직관을 더 검증하기 위해, CIFAR-10 데이터셋에서 간단한 실험을 수행함. 구체적으로, 우선 CIFAR-10에서 CNN 모델을 훈련하였다. t-SNE [33]를 사용하여 테스트 데이터셋의 숨겨진 벡터를 시각화하였으며, 이는 그림 2a에 표시되어 있습니다.
- 그런 다음, 데이터셋을 균형이 맞지 않도록 10개의 하위 집합으로 분할하고 각 하위 집합에서 CNN 모델을 훈련함. 그림 2b는 임의로 선택된 모델의 t-SNE 시각화를 보여줌. 분명히, 하위 집합에서 훈련된 모델은 부족한 특성을 학습한다. 대부분의 클래스의 특성 표현은 심지어 섞여있다.
- 그런 다음, 10개의 하위 집합에서 FedAvg 알고리즘을 실행하고 전역 모델이 학습한 표현을 그림 2c에, 선택한 로컬 모델이 학습한 표현(전역 모델을 기반으로 훈련된 것)을 그림 2d에 나타내었다.
- 그림 2d에서는 동일한 클래스의 점들이 그림 2c에 비해 더 발산하는 것을 관찰할 수 있다.
- 편향된 로컬 데이터 분포로 인해 로컬 훈련 단계는 모델이 더나쁜 표현을 학습하도록 이끌기도 한다. 이는 전역 모델이 로컬모델보다 더 나은 특성 표현을 학습할 수 있어야 하고, 로컬업데이트 사이에 변동이 있는 것을 더 확인한다. 따라서, 비 IID 데이터 시나리오에서는 변동을 제어하고 로컬 모델과 전역모델이 학습한 표현 사이의 격차를 줄여야 한다.

Method

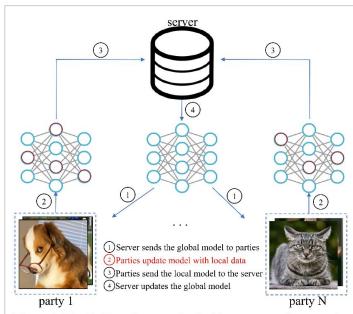


Figure 1. The FedAvg framework. In this paper, we focus on the second step, i.e., the local training phase.

- MOON은 FedAvg를 기반으로 한 간단하고 효과적인 접근 방식으로, 로컬 훈련 단계에서 가벼우면서도 독특한 수정 사항을 도입합니다.
- 로컬 훈련에서 항상 변동이 있고 전역 모델이 로컬 모델보다 더 나은 표현을 학습하기 때문에, MOON은 로컬 모델이 학습한 표현과 전역 모델이 학습한 표현 사이의 거리를 줄이고, 로컬 모델이 이전 로컬 모델이 학습한 표현과의 거리를 늘리기 위해 설계되었습니다.
- 이를 위해 주로 시각적 표현을 학습하는데 사용되는 대비적 학습의 영감을 얻었습니다. 이어서 네트워크 구조, 로컬 학습 목적 및 학습 절차를 소개하고, 대비적 학습과의 관련성을 논의합니다.

Method

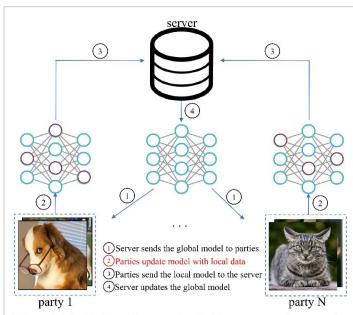
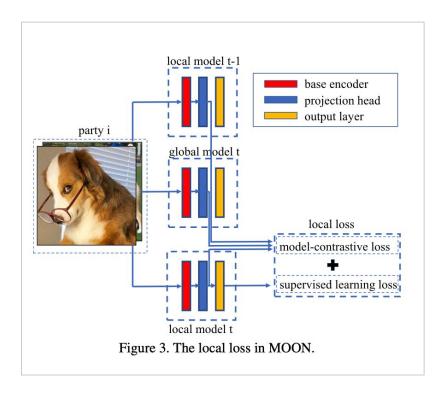


Figure 1. The FedAvg framework. In this paper, we focus on the second step, i.e., the local training phase.

- MOON은 FedAvg를 기반으로 한 간단하고 효과적인 접근 방식으로, 로컬 훈련 단계에서 가벼우면서도 독특한 수정 사항을 적용한 것
- 로컬 훈련에서 항상 변동이 있고 전역 모델이 로컬 모델보다 더 나은 표현을 학습하기 때문에, MOON은 로컬 모델이 학습한 표현과 전역 모델이 학습한 표현 사이의 거리를 줄이고, 로컬 모델이 이전 로컬 모델이 학습한 표현과의 거리를 늘리기 위해 설계되었다.
- 이를 위해 주로 시각적 표현을 학습하는데
 사용되는 대비적 학습의 영감을 얻었음.

Network Architecture



- 네트워크는 기본 인코더(base encoder), 프로젝션 헤드(projection head) 및 출력 레이어(output layer) 세 가지 구성 요소로 이루어져 있다.
- 기본 인코더는 입력으로부터 표현 벡터를 추출하는 데 사용됩니다. [3] 과 마찬가지로, 추가적인 프로젝션 헤드가 도입되어 표현을 고정된 차원의 공간으로 매핑합니다.
- 마지막으로, 우리는 지도 학습이라는 설정 하에 연구하기 때문에 출력 레이어를 사용하여 각 클래스에 대한 예측값을 생성
- Figure 3에서 보여지듯이, 우리의 로컬 손실은 두 부분으로 구성됨. 첫 번째 부분은 지도 학습에서 일반적인 손실 용어 (예: 교차 엔트로피 손실)로 표시되는 일반적인 손실(Isup)입니다. 두 번째 부분은 우리가 제안한 모델-대조 손실 용어로 표시되는 Icon
- [3] Ting Chen, Simon Kornblith, Mohammad Norouzi, and Ge- offrey Hinton. A simple framework for contrastive learning of visual representations. *arXiv* preprint arXiv:2002.05709, 2020.

Experiment

```
Algorithm 1: The MOON framework
    Input: number of communication rounds T,
              number of parties N, number of local
              epochs E, temperature \tau, learning rate \eta,
              hyper-parameter \mu
    Output: The final model w^T
 1 Server executes:
2 initialize w^0
3 for t = 0, 1, ..., T - 1 do
        for i = 1, 2, ..., N in parallel do
              send the global model w^t to P_i
             w_i^t \leftarrow \mathbf{PartyLocalTraining}(i, w^t)
 7 w^{t+1} \leftarrow \sum_{k=1}^{N} \frac{|\mathcal{D}^i|}{|\mathcal{D}|} w_k^t
 8 return w^T
9 PartyLocalTraining(i, w^t):
10 w_i^t \leftarrow w^t
11 for epoch i = 1, 2, ..., E do
         for each batch \mathbf{b} = \{x, y\} of \mathcal{D}^i do
              \ell_{sup} \leftarrow CrossEntropyLoss(F_{w_{\cdot}^{t}}(x), y)
              z \leftarrow R_{w^t}(x)
14
              z_{alob} \leftarrow R_{w^t}(x)
              z_{prev} \leftarrow R_{w^{t-1}}(x)
                -\log \frac{\exp(\sin(z, z_{glob})/\tau)}{\exp(\sin(z, z_{glob})/\tau) + \exp(\sin(z, z_{prev})/\tau)}
              \ell \leftarrow \ell_{sup} + \mu \ell_{con}
              w_i^t \leftarrow w_i^t - \eta \nabla \ell
20 return w_i^t to server
```

- MOON은 각 라운드마다 일부 파티만이 참여하는 페더레이티드 러닝에도 적용할 수 있다.
- FedAvg와 마찬가지로 각 파티는 자체적인 로컬 모델을 유지하며, 파티가 라운드에 참여하는 경우에만 전역 모델로 대체되고 업데이트 된다.
- MOON은 파티가 가지고 있는 최신 로컬 모델만 필요로 하며, 이는 (t-1) 라운드에서 업데이트되지 않았을 수도 있다.
- 주목할 점은 로컬 모델이 충분히 좋고 전역 모델과 (거의)
 동일한 표현을 학습하는 이상적인 경우를 고려할 때, 모델 대조 손실은 상수가 될 것 (즉, -log 21)
- 따라서, 이질성 문제가 없는 경우 MOON은 FedAvg와 동일한 결과를 보일 것
- 이런 의미에서, 우리의 접근 방식은 서로 다른 drift의 양에 관계없이 견고하게 작동함

Result

Table 1. The top-1 accuracy of MOON and the other baselines on test datasets. For MOON, FedAvg, FedProx, and SCAFFOLD, we run three trials and report the mean and standard derivation. For SOLO, we report the mean and standard derivation among all parties.

Method	CIFAR-10	CIFAR-100	Tiny-Imagenet
MOON	69.1% ±0.4%	67.5% ±0.4%	25.1% ±0.1%
FedAvg	66.3%±0.5%	64.5% ±0.4%	23.0%±0.1%
FedProx	66.9%±0.2%	64.6%±0.2%	$23.2\% \pm 0.2\%$
SCAFFOLD	66.6%±0.2%	52.5% ±0.3%	$16.0\% \pm 0.2\%$
SOLO	46.3% ±5.1%	22.3%±1.0%	$8.6\% \pm 0.4\%$

- 표 1은 위의 기본 설정으로 모든 접근 방식의 상위 1위 테스트 정확도를 보여줌
- Non-IID 설정에서 SOLO는 다른 페더레이티드 러닝 접근 방식보다 훨씬 낮은 정확도를 보임. 이는 페더레이티드 러닝의 이점을 보여줌.
- 다른 페더레이티드 러닝 접근 방식을 비교해보면,
 MOON이 모든 작업에서 일관되게 가장 우수한 접근 방식임을 알 수 있음.
- MOON은 모든 작업의 평균적으로 FedAvg보다 2.6%의 정확도를 높일 수 있음.
- FedProx의 경우, 정확도는 FedAvg와 매우 근접함. FedProx의 근사항은 μ가 작기 때문에 학습에 거의 영향을 미치지 않습니다. 그러나 μ를 매우 작은 값으로 설정하지 않은 경우, FedProx의 수렴이 매우 느리고 정확도가 나쁠 수 있다.
- SCAFFOLD의 경우, CIFAR-100 및 Tiny-Imagenet에서 다른 페더레이티드 러닝 접근 방식보다 훨씬 낮은 정확도를 보임.

μ: hyper-parameter

Result

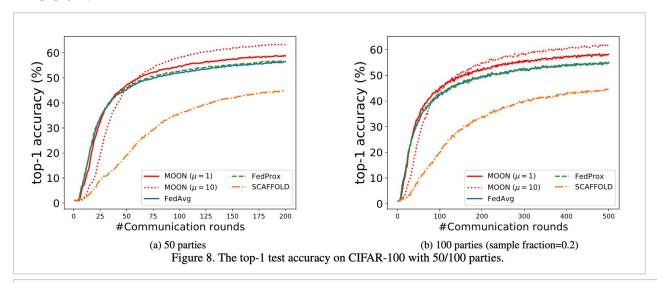


Table 4. The test accuracy with β from $\{0.1, 0.5, 5\}$.

Method	$\beta=0.1$	$\beta = 0.5$	$\beta = 5$	
MOON	64.0%	67.5%	68.0%	
FedAvg	62.5%	64.5%	65.7%	
FedProx	62.9%	64.6%	64.9%	
SCAFFOLD	47.3%	52.5%	55.0%	
SOLO	15.9%±1.5%	22.3%±1%	$26.6\% \pm 1.4\%$	

Table 5. The top-1 accuracy with different kinds of loss for the second term of local objective. We tune μ from $\{0.001, 0.01, 0.1, 1, 5, 10\}$ for the ℓ_2 norm approach and report the best accuracy.

second term	CIFAR-10	CIFAR-100	Tiny-Imagenet
none (FedAvg)	66.3%	64.5%	23.0%
ℓ_2 norm	65.8%	66.9%	24.0%
MOON	69.1%	67.5%	25.1%

감사합니다.