# **The SL & SSL Model Which Learned Data Augmentation**

|  |  |  |
| --- | --- | --- |
| 이연우 | 정민기 | 한대일 |
| 인공지능 응용학과 | 인공지능 응용학과 | 인공지능 응용학과 |
| 21102376 | 21102385 | 21102398 |

1. **서론**

이 프로젝트는 사람과 머신러닝 모델의 인식 차이에 대한 의문점을 가지고 시작하였다. 사람의 경우, 노이즈가 있는 고양이 사진을 인식할 때 그 사진을 고양이라고 인식할 수 있지만, 머신러닝 모델의 경우 고양이라고 잘 인식하지 못할 뿐더러 높은 오차를 낼 수 있다. 뿐만 아니라, 특수한 경우 아예 고양이가 아닌 다른 객체(예컨대 강아지 등)로 인식할 가능성도 있다.

우리는 위와 같은 현상을 머신러닝 모델에 이미지 왜곡에 관한 사전지식이 명확히 정의되지 않아서 발생한 것이라고 판단하였다. 따라서 이 연구는 이미지가 왜곡 또는 훼손될 수 있음을 모델에게 학습시키는 것을 목표로 한다. 그리하여 이 과정을 거쳤을 때 모델의 오차가 줄어들 수 있을 것이라는 가설을 검증하고자 한다. 즉 data augmentation 과정을 모델에게 사전 지식으로서 명시적으로 학습시킨다면, 모델의 학습 능력이 더 향상될 것이라는 아이디어를 증명하고자 하는 것이다.

1. **프로젝트 주제 기술**

이 프로젝트 에서는 기본적인 이미지 분류 모델과 data augmentation을 학습시킨 두 모델을 비교하여 그 성능을 분석하고자 하였다. 첫번째 모델은 data augmentation을 통해 증가된 데이터를 바탕으로 이미지를 분류하는 전통적인 모델이다. 그리고 두번째 모델은 전통적인 이미지 분류 모델에, 이미지에 가해진 data augmentation 방식을 예측하는 레이어를 결합한 모델이다. 즉 첫번째 모델의 경우 일반적으로 사용되었던 이미지 분류 모델이며, 두번째 모델의 경우 data augmentation에 관한 사전지식을 학습한 모델이다. 이에 더해, semi-supervised learning을 이용한 모델을 추가하여 총 4가지 모델의 결과 비교를 하고자 계획하였다.

Data augmentation의 경우 pytorch에 있는 augmentation 기법들을 이용하고자 하였다. Data augmentation을 구별하는 모델은 이러한 기법들 중 어떤 기법을 통해 변형된 이미지인지 확인할 수 있도록 구현하고자 하였다. 추후 보강이 가능하다면 한 장의 사진에 여러 개의 augmentation 기법이 이용되었을 경우에도 모두 구분해낼 수 있는 다중 출력이 가능한 모델 또한 구현해보고자 계획하였다.

일단 이 milestone 제출일 까지는 먼저 random erasing 여부를 확인할 수 있는 모델까지 구현하여 테스트 해 보았다. 데이터셋의 경우 본 실험은 ImageNet을 이용하고자 하며, 지금까지의 실험은 cifar-10을 이용하여 실험하였다. 이에 사용된 augmentation 기술은 vertical flip, horizontal flip, random erasing, gaussian blur이다. 본 실험에서의 모델은 resnet을 사용하고자 하며, 일단은 모델의 실행 가능 여부를 확인하기 위해 기본 CNN과 MLP 모델을 이용한 testnet을 구현하여 실험하였다.

1. **접근 방법**

**결과1.** Supervised learning을 이용한 이미지 분류

**결과2.** Semi-supervised learning을 이용한 이미지 분류

**결과3.** Data augmentation을 예측하는 모델과 결합 한 Supervised learning을 이용한 이미지 분류

**결과4.** Data augmentation을 예측하는 모델과 결합 한 Semi-supervised learning을 이용한 이미지 분류

Timeline

Description automatically generated with low confidence

▲ data augmentation을 적용한 이미지의 분류에서 지도학습(결과1)과 준지도학습(결과2)의 비교

Timeline

Description automatically generated

▲ 적용된 data augmentation을 예측하는 모델과 결합시킨 지도학습(결과3)과 준지도학습(결과4)의 비교

1. **실험 결과 및 분석**

|  |  |  |  |
| --- | --- | --- | --- |
| 결과1 | 결과2 | 결과3 | 결과4 |
| aug-testnet | mean teacher | dsnet | da-mean teacher |
| 0.6316 | 0.5471 | 0.6250 | 수렴 X |

모델 da는 data augmentation을 구별하는 모델로 학습 정확도는 약 99.77%가 나왔다.

예상과는 다르게 data augmentation을 구별하는 모델과 결합한 모델의 정확도가 기본 모델보다 높지 않게 나와 그 결과를 분석해 보았다. 먼저 첫번째 원인으로 예상되는 것은, testnet 자체에 이미 augmentation에 대한 학습이 충분히 진행되어 있다는 점이다. 이 때문에 결과 3과 결과4에서 처럼 명시적인 레이어를 설정하는 것이 그다지 큰 효용을 내지 못한 것 같다. 이에 관해서는 모델 4의 구현을 통해 이를 확인하는 방법으로 추후 프로젝트를 진행해보려 한다. 또한 다른 원인으로는, 아직 data augmentation을 구별하는 모델에 random erasing만 구별할 수 있게 적용하였기 때문이라는 것이다. 구별할 수 있는 augmentation의 종류를 더 늘리면 좀더 가시적인 성과를 볼 수 있을 거라고 기대된다.

1. **추후 계획**

추후 계획으로, 앞서 말했듯이 프로젝트에 resnet 모델과 ImageNet 데이터셋을 이용한 구현을 해볼 예정이며, 수렴이 되지 않은 모델 4를 분석하여 다른 모델과 함께 보완하려 한다. 또한 여러 종류의 data augmentation을 구분할 수 있는 모델을 만들어 다중 출력이 가능하게끔 구현하려 한다.