Mixup을 이용한 분포 외 데이터 감지 성능 향상

김동희, 정기석
한양대학교

queez0405@hanyang.ac.kr, kchung@hanyang.ac.kr

Improving Detection Performance of Out-of-Distribution Data with Mixup.

Dong-Hee Kim, Ki-Seok Chung
Hanyang Univ.

요 약

데이터 증강 기법은 주어진 데이터에 약간의 조작을 가한 새로운 데이터를 생성하여 모델의 성능을 향상시키는 기법이다. 데이터 증강 기법 중 Mixup 기법은 자연어 처리, 컴퓨터 비전 등 다양한 딥러닝 분야에서 성능 향상을 이루어 냈다. 본 논문은 데이터 Mixup 기법을 통해 분포 외 데이터 감지 성능을 향상하는 방법을 제시한다. 분포 외 데이터 감지기의 학습에서 Mixup 기법을 사용했을 때 교차 엔트로피 대비 296%, 그리고 Confidence loss 항만을 추가한 감지기 대비 10.6%의 성능 향상을 이루어 냈다.

Ⅰ. 서 론

깊은 신경망 (Deep Neural Network, DNNs)을 사용한 모델은 음성인식, 물체 감지, 이미지 분류 등의 분류 문제의 주요 지표로 사용되는 정확도 방면에서 뛰어난 성능을 가지고 있다. 그러나 분포 외 데이터(Out-of-distribution data)가 사전 학습된 신경망의 입력으로 들어올 경우 과한 자신감 (Overconfidence)을 가지고 분포 내 데이터 (In-distribution data)의 클래스 중 하나로 분류하는 일이 빈번하게 발생한다. 이러한 분포 외 데이터를 감지하기 위해 분포 외 데이터 또한 신경망을 학습시키는데 사용하여 분포 외 데이터 감지 성능을 증대시킬 수 있다 [1].

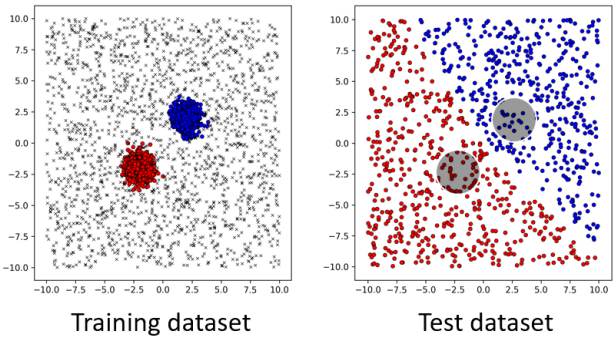
데이터 증강 기법은 수집된 데이터가 한정적일 때 신경망의 성능을 높일 때 사용된다. 데이터 증강 기법 중 하나인 Mixup 기법 [4]은 간단하지만, 다양한 깊은 신경망을 사용한 문제에서 효과적인 성능 향상을 보인다. 본 논문에서는 학습에 사용할 분포 내 데이터와 분포 외 데이터를 Mixup 기법을 사용하여, 학습할 전체 데이터의 수를 늘리는 방법으로 분포 외 데이터 감지 성능을 향상시켰다.

Ⅱ. 본론

2.1 분포 외 데이터 감지

분포 외 데이터 감지 (Out-of-distribution data detection)는 신경망에서 학습한 분포 내 데이터 외 다른 임의의 분포 외 데이터가 신경망의 입력으로 들어온 경우 이를 분포 외 데이터로 감지하는 작업을 의미한다.

그 중 일반적으로 사용되는 방법은 임계값 기반 감지기 (Threshold-based detector)를 사용하는 것이다 [2]. 임계값 기반 감지기는 신경망을 사용한 분류기에 입력을 넣었을 때, 각각의 클래스에 분류될 확률이 출력으로 나오게 되는데, 이 때 출력으로 나온 확률 중 가장 큰 확률이 특정 임계값 δ 보다 작으면 분포 외 데이터라고 추정하는 감지를 한다.



(그림 1) 신경망의 과한 자신감

그러나 분포 내 데이터만으로 학습된 신경망을 임계값 기반 감지기로 사용한다면 그 성능이 매우 좋지 않다. (그림 1)을 보면, 일반적인 네트워크의 분포 외 데이터 감지 성능이 좋지 않음을 볼 수 있다. (그림 1)의 왼쪽 그림은 빨간색을 클래스 0 으로 파란색을 클래스 1 로 하는 학습 데이터를 의미한다. 해당 학습 데이터를 얕은 다층 퍼셉트론 신경망 (Multi-perceptron network)에서 학습시킨 결과가 (그림 1)의 오른쪽이다.

분포 내 데이터만으로 학습된 신경망에 임계값 기반 감지 방법을 사용했을 때 올바른 결과가 나온다면 오른쪽 그림의 반투명한 원 부분 내부 입력값만이 클래스 0 또는 클래스 1 로 분류되고 나머지 부분은 분포 외 데이터로 분류되어야 한다. 그러나 분포 외 데이터를 올바르게 감지하지 못하고 있기 때문에

신경망은 과한 자신감을 가지고 분포 외 데이터를 분포 내 데이터로 분류한다.

분포 외 데이터를 신경망이 잘 감지할 수 있도록 하기위해는 분포 내 데이터뿐 아니라, 분포 외 데이터 또한 학습시에 사용하는 것이 바람직하다. 이때 사용하는 목표함수는 다음과 같다 [1].

$$\min_{\theta} \mathbb{E}_{P_{in(\hat{x},\hat{y})}}[-logP_\theta(y=\hat{y}|\hat{x})] + \beta\mathbb{E}_{P_{out}(x)}[KL(\mathcal{U}(y)||P_\theta(y|x))]$$

(식 1) Confidence loss 를 포함한 목표함수

(식 1)의 첫 번째 항은 일반적인 분포 내 데이터를 학습하는 교차 엔트로피 (Cross entropy)항으로 $(\hat{x}, \hat{y})$는 분포 내 데이터의 입력과 정답 레이블의 쌍을 의미한다. 두 번째 항은 Confidence loss 항이다. Confidence loss 항은 쿨백 라이블러 발산을 사용하여 분포 외 데이터의 입력 데이터를 x 라고 할 때 이 입력을 균일분포로 예측하게 하여 분포 외 데이터에 대해 과한 자신감을 갖지 않도록 유도한다. 본 논문에서는 이 방법의 정확도를 한층 더 높이기 위해서 Mixup 기법을 이용하여 데이터를 증강시킴으로써 분포 외 데이터 감지기의 정확도가 더 높아짐을 보인다.

2.2 Mixup 기법

딥러닝 학습에서는 신경망을 학습시키기 위한 데이터의 수가 중요하나 많은 수의 데이터를 확보하기에는 여러 어려움이 따른다. 따라서 제한된 데이터를 가지고 있으며 새로운 데이터를 확보하기 힘들 때 신경망의 정확성을 높이기 위해 데이터 증강 (Data augmentation) 기법을 사용한다 [3].

데이터 증강 기법 중 Mixup 기법은 두 개의 데이터를 선형적으로 결합하는 방법으로 (식 2)와 같이 표현된다.

$$\hat{\mathbf{x}} = \lambda x_i + (1-\lambda)x_j$$
$$\hat{\mathbf{y}} = \lambda y_i + (1-\lambda)y_j$$

(식 2) Mixup 생성 식

Mixup 기법은 이미지 분류뿐 아니라 문장 분류 [5], 오디오 분류 [6] Generative Adversarial Networks (GAN)를 사용한 이미지 생성 [7] 등 여러 종류의 DNN 에 효과적으로 작동하는 것으로 입증된 기법이다. 본 논문에서는 좌표평면에 임의로 분포를 생성하여 분포 내 데이터는 분포 내 데이터끼리 분포 외 데이터는 분포 외 데이터끼리 Mixup 기법을 적용하여 증강된 데이터를 통한 학습을 통해 탐지기의 성능 향상을 확인하였다.

2.3 실험 결과

본 논문에서는 Pytorch 프레임워크를 이용하여 얕은 다층 퍼셉트론 신경망을 구현하여 사용하였다. 실험은 2 차원 좌표평면 내에서 (-2, -2)를 중심으로 반경 2 이내, (2, 2)를 중심으로 반경 2 이내에서 무작위로 추출된 클래스 0 과 클래스 1 을 각각 1000 개 임의로 생성하여 분포 내 데이터로 사용했다. [-10, 10] 범위 내 분포 내에 속하지 않는 임의의 2000 개의 분포 외 데이터를 생성하여 신경망 학습을 진행하였다. 또한 [-10, 10] 범위 내 임의의 데이터 2000 개를 생성하여 임계값을 0.8 로 평가를 시행했다.

분포 외 데이터를 감지하는 성능을 비교하기 위해서는 평가 지표로 정확도가 아닌 정밀도 (Precision)와 재현율 (Recall)을 조화평균한 지표인 F1 score 를 사용한다.

(표 1)은 실험 결과를 요약해서 보여준다. (식 1)에서 첫 번째 항에 해당하는 교차 엔트로피 항만을 목표함수로 사용한 신경망은 가장 성능이 좋지 않아 F1 score 값이 0.134 와 같이 나타난다. 같은 데이터에 (식 1)의 두 번째 항에 해당하는 Confidence loss 항을 추가하여 학습한 신경망은 F1 score 가 0.48 로 이는 교차 엔트로피 목표함수를 사용한 신경망보다 258% 높은 성능을 나타낸다. 마지막으로 본 논문에서 제시한, Confidence loss 항을 가진 신경망에 Mixup 기법을 적용한 이미지를 추가로 학습시킨 결과 F1 score 가 0.531 로 계산되었다. 이는 교차 엔트로피 신경망보다는 296%, Confidence loss 만을 사용한 신경망보다는 10.6% 성능이 좋아짐을 알 수 있다.

	Cross Entropy	Confidence Loss	Ours
F1 score	0.134	0.480	0.531

(표 1) 제안하는 방법과 기존 신경망의 F1 score 비교 결과

Ⅲ. 결론

본 논문에서 사용한 방법은 한정적인 데이터에서 새롭게 데이터를 수집할 수 없는 경우 Mixup 기법을 사용하여 데이터 증강을 통해서 분포 외 탐지 성능을 향상하는 방법에 대해 다루었다. 좌표 위 임의의 데이터셋에서 분포 내 데이터와 분포 외 데이터 모두 데이터 증강 기법을 사용했을 때, 성능이 일반적인 신경망보다는 F1 score 가 296% 향상되었고, Confidence loss 를 적용한 신경망보다는 10.6% 나아짐을 보였다.

ACKNOWLEDGMENT

이 논문은 산업통상자원부 '산업전문인력역량강화사업'의 재원으로 한국산업기술진흥원(KIAT)의 지원을 받아 수행된 연구임. (2020 년 지능형반도체 전문인력 양성사업, 과제번호: N0001883)

참 고 문 헌

[1] Kimin Lee, et al., "Training Confidence-Calibrated Classifiers for Detecting Out-of-Distribution Samples" ICLR, 2018.

[2] Shiyu Liang, et al., "Enhancing the Reliability of Out-of-Distribution Image Detection in Neural Network," ICLR, 2018.

[3] Tong He, et al., "Bag of Tricks for Image Classification with Convolutional Neral Network" ICLR, 2018.

[4] Hongyi Zhang, et al., "mixup: Beyond Empirical Risk Minimization" ICLR, 2018.

[5] Hongyu Guo, et al., "Augmentation Data with Mixup for Sentence Classification: An Empirical Study" arXiv, 2019.

[6] Zhichao Zhang, et al., "Deep Convolutional Neural Network with Mixup for Environmental Sound Classification" arXiv, 2018.

[7] Thomas Lucas, et al., "Mixed Batches and Symmetric Discriminators for GAN Training" arXiv, 2018.