인공지능 이미지 인식 기술 동향

1.머리말

이미지 인식은 컴퓨터 비전(Computer Vision) 기술 중 하나

이미지 인식 대표적 세 가지 태스크(Task)

1. 이미지 내 특정 사물을 분류(Classification)하는 태스크

2. 여러 사물을 동시에 검출(Detection)하는 태스크

3. 사물들을 픽셀 단위로 식별하여 분할(Segmentation)하는 태스크

2012년 대규모 이미지 인식 경진대회 ILSVRC(ImageNet Large Scale Visual Recognition Challenge)에서 토론토 대학 연구진이 딥러닝(Deep learning)이라 불리는 새로운 기법을 활용해 기존의 방법론에 대비해 압도적인 성능으로 우승.

사람 수중을 초월한 인공지능 이미지 인식 기술은 자율주행 의료, 제조 등의 산업에 활용되는 단계로 진입하고 있다.

2.딥러닝 기반 이미지 인식 기술 동향

* 1. 안전하고 신뢰성 있는 이미지 인식

2018년 우버와 테슬라 차량이 자율주행 중 사망사고를 냈다.

이유 : 보행자 인식과 차선 인식의 오류

인공지능의 활용도가 높아질수록 기술에 대한 안전성과 신뢰성을 확보하는 것은 선택이 아닌 필수.

딥러닝은 적대적 예제(Adversarial examples)라 불리는 이미지를 엉뚱하게 판단하는데, 악의적 노이즈(Adversarial noise)를 이미지에 주입해서 적대적 예제를 만들 수 있다.

적대적 예제는 사람이 판단하기에는 문제가 없으나 인공신경망의 판정을 교란시킬 수 있다.

악용사례 : 교통표지판, 사람을 인식 못하게 만드는 사례

악의적 이미지 인식 교란에 대해서 올바른 판정을 할 수 있도록 예제 자체를 학습하는 적대적 학습(Adversarial training) 방법이나 노이즈를 제거·완화하는 노이즈 갑쇄기(Denoiser)방식 등이 연구되고있다.

인공의 노이지에 대응하는 기술에도 이미지 인식의 강건함(Robustness)자체를 개선하기 위한 연구가 활발

블러링(Blurring), 포깅(Fogging) 등 현실에서 흔하게 발생할 수 있는 노이즈가 적용된 이미지 벤치마킹 데이터 세트 ImageNet-C, ImageNet-P 등 이 공개되었다.

이를 통해서 각종 노이즈에 대해 안전성과 신뢰성을 갖춘 강건한 이미지 인식 기술이 발전할 것으로 기대됨

학습 외 분포 데이터 탐지(Out-of-Distribution Detection) : 학습하지 못한 패턴에 대한 처리, 기계학습이 가진 한계를 극복하기 위해서는 인공지능에 입력된 이미지가 학습된 확률 분포(Probability distribution)의 데이터인지, 아닌지를 식별하는 것이 중요, 이것을 학습 외 분포 데이터 탐지라 함.

학습 외 분포 데이터 탐지를 통해 인공신경망이 판단하기 어려운 이미지를 걸러 내거나 예외 처리하여 안전성과 신뢰성을 높일 수 있다.

딥러닝이 판정에 대해 얼마나 확신하는지를 나타내는 확률 값을 보정하것나, 학습 외 분포 데이터를 생성적 대립 신경망(GAN, Generative Adversarial Network)으로 생성하고 학습하여 탐지 정확도를 높이는 방법

신뢰성 확보에 있어 또 다른 접근 설명 가능 인공지능(XAL, eXpalainable AI)

XAI : 인공지능의 동작 또는 판단을 사람이 이해할 수 있는 형태로 설명하는 기술

예) 판단 결과만을 제공하는 것이 아니라, 고양이라고 판단한 근거(수염, 뾰족한 귀 등)까지 제공

왜 그렇게 작동하는지를 이해할 수 있다면, 판단결과에 대하여 신뢰여부를 결정할 수 있다. 의료 영상 분석 같이 법적 책임 또는 구정준수라 엄밀히 요구되는 분야에 인공지능을 도입할 수 있는 안전장치가 될 수 있다.

인공지능 판단에 크게 기여하는 특징(Feature) 정보를 알려주는 CAM(Class Activation Map)과 같은 기술들은 이미 활용 중

정확도 측면에서 인공지능 이미지 인식 기술이 사람 이상의 수준으로 진화되었으나 현실 세계에 적용하기 에는 안전성 및 신뢰성에 대한 추가적 보완이 요구되고 있는 실정

앞서 설명한 바와 같이 인공지능 이미지 인식기술은 품질 수준을 개선하는 방향으로 이제 막 발돋움을 하고 있는 단계

2-2. 인공지능 학습의 한계 극복

딥러닝은 학습과정에서 대규모의 데이터와 컴퓨팅 파워를 요구한다. 또한 인적 자원도 제한적이다.

세 가지 동향

첫 번째 학습 데이터 절감.

이미지 인식은 대부분 지도학습(Supervised learning)을 실시하는 만큼 출력 값이 있는 데이터가 필요. 즉, 출력값에 해당하는 라벨(Label) 또는 어노테이션(Annotation)을 준비해야 함

이미지에 대한 어노테이션은 이미지 내에 각종 사물을 구분하는 경계선을 그리거나 해당 사물에 무엇인지 기록해야 함

이미지 어노테이션은 규모와 난이도 등에 따라 많은 비용이 소요

어노테이션 비용 문제를 극복하는 최근 동향 중 하나는 자기 지도 학습(Self-supervised learning)을 활용하여 학습에 필요한 어노테이션을 줄이는 것

자기지도학습은 어노테이션 없이 데이터를 학습하는 방법에서 비지도학습(Unsupervised learning)과 유사하지만 데이터를 표현(Representation)하는 방법을 학습하는 것에 중점을 두고있다. 스스로 필요한 특징을 찾아 적절하게 표현(Feature representation)하는 방법을 학습

자기 지도 학습 후에는 미세 조정(Fine tuning) 또는 다운 스트림 태스크(Downstream task)에 해당하는 소수의 어노테이션 데이터로 지도 학습 과정을 거쳐 최종적으로 목적한 이미지 인식을 완성하게됨

자기 지도 학습 방식의 장점

고비용에 해당하는 어노테이션 데이터 절약

전이학습 등에 활용되는 사전학습 모델을 확보할 수 있다.

어노테이션 데이터 사용을 효율화하는 또 다른 방법 => 액티브러닝(Active learnign)

엑티브러닝 핵심 :

어떤 데이터를 먼저 어노테이션해서 학습에 사용할 것인가

학습에 크게 기여할 수 있는 데이터를 먼저 선별하여 어노테이션

학습한 후 점진적으로 목표한 정확도를 달성할 때까지 어노테이션 데이터를 늘려가며 학습

액티브러닝 활용 40%가량 어노테이션 데이터를 절감, 최고 정확도를 3.4% 높인 연구 사례가 있음

생성적 대립 신경망(GAN)을 활용하여 가상의 데이터를 생성, 어노테이션 데이터를 만들어내느느 시도

두 번째 이농지능 전문가를 대신할 학습 자동화

자동화된 기계학습(AutoML, Automated Machine Learning) 기술 : 학습 데이터 전처리 -> 딥러닝의 심층 신경망 구조 탐색(NAS, Neural Architecture Search) -> 학습 최적화를 위한 하이퍼파라미터(Hyper-parameter) 조정 -> 최종 모델 선택(Model selection)

딥러닝 학습 과정의 각 단계를 자동화 할 수 있다.

AutoML은 전문가 부족에 대한 극복 방안이자 인공지능 민주화(AI Democratization)을 위한 기술이라고도 할 수 있다.

세 번째 데이터와 컴퓨팅 파워 절감을 위한 전이 학습(Transfer learning) 고도화

전이학습 : 원천 도메인(Source domain)으로부터 목표 도메인(Target domain)을 학습시키는 방법의 총칭, 딥러닝 이미지 인식에서는 원천 도메인 에서 학습된 심층 신경망 모델을 목표 도메인 데이터로 추가 학습하는 방식으로 구현된다.

전이 학습이 더울 주목받는 이유

자기지도 학습, AutoML 기술 등이 고도화 되고 이를 적용한 사전 학습 모델(Pre-trained model)자체의 성능도 고도화 되면서 전이학습을 다양한 태스크에 적용할 수 있기 때문

전이 학습의 성능을 더 높이기 위한 조건 등이 연구 되면서 의료영상, 제조 비전 검사 등의 전문 도메인 영역에 특화된 사전 학습 모델들이 개발되고 있다.

* 1. 온 디바이스(On-Device) 인공지능 이미지 인식

모바일 디바이스, 경량 디바이스 등에서 인공지능 이미지 인식 기술 적용 사례가 등장하고 있다.

경량(Lightweight) 딥러닝 연구와 하드웨어 가속화 기술 연구가 진행되고있다.

경량 딥러닝 기술 : 정확도를 유지, 모델의 크기를 줄이거나 연산을 간소화 하여 작은 디바이스 등에 탑재할 수준으로 경량화 하는 것이다.

콘볼루션 신경망(CNN, Convolutional Neural Network)의 경우 필터를 변형하여 연산 차원을 축소(Reduction)하거나 큰 영향이 없는 신경망의 가중치(Weight)를 삭제하는 가지치기(Pruning), 가중치 값의 부동 소수점을 줄여 연산을 간소화하는 양자화(Quantization)등의 기법이 있다.

지식증류(Knowledge Distillation)활용도가 높아지고 있는데, 미리 잘 학습시킨 큰 신경망의 출력을 작은 신경망이 모방 학습하여 상대적으로 경량화 되면서도 정확도를 유지하는 기술