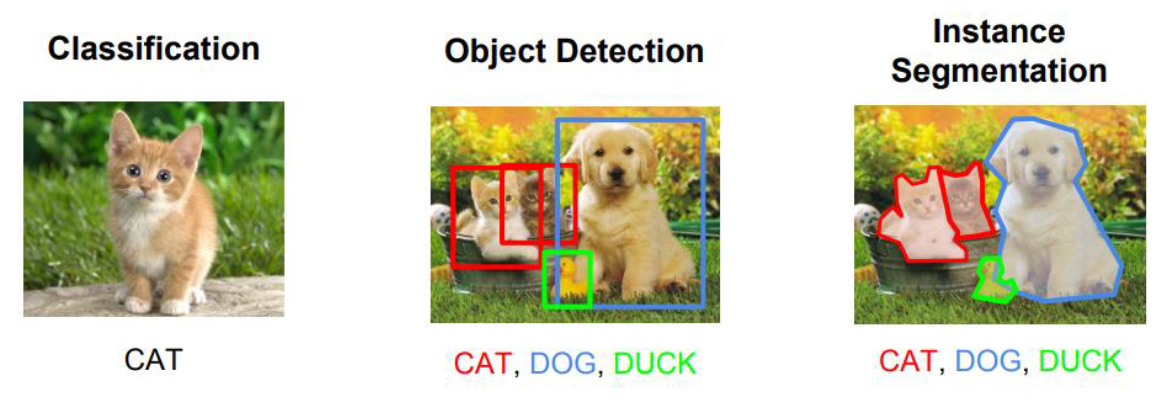
인공지능 이미지 인식 기술 동향

인공지능 이미지 인식이란 기계가 마치 사람처럼 사진이나 동영상으로부터 사물을 인식하거나 장면을 이해하는 것으로 정의할 수 있다.

이미지 인식의 세 가지 태스크(Task)

1. 이미지 내 특정 사물을 분류(Classification)하는 태스크
2. 여러 사물을 동시에 검출(Detection)하는 태스크
3. 사물을 픽셀 단위로 식별하여 분할(Segmentation)하는 태스크

출처: https://hoya012.github.io/

이미지 인식 기술들은 2012년 대규모 이미지 인식 경진대회인 ILSVRC(ImageNet Large Scale Visual Recognition Challenge)에서 토론토 대학 연구진이 딥러닝(Deep learning)이라 불리는 새로운 기법을 활용해 사람의 인식률을 발전시키는 계기가 되었다.

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

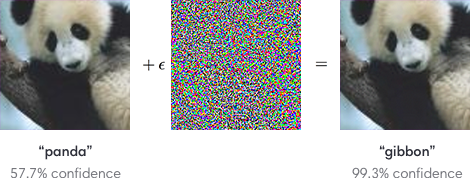
딥러닝 기반 이미지 인식 기술 동향에는 3 가지

* 안전하고 신뢰성 있는 이미지 인식
* 인공지능 학습의 한계 극복
* 온 디바이스(On-Device) 인공지는 이미지 인식

1. 안전하고 신뢰성 있는 이미지 인식

첫 번째로 안전하고 신뢰성 있는 이미지 인식은 자율주행, 의료동영상 등에서 찾아볼 수 있다. 인공지능 활용도가 높아질수록 기술에 대한 안전성과 신뢰성을 확보하는 것은 선택이 아닌 필수가 된다.

적대적 예제(Adversarial examples)

* 악의적 노이즈(Adversarial noise)를 이미지에 주입해서 이미지를 엉뚱하게 판단하게 만드는 것.
* 사람이 판단하기에는 문제가 없으나 인공신경망의 판정을 교란시킬 수 있다.
* 악용사례로는 교통표지판이나 사람 등을 인식 못하게 만드는 것.

출처: https://openai.com/

예방하기 위한 노력

* 악의적 인식 교란에 대해서 올바른 판정을 할 수 있도록 예제 자체를 학습하는 적대적 학습(Adversarial training).
* 노이즈를 제거, 완화하는 노이즈 감쇄기(Denoiser)방식 등이 연구되고 있다.
* 블로링(Blurring), 포깅(Fogging) 등 현실에서 흔하게 발생할 수 있는 노이즈가 적용된 이미지 벤치마킹 데이터 세트 ImageNet-C, ImageNet-P 등이 공개됨..

이미지 인식 기술의 근본적 불안감

* 학습하지 못한 패턴에 대한 처리: 학습 외 분포 데이터 탐지(Out-of-Distribution Detection).
* 신뢰성 확보: 설명 가능 인공지능(XAI, eXplainable AI).

학습 외 분포 데이터 탐지(Out-of-Distribution Detection)

* 입력된 이미지가 학습된 확률 분포(Probability distribution)의 데이터인지, 아닌지를 식별하는 것이 중요.
* 인공신경망이 판단하기 어려운 이미지를 걸러 내거나 예외 처리하여 안전성과 신뢰성을 높일 수 있다.
* 딥러닝이 판정에 대해 얼마나 확신(Confidence)하는지를 나타내는 확률 값을 보정(Calibration).
* 생성적 대립 신경망(GAN, Generative Adversarial Network)으로 생성하고 학습하여 탐지 정확도를 높이는 방법.

설명 가능 인공지능(XAI, eXpalinable AI)

* 인공지능의 동작 또는 판단을 사람이 이해할 수 있는 형태로 설명하는 기술.
* 판단 근거까지 제공하는 것.
* 의료영상 분석 같이 법적 책임 또는 규정 준수가 엄밀히 요구되는 분야에 안전장치가 될 수 있다.
* 인공지능 판단에 크게 기여하는 특징(Feature) 정보를 알려주는 CAM(Class Activation Map)과 같은 기술들은 이미 활용 중.

인공지능 이미지 인식 기술이 현실 세계에 적용하기에는 안전성 및 신뢰성에 대한 추가적 보완이 요구되고 있는 실정이다. 앞서 설명한 바와 같이 인공지능 이미지 인식기술을 품질 수준을 개선하는 방향으로 이제 막 발돋움을 하고 있는 단계이다.

2. 인공지능 학습의 한계 극복

두 번째로는 인공지능 학습의 한계극복이다. 딥러닝은 학습과정에서 대규모의 데이터와 컴퓨팅 파워를 요구한다. 또한 인적 자원도 제한적이다.

이러한 한계를 극복하기 위한 세 가지 동향

1. 학습데이터 절감
2. 인공지능 전문가를 대신할 학습 자동화
3. 데이터와 컴퓨팅 파워 절감을 위한 전이학습(Transfer learning) 고도화

2-1 학습데이터 절감

첫 번째로 학습 데이터 절감을 보면 이미지 인식은 대부분 지도학습(Supervised learning)을 실시한다. 그만큼 출력 값이 있는 데이터가 필요하다.

* 출력값에 해당하는 라벨(Label) 또는 어노테이션(Annotation)을 준비.
* 이미지에 대한 어노테이션은 이미지 내에 각종 사물을 구분하는 경계선을 그리거나 해당 사물이 무엇인지 기록해야 함.
* 규모와 난이도 등에 따라 많은 비용이 소요.
* 비용문제를 극복하는 최근 동향: 자기 지도 학습(Self-supervised learning).
* 어노테이션 데이터 사용을 효율화 하는 또 다른 방법: 액티브러닝(Active learning)

출처: https://mc.ai/

자기 지도 학습

* 학습에 필요한 어노테이션을 줄이는 것
* 비지도 학습(Unsupervised learning)과 유사하지만 데이터를 표현(Representation)하는 방법을 학습하는것에 중점을 두고 있다.
* 후에는 미세조정(Fine tuning) 또는 다운 스트림 태스크(Downstream task)에 해당하는 소수의 어노테이션 데이터로 지도 학습 과정을 거쳐 이미지 인식을 완성.
* 장점: 고비용에 해당하는 어노테이션 데이터 절약, 전이학습(Transfer learning) 등에 활용되는 사전적 학습(Pre-trained) 모델 확보.

액티브러닝(Active learning)

* 핵심은 어떤 데이터를 먼저 어노테이션해서 학습에 사용할 것인가이다.
* 학습에 크게 기여할 수 있는 데이터를 먼저 선별하여 어노테이션한다.
* 학습한 후 점진적으로 목표한 정확도를 달성할 때까지 어노테이션 데이터를 늘려가며 학습하는 방식이다.
* 액티브러닝을 활용하면 40%가량 어노테이션 데이터를 절감.
* 최고 정확도를 3.4% 높인 연구사례도 있다.
* 이 외에도 생성적 대립 신경망(GAN)을 활용하여 가상의 데이터를 생성하여 어노테이션 데이터를 만들어 내는 시도가 있다.

2-2 인공지능 전문가를 대신할 학습 자동화

자동화된 기계학습(AutoML, Automated Machine Learning) 기술은 학습데이터 전처리 -> 딥러닝의 심층 신경망 구조 탐색(NAS, Neural Architecture Search) -> 학습 최적화를 위한 하이퍼파라미터(Hyper-parameter) 조정 -> 최종 모델 선택(Model selection) 등과 같은 이러한 딥러닝 학습 과정의 각 단계를 자동화 할 수 있다. 자동화된 기계학습은 전문가 부족에 대한 극복 방안이 인공지능 민주화(AI Democratization)를 위한 기술이라고도 할 수 있다.

2-3 데이터 컴퓨팅 파워 절감을 위한 전이학습(Transfer learning) 고도화

전이 학습은 원천 도메인(Source domain)으로부터 목표 도메인(Target domain)을 학습시키는 방법의 총칭이며, 딥러닝 이미지 인식에서는 원천 도메인에서 학습된 심층 신경망 모델을 목표 도메인 데이터로 추가 학습하는 방식으로 구현된다.

전이 학습

* 손쉽게 학습 데이터와 컴퓨팅 파워 또는 학습 시간을 줄일 수 있는 방법.
* 딥러닝 기반 이미지 인식에 있어 기본처럼 활용되고 있다.

전이 학습이 더욱 주목받는 이유

* 자기 지도학습, 자동화된 기계학습 기술 등이 고도화됨
* 이를 적용한 사전학습 모델 자체의 성능도 고도화됨.
* 전이학습을 다양한 태스크에 적용할 수 있기 때문.
* 의료영상, 제조 비전 검사 등의 전문 도메인 영역에 특화된 사전 학습 모델들이 개발되고 있다.

3. 온 디바이스 인공지능 이미지 인식

세 번째는 온 디바이스 인공지능 이미지 인식이다. 모바일 디바이스, 경량 디바이스 등에서 인공지능 이미지 인식 기술 적용 사례가 등장하고 있다. 경량 딥러닝 연구와 하드웨어 가속화 기술 연구가 진행되고있다.

경향 딥러닝 기술

* 정확도를 유지하고 모델의 크기를 줄이거나 연산을 간소화하는 것
* 작은 디바이스 등에 탑재할 수준으로 경량화 한다.

콘볼루션 신경망

* 필터를 변형하여 연산 차원을 축소
* 가지치기, 큰 영향이 없는 신경망의 가중치 삭제
* 가중치 값의 부동 소수점을 줄여 연산을 감소화하는 양자화

지식증류

* 미리 잘 학습시킨 신경망의 출력을 작은 신경망이 모방 학습하여 상대적으로 경량화 되면서 정확도 유지하는 기술

최근 인공지능 이미지 인식 기술 동향

* 인공지능 판정은 안전하고 신뢰성을 높이기 위해 악의적 공격, 자연 발생적 노이즈, 그리고 예외상황에 대해서도 강건하고 투명하게 처리
* 학습에 필요한 막대한 비용과 자원을 최소화
* 일상 모든 곳에 인공지능 적용이 가능하도록 가볍게 만든다.

이는 결국 현재의 딥러닝 기술 동향과 동일한데, 특히 이미지 인식에 있어 중요한 기술을 중심으로 살펴보았다. 각 산업 영역에 인공지능 기술을 적용하기 위한 현실적 문제를 해결하는 것 역시 주요 기술 동향이라고 할 수 있다.