정보통신

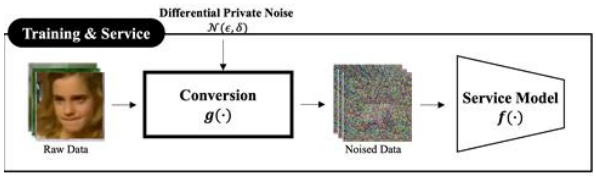
PNU Tech Offer x 부산대학교 정보컴퓨터공학부 최윤호 교수

차분 프라이버시 기반 이미지 데이터 비식별화 처리

차분 프라이버시(DP) 기반의 이미지 변형 기법을 활용하여 이미지 데이터를 노이즈가 추가된 메타데이터로 변환하여 딥러닝 모델에 학습하는 기술

적용분야 · 제품

기술개요



- 차분 프라이버시(Differential Privacy, DP) 기반의 이미지 변형 기법을 활용한 원본의 이미지 데이터 변형
- 원본 데이터의 원래의 형태 또는 내용을 알아볼 수 없을 정도의 노이즈 적용
- 이미지 데이터를 메타데이터로 변형하는 과정에서 이미지를 분석하기 위한 주요 픽셀 보존
- 프라이버시 보존 딥 러닝을 위한 차분 프라이버시 기반 이미지 데이터 비식별화 처리 방법 및 장치 기술

기술경쟁력

기존기술 ▶▶ **기술 차별성** ▶▶ **대상기술**

- 차분 프라이버시(DP)를 활용한 대표적인 기법으로는, DP-GAN 및 DP-CGAN, PixelDA 등이 있음

기술적 한계

- DP-GAN 및 DP-CGAN은, MNIST 데이터셋과 같은 아주 특수한 케이스의 데이터셋에서만 충분한 성능을 보여 실환경에 적용 어려움
- PixelDA는 원본의 데이터의 중요 정보를 그대로 가진 데이터를 생성하는 문제

- 차분 프라이버시(Differential Privacy, DP) 기반의 이미지 변형 기법을 활용
- 익스플레이너 모델에서 설명 가능 AI(eXplainable AI, XAI) 기법이 구현

기술적 우위

- 원본의 데이터의 중요 정보가 노출되지 않고 프라이버시 보존 딥러닝을 수행 가능
- 이미지 데이터를 메타데이터로 변형 시 인간 인식에 저해가 되지 않도록 주요 픽셀 보존 가능

지식재산권 현황

발명의 명칭	출원(등록)번호	출원(등록)일자
프라이버시 보존 딥러닝을 위한 차분 프라이버시 기반 이미지 데이터 비식별화 처리 방법 및 장치	출원: 10-2023-0140514	출원: 2023.10.19.

문의처

부산대학교 산학협력단 최정식 과장(공학박사) jschoi7516@pusan.ac.kr 051. 510. 3823