

딥러닝 이미지 처리 방법 및 시스템

차분 프라이버시를 통한 이미지 비식별화와 프라이버시 보존 딥러닝 기법

적용분야·제품



의료영상 데이터



자율주행 모빌리티

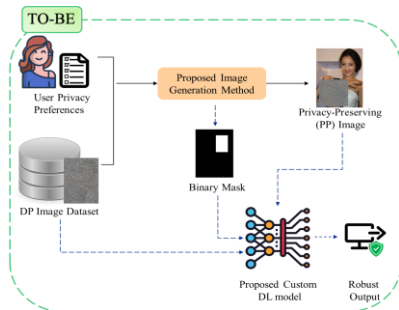


보안 카메라

기술개요



- PDDL(Privacy-Preserving Deep Learning) 분야에 많은 연구가 진행되고 있지만, 기존 딥러닝 학습시간에 걸리는 시간보다 더 많은 학습시간이 요구됨



- 사람의 식별력을 떨어뜨리면서 기계의 식별력은 그대로 보존할 수 있는 이미지 비식별화 처리를 통해 비 신뢰 구간인 클라우드 시스템을 활용한 외부 환경에서도 안전한 딥러닝 학습이 가능함

기술 경쟁력

기존기술

- 기존 기계학습 대비 대용량의 데이터 수집이 필요함
- 딥러닝 학습 모델에 사용되는 함수들의 변경 필요함

기술 차별성

- 상대적으로 적은 데이터에도 적용 가능함 (차분 프라이버시의 범용적 적용)
- 딥러닝 학습 모델에 사용되는 함수들의 변경 불필요

대상기술

기술적한계

- ▶ 소규모 데이터에서 활용 가능한 기법의 경우 데이터 복원의 가능성이 존재함
- ▶ 프라이버시 보호 강도와 데이터의 유용성 간 Tradeoff가 상당함
- ▶ 전체 이미지를 민감한 이미지로 간주함

기술적우위

- ▶ 소규모 데이터에서도 기존과 동일한 프라이버시 보호강도를 유지함
- ▶ 기존과 동일한 프라이버시 보호 강도에서 데이터의 유용성을 향상시킴(Tradeoff 완화)
- ▶ 소유자의 프라이버시 선호도에 따라 프라이버시 보존 이미지를 생성함

지식 재산권 현황

발명의 명칭	등록 번호	등록 일자
딥러닝을 위한 이미지 처리 방법 및 이미지 처리 시스템	10-2234097	2021.03.25.