

Adversarial Example 방어를 위한 이중 입력 변환 기법

적대적 사례에 강인한 심층 신경망 모델을 위한 입력 장치 및 방법

적용분야·제품



핀테크



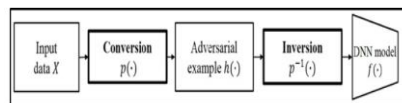
물류



마케팅/컨설팅

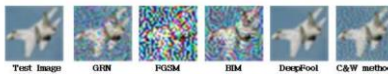
기술개요

이중 입력 변환 기반 방어 기법



- 현재 상용화 블록체인으로는 퍼블릭 블록체인, 프라이빗 블록체인, 컨소시엄 블록체인 등이 있으며, 퍼블릭 블록체인(Public blockchain)은 네트워크 참여를 허가하는 특징 관리자를 두지 않고 인터넷을 사용할 수 있는 누구나 참여 가능한 공개된 네트워크 기반 블록체인으로 공개형 블록체인이라고도 불림

Conversion 단계



Inversion 단계



- 제안기술은 공개형 블록체인을 중개하는 플랫폼에 적용될 수 있는 트랜잭션 처리 방법에 연관되며, 분산앱(DApp) 사용자의 프라이버시 보호를 위한 공개형 블록체인의 익명성 강화 기법에 관한 기술임

기술 경쟁력

기존기술

기술 차별성

대상기술

이미지 분류, 얼굴 인식 등 다양한 분야에서 인간의 능력을 뛰어넘는 성능을 보이는 딥러닝은 Adversarial Attack에 매우 취약함

기술적 한계

- ▶ 딥러닝 모델 재학습 과정에서 많은 자원을 필요로 하며, 정상 입력에 대한 성능 감소 발생
- ▶ 정상 입력에도 동일한 변환을 수행하기 때문에 정상 입력에 대한 성능 감소 발생

Adversarial Attack에 대한 높은 방어 성능을 제공함과 동시에 정상 입력에 대한 성능 감소 문제에 대한 해결을 달성

기술적 우위

- ▶ 딥러닝 모델의 구조 및 파라미터를 변경하지 않으므로, 기존 딥러닝 모델의 재학습 과정없이 그대로 사용가능
- ▶ Conversion 단계에서는 입력 데이터를 손상시킴으로써, Adversarial Attack으로 생성되는 노이즈의 크기를 감소시켜 Adversarial Attack의 위험성을 감소시킬 수 있음

지식 재산권 현황

발명의 명칭	등록 번호	등록 일자
적대적 사례에 강인한 심층신경망 모델을 위한 입력 장치 및 방법	10-2598909	2023.11.01