

오디오 딥페이크 음성 탐지 기술

송실대학교 전자정보공학부 ● 정수환 교수

기술개요

본 기술은 심층신경망 기반 딥페이크 오디오 탐지 방법 및 그 학습 방법에 관한 것임

기술성숙도(TRL)

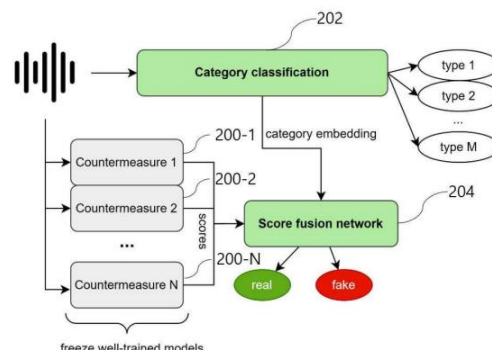
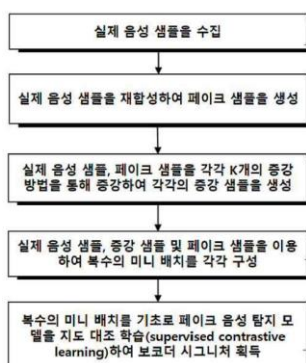
1	2	3	4	5	6	7	8	9
기초연구			실험	시작품			실용화	사업화

기술 개발 배경

- 음성 합성 및 감지 영역에서 과적합은 상당히 많은 문제가 되고 있는데, 최근 딥러닝 모델은 매개변수가 많으며, 과적합이 상대적으로 발생하기 쉬운 정교한 모델이 더 많이 사용되고 있음
- 딥페이크를 포함한 합성 음성 생성 기술이 빠르게 발전함에 따라 실제 음성 과 합성 음성을 구별하는 것은 매우 어려우며, 음성 데이터 특성상 다른 도메인에서 데이터를 수집하는 것 보다 어려운 한계가 있음

기술 차별성

- 입력된 오디오의 합성 형태 및 주변 잡음에 따라 복수의 탐지 모델 각각의 가중치를 동적으로 조정하기 때문에 딥페이크 오디오 탐지 성능을 한층 높일 수 있음
- 미니 배치에서 실제 샘플과 페이크 샘플 사이의 밸런스를 유지하고, 다양한 증강 방법을 사용하는 훈련 샘플을 신중하게 선택하여 대조 학습을 강화함으로써 딥페이크 음성 탐지 모델의 성능을 향상시킬 수 있음

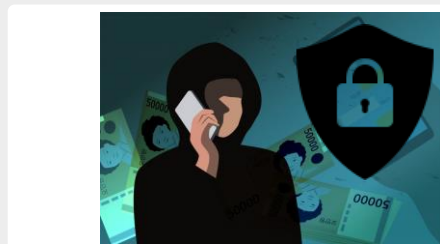


오디오 딥페이크 음성 탐지 기술

숭실대학교 전자정보공학부 ● 정수환 교수

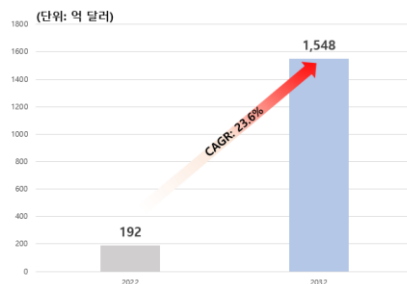
기술 활용 분야

- 인공지능(AI) 기반 보안 사업
 - 오프라인 위험 대응(음성 딥페이크 식별 및 차단, 피싱 방지)
 - 사이버 보안 위협 대응(신원 인증 강화, 프라이버시 보호)
- 엔터테인먼트
 - 콘텐츠 보호(배우, 인플루언서 목소리 무단 도용 방지)
 - AI 윤리 강화(AI 기반 콘텐츠의 기술적 제약)



시장동향/개발 현황

- 관련 시장 동향
 - Allied Market Research의 보고서에 따르면, 세계 사이버 보안 시장에서 AI는 2022년 192억 달러로 평가되었으며, 연평균 23.6%의 높은 성장률로 2032년에는 1,548억 달러에 이를 것으로 전망함
- 개발 동향
 - 과기정통부는 정보보호산업 시장규모 2025년 20조원 달성(2020년 기준 11.9 조원)을 목표로 성장을 위해 다양한 추진전략을 발표
 - 윤석열 정부는 2022년 6월 AI 반도체 강국으로의 도약을 위해 AI 반도체 산업을 성장 시키기 위한 전략을 발표함



[글로벌 사이버 보안 시장 전망(AI)]
(출처: Allied Market Research)

지식재산권 현황

No	특허명	출원번호	등록번호
1	딥페이크 음성 탐지 모델의 학습 방법 및 그 장치	KR 10-2024-0040395	-
2	심층신경망 기반 딥페이크 오디오 탐지 방법 및 장치	KR 10-2023-0176471	-