


딥페이크 방지 및 프라이버시 보호 기술

숭실대학교 소프트웨어학부 ● **최대선** 교수

기술개요

-  본 발명은 인공지능 모델의 적대적 공격 기술에 관한 것으로, 특히 딥페이크 생성을 방지하기 위한 기술에 관한 것임

기술성숙도(TRL)

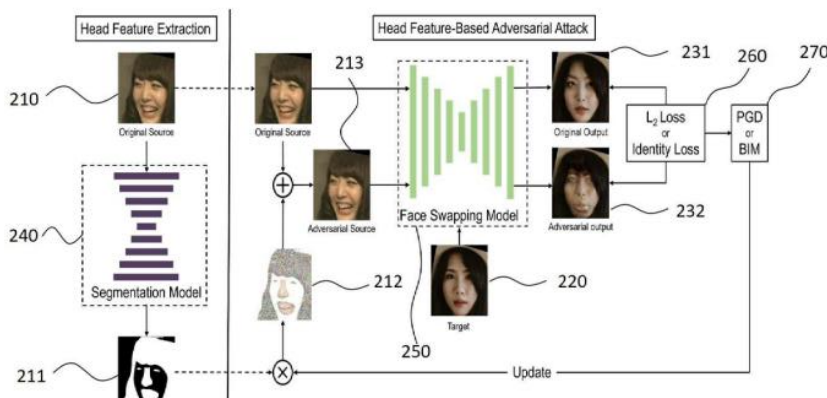
1	2	3	4	5	6	7	8	9
기초연구		실험		시작품		실용화		사업화

기술 개발 배경

- 딥페이크 기술이 불법적인 용도로 사용되면서 보안을 위협하거나 불법 합성 영상 등의 생성으로 사생활을 침해하는 등의 범죄로 빈번히 연결되는 문제가 빈번히 발생하고 있음
- 딥페이크로 생성된 이미지나 영상을 탐지하는 기술은 이미 발생한 범죄를 추적하는 데 효과적일 수 있으나 이미지나 영상이 이미 생성된 후이므로 딥페이크 범죄를 사전 예방하는 데는 한계가 있음

기술 차별성

- 딥페이크 방지 이미지를 생성함으로써 딥페이크 영상 또는 이미지를 생성할 수 없도록 하는 효과가 있음
- 딥페이크 방지 이미지는 원본과의 차이를 인식할 수 없도록 함으로써 딥페이크 방지 이미지를 원본과 동일하게 활용할 수 있는 장점이 있음



딥페이크 방지 및 프라이버시 보호 기술

숭실대학교 소프트웨어학부 ● **최대선** 교수

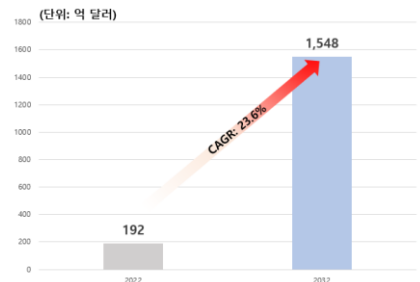
기술 활용 분야

- 인공지능(AI) 기반 보안 사업
 - 오프라인 위험 대응(영상 딥페이크 식별 및 차단, 피싱 방지)
 - 사이버 보안 위협 대응(신원 인증 강화, 프라이버시 보호)
- 엔터테인먼트
 - 콘텐츠 보호(배우, 인플루언서 사진 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	Head Feature 기반 노이즈 주입을 통한 딥페이크 생성 방지 적대적 공격 기술	KR 10-2024-0191361	-