# THE AI REPORT

생성형 AI 시대, 생체인식 기술의 기회와 도전

2024

NIA Future Strategy Team

「The AI Report」는 인공지능 기술 · 산업 · 정책의 글로벌 이슈와 동향, 시사점을 적시에 분석, 인공지능 현안에 빠르게 대응하고 관련 정책을 지원하기 위해 한국지능정보사회진흥원(NIA)에서 기획 · 발간하고 있습니다.



▶ 발행인 : 황 종 성

▶ 작 성
- 한국지능정보사회진흥원 인공지능정책본부 미래전략팀
  유주현 연구위원(rjh@nia.or.kr)

# 생성형 AI 시대, 생체인식 기술의 기회와 도전

NIA 미래전략팀 유주현 연구위원(rjh@nia.or.kr)

## 1. 생체인식 기술 개요

### 생체인식(Biometrics) 개요

○ 생체인식은 개인을 식별할 수 있는 고유한 신체적·행동적 특성을 활용하는 기술로, 이러한 특성을 전자적으로 캡처, 처리 및 측정하여 기존 기록과 비교함으로써 매우 정확한 신원 확인이 가능함

- 일반적인 물리적(Physiological) 생체인식 지표로는 지문, 얼굴, 홍채, 음성 및 DNA 등이 있으며, 행동(Behavioral) 생체인식 지표로는 개인의 걷는 방식, 제스처 및 타이핑 패턴 등이 포함됨

※ 출처 : International Biometrics+Identity Association(IBIA)

○ 생체인식에 사용될 수 있는 인간의 물리적, 행동적 특성은 다양하지만, 실제 특정한 환경에서 사용할 수 있는 생체인식 지표는 다음의 7가지 특성을 충족하여야 함

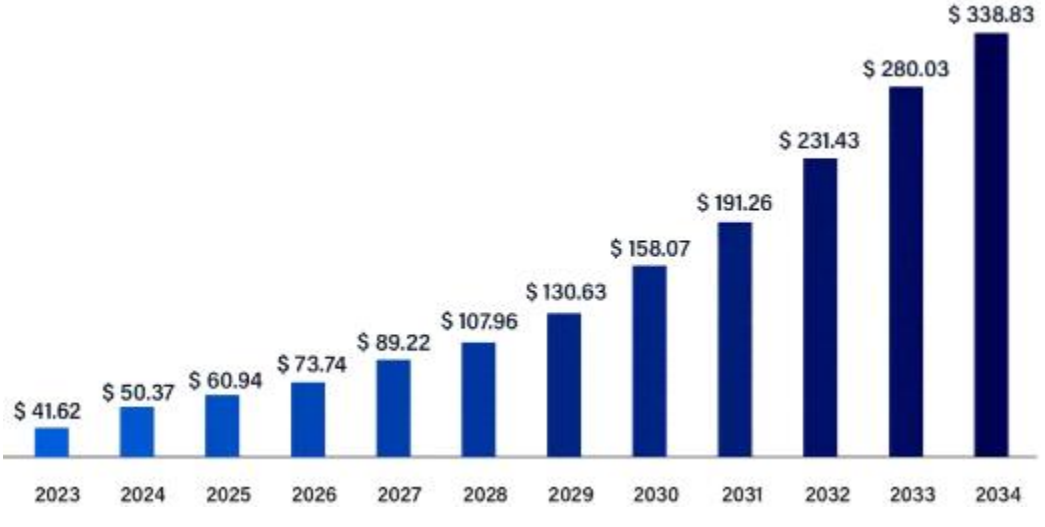
| 구 분 | 특 성 | 설 명 |
|---|---|---|
| 일반적 특성 | 보편성(Universality) | 모든 사람이 인증을 위해 동일한 생체정보를 보유하고 있어야 함 |
| | 고유성(Uniqueness) | 개인을 구별 가능하도록 생체정보가 사람마다 각각 달라야 함 |
| | 영구성(Permanence) | 생체정보가 시간에 따라 변하지 않아야 함 |
| | 측정가능성(Measurability) | 측정이 용이하고, 측정된 데이터로부터 관련 특징의 추출이 가능해야 함 |
| 신뢰성을 높이기 위한 추가적 특성 | 성능(Performance) | 시스템이 특성을 판별하고 처리하는 정확도, 처리속도 등 처리성능 |
| | 수용성(Acceptability) | 개인이 생체인식에 대한 거부감을 갖지 않고 수용하는 정도 |
| | 기만성(Circumvention) | 인공물이나 대체물을 사용하여 쉽게 모방 가능 여부 |

※ 출처 : 최근 생체인식 산업 동향과 시사점(KISTEP, 2021.04.28.) 자료를 기반으로 일부 수정

## 생체인식 시장 규모 및 주요 활용 분야

○ 글로벌 생체인식 시장은 2024년 503.7억 달러에서 2034년 3,388억 달러 규모로 성장이 예상되고 있으며, 이 기간 연평균성장률(CAGR)은 21%를 기록할 것으로 전망

[ 그림 1 ] 생체인식 시장 규모 예측 (단위 : USD Billion)




〈 출처 : https://www.precedenceresearch.com/biometric-technology-market 〉

○ 생체인식 기술은 공공 및 비즈니스 보안 분야에서 높은 수준의 안정성을 제공하며, 기존의 토큰이나 비밀번호와 비교할 때 위조 및 보안 침해를 크게 줄일 수 있어 시장의 지속적인 확장이 가능

[ 표 1 ] 생체인식 기술의 주요 활용 분야

| 분야 | 내 용 |
|---|---|
| 항공 등 국경관리 | · 공항, 철도역 등에서 생체인식을 활용한 출입국 심사 급증<br>· 유럽연합은 2025년까지 생체인식 기반 출입국 시스템 도입 예정 |
| 금융 | · 모바일 뱅킹과 전자 결제의 보안 요구가 증가하면서, 생체인식을 신원확인 및 결제인증에 활용<br>· 금융사기 방지를 위해서도 생체인식 활용 증가 |
| 모바일 기기 | · 스마트폰과 같은 모바일 기기에서 지문인식, 얼굴인식 등 생체인식을 개인정보보호와 데이터 보안을 위한 수단으로 활용 |
| 소매 및 전자상거래 | · 무인 매장이나 비접촉 결제 시스템에서의 신원확인 및 전자결제를 위해 활용<br>· 아마존의 Amazon One 서비스는 손바닥 인식으로 결제 자동화 |

## 생체인식 주요 활용 사례

### ① 얼굴인식

○ 자동출입국심사(Automated Border Control Systems, ABC)는 유인심사대가 아닌 여권, 지문인식 및 얼굴인식 만으로 본국 또는 상대국의 무인 심사대를 이용할 수 있는 출입국심사 제도로 'eGates'라고도 불림

- 우리나라의 경우 2008년 6월에 자동출입국심사 제도를 도입하였으며, 도입 초기에는 사전에 등록된 이용자만 이용 가능했지만, 2016년 7월 부터는 만17세 이상 주민등록증 소지자의 경우 누구나 이용할 수 있도록 변경

※ 만7세 이상~14세 미만의 경우 법정대리인 동반 사전등록 후, 만14세 이상~17세 미만의 경우 사전등록 후 이용 가능

- 또한 우리나라와 상호 자동출입국심사 협약을 맺은 국가(대만, 독일, 마카오, 미국, 홍콩)의 여권 소지자는 사전 등록을 통해 상호간에 자동출입국심사 이용이 가능

**[ 그림 2 ] 자동 출입국 이용 절차**


〈 출처 : 법무부 홈페이지 〉

○ 영국의 수도경찰청은 2020년 1월부터 런던 전역에 강력범죄 대응을 위한 라이브 안면인식 카메라를 배치하고, 범죄자 검거 가능성이 있는 특정 장소에서만 실시간 얼굴 감시를 진행

- 심각한 폭력 범죄, 총기 및 흉기 범죄, 아동 성 착취 혐의 등 용의자와 수배자가 대상

※ 해당 시스템은 경고 발생한 영상만을 최대 31일까지 보관할 수 있고, 일반인들의 얼굴인식 데이터는 자동으로 즉시 삭제

※ https://www.theguardian.com/uk-news/2020/feb/11/met-police-deploy-live-facial-recognition-technology

○ 러시아의 식료품 소매업체 X5 기업은 2023년 편의점과 슈퍼마켓의 셀프 서비스 결제 단말기에 얼굴인식으로 결제를 수행하는 smile-to-pay 서비스를 본격 도입

- 2023년 8월 기준 650개의 슈퍼마켓과 3,450개의 편의점에서 서비스 이용 가능

※ X5 and Sber launch world's largest smile-to-pay service(X5 Group, 2023.8.2.)

## ② 손바닥 인식

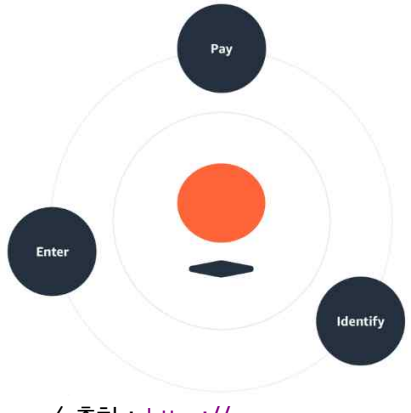
○ 아마존은 2020년 9월 손바닥 이미지를 등록하여 결제 서비스를 제공하는 Amazon One 서비스 출시

- 서비스 이용자는 신용카드·체크카드, 아마존 계정, 휴대전화 번호를 이용하여 서비스를 사전등록하고, 서비스 제공 매장에 방문하여 손바닥 이미지를 등록한 후 서비스 이용 가능

※ 2024년 부터 Amazon One 앱을 이용하여 손바닥 사진을 찍는 것으로 서비스 가입 가능

- 2023년 기준 미국 전역의 400개 이상의 매장에서 신분확인, 결제, 멤버십, 입장 등을 위해 활용

[ 그림 3 ] Amazon One 손바닥 인식 시스템


〈 출처 : https://one.amazon.com/ 〉

## ③ 홍채 인식

○ 애플은 2024년 애플 비전 프로 출시와 더불어 홍채 이미지를 통한 사용자 인증, 구매, 결제 등이 가능한 홍채 인식 서비스인 Optic ID 출시

- 고해상도 카메라와 보이지 않는 LED 광선을 통해 홍채의 고유한 패턴을 캡처하고 분석하며, 애플은 임의의 사람이 Optic ID를 사용하여 기기의 잠금을 해제할 확률은 백만분의 1미만이라고 발표

[ 그림 4 ] Apple의 생체인식 서비스


〈 출처 : Apple Hub X 〉

## ④ 목소리 인식 (화자 인식)

○ HSBC는 2016년 음성 기반 보안을 도입하면서 사용자의 신원확인을 위해 목소리 인식 기술 활용

- 서비스 이용자는 폰뱅킹 서비스와 전화통화를 통해 본인 인증 후 목소리를 등록하고, 이후 등록된 목소리를 활용 비밀번호 입력없이 음성으로 신원확인 후 전화 뱅킹 서비스 이용
- 고객의 목소리를 발음부터 음색, 음성 패턴까지 100가지 이상의 행동적, 신체적 음성적 특징 활용
- HSBC는 편리성, 보안성, 빠른인증 등이 목소리 인식 기반 폰뱅킹의 잠정이라고 말하고 있으며, 2020년 영국 HSBC는 전화뱅킹 사기가 전년도 대비 50% 감소했으며, 약 2억 4,900만 파운드의 고객 자금을 사기로부터 보호했다고 발표

※ HSBC UK's Voice ID prevents £249 million of attempted fraud(HSBC UK, 2021.5.4.)

○ 인도결제공사는 UPI(Unified Payment Interface)라는 스마트폰 기반 통합결제시스템을 2016년 도입하였으나, 피쳐폰을 사용하거나 데이터 연결이 불가능한 지역에 사는 사람들은 활용이 불가

- 2022년 피쳐폰 사용자를 위한 즉시결제서비스 UPI123 Pay를 도입하였으며, 더불어 VoiceSe라는 음성 기반 결제 시스템 출시
- VoiceSe를 통해 음성만 사용하여 기본 피쳐폰에서도 간단한 은행 거래 수행 가능

※ https://www.tonetag.com/resource/introducing-voicese-indias-foremost-voice-based-payment-system/

**[ 참고 ] 음성 인식 vs 목소리 인식 (화자 인식)**

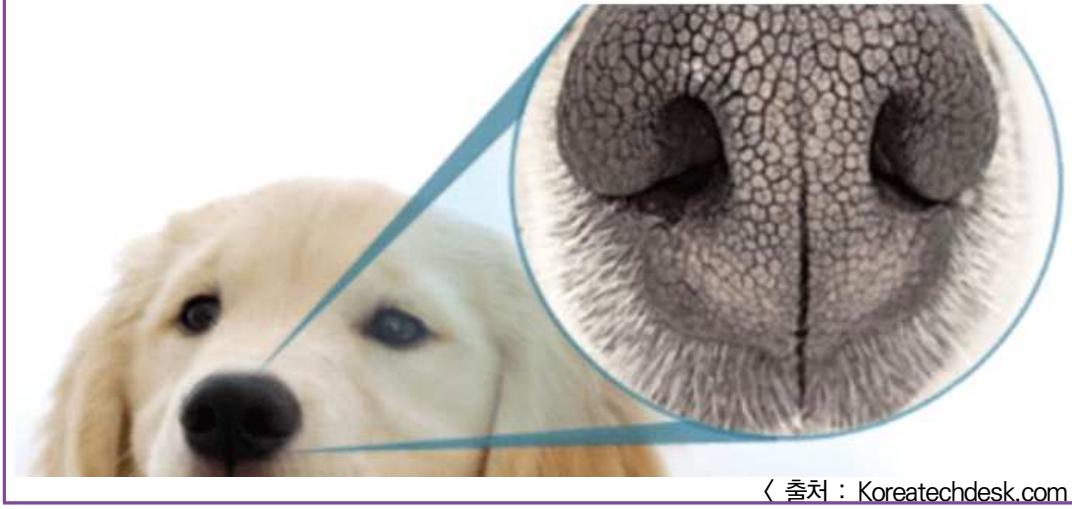
· 음성 인식(Speech Recognition)은 일반적으로 컴퓨터와 같은 기계가 인간의 음성 언어를 인식해 컴퓨터가 이해할 수 있는 문자로 변환하는 기술을 의미
  - 인공지능 기술의 발달로 음성 인식 기술의 정확성·편의성 등이 향상됨에 따라 음성 인식은 중요한 인간과 컴퓨터간의 인터페이스로 자리 잡음
  ※ 인공지능 스피커, 스마트 홈, 스마트 카, 음성 인식 챗봇 등

· 목소리 인식(Voice Recognition) 또는 화자 인식(Speaker Recognition)은 음성 인식과 구분하여 목소리를 통해 개인의 신원을 확인할 수 있는 생체인식 기술을 의미
  - 애플 siri의 경우 초기에는 음성 인식 기술을 활용하여 사용자의 요청에 반응하였으나, ios9부터 개별 음성 인식 기능(화자 인식)을 지원하고 있으며 지속적으로 성능 개선 추진

## ⑤ 기타 : 반려견 비문정보

○ 인간 중심으로 활용되던 생체인식 기술이 반려동물의 증가에 따라 반려동물의 신원확인을 위한 용도로도 활용이 증가
  - 반려동물을 위한 펫보험의 경우 보험 가입 반려동물과 병원 진료를 원하는 반려동물과의 동일성 판별의 곤란함으로 인하여, 고가의 펫보험료가 책정되고 이로 인해 가입이 저조한 실정
  - 사람에게 지문이 있듯이 반려견의 코무늬(비문)가 모두 다르다는 점을 활용하여 비문을 반려동물의 신원확인에 활용하고 있으며, 일부 보험사의 경우 반려동물 비문 등록시 보험료 할인 서비스 제공
  ※ AI 기술을 활용한 반려동물 생체인식 서비스(SNUAC 아시아브리프, 2023.12.11.)

**[ 그림 5 ] 반려견 비문**



〈 출처 : Koreatechdesk.com 〉

## 생체인식 기술의 오남용 사례

○ 영국의 주요 소매업체(Budgens, Sports Direct, Costcutter 등)에서는 절도범을 식별하기 위해 Facewatch라는 얼굴인식 보안 프로그램을 사용

- 영국에 사는 사라(가명)는 초콜릿을 사기 위해 매장에 방문했다가 절도범으로 오해를 받아 가방을 검사 받은 후 매장에서 쫓겨났고, 이 기술을 사용하는 모든 매장에 출입 금지 조치를 당함
- 얼굴인식 프로그램의 오작동으로 인해 절도범으로 오인된 사례 중 하나로 Facewatch는 실수를 인정

○ 영국의 수도경찰청은 런던 전역에 강력범죄 대응을 위해 안면인식 기술을 활용 중으로, 카메라 및 안면인식 장비가 장착된 밴을 통해 거리에서 실시간으로 범죄자를 식별하여 임의 체포가 가능

- 시스템을 통해 많은 수의 범죄자를 체포하였지만, 범죄 혐의가 없는 일반인이 범죄자로 오인되는 사례도 다수 발생하여 시민 인권 침해에 대한 논란 발생
- 런던 경찰청은 카메라가 인식한 사람 33,000명 중 1명 정도가 잘못 식별된다고 밝혔으나, 실제로는 40건당 1건 정도 오인 사례 발생

※ I was misidentified as shoplifter by facial recognition tech(BBC, 2024.5.26.)

○ 미국 조지아주에 사는 주민 랜들 리드는 2022년 루이지애나주 뉴올리언스의 한 상점에서 훔친 신용카드로 1만5천달러 상당의 명품 가방을 구입했다는 혐의로 경찰에 체포됨

- 경찰은 상점 내 감시카메라에 찍힌 범인의 얼굴을 안면인식 기술로 분석하여 랜들 리드를 용의자로 특정하였으나, 얼굴인식 오류로 인한 잘못된 체포임이 확인된 후 체포 6일만에 석방됨
- 경찰이 사용하는 안면인식 기술이 흑인 등 유색인종을 대상으로 더 많은 오류가 발생한다는 의혹이 제기됨

※ Lawsuit: Man claims he was improperly arrested because of misuse of facial recognition technology (ABC News, 2023.10.4.)

## 2. 생성형 AI 시대의 생체인식 관련 법제도 및 기술동향

### ☑ 법제도 및 정책 동향

○ EU(유럽연합)는 전 분야에 포괄적으로 적용되며 27개 회원국 내에서 직접 효력을 갖는 인공지능에 관한 사항을 규정한 AI Act(인공지능법) 제정(발효 2024.8.1., 시행 2025.2.2.~2027.8.2.에 걸쳐 순차적)

- EU는 인공지능법에서 인공지능의 위험을 4단계(금지, 고위험, 제한적 위험, 최소 위험)로 구분하였으며, 인공지능 시스템을 이용한 생체인식 시스템을 고위험군으로 분류
- 고위험군으로 분류된 인공지능 시스템들은 사람의 건강, 안전, 기본권에 심각한 피해를 발생시킬 위험이 있는 시스템으로, 공급자와 서비스 제공자에게 각각 중대한 의무를 부과하고 있으며 위반시 막대한 벌금 부과

**[ 참고 ] EU 인공지능법 규제 개요**

| 위험 구분 | 규제 대상 | 예시 | 규제 내용 |
|---|---|---|---|
| 금지 (허용불가) | - 금지되는 인공지능 이용 | 사람 잠재의식 조작 | 금지(사전 승인 등 엄격한 조건하에 일부 예외 허용) |
| 고위험 | - 고위험 AI 시스템 | 생체인식, 채용, 금융, 공공서비스 분야 AI | 품질관리체계 구축, 기술문서 등 각종 문서 작성, 로그보관, 적합성평가, 기본권영향평가 등 |
| 제한적 위험 | - 투명성 위험 대상 AI 시스템 | 챗봇, 생성형 AI, 딥페이크 생성 AI | AI 이용을 알릴 수 있도록 기술적 조치, 기계판독 가능 워터마크, 라벨링 등 |
| 최소 위험 | - 그 밖의 AI 시스템 | AI 기반 비디오 게임, 스팸 필터 등 | 업무준칙 준수 |

※ 출처 : EU AI법의 주요 내용 및 시사점(NIA 디지털 법제 브리프, 2024.7.15.)

○ 마국 GAO(회계감사원, Government Accountability Office)는 2023년 9월 미국 법무부 및 국토안보부 산하 7개의 법 집행기관에서 범죄수사를 위해 사용하는 안면인식 기술 사용 현황을 조사·발표

- 7개의 기관 중 3개 기관은 얼굴인식 기술을 소유하고 있고, 7개 기관 모두 얼굴인식 서비스를 사용하고 있으며, 3개 기관만이 시민권과 시민의 자유를 보호하기 위한 얼굴인식 관련 정책이나 지침을 보유
- GAO는 법무부와 국토안보부에 범죄 수사를 지원하기 위한 얼굴인식 기술의 사용과 관련하여 10가지 권고안을 제시 : 권고안은 시민권, 교육 및 프라이버시 보호와 같은 주제에 초점

※ Facial Recognition Technology: Federal Law Enforcement Agency Efforts Related to Civil Rights and Training(GAO, 2024.3.8.)

○ 미국 상원의 크리스 쿤스, 마샤 블랙번, 에이미 클로버샤, 톰 틸스 의원은 일명 가짜 금지법(No Fake Act)이라 불리는 The Nurture Originals, Foster Art, and Keep Entertainment Safe Act 법안을 2024년 7월 발의

- 법안에 따르면 생성형 AI를 활용하여 개인이 직접 출연하거나 승인하지 않은 영상물, 이미지, 음성 복제물 등을 만든 개인·단체는 제작, 호스팅, 공유에 대한 책임이 부과되며, 승인되지 않은 복제물을 호스팅하는 온라인 서비스 사업자는 권리자의 통지에 따라 복제본을 삭제하여야 함.
- 법안은 미국 방송배우노동조합, 음반산업협회 등 영화, 음반, 출판 관련 기업과 단체의 지지를 받았으며, Open AI사도 지지를 표명

※ Senators Coons, Blackburn, Klobuchar, Tillis introduce bill to protect individuals' voices and likenesses from AI-generated replicas(2024.7.31.)

○ 중국의 국가인터넷정보판공실은 2023년 8월 '안면인식 기술 적용 안전관리 규정' 초안을 발표

- 중국 역내에서 안면인식 기술을 이용·처리하고 상품 및 서비스를 제공하는 경우 준수해야 되는 규정으로, 개인정보보호 등 기본원칙, 기기 설치·운영 제한, 처리 및 수집·저장의 제한, 감독·관리 책임, 법률적 책임 등에 관한 사항을 규정

※ 이상우, 중국의 안면인식 기술 입법동향과 시사점(인하대학교 법학연구, 2023.12.31.)

## 기술동향

○ AI 기술의 발전으로 사진이나 영상에서 얼굴을 복제(face clone)하여 AI 아바타를 생성하거나, 이미지에서 얼굴의 특징을 추출해 다른 이미지나 영상의 얼굴로 교체(face swap)하는 서비스가 활발히 활용

- 이러한 서비스는 이미지를 업로드한 후 몇 번의 클릭만으로 쉽게 이용할 수 있고, 제작된 영상은 매우 정교하고 자연스러워 진위 여부 판별이 곤란

[ 그림 6 ] Face Swap 예시

〈 출처 : https://www.vidwud.com/free-face-swap.html 〉

○ 이미지 외에 AI를 통한 음성 복제(voice cloning) 역시 매우 손쉬운 작업으로 가능해짐

※ 음성 복제는 음성 합성을 통해 음성을 모방하는 기술로, 음색, 음조, 액센트를 포함하여 사람의 음성을 복제

- 2024년 3월 오픈AI사는 자사의 블로그를 통해 보이스 엔진(Voice Engine)의 개발을 발표하였으며, 텍스트 입력과 더불어 15초의 오디오 샘플을 사용하여 원래 화자와 매우 유사하며 감정적이고 자연스러운 음성 생성이 가능하다고 밝힘

. 보이스 엔진 서비스는 ① 사전 설정된 음성으로 자연스럽고 감정적인 음성을 통해 아동에 대한 독서 지원을 제공하고, ② 비디오와 팟캐스트 같은 콘텐츠를 화자의 음성으로 여러 언어로 번역하여 통역이 아닌 본인의 음성으로 글로벌 청중에게 제공하거나, ③ 말하기에 어려움을 겪는 언어 장애를 치료하기 위해 여러 언어로 독특하고 로봇이 아닌 음성을 제공하는 것 등 다양한 분야에 활용이 가능할 것으로 전망

※ Navigating the Challenges and Opportunities of Synthetic Voices(OpenAI, 2024.3.29.)

※ 다양한 영역에 활용가능한 음성 복제 서비스의 예시 음성 샘플 청취 가능

**[ 그림 7 ] 오픈AI사의 Voice Engine을 활용한 외국어 음성 복제 번역 서비스 샘플 캡처**


〈 출처 : OpenAI, https://openai.com/index/navigating-the-challenges-and-opportunities-of-synthetic-voices/ 〉

**[ 참고 ] 생성형 AI를 활용한 음성 복제 사례**

· 2024년 2월 발매된 장기하가 작사·작곡하고 비비가 노래하는 '밤양갱'은 곡 자체로도 큰 인기를 얻었지만, AI 커버의 시대를 연 곡으로도 유명

- 아이유, 양희은, 오혁, 장기하, 박명수 등 많은 유명인 버전의 AI 커버가 제작되었으며 실제 목소리와 구별할 수 없는 정교함으로 큰 화제가 됨

- 보이스 엔진 이외에도 수많은 AI 음성 복제 서비스가 출시되어 팟캐스트, 교육 등 많은 산업 분야에서 활용 중으로 글로벌 음성 복제 시장은 2022년 15억 달러에서 2032년 162억 달러로 증가가 예상되며 연평균 성장률은 27.3%로 전망

※ https://www.alliedmarketresearch.com/voice-cloning-market

## 3. 생성형 AI가 가져온 생체인식 기술의 명암

### 생체인식 기술과 생성형 AI

○ 최근 생체인식 기술은 생성형 AI(Generative AI)로 인해 비약적으로 발전하고 있으며, 이러한 변화는 생체인식 기술의 보안능력 향상과 사회적 위협 요소 증가의 두 가지 측면에서 발생

- 생성형 AI는 데이터 보강 및 학습, 개인화 등을 통해 생체인식의 정확성을 제고할 수 있으나, 딥페이크, 스푸핑 공격 등을 통해 생체인식의 보안 위협 요소로 작용

### 생성형 AI를 활용한 생체인식 정확도 제고

○ 아마존의 비접촉 결제 솔루션인 '아마존 원(Amazon One)'은 생성형 AI가 합성한 다양한 조건과 모양을 가진 수 백만개의 손바닥 사진을 통한 학습으로 99.9999%의 정확도를 제공

- 생성형 AI를 활용해 합성 데이터를 생성하여 데이터 수집의 어려움을 극복하고 정확한 모델 학습을 위한 다양한 데이터 확보 : 조명 조건의 변화, 손 자세, 심지어 반창고의 존재와 같은 수많은 미묘한 변화를 반영해 수백만개의 손모양 합성 데이터를 빠르게 생성
- 학습을 위한 이미지 라벨링 작업 역시 생성형 AI 활용 : 손바닥 손금, 흉터, 결혼반지와 같이 사진에 담겨있는 특징의 라벨링 또한 자동으로 생성하여 시간을 절약하고 작업속도 개선

[ 그림 8 ] 아마존 원 학습을 위해 생성된 손바닥 합성 데이터

〈 출처 : https://www.aboutamazon.com/news/retail/generative-ai-trains-amazon-one-palm-scanning-technology〉

○ 독일의 da/sec Biometric & Security Research Group은 생성형 AI를 활용하여 최초의 대규모 합성 아동 얼굴 이미지 데이터베이스를 구축하여 아동 얼굴인식 정확도 제고

- 아동 얼굴인식 학습을 위한 합성데이타는 다음과 같은 단계로 생성

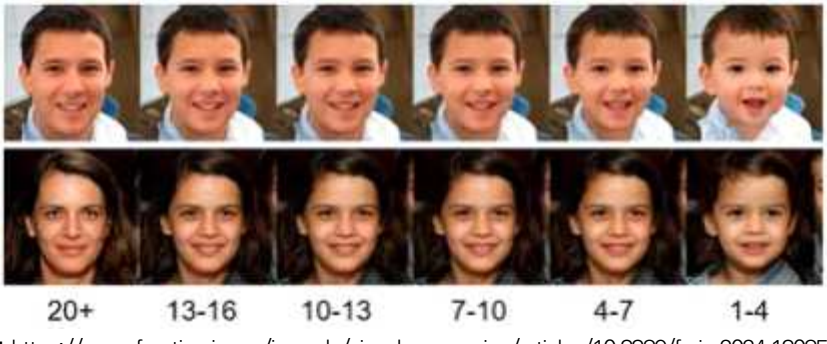
① 이미지 생성 모델을 활용하여 성인 얼굴을 생성(저품질 데이터 제거)

② 무작위로 생성된 얼굴의 성별, 인종을 균등하게 분배

③ 다양한 연령대의 성인 얼굴을 다양한 연령대의 아동 얼굴로 변환

④ 개별 아동 이미지를 다양한 형태로 변환한 이미지 생성 : 조명 밝기, 좌/우/아래/위 포즈, 웃는 얼굴 등

**[ 그림 9 ] 합성 성인 얼굴을 아동 얼굴로 변환**




〈 출처 : https://www.frontiersin.org/journals/signal-processing/articles/10.3389/frsip.2024.1308505/full〉

**[ 그림 10 ] 다양한 형태로 변환한 아동 얼굴 예시 (원본/좌/우/아래/위 포즈)**

〈 출처 : https://www.frontiersin.org/journals/signal-processing/articles/10.3389/frsip.2024.1308505/full〉

## 생체인식 기술의 위협 : 생성형 AI를 활용한 딥페이크 증가

**[ 참고 ] 딥페이크(DeepFake)**

· 딥페이크(DeepFake)는 인공지능 학습을 위해 활용되는 딥 러닝(Deep Learning)과 페이크(Fake)의 합성어로, 인공지능 기술을 활용하여 사람의 이미지, 행동(동영상), 목소리 등을 가짜로 합성하거나 제작한 결과물을 의미
  - 초기의 딥페이크는 유명인의 이미지나 영상을 영화의 CG처럼 합성한 영상 편집물을 중심으로 확산되었으나, 생성형 AI 기술의 발달로 인하여, 유명인의 목소리 복사, 가짜 뉴스·출판물 제작 등 다양한 분야로 확산

○ 미국 연방통신위원회(FCC : Federal Communication Commission)는 2024년 1월 뉴햄프셔주 대통령 예비선거에 사용된 AI 음성 복제를 활용한 딥페이크(DeepFake) 자동전화녹음에 대해 600만 달러의 벌금 부과

- 2024년 뉴햄프셔주 대통령 예비선거를 이틀 앞두고, 예비 유권자들에게 투표하지 말라는 바이든 대통령의 복제 음성을 사용한 딥페이크 오디오가 포함된 악성 자동녹음 전화가 전송됨

※ FCC Proposes $6 Million Fine for Deepfake Robocalls Around NH Primary(FCC, 2024.5.23.)

**[ 그림 11 ] 조 바이든 음성 복제 딥페이크 관련 기사**


JOE BIDEN

**Fake Joe Biden robocall tells New Hampshire Democrats not to vote Tuesday**

The call, an apparent imitation or digital manipulation of the president's voice, says, "Voting this Tuesday only enables the Republicans in their quest to elect Donald Trump again."

※ 오디오 내용 : 이번 화요일 투표는 도널드 트럼프를 다시 선출하려는 공화당의 노력에 도움이 될 뿐입니다.

〈 출처 : NBC News, 2024.1.22. 〉

○ 싱가포르 리센룽 총리는 2023년 12월, 자신의 영상을 이용한 딥페이크 영상이 암호화폐 투자와 관련해 유포되고 있다며, 이를 주의할 것을 SNS를 통해 당부

- 딥페이크 영상은 리센룽 총리의 중국 CGTN 방송사 인터뷰 영상을 위조한 것으로 영상에 등장한 총리는 특정 암호화폐 플랫폼을 홍보

※ PM Lee's deepfake video and the risk when seeing is no longer believing(CNA, 2024.1.17.)

[ 그림 12 ] 리센룽 총리의 딥페이크 영상 스크린샷


〈 출처 : CNA, 2024.1.17. 〉

○ 2024년 2월, 홍콩 경찰은 다국적 기업의 재무 담당자가 영상회의 중 딥페이크 기술을 이용해 회사의 최고재무책임자(CFO)로 가장한 사기꾼들에게 2,500만 달러를 송금하는 사건이 발생했다고 발표

- 해당 직원은 영국 본사의 CFO를 사칭한 이메일을 통해 거액의 송금을 요구받고 처음에는 이를 피싱으로 의심했지만, 영상회의를 통해 자신이 아는 얼굴과 말투를 확인하고는 의심을 접고 거액을 송금
- CFO를 사칭한 사기는 해당직원이 나중에 본사에 확인을 한 후에 발견

※ Finance worker pays out $25 million after video call with deepfake 'chief financial officer'(CNN, 2024.2.4.)

[ 그림 13 ] 2,500만 달러 딥페이크 사기 사건 관련 기사


〈 출처 : CNN, 2024.2.4. 〉

## 4. 시사점

### ☑ 생성형 AI는 생체인식 기술 활용에 양날의 검으로 작용

○ 생성형 AI 기술의 발전은 생체인식 기술의 정확성과 효율성을 크게 향상시키는 데 중요한 역할을 수행하여, 금융 서비스, 의료 시스템, 스마트 기기 등 다양한 분야에서 보안성을 제고하고 사용자 경험 향상에 기여

- 딥러닝 알고리즘을 통해 생체인식 시스템이 더 많은 데이터를 학습하고 분석할 수 있게 되면서, 오탐지나 거짓 거부율이 줄어들고, 인증의 신뢰성도 크게 향상되었으며, 손바닥인식, 얼굴인식, 음성인식과 같은 생체 인증 방식이 이전보다 훨씬 정교하고 빠르게 작동 가능

○ 하지만 생성형 AI의 발달은 긍정적인 효과와 함께 부작용도 동시에 초래하고 있으며, 그 중에서도 특히 딥페이크 기술의 발전은 생체인식 기술 활용에 큰 위협을 초래

- 딥페이크는 생성형 AI를 이용해 보다 쉽고 간단하게 사람의 얼굴이나 목소리를 조작하여 사기, 정보 왜곡, 사생활 침해 등 다양한 악의적인 용도로 사용되어 생체인식 시스템의 보안성을 위협하는 주요 요소로 작용
- 얼굴이나 음성 데이터를 기반으로 인증하는 시스템을 속이기 위해, 실제 사용자처럼 보이거나 들리는 딥페이크를 이용해 불법적인 접근을 손쉽게 시도 가능

○ 생성형 AI는 이처럼 생체인식 기술의 발전과 보안 향상에 기여하는 동시에, 딥페이크와 같은 악용 사례의 위험성을 증가시키는 양날의 검으로 작용

- AI 기술이 계속해서 정교해짐에 따라, 보안 솔루션도 딥페이크와 같은 위협에 대처할 수 있도록 지속적으로 발전해야 하며, 딥페이크 탐지 기술과 같은 추가적인 방어책이 필요
- 이러한 균형을 유지하기 위한 규제와 기술적 대응이 앞으로 더욱 중요한 과제임

### ☑ 딥페이크 위협에 대한 대응 : 멀티모달 생체 인증, 다중 요소 인증

○ 발전하는 딥페이크의 위협에 대응하기 위한 수단으로 멀티모달 생체 인증(Multimodal Biometric Authentication)과 다중 요소 인증(Multi-Factor Authentication)의 활용 고려

- 멀티모달 생체 인증은 사용자의 신원을 확인하기 위하여 두가지 이상의 생체정보를 활용하는 방식으로 보안성, 정확도, 편의성의 향상이 가능 (예) 지문+얼굴, 지문+걸음걸이, 얼굴+음성 등)

※ 멀티모달 인증을 다중 요소 인증의 의미로 사용하는 경우도 있으나 본보고서에서는 멀티모달 생체 인증의 의미로 사용

- 다중 요소 인증은 사용자의 신원을 확인하기 위하여 다양한 요소(지식 기반, 소유 기반, 생체정보)를 2가지 이상 활용함으로써 보안성을 강화하는 인증 방식

**[ 참고 ] 멀티모달 생체인증과 다중요소 인증의 차이**

| 특징 | 멀티모달 생체 인증<br>(Multimodal Biometric Authentication) | 다중 요소 인증<br>(Multi-Factor Authentication) |
|---|---|---|
| **정보의 종류** | 다양한 생체인식 지표<br>. 신체적 특징 : 지문, 홍채, 얼굴, 정맥, 음성 등<br>. 행동적 특징 : 걸음거리, 필적, 타이핑 습관 등 | 다양한 범주의 인증 방식<br>. 지식 기반 요소 : 비밀번호, 보안질문 등<br>. 소유 기반 요소 : 출입카드, OTP, 스마트폰 등<br>. 본인 고유 요소 : 생체인식 지표 |
| **주안점** | 내가 누구인지 확인 | 다양한 범주의 인증 방식 조합 |
| **주요 활용 대상** | 물리적 접근통제 시스템(출입통제) | 온라인 계정, 중요 시스템 |

※ 출처 : Beyond Fingerprints: The Power of Multimodal Biometric Authentication(OLOID, 2024.6.27.)

## 빅 브라더 이슈에 대한 대처

○ 개인을 인증하기 위한 지문, 얼굴, 홍채 등의 생체인식 정보들은 비밀번호처럼 기억할 필요가 없고, 다른 사람의 도용이 어려우며, 직관적인 사용자 경험을 제공하고, 분실 위험이 없는 장점이 있는 반면에, 오인식 가능성이나 유출되면 변경이 불가능한 특성으로 인하여 사용자의 생체정보를 수집·저장하는 과정에서 프라이버시 침해 및 악용 우려가 상존

○ 생체인식 기술을 활용하는 기업들의 생체 정보 수집·저장에 대한 사용자의 우려 및 불안감을 해소하기 위한 사회적인 합의 및 제도적인 뒷받침 필요

※ 영국의 개인정보보호 단체인 'Big Brother Watch'는 영국 경찰과 민간기업의 무분별한 얼굴인식 기술의 활용에 대한 금지 캠페인 실시

※ Stop Facial Recognition : https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/

## 〈참고 자료〉


1. https://www.ibia.org/
2. KISTEP, 2021.04.28, 최근 생체인식 산업 동향과 시사점
3. https://www.precedenceresearch.com/biometric-technology-market
4. https://www.moj.go.kr/moj/193/subview.do
5. https://www.theguardian.com/uk-news/2020/feb/11/met-police-deploy-live-facial-recognition-technology
6. X5 Group, 2023.8.2, X5 and Sber launch world's largest smile-to-pay service
7. https://one.amazon.com/
8. https://x.com/theapplehub
9. HSBC UK, 2021.5.4, HSBC UK's Voice ID prevents £249 million of attempted fraud
10. https://www.tonetag.com/resource/introducing-voicese-indias-foremost-voice-based-payment-system/
11. SNUAC 아시아브리프, 2023.12.11, AI 기술을 활용한 반려동물 생체인식 서비스
12. https://www.koreatechdesk.com/korean-startup-launching-a-nose-print-identification-for-dogs-an-alternate-to-the-microchip-embedding-process/
13. BBC, 2024.5.26, I was misidentified as shoplifter by facial recognition tech
14. ABC News, 2023.10.4, Lawsuit: Man claims he was improperly arrested because of misuse of facial recognition technology
15. NIA 디지털 법제 브리프, 2024.7.15, EU AI법의 주요 내용 및 시사점
16. GAO, 2024.3.8, Facial Recognition Technology : Federal Law Enforcement Agency Efforts Related to Civil Rights and Training
17. Senators Coons, Blackburn, Klobuchar, 2024.7.31, Tillis introduce bill to protect individuals' voices and likenesses from AI-generated replicas
18. 이상우, 2023.12.31., 중국의 안면인식 기술 입법동향과 시사점, 인하대학교 법학연구
19. https://www.vidwud.com/free-face-swap.html
20. OpenAI, 2024.3.29, Navigating the Challenges and Opportunities of Synthetic Voices
21. https://openai.com/index/navigating-the-challenges-and-opportunities-of-synthetic-voices/
22. https://www.alliedmarketresearch.com/voice-cloning-market
23. https://www.aboutamazon.com/news/retail/generative-ai-trains-amazon-one-palm-scanning-technology

24. https://www.frontiersin.org/journals/signal-processing/articles/10.3389/frsip.2024.1308505/full

25. https://thefintechtimes.com/how-will-generative-ai-revolutionise-digital-payments-in-mena/

26. FCC, 2024.5.23, FCC Proposes $6 Million Fine for Deepfake Robocalls Around NH Primary

27. NBC News, 2024.1.22, Fake Joe Biden robocall tells New Hampshire Democrats not to vote Tuesday

28. CNA, 2024.1.17., PM Lee's deepfake video and the risk when seeing is no longer believing

29. CNN, 2024.2.4, Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

30. OLOID, 2024.6.27, Beyond Fingerprints: The Power of Multimodal Biometric Authentication

31. https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/

# THE AI REPORT 2024

NIA 한국지능정보사회진흥원