

# 《 \_\_\_\_\_ 생명과학 세특 보고서 》

하이에듀

**주제** AI 기술을 활용한 생체인식과 보안 ✓전공적합성 ✓학업역량

### 개요

생명 과학은 크게 물질이나 우주의 생성 등을 연구하는 타 과학 분야와 달리 지구에 사는 생물의 특성과 다양한 생명 현상을 연구하는 학문입니다. 개체, 기관, 조직, 세포를 구성하는 분자로 세분화 할 수 있으며 생명체에서 일어나는 여러 가지 현상을 탐구하는 학문인 만큼 타 분야와 응용하여 인료가 당면한 질병, 환경오염, 기후변화, 데이터 과학 등의 과제 해결에도 이용될 수 있습니다. 이번 주제로는 “AI 기술을 활용한 생체인식과 보안”을 추천드립니다.

### 관련 단원

생명과학1 : 1단원 / 생명 과학의 통합적 특성  
생명과학2 : 6단원 / 생명 공학기술과 인간생활

[★ 난이도 Up ★] 인공지능, 나아가 인공지능경망의 기원은 생물학의 신경망에서 영감을 얻은 알고리즘입니다. 따라서 **생명과학1의 신경계**와 연결하여 인공지능경망 뉴런 모델링에 대해 탐구해도 좋습니다. 이해에 난이도가 있을 수 있지만 관심있으시다면 다음 기회에 참고하여 주제 선정하는 것도 좋겠습니다.

참고 : <https://www.aitimes.com/news/articleView.html?idxno=138838>

<b>가이드</b>	<b>서론</b> 주제 선정 이유 [자료1]
	핸드폰 페이스ID 잠금 해제, 현관 비밀번호 지문인식, 홍채인식 등 생체적 특징을 활용하여 인증 및 보안 시스템에 적용하는 모습을 자주 볼 수 있습니다. 현대 사회에서 생체인식 기술이 보안 분야에서 중요한 역할을 하는 만큼 개인정보 보호가 유출되지 않도록 하는 노력이 그만큼 중요하다고 생각되었습니다. 실제로 페이스ID 해킹이 성공한 사례, 지문 잠금 해제하는 방법 등이 유튜브에서 소개되곤 합니다. 그렇다면 대두되고 있는 AI 기술을 활용하여 생체인식 기술에 접목한다면 보안 문제를 해결하는 것에 도움이 되지 않을까 호기심이 생겨 AI 기술을 활용한 생체인식의 전망에 대해 탐구해 보고 싶어 주제로 선택하게 되었습니다.
	<b>본론</b> 호기심과 흥미로웠던 탐구 내용 : 생체인식 ① 생체인식의 정의와 종류 [자료2] ② 생체인식 기술 원리 [자료3] ③ AI 생체인식의 전망 [자료4,5]
	생체인식은 개인의 고유한 생체적 특징을 활용하여 정체성을 확인하는 기술을 의미합니다. 이러한 특징은 지문, 안면, 홍채, 손목 정맥, 음성, 심전도, DNA 패

턴 등 다양합니다. 이 중에서도 특히 얼굴 인식과 지문인식, 홍채 인식, 음성 인식이 널리 사용되고 있습니다.

각각의 인식 방법은 아래와 같습니다.

- 얼굴 인식: 카메라로 얼굴을 촬영하고 기존 데이터베이스와 비교하여 일치 여부를 확인합니다.
- 지문 인식: 지문 패턴의 유사성을 분석하여 개인을 확인합니다.
- 홍채 인식: 홍채의 형태와 패턴을 분석하여 신원을 확인합니다.
- 음성 인식: 음성의 주파수, 음성 특성, 억양 등을 분석하여 개인을 식별합니다.

생체인식 기술이 현대 사회 다양한 분야에서 편의성을 제공하는 역할을 하는 만큼 인간 고유의 생체적 특징이 타인에게 유출되거나 보안 위협을 받지 않도록 높은 신뢰성을 가져야 합니다. 최근에는 AI를 통한 발전으로 딥러닝과 신경망 기술을 적용하여 이러한 생체 특성을 더욱 정확하게 인식하고, 인식 속도를 향상 시킵니다. 한편 모순적으로 AI의 발전을 이용하여 더욱 고도화 된 해킹을 할 수 있고 여전히 디지털 차원에서의 오차를 배제할 수 없습니다.

하지만 개인의 보안(핸드폰, 은행)에서 나아가 건물 보안까지 고려한다면 인공지능 차원에서의 생체인식을 활용하면 큰 이점이 있으므로 도전 가치와 전망이 있다고 생각됩니다. 실제로 3D 카메라 등 첨단 IT 기술의 발전으로 현재 90% 이상의 스마트폰 지문인식 기능이 2023년 이후에는 얼굴인식으로 대체될 것으로 보안업계는 내다보고 있다는 기사가 있으며, 코트라에 따르면 실제로 미국에서는 안면인식 기술 관련 수많은 투자가 이뤄지고 있으며, 최근 3년간 미국 내 투자액은 7870만 달러에 달하는 것으로 알려졌습니다. [자료5]

## 결론 : 학생의 생각과 주장으로 마무리

기술의 혁신과 확산 그리고 적용은 개인정보 보호와 민감한 정보 유출에 대한 우려를 동반할 수밖에 없습니다. 따라서 적절한 규제와 보안 조치가 필요하며 근본적으로 개개인의 윤리 의식을 함양하는 교육이 필요하다고 생각합니다. AI 생체인식 기술이 조화롭게 발전 및 적용되기 위해서는 윤리와 법률, 보안과 개인정보 보호 등 다양한 측면에서 고려해 나가야하는 시행착오 단계에 있다고 생각합니다. 하나의 인증 방법이 신뢰성이 부족하다면 다중 인증 방법으로 보안을 강화하면 좋겠다는 생각을 했습니다.

개인적으로 AI 기술의 발전에 따른 생체인식은 우리의 삶을 더 편리하게 믿어줄 것이라 믿습니다. 보안과 편의성의 균형을 유지할 수 있는 미래가 오기를 기대합니다.

## 자료1 주제선정계기 활용 기사

에스원은 코로나 시대에 비대면이 일상화되면서 올해 보안업계에 △AI 기술을 탑재한 **지능형 보안솔루션의 확산** △생체인증을 접목한 무인솔루션 증가 △ICT를 활용한 정보보안 시장 확대 △빅데이터를 적용한 통합관제센터 구축 등이 트렌드로 나타날 것으로 전망했다. 이같은 흐름을 주도하기 위해 에스원은 올해 '통합 보안 플랫폼' 구축에 집중한다. 이를 위해 기술혁신을 위한 연구개발(R&D) 조직을 사업부 조직과 통합하고, 물리보안사업과 빌딩관리사업 조직을 하나로 합칠 계획이다.

출처 : <https://www.hankyung.com/economy/article/202101142720i>

팬데믹 이후 새로운 보안 기술에 대한 관심이 급격하게 고조된 가운데 업계 선두주자인 에스원은 AI, 생체인식, ICT, 빅데이터 등의 **첨단 기술을 총망라한 '통합 보안 플랫폼'을 선보이겠다고 밝혔다**. 플랫폼을 통해 압도적인 업계 1위의 위상을 공고히 하겠다는 전략이다. 이를 위해 에스원은 기술 혁신을 위한 연구개발(R&D) 조직을 사업부 조직과 통합하고 물리보안사업과 빌딩관리사업 조직을 하나로 합치는 등 '통합 보안 플랫폼' 구축에 박차를 가하고 있다. **통합 보안 플랫폼의 생체인증 기술은 무인매장 솔루션에 적용된다**. 무인매장의 비대면 출입 관리를 위해 얼굴인식 시스템의 적용범위를 확대한다는 방침도 세웠다. 에스원의 얼굴 인증 기술력은 정확도가 99.9%(한국인터넷진흥원 인증)에 달해 보안성을 높이는데 크게 기여할 것으로 기대하고 있다. 에스원은 스터디카페, 세탁소, 노래방 등 무인화가 활발히 진행되고 있는 업종을 중심으로 '맞춤형 무인 솔루션 패키지'를 출시한다는 계획이다. 한편, 올 1분기에는 **생체인증과 AI기술을 접목**해 출입관리와 체온 모니터링 기능을 동시에 제공하는 발열감지솔루션도 선보일 예정이다.

출처 : <https://www.m-i.kr/news/articleView.html?idxno=785926>

## 자료2 생체인식의 정의와 종류

### 지문

- 사람의 손가락에 있는 지문의 고유 패턴을 판별하여 본인 인증
- 장점: 편리하고 안전, 다양한 장치 사용 가능, 정확도가 우수함
- 단점: 땀, 먼지 등에 의한 인식률 저하, 위조 가능성, 주변 환경에 따른 오류

### 홍채(망막)

- 홍채 무늬, 형태, 색, 망막 모세혈관 분포 패턴 분석
- 장점: 낮은 오인식률, 고도의 보안성, 위조 불가능, 분실 위험 없음, 비접촉식
- 단점: 눈을 뜨고 있어야 하는 불편함, 인식 거리, 장비가 고가임

### 지정맥

- 근적외선을 통해 혈관 속의 헤모글로빈을 인식, 정맥 패턴을 인식
- 장점: 편리, 복제 불가능
- 단점: 높은 구축 비용, 소형화 어려움

---

### 얼굴(안면)

- 눈썹 간 간격, 코, 입 등 얼굴 요소 특징 분석
- 장점: 비접촉식으로 편리성, 시스템 비용 저렴, 원격 인증 가능
- 단점: 빛 세기, 촬영 각도, 자세, 안경, 가발 등에 따라 인식을 저하

---

### 서명

- 사용자가 서명하는 방식(펜 움직임, 속도, 압력)을 분석, 서명의 위변조 판별
- 장점: 분실, 도난 위험 없음
- 단점: 서명 복제, 위조 가능

---

### 음성

- 소리센서를 통해 얻은 음성 특징을 DB와 대조해 개인인증
- 장점: 편리성, 전화 및 인터넷으로 원격지에서 이용 가능
- 단점: 녹음으로 타인 이용 가능성, 목소리 상태에 따른 오인식

출처 :

<https://scienceon.kisti.re.kr/srch/selectPORSrchReport.do?cn=KOSEN0000000000001047&dbt=KOSEN>

---

### 자료3 생체인식의 기술 원리

홍채인식은 눈을 홍채인식 해당 장비에 대면 정색 광선을 투사해 반사된 역광을 측정해서 등록된 정보와 비교하는 기술이다.

얼굴인식은 사람 얼굴의 눈과 코, 입 턱선의 대칭적인 구도와 생김새, 머리카락, 눈의 색상 등을 분석해서 얼굴의 특징을 알아낸다. 실물은 물론이고 사진 속의 얼굴을 인식할 수도 있고, 얼굴 모양새를 통해 성별이나 나이까지도 인지할 수 있는 기술로 발전하고 있다. 얼굴인식 기술은 홍채인식 보다 앞서 나온 기술이었지만, 보안 문제와 기술적인 문제로 한동안 뒤쳐져 있다가, 최근 애플 등에서 활용하며 재부상하고 있다.

정맥인식은 핏줄의 패턴을 근적외선으로 읽어들이며 피부 아래의 정맥 패턴, 즉 정맥을 투시 촬영해 정맥 지도를 만들어서 인증한다. 그 후에는 홍채인식과 마찬가지로 패턴을 분석하는 알고리즘을 이용해 템플릿이라는 데이터를 만들고 비교해서 인식한다. 정맥인식은 오류 확률이 0.0001%이며, 특히 살아있는 사람만 인식이 가능하다는 것이 장점이다. 정맥인식에 사용하는 장비가 고가라서 널리 보급이 이뤄지지 않았지만, 최근 국내업체가 초박형, 슬립형, 저가형으로 개발해서 보급하기 시작했다.

걸음걸이 인식은 카메라를 통해 걷는 모양을 촬영한다. 사람의 신체를 △머리 △어깨 △골반 △무릎으로 구분해 이를 중심으로 움직일 때마다 발생하는 함숫값을 측정해 사용자를 인식한다. 이는 의학계에서 오래전부터 치료 목적으로 연구해 온 기술이기도 하다.

---

출처 : <http://www.dspress.org/news/articleView.html?idxno=10773>

#### 자료4 생체인식의 오류 가능성

최근 공인인증서 의무화가 폐지됨에 따라 생체인식 기술 적용의 기폭제가 되었다. 특히 생체인식 기술은 액티브X 기반 플러그인 설치, 공인인증서와 개인키 저장, 공인인증서 비밀 번호 노출의 위험성을 해결할 수 있다는 점에서 공인인증서를 보완하거나 대체할 수 있는 기술적 방안으로 부상하였다. 생체인식을 편리하다 생각지 않는 사람은 없다. **다만 유출돼 도용될 수 있다는 것이 가장 취약한 점이다.** 생체인증 보급과 함께 생체정보 유출에 따른 보안 우려가 확산되는 가운데 최근에는 찰흙으로 만든 모조 지문이나 **얼굴 사진을 출력한 종이 가면을 오인식하는 사례가 발생하여 문제가 되었다.** 인식 정확성 문제는 차차 극복되겠지만, 생체인식이 의존하는 정보가 유출, 복제당해 도용되면 그 신뢰가 깨질 수 있는데 이게 가장 취약한 점이다. 최근 **각종 해킹 기법이 지능화하면서 이제는 사람의 신체가 없어도 주민등록증 지문을 위변조해 생체정보를 탈취하는 것이 기정사실화되었다.** 3차원(3D) 프린터로 지문을 위조해 50억 원 상당의 땅을 팔거나 초과근무수당을 실리콘 지문으로 악용해 챙긴 사례, 본드 위조 지문으로 입국심사대가 뚫리는 생체보안 해킹 사례가 잇따랐다. 하지만 한발 더 나아가 주민등록증에 코팅된 지문을 점토에 복사하거나 스마트폰으로 촬영, 위변조가 가능한 사례도 확인됐다. 지문 같은 생체정보는 유출당했다고 당사자가 폐기할 수도 바꿀 수도 없다. **생체정보를 인식하는 방법은 생체정보를 서버 데이터베이스(DB)에 두고, 이용자 단에서 인식된 값을 가져와 매번 대조하는 것이다.** 암호화해 보관하더라도 **암호키와 함께 대량 유출되거나, 비교를 위해 복호화하는 시점에 털리면 소용이 없다.** 관리자 실수로 유출할 수도 있다. 2016년부터 정보통신기술진흥센터(IITP)가 전담기관으로 지원해온 “DNA 분석 및 생체인증 보호를 위한 동형암호 실용화 기술 개발” 사업을 추진하여온 한국스마트인증은 “동형암호 생체인증 기술”을 개발하였다. **이 기술은 생체인식에 접목될 수 있는 동형암호로, 생체정보 유출에 따른 위험을 없애준다.** 동형암호는 정보를 암호화한 상태에서 연산처리가 가능한 기술이기 때문이다. 생체정보를 대조하는 단계에서 복호화할 필요가 없다. 그래서 암호화한 상태로 대조할 수 있다. **생체정보를 보관하는 DB에는 암호화된 정보만 있어서, 유출되더라도 그걸 본 사람들은 그게 뭔지 알 수 없기 때문이다.**

출처 :

<https://scienceon.kisti.re.kr/srch/selectPORSrchReport.do?cn=KOSEN000000000001047&dbt=KOSEN>

지문은 여러 이유로 닳아 지워지는 경우가 있고, 땀이나 이물질 등이 묻으면 제대로 인식하지 못하는 경우도 발생한다. 홍채의 경우 눈을 장비에 갖다 대야 하기 때문에 사용자들의 거부감이 있을 수 있고, 고가의 장비가 필요하다는 단점이 있다. 얼굴인식은 성형수술을 했을 경우 어느 정도 성형을 했느냐에 따라 인식률이 달라질 위험이 있다. **오차범위에 들어오면 본인으로 확인할 것이고, 그렇지 않으면 다른 사람으로 인식한다.** 지문 및 얼굴 인식정보는 본의 아니게 유출되는 경우도 있다. 실제 일본 국립정보학연구소는 2016년에

3m 거리에서 고해상도 카메라로 촬영한 지문을 통해 복제 지문을 만들었고, 이를 이용해 지문 인증을 통과하는 시연을 했다. 요즘은 높은 디지털 카메라뿐만 아니라 스마트폰의 카메라도 해상도가 높아 일상에서 본인의 지문이 유출될 수 있다는 것을 방증하는 셈이다. 또 2014년 독일의 해커그룹 카오스컴퓨터클럽은 독일 국방장관의 사진에서 지문을 복제했다. 2016년 노스캐롤라이나주립대는 SNS에서 획득한 얼굴 사진을 이용해 얼굴인식 기반 인증을 통과하는 연구 결과를 발표하기도 했다.

출처 : <http://www.dspress.org/news/articleView.html?idxno=10773>

#### 자료5 AI 생체인식 전망

타인과의 접촉을 최소화하려는 '언택트(Untact, 비대면)' 소비문화가 확산되면서 생체인증 시장이 블루오션으로 떠오르고 있다. 최근에는 지문, 홍채, 망막에 이어 안면인식 기술이 다양한 산업에 활용되면서 빠르게 성장하고 있다. 특히 딥러닝 등 AI(인공지능)를 적용한 얼굴인식 기술의 정확도가 높아지면서 공공·출입관리는 물론, 의료·금융·유통에 이르기까지 광범위한 분야로 확대되고 있다. 특히 3D 카메라 등 첨단 IT 기술의 발전으로 현재 90% 이상의 스마트폰 지문인식 기능이 2023년 이후에는 얼굴인식으로 대체될 것으로 보안업계는 내다보고 있다.

또한 LG CNS는 AI와 블록체인, 클라우드 등 3대 IT 신기술을 결합한 '안면인식 커뮤니티 화폐' 서비스를 국내 최초로 선보였다. 이 서비스는 AI 안면인식 기술로 직원의 신원을 파악한 후 미리 등록된 블록체인 기반의 커뮤니티 화폐로 자동 결제된다. 모든 시스템은 클라우드 상에서 작동한다. 사전에 얼굴과 계좌 정보 활용에 동의한 직원들은 식당 배식대에 설치된 기기에 얼굴만 인식시키면 자동으로 결제가 이뤄진다.

안면인식 기술은 직접 접촉하지 않고도 대량의 데이터 수집이 가능해 향후 각종 산업 분야에 폭넓게 사용될 것으로 보인다. 코트라에 따르면 실제로 미국에서는 안면인식 기술 관련 수많은 투자가 이뤄지고 있으며, 최근 3년간 미국 내 투자액은 7870만 달러에 달하는 것으로 알려졌다. 하지만 일각에서는 생체 정보를 해킹하는 등 대량의 데이터가 악용될 경우 최악의 피해로 이어질 수 있고, 지나친 개인정보 침해라는 주장도 나오고 있다.

한 보안 전문가는 "얼굴인식 기술을 활용한 데이터 분석은 소비시장에서 피해갈 수 없는 흐름인 것이 사실이지만 안전하게 상용화되기까지는 풀어야 할 과제도 적지 않다"고 지적했다. 이어 "최근 중국의 경우 안면인식 기기의 기술적 한계로 이용률이 낮아지고 있다"면서 "기술개발 및 사용에 있어 개인정보 보호에 대한 접근은 필수적으로 선행돼야 하며 오류 감지 기술 등 정확도를 높인 소프트웨어의 개발이 필요하다"고 강조했다.

출처 : <http://www.trendmaker.co.kr/news/articleView.html?idxno=229749>

#### 생체인식 보안을 위한 노력

생체정보를 획득해서 복제하는 행위 자체를 막는 것은 거의 불가능하다고 봐야 한다. 결국 본인정보는 본인이 잘 관리해야 한다. 또한, 생체인식을 적용해서 고객의 생체정보를 수집하고 활용하는 기업은 보다 더 신중히 관리해서 보안 이슈가 발생하지 않도록 주의해야 한다. 이 때문에 생체정보를 저장하지 않고 특수한 암호로 전송하고 보관해 활용하는

---

FIDO 기술을 적용하는 사례가 늘고 있다. FIDO 생체정보는 해킹 하더라도 본인이 아니면 열어볼 수 없어 현재 거의 모든 기업체에서 활용하고 있다. 생체인식을 활용하는 사회로 진입한다면 '빅 브라더' 사회로 갈 위험도 있다. 빅브라더라는 말은 1984년 조지오웰의 소설에 등장하는 감시 사회를 일컫는 말이다. 2019년 인도 정부가 도입한 생체정보를 활용한 신분증 프로그램인 '아드하르'가 과도한 신체정보를 요구하며 인권 침해라는 목소리가 높아지면서 이른바 '인도판 빅 브라더' 논란이 벌어졌다. 아드하르는 12자리 주민번호를 부여받는 신분증 프로그램인데, 정부로부터 식량이나 연금, 정부 보조금 등을 배급받으려면 신분증이 있어야 한다. 문제는 이 신분증을 받으려면 지문, 홍채 등 신체정보를 입력해야만 받을 수 있다는 데에서 발생했다. 뿐만 아니라, 민감한 개인정보가 담긴 신분증은 대중교통 이용이나 은행 계좌 개설 및 휴대폰 개통, 혼인신고 등 모든 곳에 다 쓰였다. 인도 정부가 13억 명 인도인의 일거수일투족을 확인할 수 있는 셈이다. 생체인식은 편리하지만, 보안 측면에서 완벽한 것은 아니다. 이를 보완하기 위해 다중 생체인식 (multimodal biometrics)을 활용한다. 다중 생체 인식 기술은 다중센서를 통해 여러 가지 생체 요소를 2~3번 인식해서 안전성을 보완하는 인식기술이다. 지문인식을 하고 얼굴인증을 하거나, 지문인식을 하고 목소리 인증을 하는 등 2가지 이상의 생체 정보를 가지고 인식하는 기술이다. 5G 통신망 활용에서 6G로 정보통신기술이 진화·발전하면, 사람에 관한 인증뿐만 아니라 사람과 사람, 사람과 사물, 사물과 사물도 인증해야 한다. 다시 말하면 생체인식 보안을 사용하지 않을 수 없다는 것이다. 현재 테슬라의 자율주행 자동차처럼 차만이 아니라 사람이 주인이라는 상호인식과 인증을 해야 하고, 도로 위의 각종 센서를 인식해야 하며, 자동차와 자동차 간을 인식해야 사고가 발생하지 않는 안전한 주행을 할 수 있다.

출처 : <http://www.dspress.org/news/articleView.html?idxno=10773>

다만 카드업계에서는 생체 인증 서비스가 보편화되려면 상당한 시간과 비용이 들어갈 것이라고 내다봤다. 2018년 신한카드를 포함한 주요 카드사가 힘을 합쳐 시작한 정맥 인증 결제 시스템 '핑페이'는 LG히다찌, 나이스정보통신까지 파트너로 끌어들이었지만, 가맹점 확보에 실패해 결국 좌초했다. 거의 모든 스마트폰에 지문 인식이나 안면 인식 솔루션이 탑재됐지만, 여전히 안면 인식 기능이 '디지털 빅브라더' 같은 윤리적 문제에서 자유롭지 않은 것도 문제다. 한 카드업계 관계자는 "카카오페이를 포함한 QR(Quick Response)코드 결제 서비스도 도입 초반에는 가맹점 확보가 과제였던만큼, 생체 인증이 자리를 잡으려면 단말기 비용 문제가 먼저 해결돼야 한다"며 "북미권 공항에서 신체 검사를 할 때처럼 스캔한 안면 정보를 원본 파일 형태로 저장하지 않는 알고리즘을 사용하면 금융 소비자 인식도 차차 개선될 것"이라고 말했다.

출처 :

<https://biz.chosun.com/stock/finance/2021/06/17/FI7CQFCX35G03ER42WZEXBWPJU/>

---