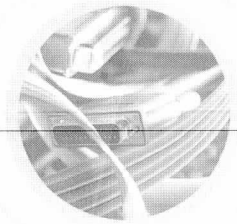
SPECIAL. Ⅱ



보안토큰을 이용한 생체인증

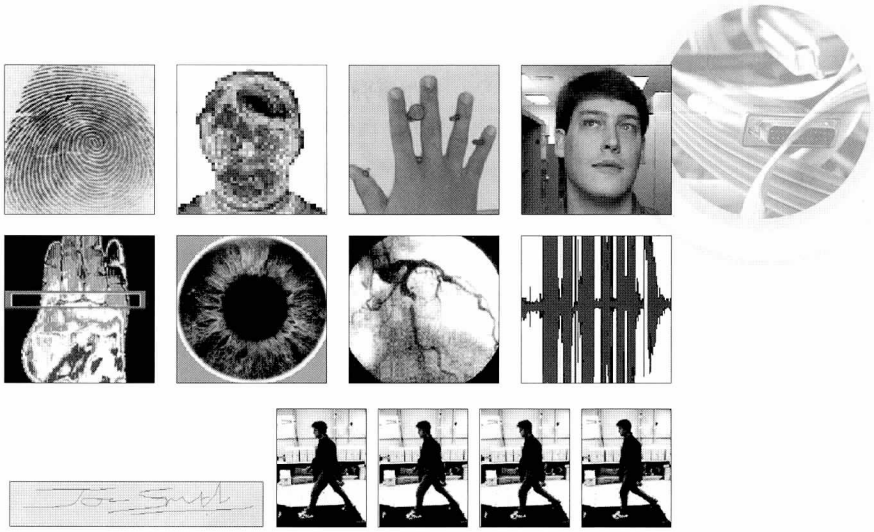
반성범, 정용화 / 한국전자통신연구원 정보보호기반연구부

인터넷을 이용한 글로벌 네트워크가 형성되어 편리하게 수집, 분석 및 가공한 개인의 중요한 정보가 타인에 의해 도용되거나 파괴되는 심각한 문제가 제기되고 있으며 나아가 국가의 중요 정보와 전자상거래 등의 경제 활동에 필요한 정보도 손실되는 현상이 발생되고 있다. 그러므로 현재까지 사용되고 있는 사용자 패스워드 또는 PIN(Personal Identification Number)만을 이용한 사용자 인증 방법으로는 개인, 산업, 국가의 중요 정보를 안전하게 보관할 수 없는 실정이다. 이러한 문제를 해결하기 위해 최근 들어 개인의 고유한 생체정보인 지문 또는 음성을 이용하여 사람의 신원을 확인하는 생체인식 기술에 관한 연구가 진행되고 있다

사용자 인증 방법은 패스워드 또는 PIN 등 사용자가 알고 있는 정보, 열쇠 또는 스마트 카드 등 사용자가 소지하고 있는 장치, 지문 또는 음성 등 사용자의 고유 정보를 이용한 방법으로 나눌 수 있다. 현재까지 일상생활에서 널리 사용되고 있는 사용자가 알고 있는 정보 또는 소지하고 있는 장치를 이용한 사용자 인증 방법은 망각, 분실 또는 도난 등의 이유로 높은 보안 성능을 제공하지 못하게 되었다. 반면에 생체인식은 개인별로 차이가 있는 사용자의 고유한 생체정보 또는 독특한 행동을 이용하는 것으로 분실 및 도난 등의 문제가 없어 기존의 방법에 비해 높은 보안 성능을 제공할 수 있다.

바이오메트릭 컨소시엄(Biometric Consortium)에서는 바이오메트릭 즉, 생체인식을 '자동화된 특정 개인의 소추된 특성을 인증하거나 신분을 인식하기 위해, 측정 가능한 특성 또는 개인의 특징을 연구하는 학문'으로 정의하고 있다. 이러한 생체정보를 이용한 생체인식의 예로는 그림 1과 같이 지문, 음성, 얼굴 모양, 홍채 패턴, 손의 형태, 손등의 정맥 분포 등 아주 다양하며, 이들은 신체의 일부분이거나 개개인의 행동 특성을 반영하므로 잊어버리거나 타인에게 대여 혹은 도난 복사가 되지 않는다. 즉, 타인이 지문 혹은 홍채 패턴을 훔쳐갈 수 없고 개인은 지문이나 홍채 패턴 등을 망각할 수 없으며, 집에 두고 올 수도 없다는 것이다. 그러므로 안전한 정보보안을 위한 분야로 활발하게 연구가 진행되고 있다. 생체인식 기술이 이러한 장점이 있지만 사용자 인증을 위해 저장된 생체정보가 타인에게 도용된다면 패스워드나 PIN과 같이 변경이 불가능하므로 심각한 문제를 발생할 수도 있으므로 보안토큰(스마트카드 또는 USB 토큰), PDA 등의 개인기기와 연동시키는 연구도 진행되고 있다.

표 1은 주요 생체 인식 기술을 비교한 것으로, 생체 인식에 이용되는 신체적 특징은 가장 활발히 상용화가 되고 있는 지문을 비롯해 얼굴, 손모양, 홍채와 망막, DNA 등이고 행동학적 특징은 음성, 서명, 걸음걸이 등이 있다. 표 1에 설명한 것과 같이 각각의 생체 인식 기술은 특성에 따라 기술 발전 정도와 적용에 차이를 보이고 있다. 음성과 서명은 편리성이 뛰어나지만 보안성이 취약하고, 홍채는 보안성은 뛰어나지만 가격이 높다는 문제점을 갖고 있다. 그러나 지문은 가장 오래된 연구를 통해 신뢰성이 입증되었고 가격이 저렴하여 적용 분야가 광범위하다.



〈그림 1〉 다양한 종류의 생체인식

생체인식의 이용 방법으로는 인증(verification, 1:1)과 인식(identification, 1:many)이 있다. 인증의 경우는 주로 지문 등을 이용한 출입 통제, 금고, 정보 보안, 전자 상거래시의 본인 확인 분야에 사용된다. 인식의 경우는 생체정보를 등록된 생체정보 데이터베이스에서 검색하여 찾아주는 기술로 AFIS (Automated Fingerprint Identification System)가 있다. 또한, 생체인식 기술은 그림 2와 같이 마우스, 키보드, ATM 단말기 등에 사용되고 있으며 휴대폰, PDA 등에 적용된 지문 인식 제품도 선보이고 있다. 홍채 인식 시스템은 다른 생체 인식 시스템에 비해 정확성이 뛰어나고 위, 변조가 불가능해 보안성이 우수하나 가격이 다소 비싸다는 단점을 갖고 있는데, 앞으로 고도의 보안을 요구하는 핵시설, 의료 분야 등을 중심으로 수요가 점진적으로 늘어날 것으로 예상되고 있다.

〈표 1〉 생체인식 기술 비교

특징	지문	손모양	망막	홍채	얼굴	서명	화자
사용편리성	high	high	low	medium	medium	high	high
에러원인	dryness, dirty, age	hand injury, age	glasses	poor lightning	lightning, age, glasses, hair	changing signature	noise, colds, weather
인식률	high	high	very high	very high	high	high	high
거부감	medium	medium	medium	medium	medium	very high	high
보안성	high	medium	high	very high	medium	medium	medium
영구성	high	medium	high	high	medium	medium	medium

현재 생체인식 기술은 PIN이나 패스워드를 대체하거나 보완하고 있으며 높은 보안을 요구하는 곳으로부터 급속도로 실생활에 사용되기 시작하였다.

2002년 국내생체인식 시장은 870억원으로 예상되고 세계시장은 2005년을 전후하여 20억 달러에 달하며, 매년 30% 이상의 급격한 성장세를 유지할 것으로 전망되고 있다.

최근 고도의 보안을 요구하는 환경에서 생체인식을 사용한 출입통제가 실용화되고 있다. 사무실 또는 빌딩 출입

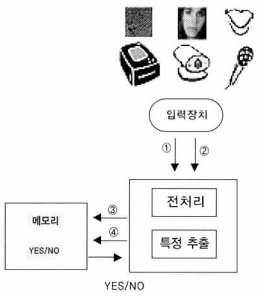
뿐만 아니라 병원, 카지노, 헬스클럽에서 사용되고 있으며 1996년 올림픽에서는 65,000명의 출입통제에 생체인식이 사용되기도 하였다. 특히, 2001년 미국 테러이후 생체 인식 기술이 급속히 보급될 수 있을 것으로 예상되는데, 미국에서는 이민 및 비자발급에 생체 인식 기술 적용을 추진 중이며 국경 보호를 위하여 생체인식 기술의 활용을 의무화하는 법안 즉, 모든 외국인에 대하여 비자 신청 시 생체정보를 요구하고, 비자 면제국들은 여권에 생체정보 저장을 의무화하는 비자면제프로그램 수정안이 법제화되었다. 영국에서도 자국민의 신원 확인을 위해, 향후 4년내에 지문 및 홍채 정보를 저장한 스마트 여권 도입을 검토 중이며, 네덜란드의 Schipol 공항(암스텔담)에서는 경찰청과 이민국 주관의 시험 기간을 거친 '홍채와 스마트카드를 이용한 자동출입국관리(Automated Border Crossing) 시스템'을 본격 도입하기 위하여, 2002년 1월부터 법무부 주관으로 시범 운용 중이다.

〈그림 2〉 생체인식 제품

단순히 생체인식이 비밀번호나 암호를 보완하거나 대체하는 것에 머물지 않고, 최근 급속한 발전을 하고있는 보안토큰이나 PKI(Public Key Infrastructure)와의 연동도 시도되고 있다. 생체인식을 적용하기 위하여 가장 큰 문제는 등록된 생체정보를 어떻게 안전하게 저장하느냐는 것인데, 그 해결책으로 개인이 소지하는 보안토큰에 암호화하여 저장하면 안전하게 저장할 수 있다. 여기에 보안성을 높이기 위하여, 단순히 저장만 하는 것이 아니라 보안토큰 내에서 사용자 인증까지 수행하는 연구도 진행되고 있다.

생체정보와 보안토큰을 연동시키는 방법으로는, 보안토큰 내에 메모리만 있는 경우, 연산 프로세서도 있는 경우, 센서까지 있는 경우에 따라 각각 Store-on-Token, Match-on-Token 및 Sensor-on-Token으로 나눌 수 있다. Store-on-Token 방식은 지문과 같은 생체정보를 중앙 집중식 DB에 저장하지 않고 보안토큰 내의 메모리에 저장한 후, 인증을 요청할 시에 저장된 생체정보를 단말에 보내어 단말기에서 인증을 하는 시스템이다. 반면, Match-on-Token은 저장된 생체정보와 인증 요청용 생체정보 비교를 보안토큰내의 프로세서가 수행하는 것으로, 보안토큰에서는 인증 결과만을 단말 쪽으로 보내는 것이다. 마지막으로, 위 두가지 방식은 생체정보 획득이 단말기에서 이루어지는 반면, Sensor-on-Token은 생체정보 획득이 보안토큰 상에서 이루어진다는 차이가 있다.

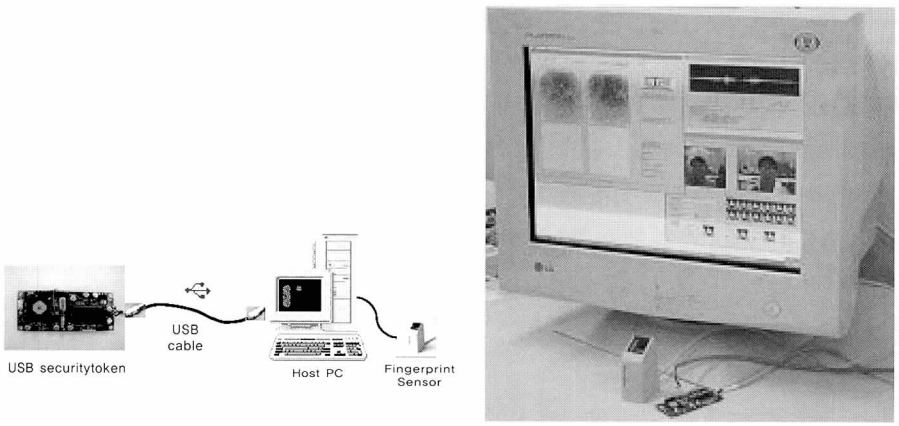
예를 들어, 사용자 생체정보를 중앙 집중식 DB에 저장하는 방식을 택할 경우, 중앙 DB를 유지하고 관리하는데 어려움이 있고 해킹의 위험, 프라이버시의 침해 등의 문제가 발생할 수 있다. 그러므로 개인의 생체정보를 보안토큰(Store-on-Token)에 저장하여 각 개인이 보유하게 함으로써 앞에서 언급한 문제 등을 해결할 수 있고, 인증 절차가 보안토큰 내의 생체정보를 이용하여 단말기에서 수행됨으로써 비용 및 처리 시간을 줄일 수 있는 장점이 있다.



〈그림 3〉
Match-on-Token 시스템

그러나 이 경우 보안토큰은 생체 특징 정보를 저장한 단순한 메모리 기능만 제공할 뿐 사용자 인증 기능을 수행하지 않아, 보안성에 문제가 있다. 즉, 입력된 생체정보에 대한 인식 처리가 단말기내의 프로세서에서 수행되기 위하여 그 생체정보가 단말기로 전송될 때, 정보 누출의 위험성이 있다. 따라서 개인 정보 누출의 위험을 최소화하여 고도 보안 응용에 적용하기 위해서는, 그림 3과 같이 개인의 생체정보를 보안토큰 내에 저장할 뿐만 아니라 보안토큰 내의 프로세서를 이용하여 인식 처리까지 수행함으로써 개인의 정보가 보안토큰 외부로 유출되지 않도록 하여야 한다. 그림 4는 한국전자통신연구원에서 개발한 USB 토큰용 인증용 생체인증 시스템으로 토큰내부에서 지문/얼굴/화자 사용자 인증을 수행하도록 되어있다.

현대 정보화 사회에서 정보는 개인, 기업과 국가의 가장 중요한 자산으로 인식되고 있다. 이러한 정보는 네트워크의 발달로 인해 효과적이고 편리하게 사용이 가능하게 되었으나, 저장된 중요한 정보가 타인에 의해 파괴되거나 도용 당하는 등의 악영향을 피할 수 없는 실정이다. 본 고에서는 이러한 문제를 극복하기 위한 해결책으로 여겨지는 개개인의 고유한 특징에 따라 사람들의 신원을 확인하는 생체인식 기술에 대하여 알아보았다. 또한 실생활에 적용되기 시작한 생체인식 시스템 응용 기술에 대하여 설명하였다. 참고로 생체인식 관련 주요자료를 구할 수 있는 곳은 생체인식포럼(www.biometrics.or.kr) 뿐만 아니라 The Biometric Consortium (www.biometrics.org), Association for Biometrics (www.afb.org.uk), Avanti(homepage.ntlworld.com/avanti), International Biometric Industry Association (www.ibia.org) 등이 있다.



〈그림 4〉 USB 토큰용 생체인증 시스템