생체 인식 보안

지도교수 : 김 윤
연 구 자 : 이 채 영

< 목 차 >

요 약

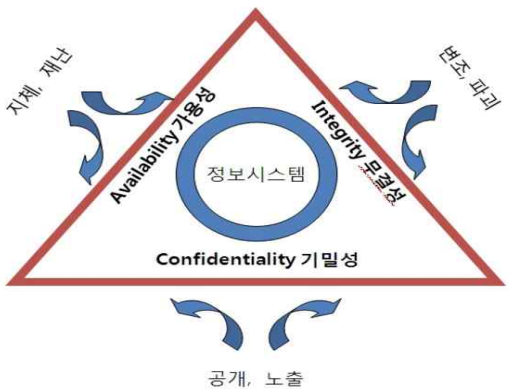
개인을 고유하게 정의하는 생체적 특징에는 여러 가지 방법이 있다. 이런 특징을 포착하고 식별자로 사용하고자 하는 기술들이 도입되고 있다. 본 논문은 정보보안, 생체인식에 대한 개념에 대해 정의하고 여러 생체 인식 기술에 대해 조사 분석한 내용이다.

주요어 : 생체인식, 지문, 보안

1. 서론

1.1. 정보 보안이란

정보 보안 분야에서 생체인 식의 위치와 인증 시스템의 실현방식을 기술한다. 일반적으로 정보 보안의 요소로는 기밀성, 정확성, 가용성이 있다. 기밀성은 정보가 부당한 상대에게 전달되지 않는 것이고, 정확성은 정보의 소실, 변조의 방지이고 가용성은 정보가 필요한 때 이용 가능한 것이다. 여기에 덧붙여 인증도 중요하게 여겨진다. Authenticity라고 하는 것은 서비스를 요구하는 상대방에 적정한가에 대한 본인 인증에 관한 것으로 제 3자에 의한 「대리인 행세」와 「거래 후의 부인」등을 방지하는데 유효한 보호 대책이다. 정보 시스템 기술의 급속한 발전, 특히 개방형 네트워크를 전제로 한 비대면의 상거래가 더욱더 활성화되고 있다. 이것에 의해 사이버 범죄도 증가하고 복잡화되어지는 경향이다. 따라서 정보 시스템에 대한 보호 대책의 강화, 특히 비대면 상거래에 있어서 본인의 인증이 필요하게 된다. 본인인증의 방법으로서는 다음과 같다. 본인 소유물에 의한 인증, 본인이 가지고 있는 지식에 의한 인증, 본인의 신체적 특징에 의한 인증이 있다.



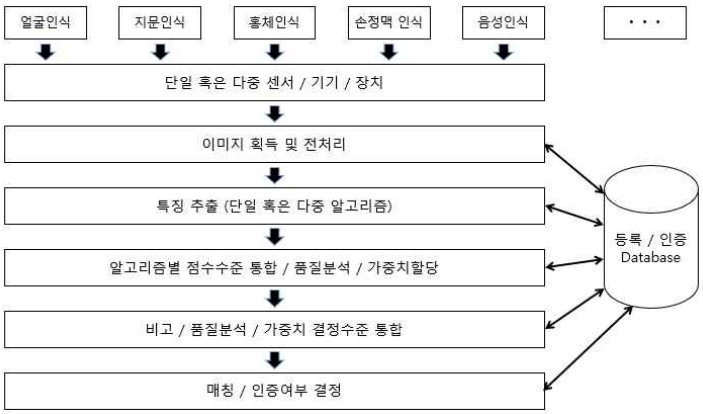
[사진 1] 정보보안 요소

1.2. 생체 인식이란

생체인식 인증기술은 지문, 홍채, 얼굴, 음성과 같은 개인의 신체 고유 정보를 자동화된 수단으로 등록 시 제시한 정보와 비교/판단하는 것이다. 얼굴 모양, 홍채, 망막, 정맥, 지문, DNA 등의 신체적 특성을 이용한 방법과 서명, 음성, 걸음걸이 등의 행동학적 특성을 이용하는 방법으로 분류할 수 있다.

생 체	장 점	단 점	보안	센 서	비용
음성	편리함	노이즈	보통	비접촉	저
얼굴	원격 수집	광조건	보통	비접촉	저
지문	광범위적용	피부조건	양호	접촉	저
홍채	고 정밀도	안경착용	상급	비접촉	고
정맥	고 보안수준	적음	상급	비접촉	저

[사진 2] 생체인식 특성 비교



[사진 3] 다중 생체인식 인증 프로세스

2. 생체 인식의 종류

2.1. 지문

1880년 손가락 끝의 볼록한 부분에 있는 와상의 모양이 세계의 모든 사람이 서로 다르다는 사실이 헨리 폴즈의 학회발표에 의해 알려졌다. 또, 그것들이 말발굽 모양, 소용돌이 모양 등과 같이 몇 가지의 대표적인 범주로 분류될 수 있음을 알았다. 그러나 이 전에도 1685년 피부 무늬에 관한 논문이 있고 1858년에 연금 지불을 적정화하기 위해 지문을 채취해서 본인인증에 활용하였다고 전해져오고 있다. 그 후, 지문 영상의 처리방법으로서 여러 가지 분석 방법이 고안되어졌으며 주로 범죄 수사와 사법 분야에 이용되어 왔다. 이후, 지문인식 기술은 범죄 수사의 정밀도를 높이기 위한 필요성과 함께 연구가 진행되어 기술혁신이 이루어졌다. 지문이나 홍채의 경우, 동일한 경우가 희박하다 생각하기 때문에 흔히 생체 정보를 이용한 보안을 안전하다 생각한다. 지문을 통한 생체 인식 인증은 이제 보편화 된 기술로, 휴대폰이나 노트북, 태블릿 뿐만 아니라 다양한 기기에 광범위하게 사용되고 있다.

지문인식 시스템은 일반적으로 지문 융기의 분기점, 끝점 등으로 구성되는 특징점의 위치와 속성을 추출, 저장, 비교하는 알고리즘을 채용하고 있는데, 땀이나 물기가 스캐너에 배어 있는 경우 오류 발생률이 크게 높아진다는 점, 여러 사람이 연속적으로 접촉한 곳에 자신의 손가락을 댄다는 불쾌감, 지문이 닳아 없어진 사람도 간혹 있다는 점 등이 지문인식 시스템의 한계로 인식되고 있다.

2.2. 정맥 패턴

사람의 손바닥, 손가락, 손등 등을 적외선을 사용하여 혈관을 투시한 후 잔영을 이용해 신분 확인을 하는 것으로 복제가 거의 불가능하여 높은 보안성을 가진다. 사람마다 정맥이 다르고 평생 변하지 않는다는 것이 아직 증명되지 않았으며, 하드웨어 구성이 복잡하고 전체적인 시스템 비용이 커서 활용 범위가 제한된다.

2.3. 얼굴

얼굴을 이용한 인식 방법은 생체인식 방법 중 가장 자연스러운 방법으로, 지문과 같이 지문 입력 장치에 손가락을 접촉하지 않고 비접촉으로 자연스럽게 인식할 수 있는 장점이 있다. 그러나 세월이 흐르면서 생기는 얼굴 변화 등의 약점을 가지고 있다. 얼굴인식에서 가장 중요하고 어려운 문제 중 하나는 입력된 영상으로부터 처리 대상인 얼굴 영역을 추출하는 방법으로, 얼굴의 열상을 이용하는 방식과 2/3차원 얼굴 영상을 이용하는 방식으로 크게 구분된다. 특히, 얼굴의 열 분포를 이용하는 방식은 얼굴 혈관에서 발생하는 열을 적외선 카메라로 촬영, 디지털 정보로 변환해 저장하는 것으로, 얼굴에 외과적인 손상이 발생하더라도 변하지 않는 장점이 있다.

2.4. 손 모양

생체인식 분야에서 가장 먼저 자동화된 기법으로, 스탠포드 대학의 한 연구팀이 개인마다 손가락 길이가 다르다는 점에 착안, 약 4,000명의 손가락 형태를 분석하여 이를 데이터화하여 만든 시스템이다. 이처럼 손 및 손가락의 모양도 사람마다 고유한 특징을 가지므로, 손가락의 길이와 형태를 3차원으로 측정한 기하학적 정보는 수집 및 처리가 비교적 쉽다. 그러나 상대적으로 정확도가 떨어져 보안의 중요성이 그다지 높지 않은 곳에 쓰였다. 즉, 지문이나 눈을 이용하는 시스템에 비해서는 열악한 환경에서도 안정적으로 동작하고 정보 저장량이 적기 때문에 건설 현장이나 야외에서 주로 사용된다.

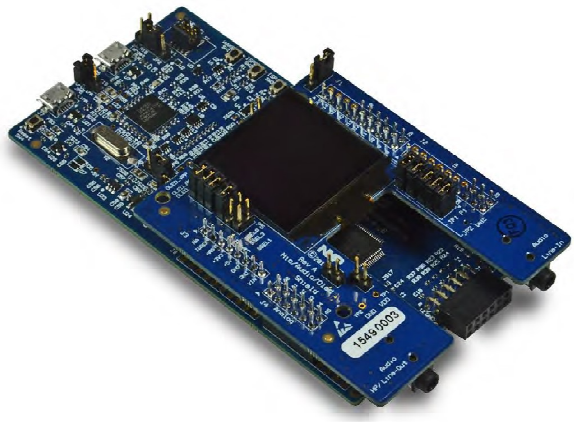
2.5. 홍채/망막

홍채는 까만 눈동자의 안쪽 측으로 부터 동공보다 바깥쪽에 있는 부분을 말하고, 동공의 열린 정도를 조절하는 근육으로 구성된다. 즉, 홍채 외계로부터 안구 내부로 들어오는 빛의 양을 조절하는 기능을 가지고 있는 부분이다. 동공의 부분에 구멍이 열려, 개구부인 동공으로부터 바깥쪽으로 향해서 가오스 형상의 주름이 발생한다고 알려져 있다. 이 주름의 성장은 생후 2년 정도에 멈추고 그 이후 변화하는 경우는 없다. 이러한 이유로 홍채의 무늬는 지문 등과 같이 그 사람의 고유의 패턴이 되고, 동일인의 좌 우 눈도 다르며, 일란성 쌍둥이도 다른 패턴을 갖는다. 홍채인식이라고 하는 것은 디지털 카메라로 촬영한 홍채의 패턴 영상을 데이터화하고 미리 등록되어 있는 본인의 홍채 데이터와 비교조회 하는 것에 의해 개인을 식별하는 것이다. 홍채인식은 인식 정도가 높고 비접촉으로 인식이 가능하며 위조를 하기 어렵다. 또, 홍채는 일생동안 거의 변화가 없기 때문에 재등록을 할 필요가 없다.

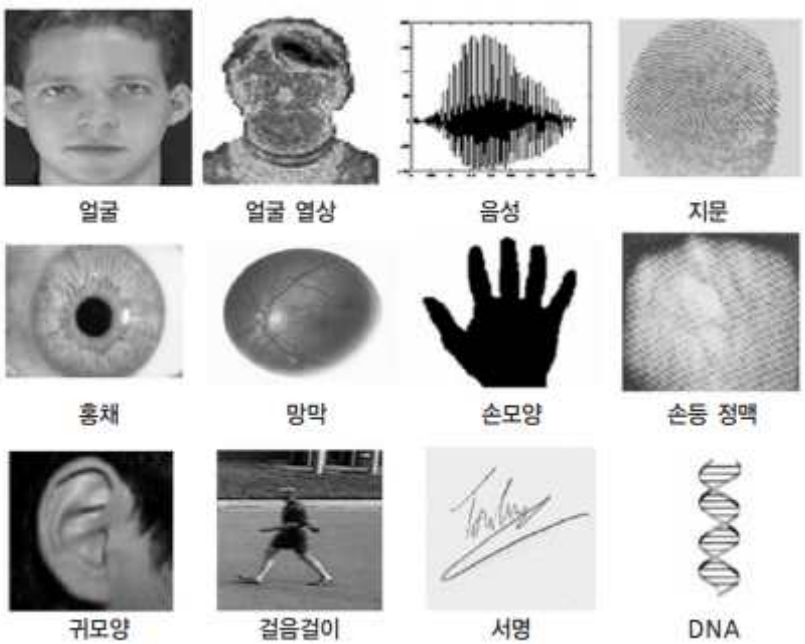
2.6. 음성 인식

목소리도 고유한 식별자가 될 수 있다. 몇몇 스마트폰 제조사들은 이 기술을 사용하고 있으며, 스마트 홈 시스템 업체들도 가전기기 제어에 음성 인식을 사용하는 중이다. 모바일 결

제 업체, 뱅킹 애플리케이션에서도 활용되고, 사용자 계정에 접근하는 것을 확인하기 위해 한 곳 이상의 유명 통신사가 목소리 인식 기술을 사용하고 있다. 음성 인식 기술에는 고수준 알고리즘을 실행해야 하고, 이를 위해 서버가 필요하다. 그러나 칩과 컴퓨팅 기술이 계속 발전하고 있어, 스마트폰의 마이크로프로세서로 기술을 임베딩 할 수 있을 것이다.



[사진 4] 음성 인식 개발 보드



[사진 5] 여러 가지 생체인식 방법

3. 사례

3.1. 생체인식 사례

펜데믹 현상이 이어지면서 생활 속 언택트 비대면 방식이 활성화됨으로서 기존의 지문인식 방식에서 얼굴인식, 홍채인식 등으로 관심이 커졌다. 이에 배달, 택배 서비스 선호도가

꾸준히 상승하고 있다. 이에 비접촉식 인증 방식을 채택하는 곳도 점차 증가하고 있는데, 이번 도쿄 올림픽에서도 일본 NEC가 안면인식 신원 확인 시스템 '네오페이스 워치'를 공급한 게 대표적 사례다. 미 플로리다주에 위치한 디즈니 월드에서도 방문객을 위한 안면인식 시스템을 제공했는데, 이처럼 점차 원거리에서도 사용 가능한 생체인식 보안 시스템이 확산되고 있다. 국내 생체 인식 보안 기업에서도 생체인식 보안 시스템을 출시하고 있다. 하지만 과거 휴대폰에 탑재된 홍채인식과 안면인식 보안이 뚫리는 영상이 공개된 적이 있다. 디지털 카메라로 휴대폰에 입력할 홍채 사진을 직은 뒤 레이저 프린터로 인쇄했다. 안구 곡면은 레이저 프린터로 인쇄한 홍채 사진 위에 콘택트렌즈를 올려 구현했다. 콘택트렌즈를 올린 사진 한 장으로 휴대폰 잠금이 해제되는 것을 볼 수 있었다. 이때 홍채 인식은 지문 인식보다 위험이 높으므로 휴대전화 데이터를 보호하고 결제를 할 경우 생체 인식보다 기존의 핀 방식을 사용하는 것이 더욱 안전하다 말했다. 하지만 기술이 발전함에 따라 지문인식만큼의 보안성을 유지할 수 있게 되었다. 또, 안구 손상이 일어날 확률이 드물기 때문에 지문이 희미해지면 인식할 수 없다는 단점을 보완할 수 있어 더 안전하다는 평가를 받는다. 그러나 보완해야할 단점도 존재한다.

3.2. 생체인식 활용

생체정보를 활용한 서비스가 다양하게 등장하면서 많은 문제가 불거지고 있다. 그럼에도 불구하고 생체정보 활용 서비스가 확장되는 추세는 거스를 수 없다. 생체정보는 다양한 서비스에 사용될 수 있다. 그 중 가장 일반적으로 사용되는 것이 본인인증이다. 출입통제 시스템, 비대면 거래, 온라인 신원확인 등에서 생체정보를 이용하는 것이 일상화됐다. 센서에 지문이나 얼굴을 대면 본인확인이 되기 때문에 복잡한 비밀번호를 입력하거나 별도의 인증 단말을 소지하지 않아도 된다. 비밀번호 없는 세상을 넘어 지갑 없이도 상거래를 할 수 있는 세상이 됐다. 생체정보를 통한 인증을 비밀번호를 대체하는 용도로 가장 많이 사용된다. 데이터 유출 사고의 80%는 데이터 접근 권한이 탈취돼 발생한 것이다. 비밀번호가 제대로 관리됐다면 막을 수 있는 사고다. 그러나 비밀번호를 완벽하게 관리하는 것은 불가능하다. 길고 복잡한 문자·숫자 조합의 비밀번호를 사용하고 자주 바꾼다 해도 비밀번호 유출을 막을 수 없다. 공격자는 봇을 이용해 사용자의 단말을 들여다보면서 어떤 값이 입력됐는지 자동으로 인식해 비밀번호를 빼간다. 무작위로 숫자, 문자를 입력해 비밀번호를 알아내는 부르트포스 공격은 AI를 적용해 한층 더 빠르고 정확하게 비밀번호를 찾아낸다. 다크 웹 등에서 판매되는 개인정보를 이용해 온라인 서비스에 접속한 후 추가 정보를 수집해 고급 개인정보 DB를 완성하기도 한다. 비밀번호의 한계를 해결하기 위해 ID/PW와 OTP를 함께 사용하는 등 2가지 이상 인증 요소를 함께 사용하는 복합인증이 제안된다. 이 방법 역시 사용자를 불편하게 하지만 공격을 어렵게 만들지는 못한다. 비밀번호와 OTP를 입력하는 과정에 중간자 공격으로 거래 정보를 탈취할 수 있다. 생체정보를 이용한 인증은 이러한 한계를 모두 해결해준다. 생체인증은 본인의 생체정보가 입력되지 않으면 본인확인이 이뤄지지 않는다. 공격자가 탈취할 수 있는 비밀번호가 없다. 생체정보는 이미지가 아니라 생체의 특징을 분석해 해시 값으로 저장하기 때문에 유출된다 해도 공격자가 사용할 수 없다. 실리콘 등으로 사용자 생체 정보를 정교하게 위장한다 해도 라이브 한 생체정보가 입력되지 않으면 인증이 이루어지지 않는다.

3.3 지문인식 활용

지문인식은 오래 전부터 가치를 인정받아 사용되어 왔고 지금도 여전히 활발히 사용되고 있다. 지문은 개인마다 모두 다른 고유성을 띄지만 기술의 발전으로 광학적 CMOS 센서를 활용하여 비교적 저렴하게 지문 정보를 포착 비교할 수 있게 되었다. 시드 스튜디오의 그로브 시스템 모듈 제품은 사용이 편리한 빌딩 블록 접근법을 제공해 빠른 개발을 지원한다. 센서는 AS601 임베디드 디지털 신호 프로세서를 채택했다. 이는 지문 식별용으로 개발된 제품이다. 오픈 소스 플랫폼과 연동한 뒤, 윈도우 기반 PC로 연결해 센서의 직렬 포트를 제어할 수 있다. 웹 기반 소프트웨어 개발 플랫폼 깃허브에 저장된 라이브러리와 데이터를 비교할 수도 있다.

낮은 가격대의 지문인식과 스캐닝 센서 모듈도 있다. TTL 시리얼을 사용해 데이터를 통신해 원하는 프로젝트로 모듈을 손쉽게 임베딩 할 수 있다.

[사진 6] 지문인식 모듈

4. 결론

다양한 생체적 특징을 고유 식별자로 사용할 수 있으나, 애플리케이션에 따라 적합한 기술이 달라질 것이다. 항상 고려해야 할 중요한 부분은 데이터 보안이다. 두 가지나 그 이상의 기법들을 결합하면 한 가지만 사용하는 것보다는 훨씬 높은 보안 수준을 달성할 수 있다. 익숙한 얼굴도 조명이 다른 곳에서는 낯설어 보이는 상황이 있다. 예를 들어, 비밀번호와 얼굴 인식 기술을 함께 사용한다면, 나와 닮은 사람이 우연의 일치로 나의 데이터를 보는 일은 막을 수 있을 것이다.

대량의 데이터를 저장하고 처리하는 능력은 계속 향상되고 있기때문에 여러 기법을 결합한 결과를 컴퓨터가 관리하는 것은 점점 쉬워지겠지만, 무단으로 조작하는 능력 또한 고도화될 것이므로 이에 대비해야 한다.

참고문헌

[1] 송영기, 강환일.2004.생체인식의 길.서울:인터비젼
[2] 야마다 신이찌로.2003.알기쉬운 생체인식의 세계.서울:인터비젼
[3] 문기영.“생체인식 기술현황 및 전망,”(한국전자통신연구원 정보보호연구단 생체인식기술 연구원)
[4] 정맥인증.지식백과.2016
https://terms.naver.com/entry.naver?docId=865883&cid=42346&categoryId=42346
[5] 조병철,박종만.다중 생체인식 기반의 인증기술과 과제.The Journal of Korean Institute of Communications and Information Sciences.2015
[6] 서연수.생체인식 기술의 종류와 적용 사례.2020
https://www.epnc.co.kr/news/articleView.html?idxno=95059