생체인식을 이용한 출입통제 시스템에 대한 연구

전하린* 임현지* 사예* 이병권*
*동국대학교 멀티미디어공학과
e-mail:sonic747@dongguk.edu

A Study on Access Control System Using Biometrics

Ha-rin Jeon* Hyun-Ji Im* Sa Ye* Byong-Kwon Lee*
*Dept of Multimedia Engineering, Dongguk University

요 약

기존 아이디-패스워드 방식의 사용자 인증에서 망각, 도난, 분실, 복제의 피해가 증가하자, 그러한 문제가 보완된 새로운 인증 수단인 생체 인증 시스템이 주목을 받기 시작했다. 본 연구에서는 생체 인증 시스템 중 얼굴 인식을 통해 등록된 사용자를 인증, 출입문을 통제하는 방법에 대해 다루었다.

1. 개요

스마트 시대의 도래와 함께 보다 많은 정보가 사이버 망을 통해 전달되고 있다. 그와 동시에 정보 보호의 중요성이 대두되었다. 해킹을 통한 개인 정보의 도난이나 계좌 사기 등의 범죄율은 점점 증가해왔고 그 피해액 역시 이전의 배로 뛰었다.

현재까지 대부분의 사이트에서 사용되는 아이디-패스워드 방식은 인증 수단이 유출될 위험이 크며, 아이디와 패스워드를 잊는 문제, 해킹범이 비밀번호를 바꿔 다시 로그인을 할 수 없는 문제 등이 종종 발생하고 있다.

때문에 망각, 도난, 분실, 복제의 위험성이 적은 새로운 인증 수단의 필요성이 증가했다. 그 중 가장 주목받는 것은 사람의 신체 일부를 이용한 '생체 인식'이다. 사람의 신체는 한 사람당 하나밖에 존재하지 않는 고유한 속성이며, 결코 분실할 수 없다. 그들을 이용한다면 무엇보다 강력한 '개인 인증 수단'을 만들 수 있다. 이미 지문, 홍채를 이용한 생체 인식은 애플의 아이폰, 삼성의 갤럭시 노트7등에서 기기 잠금에 이용된 바 있다.[1][2] 그림 1은 갤럭시 시리즈의 홍채 인식 기능을, 그림 2는 아이폰 시리즈의 지문 인식 기능을 보여준다.

(그림 1) 갤럭시 시리즈의 홍채 인식 기능

(그림 2) 아이폰 시리즈의 지문 인식 기능

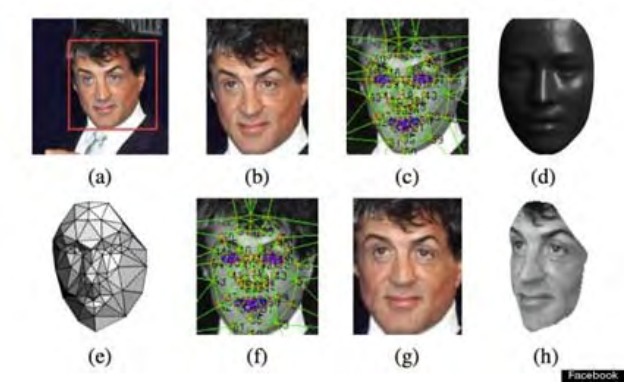
개인의 고유한 속성 중 얼굴은 사람을 구분하는 가장 보편적인 구분 기준이다. 눈의 길이, 코와 입술 사이의 거리, 턱의 길이 등 많은 정보를 보유한 뚜렷한 생체 아이디이기 때문이다. 무엇보다, 얼굴 특징의 파악은 별도의 인식 도구 없이 시각, 즉 '카메라'만으로 확인할 수 있기 때문에 모바일 기기에 적용하기 용이한 인증 수단이다.

실제로 애플 사(社)는 얼굴 인식 기술 '리얼페이스'를 인수함으로써 이후의 아이폰 시리즈에서 얼굴 인식을 도입할 조짐을 보이고 있다. 스마트폰이 대중화되고 있는 현재, 얼굴 인식은 가장 유력한 차세대 인증 시스템으로 떠오르고 있다.

2. 관련 현황

2.1. 페이스북-딥 페이스(Deep Face)

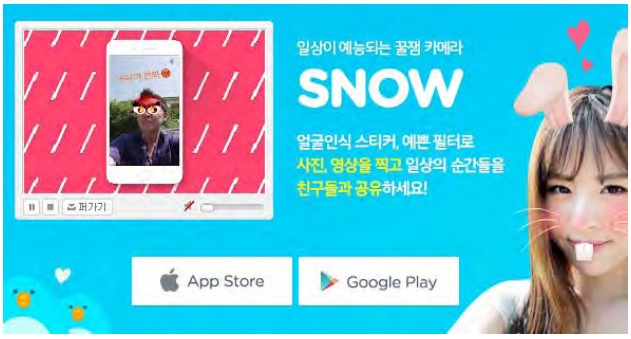
페이스북(Face Book)이 개발하고, 2014년 발표한 인공지능 알고리즘이다. 페이스북 사용자가 SNS상에 업로드한 사진 속 얼굴을 분석해 같은 사람을 연결해 준다. 인간의 눈과 거의 유사한 97.25%의 정확도를 자랑한다. 그림 3은 딥페이스의 영상처리 과정을 보여준다.[3]



(그림 3) 딥페이스(Deep Face)의 원리

(a) 사진에서 얼굴 부분을 인식
(b) 인식한 얼굴 부분을 별도 추출
(c) 얼굴의 주요 부분 67곳에 점을 찍어 델로네 삼각 분할 법으로 얼굴의 윤곽을 나눔
(d) 나눠진 조각을 컴퓨터 작업을 거쳐 3차원으로 변환
(e) 얼굴 특징의 중요도에 따라 밝기를 조절
(f) 67개의 점을 기준으로 3차원 얼굴을 다시 2차원으로 변환
(g) 최종적으로 정면을 바라보는 사진으로 조정

2.2. 네이버-스노우(SNOW) 카메라



(그림 4) 스노우 카메라 소개 영상

그림 4는 스노우 카메라 검색 시 나타나는 소개 영상이다. 전면카메라로 얼굴을 비추면 자신이 선택한 아이템이 얼굴에 재미있게 입혀지는 카메라 어플리케이션이다. 단순히 얼굴에 스티커가 덧붙여지는 것이 아니라, 사용자의 눈, 입의 움직임 등에 따라 스티커가 변화하는 다양한 애니메이션 효과를 제공한다.

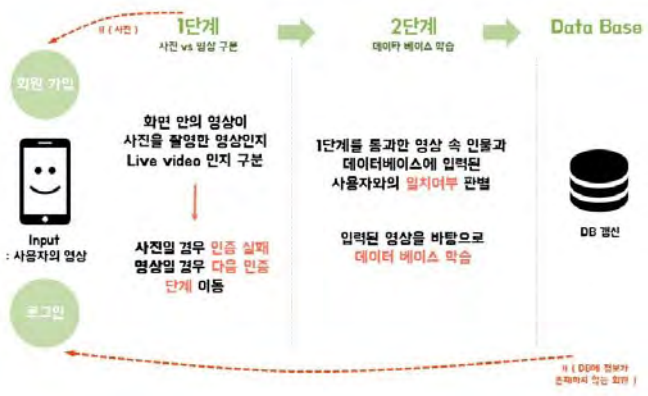
얼굴을 꾸며주는 '스티커'는 단순한 기술은 아니다. 기반이 되는 안면인식기술이 제대로 작용하려면 사용자마다 다른 얼굴형, 눈 크기, 코 높이, 입 모양 등을 추정해 내야 한다. 이를 위해 머신러닝(machine learning)과 윤곽선 정보 훈련이 병행된다.

사람의 얼굴은 높낮이에 따라 밝기가 다르게 나타난다. 스노우는 이러한 패턴을 분석해 얼굴을 인식한다. 이 과정에 머신러닝 기술이 활용된다. 수천만개의 얼굴 데이터가 입력되고 얼굴패턴 인식이라는 결과가 도출되는 과정에서 필요한 알고리즘이 자동 형성되는 것이다. 스노우는 얼굴의 특징이 담긴 영상들의 패턴을 머신러닝을 통해 비교해 보면서 가장 많은 패턴이 일치하는 영역을 얼굴이라고 판단한다. 머신러닝을 통해 알고리즘이 형성되고 윤곽선 정보 훈련 데이터가 쌓일수록 얼굴인식 정확성과 속도가 향상된다.[4]

본 연구에서는 '출입 통제'를 위한 사용자 인증 과정을 다룬다. 이 경우, 사용자가 인증 시에 반드시 얼굴 정면에 카메라가 위치하므로, 딥페이스와 같은 3D 모델링 과정보다 얼굴 정면에서 볼 수 있는 성분을 충분히 활용하고, 그 정보를 학습하는 데에 의의를 둔다.

3. 생체인식 출입통제 시스템

그림 5는 본 연구에서 다루는 생체인식 출입통제 시스템의 절차를 나타낸 것이다.



(그림 5) 시스템 로직

사용자 인증 단계는 크게 회원가입과 로그인 기능으로 구분할 수 있고, 두 기능에 적용되는 주요 기술로는 사진-영상을 구분하는 영상처리와 데이터베이스를 보완해 나가는 기계학습 과정이 있다. 모든 과정에서 영상처리가 기계학습보다 우선적으로 수행되므로 영상처리를 1단계, 기계학습을 2단계로 두었다.

3.1. 1단계 사진-영상 구분

1단계의 목표는 카메라 앞에 사진을 대어 로그인하고자 하는 사용자를 구분해 내는 데에 있다. 화면 안의 영상이 사진을 촬영한 영상인지, 실제 영상인지를 구분해 사진인 경우 인증에 실패해 초기 화면으로 돌아가며 실제 영상일 경우 다음 인증 단계(2단계)로 이동한다.

현재까지 나온 방안으로는 ①영상의 사용자와 배경을 분리해 배경과 사진이 동시에 움직이면 사진이라 판별하는 방법, ②사용자에게 '고개를 돌려라', '눈을 감았다 떠라' 등의 동작을 요구해 행동이 없으면 사진이라 판별하는 방법, ③음성인식을 통해 구분하는 방법 등이다. 다양한 방법을 시도해 보며 가장 효율적인 방법을 채택할 예정이다.[5]

3.2. 2단계 데이터 베이스 학습

2단계의 기능은 1단계를 통과한 영상 속 인물과 데이터베이스에 저장된 회원 목록을 대조해 일치하는 사용자가 있는가를 탐색하는 것이지만, 실질적인 목표는 로그인 기준 자료로써 완벽한 데이터베이스를 만들어내는 시스템의 고안이다.

가장 먼저 최초의 기준 자료가 되는 것은 회원가입시의 사진 이미지이다. 이 이미지는 밝기, 각도 등의 측면에서 이후 들어온 영상과 비교하기 가장 용이한 형태로 변형되어 저장된다.

기존 유사 시스템은 대부분 '기준 데이터'를 정해두고 해당 데이터하고만 비교를 한다. 하지만 그 경우 성장, 주변 조명, 컨디션 난조 등이 고려되지 않는다. 때문에 해당 프로젝트에서는 로그인을 성공할 때 마다 정보를 갱신, 기준 데이터의 변경으로 보다 적합하게 사용자 인증이 이뤄질 수 있도록 '로그인 기준'이 될 수 있는 기준 데이터를 설정한다.

이후 기준 데이터와 비교해 로그인이 성공하면, 사용자는 학습 과정을 이행할 수 있고, 로그인 시에 전달된 영상은 데이터베이스로 전달되어 기준 자료와 비교, 기준 자료의 추가, 변형 등을 통해 사용자 인식률을 높인다.[6][7]

4. 결론

해당 시스템은 '로그인 어플리케이션'의 형태로, 이후 다양한 어플리케이션과 융합될 수 있다. 특히 철저하게 정보를 보호해야하는 금융 어플리케이션이나, 회원제로 운영되는 학생·직원용 어플리케이션 등의 사용자 인증 단계에서도 유용하게 이용될 것이다. 필요한 인식 장치는 전방 카메라뿐인 것 역시 모바일 적용을 용이하게 해준다.

가장 효과를 기대하는 측면은 단연 '보안 강화' 측면이다. 개인의 얼굴은 해킹을 한다 하여 쉽게 가져올 수 있는 정보가 아니다. 특히 해당 어플리케이션은 실제 영상과 사진을 구분하기 때문에 사진을 구해 이용하는 것 역시 불가능하다. 기존의 출입통제 방식인 카드키, 비밀번호 방식 또 대부분의 어플리케이션에서 이용되는 아이디-패스워드 방식에 비해 월등한 보안 효과를 낼 것으로 예상된다.

신원 도용은 2014 년에만 1,760 만명이 피해를 입은 매우 지속적인 문제이다. 이후 신체 인증 시스템을 이용하면 62%가까이 데이터 침해 사고를 방지할 수 있다는 조사 결과가 나왔다.[8] 이러한 측면에서 보안 강화와 피해액 절감을 기대해 볼 수 있다.

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음 (2016-0-00017)

This research was supported by the MISP(Ministry of Science, ICT & Future Planning), Korea, under the National Program for Excellence in SW)(2016-0-00017) supervised by the IITP(Institute for Information & communications Technology Promotion)

참고문헌

[1] 허란, "비밀번호가 사라진다?…갤럭시노트7 '홍채인식' 기능에 관심 증가", Focus News

[2] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, Konstantin Beznosov, "On the Impact of Touch ID on iPhone Passcodes", Symposium on Usable Privacy and Security, 2015

[3] Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, Lior Wolf, "DeepFace: Closing the Gap to Human - Level Performance in Face Verification", Neural Network, 2014

[4] 김나영, "1020 여성 취향 저격 '스노우' 비밀병기는 무엇?", 서울경제-바이오&ICT, 2016

[5] Dominik Jelsovka, Robert Hudec, Martin Breznan, Patrik Kamencay, "2D-3D face recognition using shapes of facial curves based on modified CCA method", Radioelektronika (RADIOELEKTRONIKA), 2012

[6] D. Datcu and L.J.M. Rothkrantz, "MACHINE LEARNING TECHNIQUES FOR FACE ANALYSIS", Interactive Collaborative Information Systems (ICIS)

[7] Joshua Kopsten, "Machine learning algorithm can identify your face even if it's partially hidden", Futuristech Info, 2016

[8] Ryan Davis, "Biometric Security and Surveillance: More than the Subject of Science Fiction", Video Surveillance, 2017