Journal of KIIT. Vol. 15, No. 12, pp. 147-156, Dec. 31, 2017. pISSN 1598-8619, eISSN 2093-7571 147
http://dx.doi.org/10.14801/jkiit.2017.15.12.147

다중 생체인식 알고리즘을 적용한 개인 인증 시스템

임 대 환*

Personal Authentication System Using Multimodal Biometric Algorithm

Dai-Hwan Lim*

본 연구는 2017학년도 서경대학교 교내연구비 지원에 의하여 이루어졌음.

요 약

본 논문에서는 다중생체신호를 이용한 실시 간 모바일 개인 인증 시스템을 개발하였다. 이용된 다중생체신호는 얼굴과 눈, 지문, 그리고 PIN입력을 사용하였다. 이용된 생체신호의 Face recognition 알고리즘은 Raw Data에서 특정 채널만 추출하여 얼굴을 검출하고 노이즈를 제거하기 위하여 Median filtering을 적용하였고, Eye Detection은 학습된 사용자의 눈의 위치 및 시선을 현재 사용자와 비교하여 인증하는 알고리즘을 적용하였다. 지문은 그래디언트 기반의 인식 알고리즘을 사용하여 특징과 지문 영역 추출하여 인증에 사용하였다. 이를 통하여 세계 최초의 16개 조합의 인증 알고리즘이 구현되어 단일 인증 방법 대비 향상된 보안 인증시스템을 구현하였다.

Abstract

In this paper, a mobile personal authentication system was developed using multimodal Biometrics signals. The multimodal Biometrics signals used were used with facial, eye, fingerprint, and PIN input. In the biological signal used, the Face Correction algorithm extracted only a specific channel from the raw data to detect faces and Median Filtering was applied to eliminate noise. The Eye Detection algorithm is applied to compare the eye position and eye line of the learned user with the current user. The algorithm used for fingerprint recognition is based on gradient-based fingerprint recognition algorithm. The fingerprint area and features are extracted through this, 16 combination algorithm that can perform real-time authentication processing for the first time in the world has been developed.

Keywords
certification, biometric, identification, fingerprint, face recognition, eye recognition, multimodal biometrics

* 서경대학교 컴퓨터공학과 교수
- https://orcid.org/0000-0002-0749-7983

· Received: Oct. 11, 2017, Revised: Nov. 18, 2017, Accepted: Nov. 21, 2017
· Corresponding Author: Dai-Hwan Lim
Computer engineering , Seokyeong University, Republic of Korea
Tel.: +82-2-940-2911, Email: jpeace1226@gmail.com

Ⅰ. 서 론

최근 사물인터넷 환경과 더불어 다양한 분야의 모바일 디바이스의 기술이 발전하면서 모바일 디바이스 수요가 급속도로 확대되고 있다. 이러한 모바일 디바이스는 다양한 인터페이스를 통하여 시간과 장소 등에 제안을 받지 않고 웹 서핑과 쇼핑, 금융 등과 같은 다양한 환경에 사용되도록 개발되고 있다. 이러한 사물인터넷 환경에 최적화된 모바일 디바이스의 활성화로 인하여 유선 인터넷 환경에서 이슈가 되었던 보안 사항들이 모바일 디바이스 환경에서도 발생하면서 또 다른 보안 요구사항이 되고 있다. 이에 따라 PC 환경에서 사용되었던 다양한 생체 인식(얼굴, 지문, 음성 등)기술들이 모바일 환경에서도 사용자의 개인 인증을 위한 생체인식기술로 사용되고 있다. 현재 모바일에서 가장 많이 활용되고 있는 기술로는 지문인식, 얼굴인식, 홍체인식등이 활용되고 있다[1]-[4].

최근 주로 사용되고 있는 지문인식 기술은 도어락 시스템, 사무실 출입관리, 노트북, 프리미엄급의 스마트폰과 같은 고급 모바일 디바이스 등에서 개인 인증을 위한 방법으로 이용되고 있다.

더불어 최근의 금융분야에서 이슈화되고 있는 핀테크와 같은 분야에서 모바일 디바이스의 지문인식 기술을 활용하여 개인 인증 수단으로 사용되고 있다. 이러한 생체인식은 기존의 숫자등을 활용한 인증 시스템보다 간편하고 보안성 또한 높다.

그렇지만, 이러한 생체 인증 또한 최근에는 다양한 방법을 통하여 해킹되는 사례가 빈번하게 발생하고 있다. 이러한 생체인증 데이터가 한번 유출되면 기존의 비밀번호나 공인인증서와 달리 수정이 불가능해 더욱 위험할 수도 있다[5].

이러한 이유로 스마트폰과 같은 모바일 디바이스에서 보다 강력한 보안 인증 절차가 요구되기도 하고 있으며, 공인인증서의 경우도 복잡한 2단계 암호 입력 절차 및 OTP(One Time Password, 일회용 패스워드) 코드 입력, 공공 아이핀 입력등의 외우기 힘들고 복잡한 인증 방법을 요구하고 있으며 많은 사용자들의 불만 또한 높아가고 있다. 이로 인해 최근 사용자들은 보안과 사용자 편리성의 측면, 두 가지 관점을 모두 만족할 수 있는 새로운 인증 방법을 요구하고 있다.

이에 기존의 복잡하고 번거로운 방법보다 안전하고 신뢰할 수 있는 사용자 인증방법으로 복합 생체인증 기술이 부각되고 있다. 복합 생체 인증의 경우 기존 2단계 다양한 문자를 사용한 암호등을 사용자가 기억하거나 항상 소지할 필요가 없으며, 기존의 한가지 생체 인증을 통한 개인인증 보안 방법보다 높은 보안 성능을 제공할 수 있으며, 보안성을 더욱 더 강화한 복합생체인식 기술을 요구하고 있다[6].

본 논문에서는 이러한 복합생체인식 기술로서 간편한 인증 절차와 보안성이 강화된 개인 인증을 위한 복합생체인증 알고리즘을 개발하였으며 이를 통하여 보안과 사용자 편리성, 두 가지 관점을 모두 만족하는 개인 인증 시스템 구현을 제안한다.

Ⅱ. 관련 연구

2.1 지문인식

생체인식기술의 하나로 사람 각 개인마다 특징적으로 갖고 있는 지문을 통해 사용자를 인식하는 방법이다. 지문인식기술을 사용하기 위해서 사용자는 먼저 자신의 지문을 시스템에 등록해야 한다. 등록된 지문은 등록한 사람의 이름 혹은 다른 개인정보와 함께 저장된다. 이후 사용자가 자신의 지문을 입력하면 전에 등록되어 있던 사용자의 지문과 비교를 함으로써 시스템이 인지하여 그 사람을 인식한다. 지문인식기술이 적용된 기기는 다른 생체인식기술을 적용한 기기에 비해 가격이 낮으며, 인식하는 속도가 빨라 많이 사용되고 있는 추세다. 적용 범위는 출입통제, 근태관리, 빌딩통합시스템, 금융자동화기기, 컴퓨터보안 분야, 전자상거래 인증, 공항정보시스템 등 다양하다[7].

2.2 얼굴 인식

사람 얼굴의 대칭적인 구도, 생김새, 머리카락, 눈의 색상, 얼굴 근육의 움직임 등을 분석해 얼굴의 특징을 알아내는 작업을 말한다. 실물 또는 사진 속의 얼굴을 인식할 수 있으며 얼굴 모양새를 통해 성별과 나이도 인지해 낼 수 있다. 정지된 얼굴뿐

아니라 웃는 표정을 포함한 얼굴 요소의 움직임과 근육의 변화도 파악하는 방향으로 진화하고 있다. 홍채 · 정맥과 함께 대표적인 생체 인식 기술 중 하나로 손꼽힌다. 얼굴 인식은 분실이나 복제될 우려가 없다는 점에서 최근 차세대 신원확인 시스템으로 주목 받고 있다. 출입관리를 위한 보안에 가장 빠르게 확산되고 있으며 유통산업에서 맞춤형 홍보에도 적용되고 있다.

보안 시스템에는 사람을 식별해 비관계자 출입을 막는 기술이 주로 적용되며 홍보에는 남녀 성별과 나이 등을 인지해 다른 광고물을 보여주는 방법 등이 쓰인다. 미세한 근육 움직임을 파악해 서비스를 사용하는 사람의 감정을 분석하는 데도 쓰이고 있다.

2.3 홍체 인식

지문인식기술에 이어 등장한 보안 시스템으로 사람마다 고유한 특성을 가진 안구의 홍채 정보를 이용해 사람을 인식하는 기술 또는 그러한 인증 체계를 일컫는데 1980년대에 미국에서 처음으로 소개되었다. 지문보다 많은 고유한 패턴을 가지고 있고, 안경이나 렌즈를 착용해도 정확히 인식할 수 있으며, 비접촉 방식이라 거부감이 없는 것이 장점이다.

사람의 홍채는 생후 18개월 이후 완성된 뒤, 평생 변하지 않는 특성을 가지고 있다. 홍채 패턴은 한번 정해지면 거의 변하지 않고, 또 사람마다 모양이 모두 다르다.

홍채인식은 사람마다 각기 다른 홍채의 특성을 정보화해 이를 보안용 인증기술로 응용한 것이다. 즉, 홍채의 모양과 색깔, 망막 모세혈관의 형태소 등을 분석해 사람을 식별하기 위한 수단으로 개발한 인증방식으로, 1980년대에 미국에서 처음으로 소개되었다.

홍채의 패턴을 코드화해 이를 영상신호로 바꾸어 비교·판단하는데, 일반적인 작동 원리는 다음과 같다. 먼저 일정한 거리에서 홍채인식기 중앙에 있는 거울에 사용자의 눈이 맞춰지면, 적외선을 이용한 카메라가 줌렌즈를 통해 초점을 조절한다. 이어 홍채 카메라가 사용자의 홍채를 사진으로 이미지화한 뒤, 홍채 인식 알고리즘이 홍채의 명암 패턴을 영역별로 분석해 개인 고유의 홍채 코드를 생성한다. 마지막으로 홍채 코드가 데이터베이스에 등록되는 것과 동시에 비교 검색이 이루어진다.

지문보다 많은 고유한 패턴을 가지고 있고, 안경이나 렌즈를 착용해도 정확히 인식할 수 있으며, 비접촉 방식이라 거부감이 없는 것이 장점이다. 또 처리 속도가 길어야 2초 정도밖에 걸리지 않아 지문이나 망막인식 기술보다 한 단계 진보한 생체인식 기술로 평가받는다. 적용범위는 출입통제, 근태관리, 빌딩통합시스템, 금융자동화기기, 컴퓨터보안 분야, 전자상거래 인증, 공항정보 시스템 등 다양하다[8].

시선 인식은 영상처리 분야에서 사용자의 눈을 검출하는 방법은 오래전부터 활발하게 연구되고 다양한 응용분야에서 활용되고 있다. 그 예로 자동차에서 사람의 눈 움직임을 검출하여 졸음운전을 방지하는 시스템, 그리고 생체인식 관련연구 중 사람의 홍채 정보를 이용한 보안시스템 등 사용자의 편의성을 고려한 비 접촉식 시스템에서 활발하게 연구가 진행되고 있다. 특히, 실시간의 눈 검출에 관련된 CAMShift기법과 Adaboost기법이 사용되고 있다.

CAMShift알고리즘은 전체 영상에서 물체가 존재할 영역을 예측하여 물체를 검색할 중심위치를 검색영역으로 지정하여 물체를 검색 한다. CAMShift 알고리즘에서는 물체의 크기 및 각도를 계산하여 매 프레임 마다 탐색윈도우의 크기가 정해지기 때문에 물체의 크기의 변화에 상관없이 검출이 가능하다. 하지만 이전 영상의 아무런 정보 없이 검색영역을 예측 하기란 불가능하다[9][10].

2.4 음성 인식

음성인식기술은 컴퓨터가 마이크와 같은 소리 센서를 통해 얻은 음향학적 신호(Acoustic Speech Signal)를 단어나 문장으로 변환시키는 기술을 말한다. 음성인식기술은 일반적으로, 음향 신호를 추출한 후 잡음을 제거하는 작업을 하게 되며, 이후 음성 신호의 특징을 추출하여 음성모델 데이터베이스와 비교하는 방식으로 음성인식을 하게 된다. 음성인식기술 역시 센싱과 데이터 분석 기술이 결합하여 있기는 하지만, 측정하고 분석해야 하는 데이터가 음성 데이터 하나라는 점에서 보다 손쉽고 정확하게 사람의 의도를 파악할 방법으로 알려졌다[11].

음성인식기술을 바탕으로 한 다양한 음성인식 서비스들은 2000년대 후반에 본격적으로 소개되기 시작했다. 대표적인 것이 2011년에 출시된 애플의 음성 기반 개인비서 서비스인 '시리(Siri)'다. 시리는 아이폰 사용자의 음성명령을 바탕으로 모바일 검색은 물론, 일정관리, 전화 걸기, 메모, 음악 재생 등 다양한 생활편의 서비스를 제공하는 개인비서 서비스다. 애플의 시리 출시 이후, 구글은 '구글 나우(Google Now)', 마이크로소프트는 '코타나(Cortana)'와 같은 음성인식 기반의 개인비서 서비스를 출시했으며, 일본의 NTT도코모는 '샤베테콘쉐루(しゃべってコンシェル)'라는 외국어 통역 서비스를 출시하기도 했다. 최근에는 SKT의 "누구"와 KT의 기가 "지니" 등이 대표적인 음성인식 기술을 기반으로 한 서비스 장치(Service Device)이 출시되고 있다.

2.5 OTP

OTP를 이용한 인 증방식은 기존의 아이디 패스워드 인증방식에서 문제가 되었던 패스워드 재사용 공격, 키로거(Keylogger) 프로그램을 이용한 패스워드 탈취 공격 등으로 부터 안전성을 제공할 수 있어 금융권의 전 자금융거래, 기업체 사내정보시스템의 접근통제, 인 터넷포털 사이트의 사용자 인증 등 민감한 자원을 다루는 분야에서 많이 사용되고 있다. OTP 이외의 사용자 인증 수단으로는 사용자 아이디 및 암호를 이용한 방식, 추가적인 질의응답을 이용한 방식 등 여러 가지가 있는데, 대부분 한 번 인증 값이 유출되고 나면 인증 값을 바꾸기 전에는 해킹을 당하기 쉽다는 문제점을 가지고 있다. 이를 보완하기 위한 인증 수단으로 보안 카드가 있지만, 이 역시 정해진 수십여 개의 번호를 사용할 뿐이므로 여전히 유출에 의한 위험성을 가지고 있다[12].

III. 제안 시스템

3.1 Biometrics 패턴 알고리즘을 적용한 복합 개인 인증 시스템 개발

생체인증은 식별성이 높고 위변조가 어려워 간편 인증의 범용 인증수단으로 수요가 높으나, 인증기술은 위변조에 대응하고 범용성, 편의성, 보안성 등의 시장경쟁력을 만족시켜야 하는 새로운 문제 직면하고 있다.

본 논문에서는 이러한 요구사항을 바탕으로 생체(Face, Fingerprint, Eye) 인증과 PIN인증을 융복합 처리하는 간편인증 시스템을 설계하고 개발하였으며, 개발된 시스템은 인증 시스템 강화를 위하여 최근 각광을 받고 있는 인공지능(A.I.)의 핵심인 머신러닝 알고리즘을 적용하여 범용성, 보안성, 편리성의 3가지 특징으로 개발된 국내외 최초 사용자 다중 생체인증 알고리즘을 적용한 개인 인증 시스템이다.

본 논문에서 제안된 시스템은 다음과 같이 다중 생체인증 알고리즘을 구성하기위하여 Face recognition 알고리즘, Eye recognition 알고리즘, 그리고 Fingerprint 알고리즘을 개발 적용하였다.

먼저, Face recognition 알고리즘은 그림 1과 같은 구조로 개발되었다. Face Detection은 Raw Data에서 특정 채널만 추출하여 얼굴을 검출하도록 구성되어져 있다. 성능을 위하여 감마 보정을 통하여 조도를 향상 시켰으며, 노이즈를 제거하기 위하여 Median filtering을 적용하였고, 영상 내, 선, 면, 코, 에지 등의 특징을 히스토그램을 통해 특징 점을 표현하기 위하여 LBP를 사용하였다. LBP는 center pixel(M)을 기준으로 8개의 neighbor pixels의 비교하여 구성하도록 8bits로 표현하고, 3*3 영역의 형태로 사용되었다.

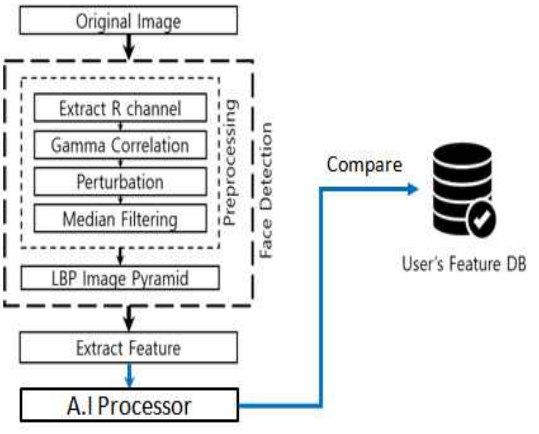
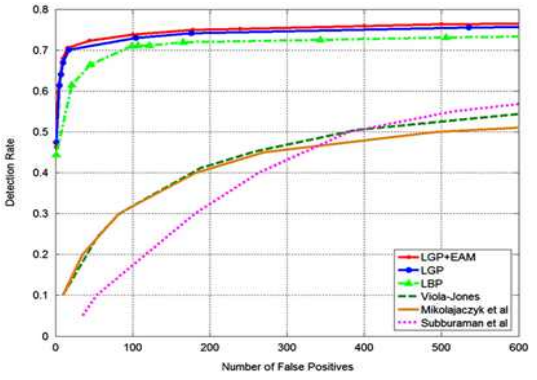


그림 1. 얼굴 인식 알고리즘 블록도
Fig. 1. Face recognition algorithm block diagram

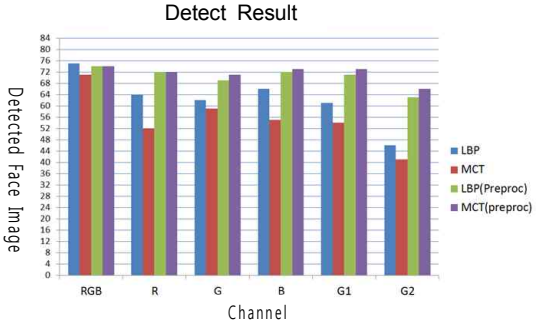
<FDDB database>



<LBP, LGP>

그림 2. 얼굴 검출 성능

Fig. 2. Face detection performance



Bayer Channel detect (R.B channel)

	Extraction channel(R,B)
Extract channel(R,B)	0.667
Transpose	0.872
Flip	0.069
Total	1.663

LBP vs MCT Speed compare

	Original	Preprocessing
LBP	4.2	19.6
MCT	4.1	19.4

그림 3. 얼굴 검출 결과 및 속도

Fig. 3. Result of face detection and speed

그림 2에서와 같이 Face 검출 성능은 LGP(Local Gradient Patterns)는 LBP에 비해 검출 성능은 높지만, 처리 속도가 느리기 때문에 본 연구에서는 LBP를 사용하였다. LBP+Adaboost를 이용한 얼굴 검출은 조명변화에 강인하고, 고속 처리가 가능한 장점을 가지고 있다. 머신 러닝을 위한 학습 데이터로는 Positive 영상 40만장, Negative 영상 60만장 사용하였고, 학습은 약 하루 소요되었다. Cascade는 4단계로 구성하였고, 각 스테이지의 특징 수는 각 [26, 60, 144, 360]로 사용 하였다. 평가는 FDDB를 이용하였고, 기존 연구들에 비해 성능이 우월하다.

그림 3은 본 논문에서 설계한 Face Recognition 검출 결과와 검출 속도를 보여주고 있다. 테스트 DB는 총 84장의 DB를 이용하여 평가하였다. Face Recognition 테스트를 위하여 구축한 DB에서 역광, 얼굴 포즈 기울임, 저조도, 폐색에 대한 영상들의 경우 RGB 채널에서도 검출 되지 않았다. 인식 속도는 MCT(Modified Census Transform)와 비교를 하였다. 기존의 MCT보다 다소 우수한 인식 속도를 보여주었다. 평가 환경은 Intel® CoreTM i7 CPU, 16.0GB, Window OS, 1980x1200 Raw Data로 구성하였다.

이를 통해서, 본 연구에서는 Face Detection 알고리즘을 이용하여 얼굴 검출 부분에서 조명변화에 강인하고, 고속 처리가 가능하도록 구성하였으며, 이를 위한 평가는 FDDB를 이용하였고, 기존 연구들에 비해 성능이 우월한 결과를 가져올 수 있었다.

Eye Detection은 학습된 사용자의 눈의 위치 및 시선을 현재 사용자와 비교하여 인증하는 알고리즘을 적용하였다. 그 구조는 그림 4와 같다. Eye 검출의 위해서는 먼저 두개의 Sub-regions 나눈 후 영상 피라미드를 만든다. 그 후 그림 5와 같이 Eye 후보군을 선택하고 가장 높은 누적 교차수를 선택하게 된다.

Raw data에서의 Eye 검출은 RGB/R/G/B/G1/G2 channel에서 수행하였다 검출 결과는 그림 6과 같이 대부분의 채널에서 비슷한 성능을 보여주었다. 데이터베이스는 ID는 1,521 gray level 저수준 images가 사용되었으며, ColorFERET은 정면 및 대체 정면 포즈가 있는 2,722개의 얼굴 이미지를 사용하였다.

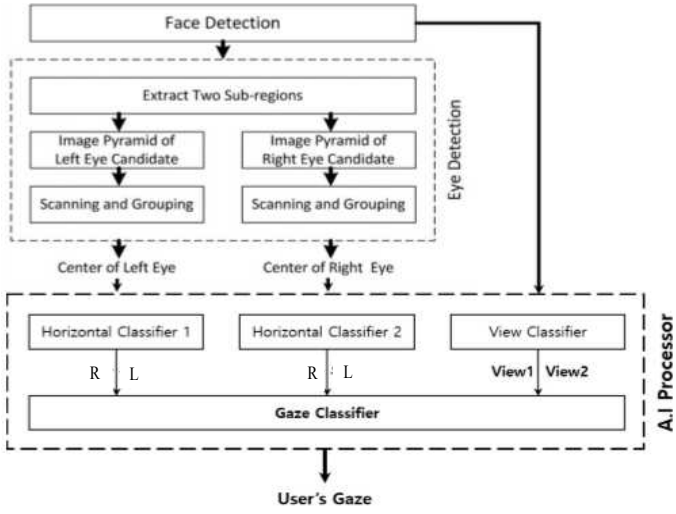


그림 4. 시선인식 알고리즘 구조도
Fig. 4. Eye recognition algorithm block diagram

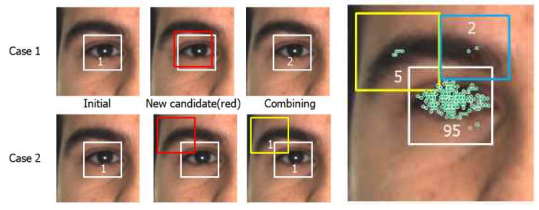


그림 5. Eye 후보군 선택
Fig. 5. Selecting eye candidate group

Criterion (err)	Accuracy	Criterion (err)	Accuracy
0.01	0.24	0.14	99.61
0.02	6.6	0.15	99.61
0.03	19.89	0.16	99.61
0.04	44.71	0.17	99.63
0.05	66.06	0.18	99.69
0.06	81.03	0.19	99.71
0.07	88.99	0.20	99.71
0.08	93.74	0.21	99.71
0.09	96.41	0.22	99.71
0.10	97.67	0.23	99.71
0.11	98.56	0.24	99.74
0.12	99.19	0.25	99.74
0.13	99.45		

GrayFERET

Criterion (err)	Accuracy	Criterion (err)	Accuracy
0.01	1.31	0.14	98.75
0.02	17.42	0.15	99.15
0.03	42.34	0.16	99.28
0.04	62.59	0.17	99.34
0.05	79.29	0.18	99.34
0.06	87.31	0.19	99.54
0.07	91.65	0.20	99.67
0.08	94.02	0.21	99.8
0.09	95.73	0.22	99.8
0.10	96.84	0.23	99.8
0.11	97.63	0.24	99.87
0.12	98.03	0.25	99.87
0.13	98.29		

BioID

BioID

Method	err				
	0.03	0.05	0.07	0.10	0.25
LBP	48.13	81.20	92.44	97.11	99.28
MCT	**51.02**	**84.48**	**93.69**	**96.98**	**99.34**
MB-MCT	**63.64**	**87.57**	**94.67**	**97.83**	**99.67**
Campadelli	N/A	80.70	N/A	93.20	99.40
Valenti	N/A	86.09	N/A	91.67	98.00

ColorFERET

Method	err				
	0.03	0.05	0.07	0.10	0.25
LBP	17.15	61.62	87.43	97.93	100
MCT	**17.66**	**65.23**	**90.59**	**98.47**	**100**
MB-MCT	**23.92**	**69.01**	**91.44**	**98.24**	**99.91**
Campadelli	N/A	67.00	N/A	89.50	96.50
Valenti	N/A	74.38	N/A	96.27	99.17

그림 6. Eye 검출 결과
Fig. 6. Eye detection performance

지문인식 알고리즘은 그림 7과 같이 개발되었다. 지문인식에 대한 작동 원리는 다음과 같다. 특히 본 논문에서 개발된 지문인식은 효과적인 인증을 위하여 지문인식과 무작위로 생성되는 난수의 일회용 패스워드를 이용하는 사용자 인증 방식중의 하나인 OTP를 적용하여, 보안상 발생할 수 있는 다양한 취약점을 극복할 수 있도록 하였다. 지문은 지문 융선 방향으로 정보를 추출하여 지문을 인식하도록 개발되었다. Fingerprint recognition (OTP) method 작동 원리는 다음과 같다. N개의 Fingerprint에 대한 Randomic Request를 다음의 과정으로 진행된다.

1. 현재 지문 인식 기계 + 지문 OTP S/W (지문 n 개 등록)
2. 인증 시 Randomic한 Fingerprint 요청
3. 요청된 지문 ID 확인 (기존 방식의 보안)

지문인식을 위하여 사용한 알고리즘은 그래디언트 기반의 인식 알고리즘을 사용하여 지문의 특징을 추출하고 지문 영역 추출하였으며, 요구된 지문 ID 확인을 위한 주요 과정은 그림 8에서와 같이 진행된다[13]. 먼저 랜덤으로 요청된 지문과 등록된 지문 비교한다. 이 부분에서 3번 불일치 시 두 번째 랜덤 등록 지문 요청하고 Request된 등록 지문 불일치 시 자동 Lock 기능이 수행된다. 비교 일치 시 본인인증이 되면 인증에 성공하게 된다.

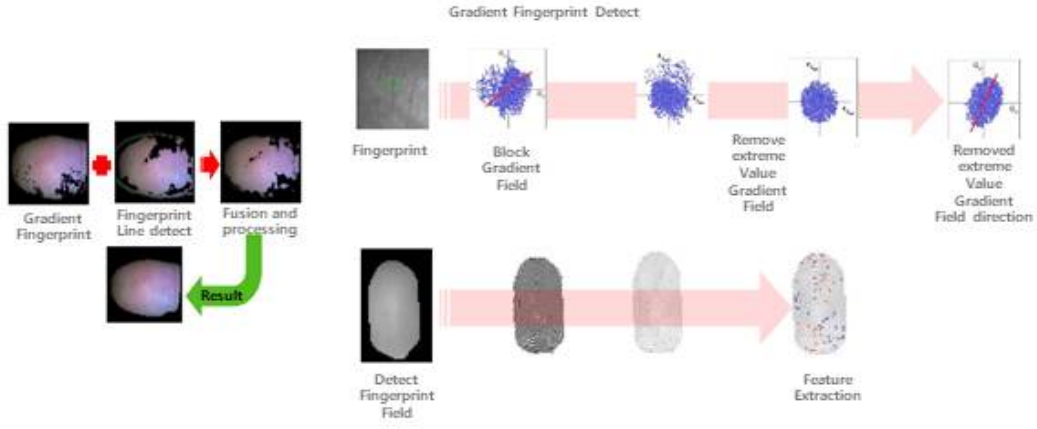


그림 7. 지문인식 알고리즘 작동원리
Fig. 7. Fingerprint recognition method

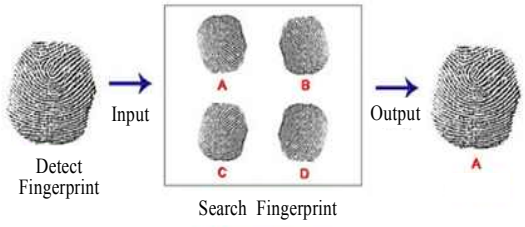


그림 8. 지문인식 알고리즘 핵심 진행과정
Fig. 8. Fingerprint recognition core flower

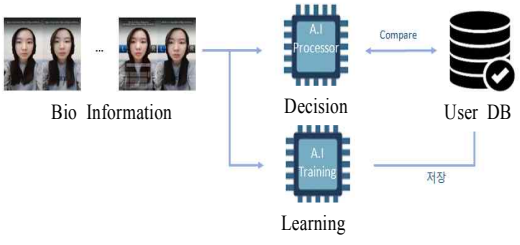


그림 9. 인공지능 알고리즘 적용
Fig. 9. AI processor apply

마지막으로 일반적으로 사용되는 PIN번호 입력 방식을 추가하여 사용자가 제시된 인증 알고리즘을 선택하여 인증할 수 있도록 구현하였다.

본 논문에서는 개발된 인증 시스템을 더욱더 효과적으로 사용하기 위하여 그림 9와 같이 지능형 알고리즘을 적용하였다. 적용된 AI Processor는 Face와 Eye 검출에 사용되었다. 사용자의 생체 정보를 학습하고 이를 통해 사용자 인증에 대한 정확성을 높여주고 보안성을 강화하도록 구성하였다.

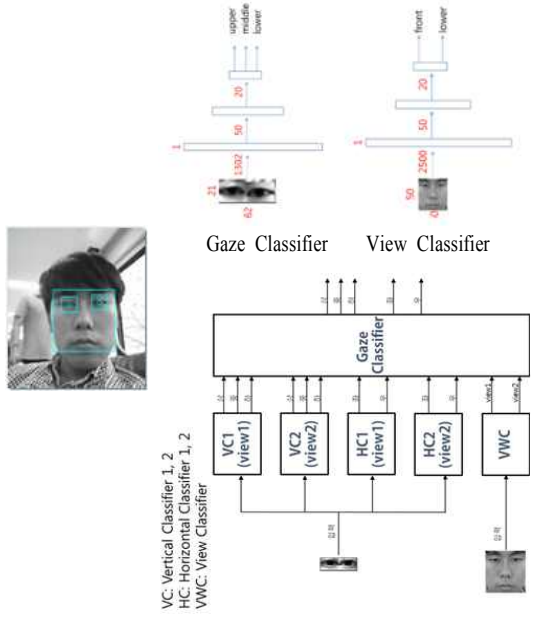


그림 10. Neural Network 구조
Fig. 10. Neural network structure

적용된 AI Processor의 Neural Network 구조는 그림 10과 같이 시선 분류기와 View 분류기로 구분하였다. 분류기는 정면 뷰에서의 상중하 분류기, 하단 뷰에서의 상중하 분류기, 정면 뷰에서의 좌우 분류기, 하단 뷰에서의 좌우 분류기, 정면 뷰, 하단 뷰 분류기로 구성되며 Eye 분류를 위해서 사용된 수식은 그림 11과 같다. 상중하의 경우 “a"가 사용되며, 좌우 분류는 ”b"가 사용되었다.

실제 개발된 융복합 인증 화면은 그림 12와 같이 개발되었으며 본 인증 시스템은 모바일 기반으로 안드로이드에 적용되었으며 다양한 계정 등록을 통하여 보다 편하고 빠르게 그리고 안전하게 개인 정보를 보호할 수 있도록 개발 되었다.

$$\text{(a)}\quad j = \operatorname{argmax}_j\left(\sum_{i=1}^{2} V_{ij} W_i\right),\ j = 1,2,3$$

$$\text{(b)}\quad k = \operatorname{argmax}_k\left(\sum_{i=1}^{2} H_{ik} W_i\right),\ k = 1,2$$

그림 11. Neural Network 구조
Fig. 11. Neural network structure

그림 12. 복합 생체 인증 구현 화면
Fig. 12. Result of multi biometrics application

본 개발된 알고리즘은 사물인터넷 기반의 디바이스에서도 적용 가능하도록 개발되었다. 사용된 언어는 자바와 C를 사용하여 개발 되었다.

성능평가는 앞서 언급한 그림 3과 그림 6과 같이 Face detection 처리 속도 부분과 Eye detection 부분의 수행 능력부분에 대해서 측정하였다. 측정 결과는 속도 측면에서 우수한 결과를 가지고 있는 것으로 판단되었다. AI Processor의 경우 그림 13과 같이 평균 90%이상의 학습 결과를 가져 왔다. 테스트를 위한 단말기는 L사의 휴대 단말기를 사용하였다.

그림 13과 같이 개발된 알고리즘(Face 인식, Eye 인식, Fingerprint인식)을 통한 생체 인증 방안과 일반적으로 사용되는 PIN인증방법을 적용하여 그림 14와 같이 세계 최초의 16개 조합을 실시간으로 인증 처리할 수 있는 다중 생체인증 알고리즘이 개발되었다.

```
G2 얼굴포즈 50명
Elapsed time is 78314.877740 seconds.
Train # misclassified: 14 (from 248370). Test # misclassified: 7 (from 27570) - 99.97%

G2 view1 상중하 50명
Elapsed time is 30468.947699 seconds.
Train # misclassified: 1158 (from 78210). Test # misclassified: 181 (from 8670) - 97.91%

G2 view2 상중하 50명
Elapsed time is 24927.226249 seconds.
Train # misclassified: 1698 (from 70860). Test # misclassified: 218 (from 7860) - 97.22%

G2 view1에서 좌우 50명
Elapsed time is 26889.312960 seconds.
Train # misclassified: 82 (from 51990). Test # misclassified: 24 (from 5760) - 99.58%

G2 view2에서 좌우 50명
Elapsed time is 16263.758081 seconds.
Train # misclassified: 310 (from 47280). Test # misclassified: 59 (from 5250) - 98.87%

G2 view1에서 좌중우 50명
Elapsed time is 24202.285443 seconds.
Train # misclassified: 4772 (from 78150). Test # misclassified: 587 (from 8670) - 93.22%

G2 view2에서 좌중우 50명
Elapsed time is 21354.594174 seconds.
Train # misclassified: 6597 (from 70770). Test # misclassified: 875 (from 7860) - 88.86%
```

그림 13. AI Processor 성능 수행 결과
Fig. 13. Result of AI processor

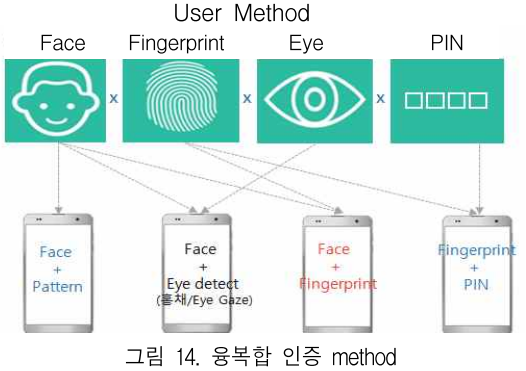


그림 14. 융복합 인증 method
Fig. 14. Method of multimodal

표 1. 제안 알고리즘의 특징
Table 1. Characteristics of the proposed algorithms

	Universality	convenience	Advantages	Characteristic and UX
Face/ Iris/ Eye recognition	Verification of biometric information that can be grasped by camera over 3 million pixels	Can be authenticated without separate screen when setting camera authority	Gaze recognition algorithm to solve existing face recognition disadvantage and secure security	Recognition speed: 500ms Recognition method: 1. Face recognition + Pattern algorithm 2. Face recognition + EYE detect algorithm Iris/EYE Gaze) 3. Face recognition + Fingerprint algorithm 4. Fingerprint with OTP algorithm
Finger print recognition	Expanded rapidly in recent 2 years with built-in fingerprint sensor of new mobile phone	High convenience with error rate within 0.5% and quick verification within 1 second	Secure (more than 101) than the existing one fingerprint authentication through OTP-based intelligent fingerprint recognition algorithm	Recognition rate: 99%

본 논문에서의 제안된 알고리즘을 통하여 표 1과 같이 기존의 단일 인증방법보다 인증의 강도를 더욱 증가하게 되어 기존 보다 보안성을 높이는 효과를 가져왔다.

본 논문을 통해 개발된 인증 시스템으로 사용자는 자신이 원하는 인증 방법을 선택하여 쉽고 빠르게 인증을 진행 할 수 있도록 개발하였다.

Ⅳ. 결론 및 향후 과제

본 논문을 통해서 개발된 알고리즘은 단일 인증이라는 보안의 취약점을 보완하기 위하여 개발된 알고리즘이다. 기존의 단일 디바이스를 통한 인증 시스템은 다양한 불편함과 속도 등의 여러 문제들이 발생하였는데 이러한 문제를 해결하고자 현재 급속도로 발전되고 있는 안드로이드 기반의 스마트폰을 활용하여 빠른 속도와 편리함을 동시에 구현하게 되었다. 아직 이러한 보안 시스템을 시장에서 많이 요구하고 있지 않지만 현재 급속하게 변화되고 있는 4차 산업 환경에서 반드시 필요한 부분이 될 것으로 판단하고 있다. 현재 개발된 시스템은 신용평가사가 운영 중인 공공 아이핀에 적용하기 위한 작업이 진행 중이다.

전 세계 생체인식 시장 규모가 2016년 약 12조6천억, 국내 3천2백억 규모로 커질 정도로 시장수요가 확대 되고 있으며, 모바일 기능 확대, 핀테크와 인터넷뱅크의 금융 비대면 인증 증가, IOT 및 Wearable device의 융합 서비스 확장 등으로 인증수요가 증가할 것이며 이와 더불어 인증분야는 범용성, 편의성, 보안성 등의 시장경쟁력을 만족시켜야 하는 새로운 문제 직면하게 될 것이다. 향후에는 본 논문에서 적용된 인공지능 부분에서도 최근 이슈가 되고 있는 딥러닝 기반의 지능형 시스템으로 추가 개발하여 더욱더 견고하고 편리한 개인인증 시스템을 개발 하는 것이 향후 진행할 과제로 할 것이다.

References

[1] J. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE. Trans. on Pattern Analysis and Machine Intelligence, Vol. 14, No. 11. pp. 1148-1161, Sep. .1993.

[2] Dosung Ahn, Sung Bum Pan, "Overview of Biometric Technologies and Its Adoption in Travel Document", Journal of KIIT, Vol. 1, No. 1, pp. 95-102, Dec. 2003.

[3] Biometrics Consortium : http://www.biometrics.org.

[4] Byung-Joo Kim, "Feature Extraction Algorithm for Embedded Biometric System", Journal of KIIT,

Vol. 7, No. 2, pp. 89-97, Apr. 2009.
[5] http://thenextweb.com/google/2011/11/11/android-4-0-face-unlock-feature-defeated-using-a-photo-video/
[6] A. Jain, R. Bolle and S. Pankanti, "Biometrics Personal Identification in Networked Society", Kluwer Academic Publisher, 1999.
[7] D. Reisfeld, H. Wolfson, and Y. Yeshrun, "Detection of Interest Points Using Symmetry", Proceedings of the 3rd ICCV, 1990.
[8] Han-Soo Cho, "An Efficient Filter Design for Eye Detection in Color Images under Varying Lighting Conditions", Journal of KIIT, Vol. 6, No. 2, pp. 100-107, Apr. 2008.
[9] J. G Allen, R. Y. D. Xu, and J. S Jin, "Object Tracking using CAMShift Algorithm and Multiple Quantized Feature Spaces", Proof Pan-Sydney Area Workshop on Visual Information Processing (VIP2003), Conference in Research and Practice in Information Technology, Vol. 36, pp. 3-7, Jan. 2003.
[10] M. Boyler, "The Effects of Capture Conditions the CAMShift Face Tacker", Technical Report 2001-6 91-14, Department of Computer Science, University of Calgary, Alberta, Canada, 2001.
[11] Thomas F. Quatieri, "Discrete-Time Speech Signal Processing Principles and Practice", Prentice Hall, 2001.
[12] Nam-Ho Kim, "Voice-based OTP Generation Techniques for Mobile Banking", Journal of KIIT, Vol. 11, No. 5, pp. 113-119, May 2013.
[13] Wang-Su Jeon and Sang-Yong Rhee, "Fingerprint Pattern Classification Using Convolution Neural Network", International Journal of Fuzzy Logic and Intelligent, Vol. 17, No. 3, pp. 170-176, Sep. 2017.

저자소개

임 대 환 (Dai-Hwan Lim)

2002년 2월 : 한양대학교 정보처리공학과(공학석사)
2014년 2월 : 한양대학교 정보통신공학과(공학박사)
2008년 9월 ~ 2014년 3월 : LG전자 연구원
2015년 3월 ~ 현재 : 서경대학교 컴퓨터공학과 교수
관심분야 : 인공지능, 사물인터넷(IoT), 자율주행 시스템