Journal of Convergence for Information Technology
Vol. 9. No. 7, pp. 100-105, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.7.100

사적공간의 스마트미러에서 사용자 식별 및 인증 기법 연구

문형진
성결대학교 정보통신공학과 교수

A Study on the User Identification and Authentication in the Smart Mirror in Private

Hyung-Jin Mun
Professor, Dept. of Information and Communication Engineering, Sungkyul University

요 약 IoT 기술 발달로 인해 초연결사회가 되면서 다양한 사용자 맞춤 서비스가 요구된다. 맞춤 서비스로 활용되는 차세대 디스플레이인 스마트 미러를 멀티미디어 기기에 접근하여 다양한 서비스를 제공함으로 정보가 필요한 성인 뿐만 아니라 어린아이의 사회학습 도우미 및 노인의 생활 도우미 역할이 가능하다. 개인별로 차별화된 서비스를 위해서는 스마트 미러가 사용자를 식별하는 것이 가능해야 한다. 스마트 미러는 누구나 쉽게 접근 가능한 기기이므로 스마트 미러에 저장된 개인의 패턴이나 습관 등의 정보가 외부로 노출될 가능성이 있다. 사적 공간의 스마트 미러에 저장된 개인의 일정이나 약속 등 개인의 위치정보 유출 가능성이 있고, 개인 사진을 통해 건강상태를 확인할 수 있어 이를 통한 프라이버시 침해 가능성도 존재한다. 본 연구는 사용자가 얼굴 등의 생체정보를 등록하여 사용자를 식별하고 사용자 인증 후 개인에 맞는 서비스를 제공하고, 인증이 되지 않는 사용자에게는 최소한의 정보와 서비스만 제공하는 시스템을 제안한다.

주제어 : 스마트 미러, 사용자 인증, 개인별 서비스, 프라이버시, IoT

Abstract As IoT Technology develops and Era of Hyperconnectivity comes, various kinds of customized services became available. As a next-generation display, a smart mirror accesses multimedia devices and provides various services, so it can serve as a social learning tool for the children and the old ones, as well as adults who need information. Smart Mirror must be able to identify users for individualized services. However, since the Smart Mirror is an easily accessible device, there is a possibility that information such as an individual's pattern and habit stored in the smart mirror may be exposed to the outside. Also, the other possibility of leakage of personal location information is through personal schedule or appointment stored in the smart mirror, and another possibility that privacy can be violated is through checking the health state via personal photographs. In this research, we propose a system that identify users by the information the users registered about their physique just like their face, one that provides individually customized service to users after identifying them, and one which provides minimal information and service for unauthenticated users.

Key Words : Smart mirror, User authentication, Personal service, Privacy, IoT

*Corresponding Author : Hyung-Jin Mun(jinmun@gmail.com)
Received June 28, 2019
Revised July 8, 2019
Accepted July 20, 2019
Published July 28, 2019

1. 서론

현재 IoT 기술의 발달로 인해 초연결시대가 도래되면서 개인별로 맞춤 서비스가 요구된다. 자신의 실제모습을 보여주는 거울이 ICT 기술과 접목되면서 스마트 미러로 발전하여 사용자가 원하는 다양한 서비스가 제공되고 있다. 스마트 미러는 거울(Mirror)과 디스플레이(Display)의 결합된 차세대 디스플레이로 평상시에는 거울이지만 사용자가 접근하면 근접센서가 반응하여 사용자에게 원하는 정보를 제공하는 디스플레이이다. 기존 거울을 통해 볼 수 없는 영역까지 확인이 가능하고, 심지어 옷을 입지 않은 상태에서도 가상으로 옷을 입은 상태의 모습을 보여줄 수 있는 코디네이터 기능도 가능하다. 스마트 미러를 통해 타인으로부터 좋은 평판을 얻을 수 있고, 백화점 등에서 스마트미러가 고객과 커뮤니케이션하여 의상에 대한 다양한 피드백을 제공하여 구매를 촉진할 수 있다. 또한 사용자가 외출하기 전에 오늘의 날씨를 확인하여 비가 올 확률이 높은데 우산을 준비하지 않는 사용자에게 우산을 준비하라는 메시지, 미세먼지가 심할때는 마스크 착용을 권고하여 사용자가 미처 준비하지 못한 부분까지 코칭하는 단계까지 가능하다. 스마트 미러는 세대별로 다양한 서비스가 가능하다. 특히, 어린 아이가 스마트 미러를 보면서 양치질을 할 때 올바른 양치질을 유도할 수 있고, 주기적으로 사용자의 얼굴을 촬영하고 이를 기반으로 안색을 파악하고, 컨디션이나 건강상태도 파악할 수 있다. 독거 노인들에게는 스마트 미러가 말동무가 되어 줄 수 있고, 가스나 문단속과 같은 안전 서비스를 제공할 수 있다. 집에 있는 스마트 미러의 경우에는 여러 사용자가 존재하기 때문에 차별화된 서비스를 제공하기 위해서는 사용자를 식별하고 식별된 사용자에 맞게 서비스를 제공할 수 있어야 한다[1]. 최근 스마트 미러를 통해 사용자의 성별, 나이 등을 촬영된 사진을 통해 파악하는 것이 가능하다. 하지만 식별된 정보를 가지고 더 나은 서비스를 제공하기에는 더 정확한 식별 기법이 필요하다. 또한 스마트 미러가 사용자를 식별하고, 서비스를 제공할 때 발생가능한 다양한 문제가 존재한다. 스마트 미러는 누구나 접근 가능한 기기이므로 이를 통해 사용자의 사진뿐만 아니라 생활 패턴이나 습관 등이 외부로 유출가능성이 존재한다. 특히, 차별화된 서비스를 위해 제한된 공간, 예를 들어 집이나 개인사무실 등에서 개인용 스마트 미러 등에 사용자의 일정, 약속, 개인적인 사진 등이 연동 될 수 있다. 이 때 제 3자가 스마트 미러에 접근하여 사용자의 일정이나 생활 패턴 등을 확인할 수 있어 프라이버시 침해 가능성이 존재한다. 정보가 저장되고, 가공되어 서비스를 제공하는 스마트 미러는 사용자 식별이 필요하다. 얼굴인식 기술을 이용하여 사용자의 얼굴을 인식하고, 이를 기반으로 사용자 식별을 통해 사용자 인증을 하고, 인증된 사용자에 한하여 정보에 기반한 세밀한 서비스를 제공하고, 식별이 되지 않는 사용자는 익명 사용자로 인식하여 인증 없이 서비스가 가능한 최소한의 정보만 제공하는 시스템을 구축하는 것이 필요하다.

스마트 미러 관련 특허나 제품 개발은 공공장소에서 사용 가능한 기능 중심으로 되어 있다. 이와 다르게 개인 및 사적인 공간에서의 사용가능한 스마트 미러에 대한 다음과 같은 요구사항이 필요하다.

- 개인별 서비스를 제공하기 위해 스마트 미러의 사용자에 대한 식별이 가능해야 한다.
- 저장된 개인 성향 및 정보가 있는 상태에서의 개인별 서비스를 제공하기 위해서는 사용자 식별이 아닌 사용자 인증이 필요하다.
- 사용자 인증시 MITM 등과 같은 공격에 안전성이 보장되어야 한다.

본 연구에서는 사용자의 얼굴 식별과 간단한 인증정보를 사전에 등록하고, 이를 기반으로 사용자를 식별하고, 인증하여 사적공간에서 사용가능한 스마트 미러의 요구사항을 만족하는 기법을 제안하고자 한다.

2. 관련연구

2.1 Raspberry Pi

Raspberry Pi 3 B+은 Fig. 1과 같이 Cortex-A53 1.4GHz, HDMI, IEEE 802.11b/g/n/ac 무선 LAN, Bluetooth 4.2 모듈을 내장되어 있다[2,3]. 라즈베리파이는 PC가 할 수 있는 기능을 가진 저가형 컴퓨터로 지문인식 스캐너, 카메라를 장착하여 IoT 구현이 가능하다.

Fig. 1. Raspberry Pi 3 B+

라즈베리파이를 이용하면 스캔된 이미지를 AES 암호알고리즘을 이용하여 전송이 가능하여 인증 서비스, 보안성 및 확장성이 가능하여 스마트 미러 구현에 적합한 기기이다[4-6]. 최근에 사양이 향상된 Raspberry Pi 4 가 출시되어 유통되고 있다.

Raspberry Pi에는 다양한 운영체제를 설치할 수 있지만 Raspberry Pi 재단에서 Debian 리눅스 기반으로 개발된 Raspbian을 주로 사용한다. Raspbian은 저성능 ARM CPU 사용자나 개발자을 위한 최적화된 운영체제이다[6-8].

2.2 LattePanda

LattePanda 는 Windows 10 기반의 싱글보드 컴퓨터로써 로봇개발 및 데이터 처리에 활용이 가능하다. Fig. 2과 같이 Quad-core 1.8GHz, eMMC 32-64GB, Giga Ethernet, USB 3.0 등 이 내장되어 있다. 최근 Image processing, Voice recognition, NN processing, BigData processing에도 사용이 가능하다[9].

Fig. 2. LattePanda

2.3 사용자 인증

차별화된 서비스를 제공하기 위해서는 사용자가 적합한 사용자인지를 확인하는 절차가 필요하다. 사용자인증은 아이디 기반 인증이 대다수를 차지하고 있다. 하지만 스마트에 스캔 기능으로 지문인증, 홍채인증 등 다양한 생체인증정보를 통해 적합한 사용자인지 확인하고 있다. 하지만 생체인증의 경우 쌍둥이나 닮은 사람 간에 얼굴의 오류인증이나 사용자의 지문 손실 등으로 지문인증이 안되는 경우가 발생한다. 즉, 오탐(False Positive)과 미탐(False Negative)가 존재하는 생체인증으로 사용자 인증이해결되지 않는 경우가 발생한다.

다중 인증은 생체 인증의 보완책이 될 수 있다. 다중 인증은 한번의 인증으로 인증완료 하는 것이 아니라 인증 수단을 여러 개를 사용하여 임계치에 도달하는 경우에 인증을 완료하는 방식이다. 대체적으로 아이디로 1차 인증을 하고, 2차로 생체인증을 하는 방식이 주로 사용된다. 2차 인증 수단으로 사용자의 글쓰는 패턴을 이용하기도 한다[10].

3. 스마트 미러 설계

3.1 얼굴인식 기술

Raspberry Pi와 카메라를 통해 입력되는 영상을 실시간으로 분석하여 사용자 식별하는데 OpenCV를 사용한다. OpenCV는 영상처리와 오픈 소스 라이브러리를 이용하여 얼굴 검출과 객체 인식 등에 응용 분야에 활용된다[11]. 이러한 얼굴인식 기술은 영상처리, 영상보안, 패턴인식 분야에서 사용되고 있다[12,13].

Fig. 3은 입력된 얼굴이미지를 통해 정보를 추출하고, 이미지를 분류하여 얼굴을 인식한다[10]. 뿐만 아니라 얼굴을 인식하여 사용자의 나이, 성별, 감정, 자세, 미소, 수염 등 얼굴 이미지를 통해 다양한 특징 정보를 추출할 수 있다[14].

얼굴인식 기술은 신분조회, 보안분야, 감시분야에서 사용되고, 이 기술을 통해 모아진 개인 자료는 프라이버시 침해 가능성이 높아진다.

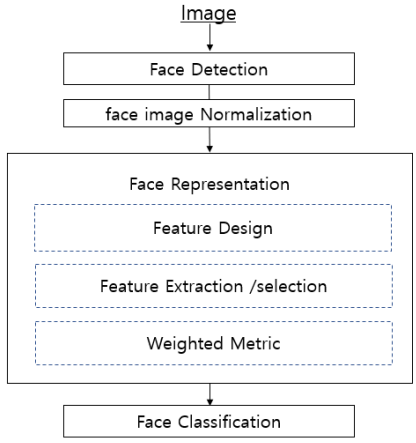

Fig. 3. Face Recognition System

3.2 스마트 미러의 구성요소

스마트 미러 시스템을 구축하기 위해서는 Raspberry Pi 3, 소형 USB 마이크, 디스플레이, 정보를 제공받기 위한 LAN 모듈 등이 필요하다[15].

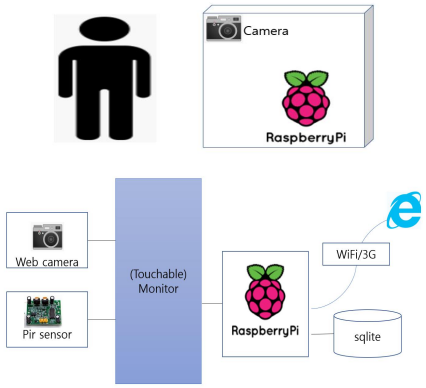

Fig. 4. The component of Smart Mirror

사용자는 스마트 미러 앞에 있으면 스마트 미러는 근접 센서를 통해 사용자를 인지하고, 카메라로 사진을 찍어 사용자를 식별한다. 스마트 미러의 구성요소는 Fig. 4와 같다. 스마트 미러에는 카메라, PIR 근접센서, 라즈베리 파이와 터치가 가능한 모니터로 구성되어 있다.

4. 스마트 미러의 사용자 인증 기법

4.1 사용자 등록 프로세스

스마트 미러가 사용자 인증을 하기 위해서는 시스템내에 사용자를 식별하는 정보를 사전에 등록해야 한다. Fig. 5와 같이 사용자의 정보를 등록하기 위해서 사용자는 얼굴을 스마트 미러 앞에 비치면 근접센서가 반응하게 되고, 스마트 미러에 있는 웹카메라를 통해 스캔하고, 얼굴을 인식하여 나이, 성별, 안경여부 등의 정보를 수집한다[14]. 이 정보를 라즈베리파이에 있는 DB에 등록하고, 비슷한 얼굴 등으로 인증되지 않기 위해 2차 인증정보를 요구한다. 이는 얼굴을 스캔한 정보만으로 사용자를 무분별하게 식별할 수 없게 한다. 예를 들어 자매간이나 부자간의 얼굴은 비슷하고, 이로 인해 잘못된 인증이 가능하다. 2차 인증정보는 다양하게 존재하지만 식별만을 위해서 간단한 패턴이나 핀 번호 등을 활용할 수 있다. 2차 인증정보는 터치가 가능한 모니터를 통해 입력이 가능하다.

1차적으로 얼굴 이미지로 전체 사용자집단을 필터링하고, 그 중에서 필터링 된 사용자중에서 2차 정보로 정확하게 식별한다. 사용자의 얼굴로 파생된 다양한 정보와 2차 인증정보를 서버인 라즈베리파이에 내장된 DB(sqlite)에 등록한다.

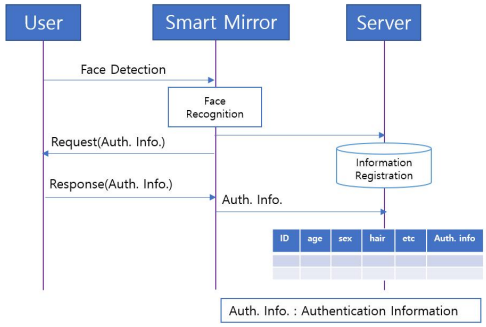

Fig. 5. Registration of User for Smart Mirror

4.2 사용자 인증 프로세스

사용자 등록이 끝난 후에 스마트 미러를 통해 서비스를 받기 위해서는 사용자 인증 절차가 필요하다. 스마트 미러 시스템에 사전에 등록된 정보를 활용하여 사용자를 식별하고, 인증을 한다. Fig. 6는 사용자가 스마트미러 앞에 서면 근접센서가 반응하여 스마트 미러가 웹카메라를 통해 사용자의 얼굴을 인식한다. 인식된 얼굴 이미지를 사용해 API를 통해 얼굴정보를 생성하고, 이를 서버로 전달한다. 사용자를 정확하게 식별하기 위해 2차인증정보를 요구한다. 2차 인증정보는 터치가 가능한 모니터에 패턴이나 핀번호를 입력한다.

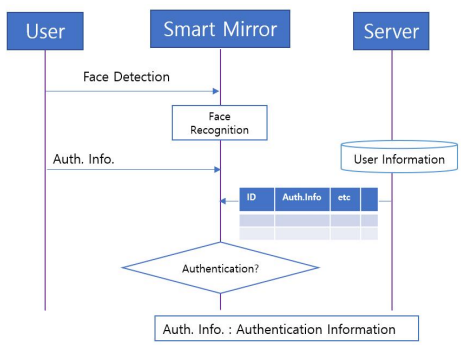

Fig. 6. Authentication of User for Smart Mirror

얼굴을 인식하여 얻은 사용자 정보를 기반으로 서버내에 저장된 정보를 필터링한 정보테이블에서 2차인증정보를 비교하여 사용자를 식별한다. 즉, 2차정보는 사용자의 식별정보이면서 비밀정보로 활용된다. 얼굴정보에 맞는 2차인증정보가 없을 경우 서버에서는 2차인증정보를 기반으로 다시 서버의 사용자 정보를 조회하여 사용자를 확인한다. 인증이 실패한 경우는 등록되지 않는 사용자이므로 익명사용

자로서 최소한의 서비스를 받거나 새롭게 사용자로 등록하는 과정을 수행한다.

4.3 서비스 제공 프로세스

사용자는 스마트 미러를 통해 차별화된 서비스를 제공받고자 한다. 사용자 인증이 끝난 후, 스마트 미러 시스템은 인터넷과 연결되어 사용자의 스케줄이나 날씨정보, 사용자가 흥미를 가질 수 있는 정보를 검색하고, 다양한 서비스를 제공한다. Fig. 7은 사용자가 스마트 미러를 통해 인증이 완료되면 스마트 미러는 해당 사용자가 원하는 정보나 서비스 목록을 서버에 요청하고, 그 서비스를 제공한다. 이때 기존에 서비스된 정보목록과 같은 카테고리에 있는 사용자들이 원하는 서비스를 추천하여 제공한다.

차별화되고, 다양한 서비스를 제공하기 위해 스마트 미러에 AI 스피커 기능을 추가하여 서비스를 제공할 수 있다. AI 스피커를 통해 입력된 정보를 DB에 등록하면 사용자의 취미, 성향 등을 파악하여 사용자가 원하는 서비스를 제공할 수 있다.

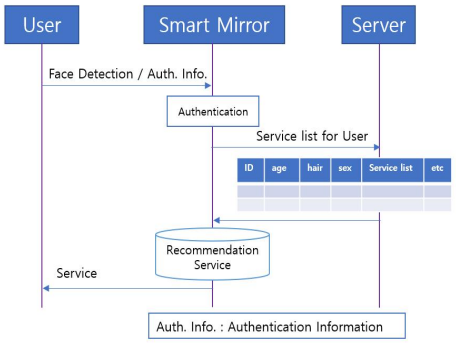

Fig. 7. Authentication of User for Smart Mirror

4.4 분석 및 평가

스마트 미러 시스템는 사용자 식별 뿐만 아니라 인증기능을 제안함으로서 사용자별 서비스를 적절히 제공할 수 있다. 다음은 개인이나 사적공간에서 사용가능한 스마트 미러의 요구사항을 만족하는 사용자 인증기법을 제안하였다.

첫째, 사전에 사용자별로 얼굴 정보와 2차 인증정보를 DB에 등록한다. 사용자의 얼굴 이미지를 API를 통해 얼굴 이미지를 전송해서 사용자의 정보를 수신받아 DB에 저장하여 이를 기반으로 사용자 식별을 수행한다.

둘째, 얼굴 이미지만을 통해 사용자 식별이 무분별하게 수행되지 않는다. 사용자 등록시 입력한 2차 인증정보를 통해 사용자 인증 정보로 활용된다. 이는 터치 등을 통해 입력한 2차 인증정보도 DB에 등록하여 이를 기반으로 사용자를 인증하는 것이다. 즉, 이중 인증(Two-Factor Authentication)을 수행하는 결과를 가진다[16].

셋째, 웹 등 다양한 서비스에서 사용자 인증시 비밀정보가 인터넷을 통해 전송되는 과정에서 MITM을 비롯한 다양한 공격이 나타나지만 제안기법에서는 소수의 사용자 정보를 라즈베리 파이 내에 있는 SQLite 에 등록함으로써 외부와 연결 없이 인증이 가능하여 MITM 공격과 같은 사용자 인증에서 빈번하게 발생가능한 공격에 안전하다.

얼굴을 통해 사용자 식별을 하고, 2차 인증정보를 통해 사용자인증을 수행하지만 경우에 따라 화장이나 머리스타일 등 얼굴에 다양한 변화가 있을 경우 사용자 식별이 정확하게 되지 않을 수 있다. 이때 2차 인증정보가 사용자 식별에 활용될 수 있다.

인증에 실패할 경우 사용자 등록을 수행하거나 익명 사용자가 인식하여 최소한의 서비스만 제공한다. 즉, 얼굴인식을 통해 나이, 성별을 식별하고 그에 맞는 서비스를 제공받는다.

본 제안 기법은 가정 집이나 개인 사무실과 같이 제한된 공간에서는 스마트 미러의 사용자를 제한하여 소수의 사용자의 정보만을 등록하고, 식별하고, 인증하는 기법이다. 사적 공간에서 인증 기법이 적용된 AI 스피커나 스마트 미러가 있는 스마트 홈에 적용된다면 개인에 맞는 서비스를 다양한 기기를 통해 서비스를 받을 수 있다. 뿐만 아니라 고객의 취향이나 Needs 중심의 헤어샵 등에서 고객의 정보를 등록하고 고객관리를 한다면 단골 고객의 Needs 에 맞게 고객이 원하고, 트랜드에 맞는 머리 스타일을 제공하는 등의 서비스를 제공할 수 있다.

5. 결론

ICT 발달로 인해 개인 사용자의 요구 및 서비스가 다양해지고 있다. 현재 스마트 폰을 통해 사용자의 요구 및 서비스를 제공하고 있지만 단말기의 크기가 작아 제공되는 서비스의 제한이 있다.

사용자는 자신의 모습을 거울을 통해 수시로 보고 있기 때문에 스마트 미러를 통해 사용자의 다양한 서비스를 수시로 제공받을 수 있다. 특히, 화장실이나 엘리베이터 같은 공간에서 낭비되는 시간에 날씨나 뉴스 등 간단하면서 필요한 정보를 제공할 수 있는 스마트 미러의 수요가 늘어나고 있다.

스마트 미러를 통해 다양한 서비스의 요구가 있지만 기

존 스마트 미러는 단순한 정보나 일률적인 서비스만을 제공하고 있다. 이는 스마트 미러가 사용자별로 식별 없이 얼굴 인식을 통해 나이, 성별 등의 큰 카테고리를 인식하고 서비스를 제공하기 때문이다. 가정이나 개인 사무실과 같은 사적인 공간에서 사용자 인증 후 맞춤형 서비스가 가능하다.

본 논문에서는 먼저 사용자를 등록하고, 사용자를 식별하여 사용자가 저장하고, 원하는 서비스를 구별하여 제공하고자 하였다. 이를 통해 더 다양하고, 민감한 정보를 안전하게 제공하게 되었다. 제안기법은 스마트미러이외에도 AI 스피커와 같이 IoT 기기에서도 사용자 식별 및 인증 후 개인별로 차별화된 서비스가 가능하다.

향후 연구로는 홍채인증이나 음성인증 등을 통해 터치 방식의 2차인증정보 없이 사용자를 식별하고 인증할 수 있는 스마트 미러 연구 및 개발이 필요하다.

REFERENCES

[1] Billy Choi. (2012). The Direction of Smart Mirror. *Communications of the Korean Institute of Information Scientists and Engineers, 30(4),* 25-28.

[2] Raspberry Pi 3 Model B+, The latest revision of our third-generation single-board computer. https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/

[3] S. W. Lee, D. M. Ji, H. S. Shin, Y. B. Chae & Y. G. Kim. (2018). A Personalised Smart Mirror Based on Face Recognition. *Proc. of Korea Information Science Society,* 1644-1646.

[4] J. W. Kim. (2017). IoT based Authentication System Implementation on Raspberry Pi. *Journal of Korean Industrial Information Systems Society, 22(6),* 31-38. DOI : 10.9723/JKSIIS.2017.22.6.031

[5] J. R. Cho, H. S. Kim, D. K. Chae & S. J. Lim. (2017). Smart CCTV Security Service in IoT(Internet of Things) Environment. *Journal of digital contents society, 18(6),* 1135-1142. DOI : 10.9728/dcs.2017.18.6.1135

[6] P. Y. Kumbhar, A. Mulla, P. Kanagi & R. Shah. (2018). Smart Mirror Using Raspberry PI. *International Journal for Research in Emerging Science and Technology, 5(4),* 2349-2610.

[7] Raspbian. (2019). *Raspbian.* Wikipedia(Onlie). https://en.wikipedia.org/wiki/Raspbian

[8] W. Harrington. (2015). *Learning Raspbian.* Packt Publishing Ltd.

[9] LattePanda. https://www.lattepanda.com

[10] J. Shin, Z. Liu, C. M. Kim & H. J. Mun. (2018). Writer identification using intra-stroke and inter-stroke information for security enhancements in P2P systems. *Peer-to-Peer Networking and Applications, 11(6),* 1166-1175. DOI : 10.1007/s12083-017-0606-0

[11] Y. C. Hwang, H. J. Mun & J. W. Lee. (2015). Face Recognition System Technologies for Authentication System-A Survey. *Journal of Convergence for Information Technology, 5(3),* 9-13. DOI : 10.22156/CS4SMB.2015.5.3.009

[12] S. Xie, S. Shan, X. Chen & J. Chen. (2010). Fusing local patterns of gabor magnitude and phase for face recognition. *IEEE transactions on image processing, 19(5),* 1349-1361. DOI : 10.1109/TIP.2010.2041397

[13] J. K. Park, M. J. Bae & W. G. Hong. (2017). IoT Device 'Smart Mirror' using Raspberry Pie. *Proceedings of KIIT Conference.* 460-461.

[14] Face API. https://azure.microsoft.com/ko-kr/services/cognitive-services/face

[15] K. W. Bowyer. (2004). Face recognition technology: security versus privacy. *IEEE Technology and society magazine, 23(1),* 9-19. DOI : 10.1109/MTAS.2004.1273467

[16] H. J. Mun. (2018). Biometric Information and OTP based on Authentication Mechanism using Blockchain. *Journal of Convergence for Information Technology, 8(3),* 85-90. DOI : 10.22156/CS4SMB.2018.8.3.085

문 형 진(Hyung-Jin Mun) [종신회원]

· 2008년 2월 : 충북대학교 전자계산학과(이학박사)
· 2009년 3월 ~ 2012년 8월 : 중국 연변과학기술대학교 컴퓨터전자통신학부 조교수, 부교수
· 2017년 3월 ~ 현재 : 성결대학교 정보통신공학부 조교수

· 관심분야 : 정보보안, 사용자 인증, 빅데이터분석
· E-Mail : jinmun@gmail.com