Journal of Knowledge Information Technology and Systems(JKITS), Vol. 15, No. 4, pp. 451-461, August 2020
https://doi.org/10.34163/jkits.2020.15.4.001

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Smart Entrance Control System Using Face Recognition and OTAC

Soon-Chul Baek, In-Sik Hong*

Department of Computer Science and Engineering, Soonchunhyang University

ABSTRACT

In modern society, security-enhanced access control systems are an important factor. In this paper real-time smart access control system using a face recognition camera and OTAC(One Time Access Code) is proposed. This system especially focuses on the response speed of the embedded board to implement a delay-free system. Most access control systems on the market uses RFID to authenticate users. RFID has the advantage of fast authentication time and high usability. However, system's weak points arise because others can steal and manipulate them. There are biometric recognition methods as supplant method, such as facial recognition, vein matching, iris recognition and fingerprint recognition are used as technical methods. The method proposed in this paper uses facial recognition technology and OTAC authentication. This is implemented on the embedded board by linking the depth information camera and the user DB server which is built on cloud environment. The embedded system was designed using Python, C++, C and PHP on Raspberry Pi 3 Model B+, Ubuntu 18.04 LTS and Arduino Due. Then communicated with each other using Wi-Fi and Serial Communication. In addition, the driving speed, one of the important specs, was 300 ms, which resulted in conformity with the designed specification. This system's prototype was manufactured to prove the practicality and efficiency of the system.

KEYWORDS: Face recognition cameras, One time access code, Access control systems, QR code, RFID tags

ARTICLE INFO: Received 16 June 2020, Revised 30 June 2020, Accepted 10 August 2020.

*Corresponding author is with the Department of Computer Science & Engineering, SoonChunHyang University, 31538, 22 Soonchunhyang-ro, Sinchang-myeon, Asan-si, Chungcheongnam-do, KOREA.
E-mail address: ishong@sch.ac.kr

1. 서 론

보안이 강조된 출입통제 시스템은 각 가정에서부터 회사, 연구소 그리고 정부 주요 시설에 이르기까지 다양한 장소에서 사용되고 있으며, 여러 종류의 시스템이 개발되고 있다[1-4].

이 중 PIN(Personal Identification Number) 인증 시스템은 주변에서 흔히 볼 수 있는 도어락에 적용되어 있다. 구조가 간단하여 설치가 용이하고 사용자의 사용이 편하다는 장점이 있지만 사용자가 PIN을 분실할 경우 출입이 불가능해진다. 건물 단위에 설치하여 운영되는 RFID(Radio-Frequency IDentification) 인증 시스템은 출입자별로 카드를 발급하여 사용한다[5]. 상대적으로 초기 투자비용이 많이 소요되지만 사용자 별로 권한을 부여할 수 있고 방문자 출입에도 대응할 수 있다는 장점이 있다. 하지만 카드 분실 시 보안 취약점이 발생할 수 있다는 문제가 있다. 생체 인증을 사용하는 지문 인증, 정맥 인증, 안면 인식 시스템은 비교적 구축비용이 크지만 출입 시 필요한 PIN이나 카드가 없다[6-10].

본 논문에서는 기존 출입통제 시스템의 보안성을 강화하기 위하여 QR(Quick Response) 코드 인증과 안면인식 기술을 활용하여 사용성이 용이하면서도 안전성 면에서 개선된 시스템을 제안하고 구현한다.

2장에서는 기존 출입통제 시스템의 개념에 대하여 알아본다. 그리고 본 시스템에서 사용할 ARP(Address Resolution Protocol)의 기술적 내용과 그 기능을 설명한다. 3장에서는 전체 시스템 구조와 안면인식 카메라의 적용, 서버와 단말기 간의 통신 프로토콜과 인증 절차, 그리고 OTAC(One Time Access Code) 태그의 구조를 기술한다. 4장 시스템의 구현에서는 기존 출입 시스템과의 연동 방법 및 제안된 시스템의 구동과 평가 결과를 서술한다. 마지막으로 5장에서 결론을 기술한다.

2. 관련 연구 및 기술

2.1 기존 출입통제 시스템

기존 출입통제 시스템 중 RFID 인증 시스템은 중앙 관리 서버, 개폐기, 인증 단말, RFID 카드로 구성된다. 사용자별로 카드 발급이 이루어져 방문자의 추가 및 제거가 간편하며 출입 기록 관리가 가능하다. 지문 인증 시스템은 RFID 인증 시스템과 유사한 구성에 지문 판독기가 추가된 형태이다. 사용성이 우수하지만 지문 복제, 인식률 저하의 문제가 존재한다[11-14].

상기한 내용들은 RFID가 가지고 있는 도용 문제 및 생체 데이터를 인식하는 데 필요한 시간의 지연 문제 등 신속하면서 안전한 입출입 시스템에 부적합한 면이 존재하였다[15].

본 논문에서는 보다 강화된 인증 기술을 사용자가 불편하게 느끼지 않을 짧은 지연시간으로 구현하며 기존 시스템들의 도용 문제 등을 확실히 해결한 OTAC 인증 방식 등을 제안한다.

2.2 ARP(Address Resolution Protocol)

ARP는 링크 계층의 주소 질의에 사용하는 프로토콜로써 RFC(Request for Comments) 826에 의하여 정의되었고, STD(Internet Standard) 37로 채택되었다[16]. 인터넷 계층 주소의 링크 계층 주소를 찾을 때 사용되며 보통 MAC 주소와 IPv4 주소의 연관에 사용한다. MAC 주소는 네트워크 어댑터마다 고유하므로 기기 식별에 사용할 수 있다[17].

상기 ARP는 사용 구조가 대중화되어 있어 개발 편의성을 위하여 본 시스템의 방문자 단말기 인증 프로토콜에 사용하였다. ARP와 함께 OTAC 발급은

QR 코드 형태로 진행되는데, 이는 스마트폰의 화면 인증 능력과 부합되어 채택하였다.

2.3 QR(Quick Response) 코드

QR 코드는 1차원 바코드의 용량 제한 문제를 극복한 2차원 바코드이다. 1994년 일본의 Denso Wave사가 개발하였으며 2000년에 ISO/IEC 18004 표준으로 제정되었고 2015년에 내용 개정을 거친 ISO/IEC 18004:2015 표준이 발행되었다. 최대 2,953 바이트 정도의 표현 능력을 가지며 그래픽이 손실되어도 7~30% 까지는 복원 가능하다[18,19]. 본 논문에서 인증용으로 발행되는 OTAC는 그 용량이 약 55~83바이트로, QR 코드의 사용이 적절하여 이를 본 시스템의 방문자 인증 프로토콜에 사용하였다.

3. 시스템의 설계

입출입 시스템은 보통 건물에 상주하는 거주자와 방문자로 나누어 적용된다. 본 논문에서는 안면인식을 통하여 건물 거주자가 번거로움 없이 출입이 가능하며, 방문자는 단말기 인증을 거쳐 스마트폰에 발행된 QR 코드를 통하여 도용 문제가 없이 간단히 인증 가능한 시스템으로 구축하였다. 안면인식의 경우는 안면인식과 시스템 처리 지연시간을 최소화하여 거주자가 부지불식간에 출입할 수 있도록 구현하며 방문자의 경우는 최소한의 동작만으로 스마트폰 상에 QR 코드를 발행 받아 출입하는 것을 목표로 하였다.

3.1 시스템의 구조

스마트 출입통제 시스템은 사용자가 입출입 카메라 앞에 서는 것으로 시작되며 거주자와 방문자로 나누어 적용한다. 구조는 다음 <그림 1>과 같다.

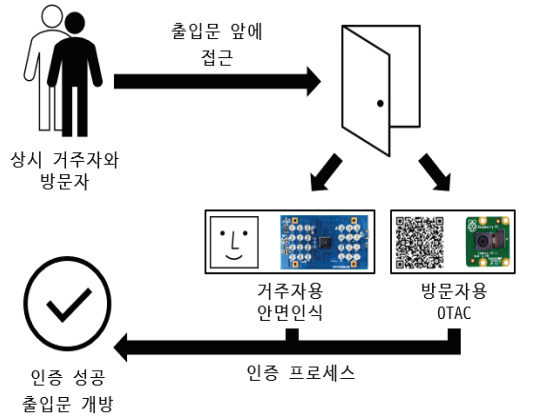

그림 1. 시스템 구조도
Figure 1. Block Diagram of Proposed System

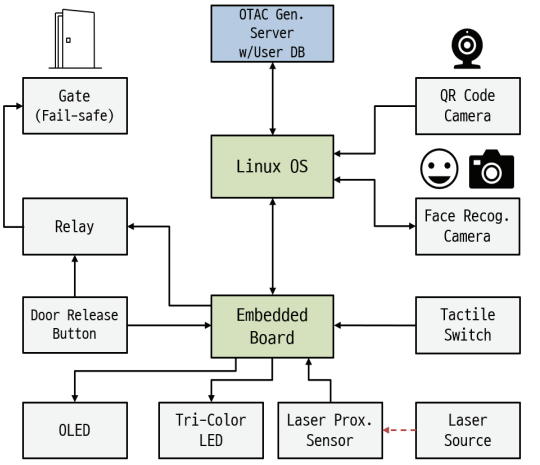

그림 2. 제안된 출입통제 시스템의 구조
Figure 2. Schematic of Proposed Access Control System

시스템은 <그림 2>와 같이 OTAC 발급/인증 서버와 리눅스 OS, 그리고 임베디드 보드로 구성된다. OTAC 발급/인증 서버는 사용자 DB 역할을 겸하며 클라우드에서 동작한다. 리눅스 OS는 2종 카메라 인터페이스, OTAC 발급/인증 서버의 연결, 방문자 단말 인증, 임베디드 보드와의 연결을 담당한다. 임베디드 보드는 센서 데이터를 처리한다.

3.2 OTAC 태그의 구조

OTAC 태그는 QR 코드 생성을 위한 방문자의 이름과 인증 정보로 구성되어 있으며 통신의 편의성을 위하여 <그림 3>과 같은 구조로 설계한다.

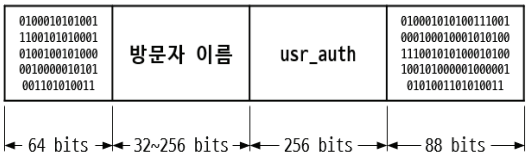

그림 3. OTAC 태그의 구조
Figure 3. Structure of OTAC Tag

태그의 필드는 ASCII 문자 ';'로 구분되며 'ENTRPASS;realname;usr_auth;ENDENTRPASS'와 같은 형식의 헤더, 방문자 이름, usr_auth, 트레일러로 구성된다. 각 필드는 3.5의 <그림 10>과 같이 정의할 개인 정보 DB에 맞추어 설계하였다.

3.3 안면인식 카메라의 적용

거주자용 안면인식 시스템은 안면 깊이 정보 측정 기술이 적용된 카메라를 사용한다. 상용화된 모델로는 HVC-P2, Voyager 등 여러 종류가 있으며 본 논문에서는 중규모 조직부터 대규모 조직까지 10,000명 이상의 인원 등록을 적용하기 위하여 다음 <그림 4>의 Voyager-2H를 선정하였다.

Voyager-2H는 최대 30,000명의 얼굴 등록이 가능하며 오수락률(False Acceptance Rate)은 0.1%부터 0.001%까지 선택 가능하다. 0~8,000 lux의 작동 조도 범위를 가져 일반적인 사무실(30~1,500 lux)의 설치에 적합하다[20]. 이와 더불어 인증에 1초 미만이 소요되어 빠른 출입이 가능하다[21].

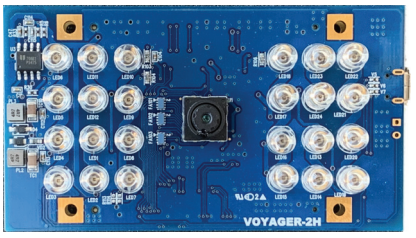

그림 4. 안면인식 카메라 Voyager-2H
Figure 4. Face Recognition Camera Voyager-2H

3.4 거주자 및 방문자 인증 프로토콜의 설계

본 논문에서 제안한 시스템 프로토콜은 리눅스 OS, OTAC 발급/인증 서버, 임베디드 보드, 안면인식 카메라, 그리고 사용자 스마트폰 상에서 다음과 같은 흐름으로 전개된다. 사용자 스마트폰이 리눅스 OS와 같은 네트워크에 접속한 상태에서 진행된다. 본 시스템은 다음과 같은 4개의 프로토콜로 구성된다.

- 상시 거주자 출입 프로토콜
- 방문자 사전 등록 프로토콜
- OTAC 발급/인증 프로토콜
- 상시 거주자 등록 프로토콜

방문자와 거주자에 대한 인증 프로세스는 동시에 수행되며 두 프로세스 중 한 개의 인증 과정만으로도 출입이 허용된다. 상시 거주자 출입 프로토콜은 다음과 같은 순서로 진행되며 <그림 5>와 같다.

① 레이저 근접 센서가 사용자의 접근을 감지함
② 안면인식 프로세스를 시작함
③ 안면인식 프로세스의 타임아웃은 10초로 설정하였으며 변경 가능함
④ 안면인식에 성공할 경우 리눅스 OS에게 알림. 상태 코드와 안면 고유 ID를 전송함

⑤ 거주자에게 시각 신호를 표시하고 출입문 개방 신호를 전송함

타임아웃 내에 인식이 완료되지 않을 경우 안면인식 카메라가 안면인식 실패 메시지를 전송하며 시각 신호 표시를 위해 리눅스 OS는 이를 임베디드 보드에게 전달한다. 안면인식 실패의 경우에는 <그림 5>의 ①~③, ⑥~⑦을 따른다.

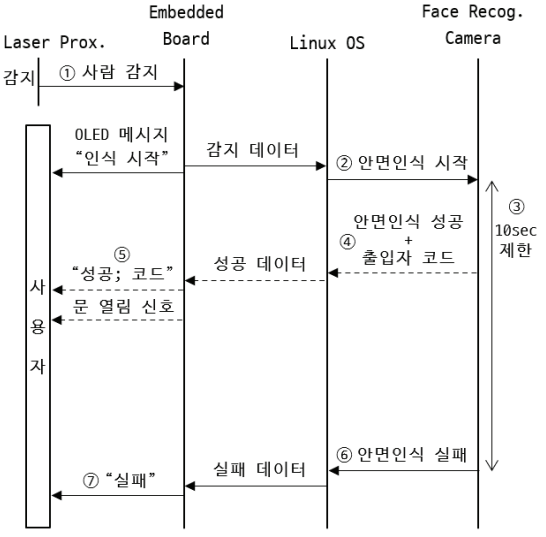

그림 5. 상시 거주자 출입 프로토콜
Figure 5. Resident Authentication Process Data Protocol

방문자 사전 등록 프로토콜은 다음과 같이 진행되며 <그림 6>과 같은 순서로 진행된다.

① 관리자가 OTAC 발급/인증 서버에 접속하여 방문자의 이름, 이메일, 단말기 MAC 주소를 입력함

② OTAC 발급/인증 서버가 각각 256비트의 tempkey, usr_auth 키를 생성하여 인증 및 출입정보 DB에 ①의 정보와 함께 삽입함

③ 방문자에게 OTAC 발급 링크와 안내문이 담긴 이메일을 발송함

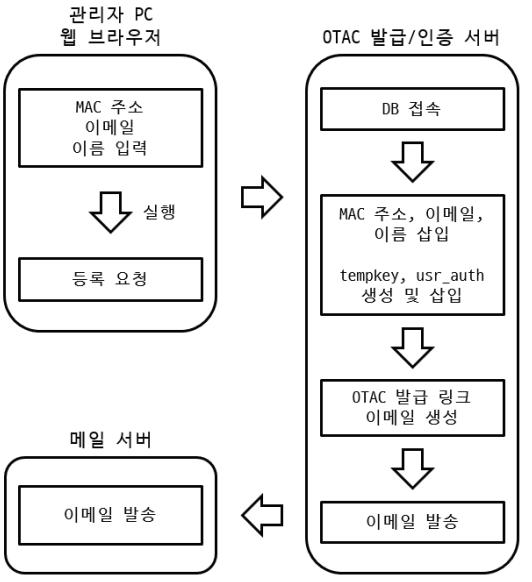

그림 6. 방문자 사전 등록 프로토콜
Figure 6. Visitor Pre-Registration Process Data Protocol

OTAC 발급/인증 프로토콜은 다음과 같은 순서로 진행된다.

① 방문자가 이메일 내의 발급 링크를 클릭함

② 방문자 스마트폰에 MAC 주소를 질의함

③ MAC 주소, tempkey를 OTAC 발급/인증 서버에 전송함

④ tempkey와 MAC 주소가 일치할 시 OTAC (QR 코드)를 전송함. DB에서 tempkey를 삭제함

⑤ 방문자가 OTAC를 카메라에 태그함

⑥ OTAC 태그의 usr_auth 필드를 OTAC 발급/인증 서버에 전송함

⑦ 인증 성공 시 문 개방 신호를 전송함. DB에서 usr_auth를 삭제함

OTAC 발급/인증 프로토콜은 다음 <그림 7>과 같다.

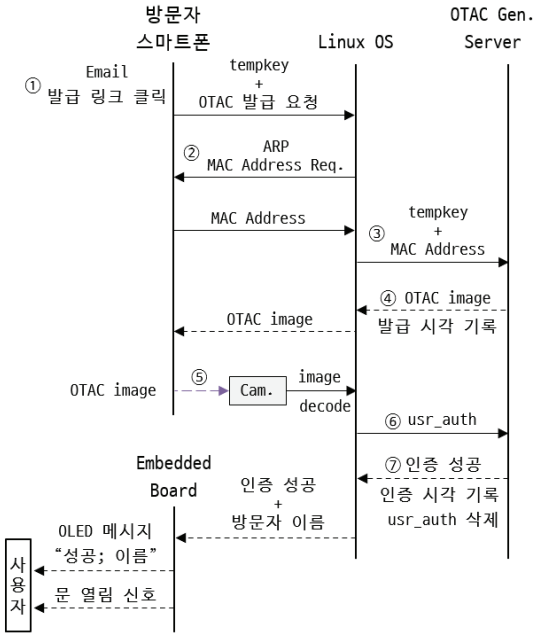

그림 7. OTAC 발급/인증 프로토콜
Figure 7. OTAC Generation/Authentication Data Protocol

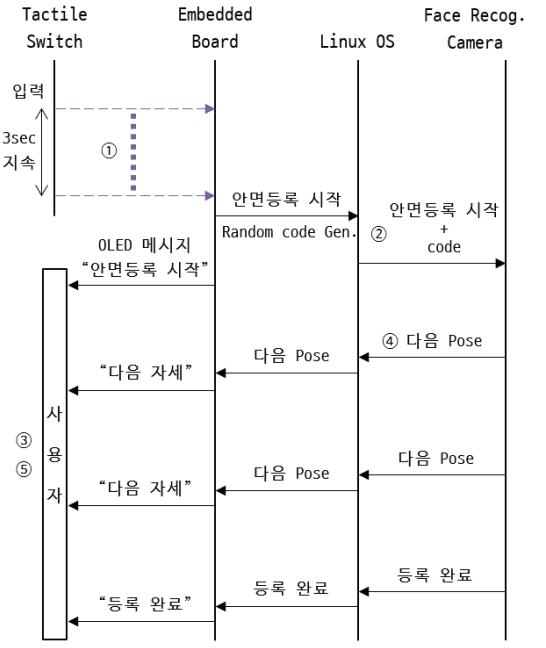

그림 8. 상시 거주자 등록 프로토콜
Figure 8. Resident Registration Data Protocol

상시 거주자 등록 프로토콜은 다음과 같은 순서로 진행된다.

① 텍타일 스위치를 3초간 눌러 상시 거주자 등록을 요청함
② 리눅스 OS가 안면등록 프로세스를 시작함
③ 거주자가 안면인식 카메라 정면을 응시함
④ 해당 자세 등록 완료 시 ‘다음 자세로 변경’ 메시지를 출력함
⑤ ③~④ 단계를 3번 반복함

상시 거주자 등록 프로토콜은 다음 <그림 8>과 같다.

리눅스 OS와 임베디드 보드 간의 시리얼 통신은 본 논문에서 제안하는 패킷 형태로 상태 정보를 전달하며 그 형태는 다음과 같다. 헤더와 트레일러를 포함한 ‘;’로 구분된 블록으로 구성되며 <그림 9>의 패킷을 UTF-8로 인코드하여 전송한다.

<그림 9>의 패킷은 설계자의 편의를 위하여 시스템 제어에 필요한 제어 변수를 나열한 형태이나, 추후 표준화 등을 통하여 시스템 공통 형태로 개발할 필요성이 있다.

* Linux OS -> Embedded Board
OTAC Tag 인증 성공
realname과 현재 시각 전송

```
SUCCESS;realname;ENDNAME;CURTIME;time.now();ENDCURTIME;END;
```

인증 실패

```
FAILURE;;END;
```

안면인식 카메라: 안면인식 성공

```
SUCCESS;출입자 이름;ENDNAME;VOYEND;
```

안면인식 카메라: 안면인식 실패

```
VOYFAILURE;
```

그림 9. 시리얼 통신 패킷 구조
Figure 9. Packet Structure of Serial Communication

3.5 인증 및 출입정보 개인 DB의 설계

인증 및 출입정보 DB는 방문자의 인증과 OTAC 태그의 발급 현황을 기록하기 위하여 <그림 10>과 같이 설계하였다.

* index 컬럼은 밑줄로 표시
* unique 컬럼은 이탤릭체로 표시

idx	realname	email	*tempkey*	*usr_auth*
int (20)	varchar (32)	varchar (255)	varchar (64)	varchar (64)
1	백순철	soonchul.baek @gmail.com	1wVPfpLf STRPcHz1 TQvftxRcG HfYM1CY	vy2WaXcE dlzCppyeY ZOrhgCTc 7LJf97N

hardwareaddr	creationtime	modifiedtime
varchar (32)	timestamp	timestamp
XX:XX:XX:XX:XX:XX	2019-12-06 08:12:37	*NULL*

그림 10. 인증 및 출입정보 DB의 형태
Figure 10. Table Diagram of Authentication and Access Log DB

idx는 인덱스 관리에 사용되며 realname과 email은 방문자 이름과 이메일 주소이다. tempkey는 OTAC 발급을 위해 생성되는 키이며 usr_auth는 OTAC 태그에 삽입되는 키다. hardwareaddr는 방문자 스마트폰의 MAC 주소이다. 관리자가 방문자의 정보를 등록할 때 등록 시각이 creationtime에 저장된다. 인증 발생 시 modifiedtime에 실행 시각이 저장된다.

4. 출입통제 시스템의 구현

4.1 적용 보드 및 인식 카메라의 연결

제안한 시스템은 사용자의 출입 시 2가지의 방법으로 인증한다. 첫 번째로 OTAC를 사용한 인증은 방문자의 출입 허가에 사용한다. 이 인증 방식의 구현을 위해서는 카메라 영상의 실시간 처리, 네트워크 연결, 시리얼 통신이 필요하다. 카메라 영상 처리는 Python 3.7.5 상에서 OpenCV pyzbar 라이브러리를 사용하였다.

두 번째로 안면인식 카메라를 사용한 인증은 상시 거주자의 출입 허가에 사용한다. 안면인식 카메라의 오수락률은 0.1% 이내로 설정하였으며 리눅스 OS와 안면인식 카메라의 통신 프로토콜 구현은 카메라 제조사에서 제공한 SDK를 사용하였다. 상호 간 통신에는 115,200bps 대역폭의 시리얼 통신을 사용하였다. 위와 같은 기능을 구현하기 위하여 Raspbian Buster가 설치된 Raspberry Pi 3 Model B+ 보드를 선택하였다[22].

OTAC 발급/인증 서버는 Ubuntu 18.04 LTS 기반의 PHP 7.1.28, Apache 2.4.39, MySQL 5.7.25 상에서 동작하며 Amazon Lightsail의 512MB RAM 플랜을 사용하여 구동하였다[23]. 이메일은 PHPMailer를 사용하여 Gmail SMTP 서버로 발송하였다. OTAC 발급은 PHP QR Code 라이브러리, ARP 요청을 통하여 이루어진다.

본 시스템은 기존 시스템과의 연동을 위하여 모듈 방식으로 개발하였으며 기존 출입자 인증 단말, 출입통제 서버에 추가되거나 완전한 대체도 가능하다. 테스트를 위하여 프로토타입으로 제작한 시스템에 구현된 방식은 적용 편의를 위해 릴레이를 사용한 버튼 제어 방식이며 시리얼 및 네트워크 통신을 사용하였다.

4.2 시스템 구동 및 평가

시스템 구동은 출입통제 시스템을 프로토타입으로 제작하여 진행하였다. Arduino M0 Pro를 사용하여 기존 출입통제 시스템을 구현하였다[24]. 제안된 출입통제 시스템을 Raspberry Pi 3 Model B+, Arduino Due, Voyager-2H, Amazon Lightsail로 구현

하여 테스트를 진행하였다. <그림 11>과 같이 상시 거주자 인증 테스트가 성공한 것을 확인할 수 있다.

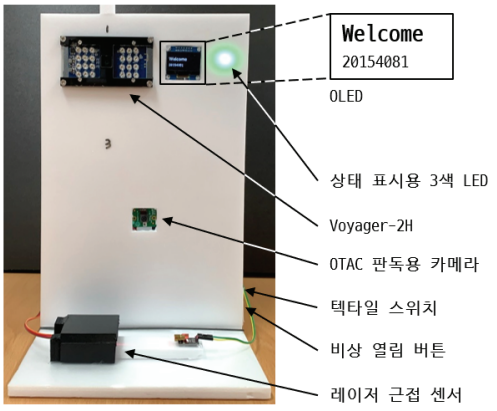

그림 11. 상시 거주자 인증 테스트
Figure 11. Resident Authentication Test

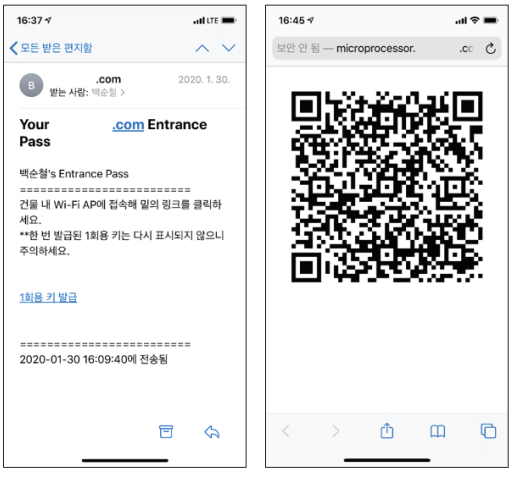

그림 12. 방문자 인증 테스트
Figure 12. Visitor Authentication Test

시스템의 신뢰성 평가를 위해 10명의 표본 집단으로 100번의 인증을 시행하였다. 테스트는 상시 거주자 인증 50회, 방문자 인증 50회로 구성하였다. <그림 12>의 (a)는 방문자가 수신하는 이메일을 나타내고, (b)는 링크를 클릭하여 발급된 OTAC 이미지가 표시된 화면을 나타낸다.

상시 거주자 인증에 대한 소요 시간은 사용자 접근 인지 시점부터 문 개방 신호 송신까지의 시간을 측정하였고 방문자 인증은 방문자 OTAC 이미지 인식 시점부터 문 개방 신호 송신까지의 시간을 측정하였다. 상시 거주자와 방문자의 등록, 이메일 발송은 사전에 완료되었다고 가정하여 테스트한 결과가 다음 <표 1>과 같이 도출되었다.

표 1. 시스템 테스트 결과
Table 1. System Test Result

인증 방법	조건	시행 횟수	성공 횟수	성공률	
상시 거주자	안경 착용	10	9	90%	98%
	모자 착용		10	100%	
	스카프 착용		10	100%	
	앞머리 없음		10	100%	
	앞머리 있음		10	100%	
방문자	-	50	50	100%	

<표 2>는 각 기능별 소요 시간으로, 18ms의 RTT(Round Trip Time)를 제외하였다.

표 2. 기능별 소요 시간
Table 2. Execution Time of Each Task

기능	소요 시간
방문자 등록	2 ms
이메일 발송	2970 ms
OTAC 발급	147 ms
방문자 인증, 문 개방 (신호 전송)	5 ms
상시 거주자 인증, 문 개방	951 ms

테스트 결과 총 성공률은 약 98%를 기록하였으며 상기 테스트에서 실패한 경우에는 재인식을 시도하여 대부분 성공하였다. 인증 실패의 원인은 카메라 촬영 시 흔들림이나 얼굴 각도 등의 문제로 나타났다.

5. 결 론

본 논문에서는 기존 입출입 시스템의 보안 취약점과 사용자 편의성을 개선한 출입통제 시스템을 설계하고 구현하였다. 제안한 시스템은 RFID 카드 등의 복제, 분실 문제를 보완하기 위하여 방문자 인증에 OTAC 태그와 ARP를 사용한 사용자 단말기 인증을 도입하였다. OTAC 태그와 발급 링크를 모두 1회용으로 설계하여 코드 탈취에 대응할 수 있었으며, 사전에 등록된 단말기만 인증 가능하다. 이와 더불어 비상 열림 버튼과 fail-safe 구조를 출입문에 적용하여 정전이나 재난 발생 시 자동으로 문이 개방되도록 하였다.

프로토타입은 Raspbian Buster가 설치된 Raspberry Pi 3 Model B+, Ubuntu 18.04 LTS, Arduino Due, Voyager-2H를 사용하여 제작하였다. 제작한 프로토타입의 테스트를 진행한 결과 방문자 인증, 상시 출입자 인증 모두 충분히 실생활에서 사용할 수 있는 높은 성공 확률과 빠른 속도를 얻을 수 있었다. 기존 시스템에 비하여 적은 비용으로 구축하여 어느 정도의 예산절감 효과도 있을 것으로 기대한다.

향후 MAC spoofing에 대한 탐지 방식, 타인의 단말기 사용 감지에 관한 방법, 자동화재탐지설비와의 연동에 관한 연구를 통하여 시스템을 업그레이드할 예정이다.

References

[1] *KISTI MARKET REPORT(2017-06) : Face recognition : Expansion of application to security and criminal investigation*, Korea Institute of Science and Technology Information, 2017.

[2] I-K. Hwang, and J-W. Baek, *Wireless access monitoring and control system based on digital door lock*, IEEE Transactions on Consumer Electronics, Vol. 53, No. 4, pp. 1724-1730, 2007.

[3] Y. K. Lee, L. Batina, and I. Verbauwhede, *EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol*, 2008 IEEE International Conference on RFID, pp. 97-104, 2008.

[4] M. Sahani, C. Nanda, A. K. Sahu, and B. Pattnaik, *Web-based online embedded door access control and home security system based on face recognition*, 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], pp. 1-6, 2015.

[5] H-Y Chien, *Secure access control schemes for RFID systems with anonymity*, 7th International Conference on Mobile Data Management (MDM'06), pp. 96-96, 2006.

[6] Y. Wang, W. Xie, X. Yu, and L. Shark, *An automatic physical access control system based on hand vein biometric identification*, IEEE Transactions on Consumer Electronics, Vol. 61, No. 3, pp. 320-327, 2015.

[7] H. Zhang, and D. Hu, *A palm vein recognition system*, 2010 International Conference on Intelligent Computation Technology and Automation, pp. 285-288, 2010.

[8] E. C. Lee, H. C. Lee, and K. R. Park, *Finger vein recognition using minutia-based alignment and local binary pattern-based feature extraction*, International Journal of Imaging Systems and Technology, Vol. 19, pp. 179-186, 2009.

[9] Z. Boriev, A. Nyrkov, S. Sokolov, and S.

Chernyi, *Software and hardware user authentication methods in the information and control systems based on biometrics*, IOP Conference Series: Materials Science and Engineering, Vol. 124, 2016.

[10] S. Ayeswarya, and J. Norman, *Seamless personal authentication using biometrics*, 2019 Innovations in Power and Advanced Computing Technologies (i-PACT), pp. 1-5, 2019.

[11] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, *Fake fingerprint detection by odor analysis,* International Conference on Biometrics 2006: Advances in Biometrics, pp. 265-272, 2005.

[12] T. Chugh, K. Cao, and A. K. Jain, *Fingerprint spoof buster: Use of minutiae-centered patches*, IEEE Transactions on Information Forensics and Security, Vol. 13, No. 9, pp. 2190-2202, 2018.

[13] I. Goicoechea-Telleria, A. Garcia-Peral, A. Husseis, and R. Sanchez-Reillo, *Presentation attack detection evaluation on mobile devices: Simplest approach for capturing and lifting a latent fingerprint*, 2018 International Carnahan Conference on Security Technology (ICCST), pp. 1-5, 2018.

[14] M. Espinoza, C. Champod, and P. Margot, *Vulnerabilities of fingerprint reader to fake fingerprints attacks*, Forensic Science International, Vol. 204, Issues 1–3, pp. 41-49, 2011.

[15] K. C. Shin, *A study on design of robust remote user authentication scheme with enhanced for anonymity and confidentiality*, Journal of Knowledge Information Technology and Systems, Vol. 14, No. 1, pp. 11-24, 2019.

[16] D. Plummer, *An ethernet address resolution protocol: Or converting network protocol addresses to 48.bit ethernet address for transmission on ethernet hardware*, STD 37, RFC 826, 1982.

[17] B. J. Nikkel, *Improving evidence acquisition from live network sources*, Digital Investigation, Vol. 3, Issue. 2, pp. 89-96, 2006.

[18] DENSO WAVE INCORPORATED, https://www.qrcode.com/en/, Nov. 2019.

[19] deltalab, http://phpqrcode.sourceforge.net/, Dec. 2019.

[20] *KS A 3011 : 1998 Recommended levels of illumination*, Korean Agency for Technology and Standards, 2018.

[21] CrasID, http://www.crasid.com/, Oct. 2019.

[22] Raspberry Pi Foundation, https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/, Dec. 2019.

[23] U-H. Lee, and Y-K. Lee, *Quality factors and SLA for cloud digital records*, Journal of Knowledge Information Technology and Systems, Vol. 13, No. 6, pp. 819-833, 2018.

[24] Arduino AG, https://www.arduino.cc/, Oct. 2019.

안면인식과 OTAC를 사용한 스마트 출입 통제 시스템

백순철[1], 홍인식[2]

[1]*순천향대학교 컴퓨터공학과 학부생*
[2]*순천향대학교 컴퓨터공학과 교수*

요 약

현대 사회에는 보안이 강화된 입출입 시스템이 중요한 요소로 자리 잡고 있다. 본 논문에서는 안면인식 카메라와 OTAC(One Time Access Code)를 이용한 실

시간 구동 입출입 시스템을 제안한다. 특히, 임베디드 보드의 응답 속도에 초점을 맞추어 딜레이 없는 시스템을 구현한다. 현재 시판되는 대부분의 출입시스템은 RFID를 이용하여 사용자를 인증한다. RFID는 인증 시간이 빠르고, 사용자의 수용성이 높다는 장점이 있다. 하지만 타인이 도용하여 사용할 수 있기 때문에 취약점이 발생한다. 이를 대체할 인증 방식으로 생체 인식이 있으며 기술적 방식으로는 안면인식, 정맥인식, 홍채인식, 지문인식 등이 사용되고 있다. 본 논문에서 제안한 방식은 안면인식 기술과 OTAC 인증을 사용한다. 이를 깊이 정보 카메라와 클라우드 환경에 구축된 사용자 DB 서버를 연동하여 임베디드 보드 상에서 구현한다. 임베디드 시스템은 Raspberry Pi 3 Model B+, Arduino Due, Ubuntu 18.04 LTS 상에서 Python, C++, C, PHP를 사용해 구성하였으며 와이파이, 시리얼을 통해 상호 간 통신하였다. 또한 중요한 스펙 중 하나인 구동 속도는 300ms로, 설정 스펙에 부합하는 결과를 얻을 수 있었다. 본 시스템을 프로토타입으로 제작하여 시스템의 실용성 및 효율성을 입증한다.

감사의 글

본 연구는 순천향대학교 학술연구비 지원으로 수행하였음.

Soon-Chul Baek is an undergraduate student at Soonchunhyang University. He has been a researcher at Embedded System Laboratory since 2019. His research interests include Cloud Computing, Computer Networks, Embedded System and Information Security.

E-mail address: soonchul.baek@gmail.com

In Sik Hong received an M.S. and Ph.D. in the Department of Electronic Engineering from Hanyang University in South Korea, in 1981 and 1988, respectively. He was senior researcher at Frontier Research Program for Water Resources from 2002 to 2011. He has been a professor at Soonchunhyang University in South Korea since 1991. His research interests include AR Technology, GIS, Embedded System and IT Convergence Technology.

E-mail address: ishong@sch.ac.kr