# 얼굴인식 출입인증 설비의 보안강화를 위한 위조 얼굴인식 성능평가 시스템 개발 연구

백영현, 김선동, 이준명, 김석윤, 김창후

유니온커뮤니티

neural76@unioncomm.co.kr, ksdskd9@unioncomm.co.kr, ljm@unioncomm.co.kr,
blacswansong@unioncomm.co.kr, kch@unioncomm.co.kr

# Fake Face Recognition Performance Evaluation System for Security Enhancement of Access Authentication Facilities

Young Hyun Baek, Sun Dong Kim, Jun Myung Lee, Seok Yun Kim, Chang Hu Kim

UNIONCOMMUNITY Co., Ltd

요 약

본 논문은 얼굴인식을 통한 출입자의 신원확인 및 보안성을 향상시키고, 불법 침입자 검색에 대한 강화된 보안성 제공을 목적으로 한다. 얼굴인식 출입인증 설비의 보안강화를 위해서는 위조 얼굴을 이용한 출입 공격 방어가 필요하다. 본 논문에서는 위조 얼굴인식 성능을 평가할 수 있는 시스템을 제안함으로써 출입인증 설비의 보안 향상을 목적으로 한다. 제안된 시스템의 성능평가를 위해 성능평가 지그 제작 및 성능평가 시스템 개발을 수행하였다. 그리고 위조 얼굴인식 성능평가 시나리오와 성능시험 항목 정의한다. 성능평가 실험을 통해 테스트에 사용된 출입인증 설비의 위조 얼굴인식 성능평가의 성능 비교를 위한 위조 허용률(SAR) 82%와 위조 검출율(SDR) 18%를 검출하고 시각화하는 결과를 보였다.

## Ⅰ. 서 론

생체인식 출입인증 기술이란 사람의 측정 가능한 신체적 특징정보를 이용하여 본인 여부를 비교, 확인 후 출입을 승인하는 기술이다. 생체인식을 이용하면 분실 및 도용의 위험이 없으며 신체 일부분을 활용한다는 점에서 편의성을 가지면서도 높은 보안 효과를 가진다. 생체인식 기술이 적용된 출입인증 설비는 지문인식, 얼굴인식, 홍채인식, 정맥인식이 적용되어 물리보안 시스템 등으로 적용되고 있다[1-3]. 출입인증 설비로 대표되는 물리보안 시스템은 물리적인 방법으로 인명과 시설뿐만 아니라 정보를 보호하는 것으로 표 1과 같이 물리적 위협에 대해 출입관리와 시설보호, 비인가자의 출입통제, 방범 관리 등을 통해 보안을 지키는 것을 의미한다.

표 1. 물리보안 응용 시스템

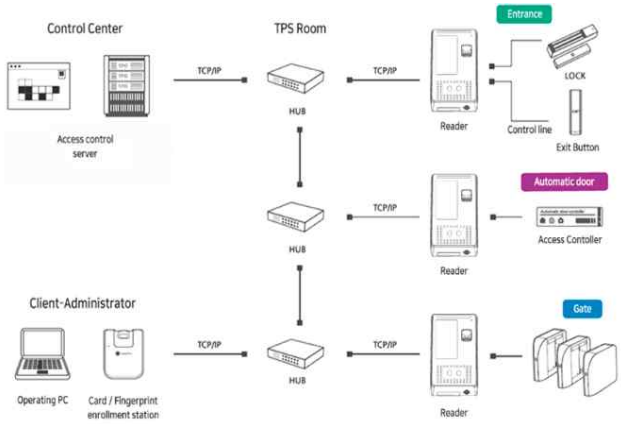
| 구분 | 기능 | 주요장비 |
|---|---|---|
| CCTV 시스템 | - 실시간 모니터링<br>- 영상 인식 및 알람 기능<br>- 비디오 전송 기능 | - Cameras, Lenses, PTZ<br>- DVR, Motion Detector<br>- Image recognition S/W |
| 출입통제 시스템 | - 출입(사람, 차량 등) 통제 기능<br>- 출입 물품 검색 및 통제 기능 | -Biometrics, Smart cards,<br>-Xray finder, Metal detector |
| 침입감지 시스템 | - 비인가자 침입 알람 기능<br>- 침입 감지 및 대응 기능<br>- 무인 보안 서비스 및 감시기능 | - Sensors, Alarms<br>- Control S/W |

본 논문에서는 얼굴인식이 적용된 출입인증 설비의 성능평가를 통해 출입자의 신원확인 및 보안성을 향상시키고, 불법 침입자 검색에 대한 강화된 보안성 제공을 목적으로 한다. 본 논문의 구성은 다음과 같다. 2장 본론에서는 얼굴인식 및 위조 얼굴 연구 현황, 그리고 성능평가 방법을 제안한다. 3장에서는 결론 및 향후 연구내용에 대해 기술한다.

## Ⅱ. 본론

### 2.1 출입인증 시스템

생체인식 출입인증 시스템은 출입자 현황파악의 효율적인 관리 지원과 비상시 원격제어를 통해 출입관리의 편의성 및 보안성을 확보한 시스템이며, 시스템 구성은 TCP/IP 통신환경과 Access Control 및 카드리더기 등으로 그림 1과 같다.




(그림 1) 출입인증 시스템 구성도.

### 2.2 얼굴인식

얼굴인식은 사용자가 특정 행동이나 별도의 접촉 없이 카메라만 응시하면 되므로 신체적 접촉을 요구하지 않는다는 점에서 거부감이 적고 자연스러움이 장점인 기술이다[5]. 각 개인마다 다른 얼굴의 DB를 등록해 두고, 입력되는 사람 얼굴 형태를 기존 구축 DB와 얼굴 외곽 윤곽선, 눈·눈썹·코 모양, 눈·코·턱 간격 등을 비교해 인증한다[3,4].

### 2.3 위조 얼굴인식 성능평가 시나리오

제안된 위조 얼굴인식 성능평가 시나리오에 따라 시험대상 제품에 본인의 실제 얼굴이 정상 등록·인증되는지 여부 및 제작한 위조 얼굴인식 정상 탐지 여부를 시험한다. 표 2는 위조 얼굴인식 성능평가 시나리오이다.

표 2. 위조 얼굴인식 성능평가 시나리오

| 시나리오 세부내용 | 시험기준 |
|---|---|
| • 등록 : 실제 얼굴인식<br>• 인증 : 위조 얼굴인식 | • 위조 얼굴인식 탐지 여부에 대한 정량적 평가 |

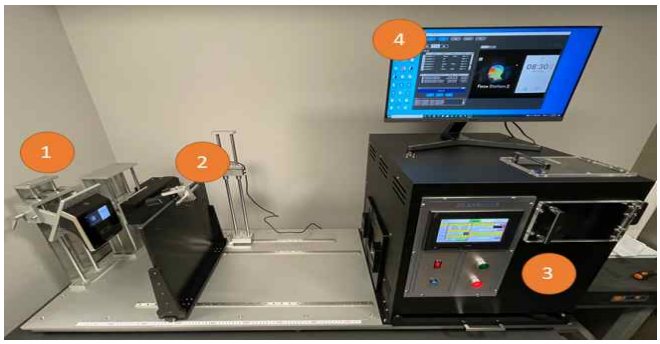
위조 얼굴인식 방어력 성능시험 항목은 표 3과 같이 FTE(Failure to Enroll), FTA(Failure to Acquire), SDR(Spoof Detection Rate), SAR(Spoof Acceptance Rate)로 정의되며, 정량적 결과를 기반으로 성능평가를 진행한다[5,6].

표 3. 위조 얼굴인식 방어력 성능시험 항목

| 시험항목 | 세부내용 |
|---|---|
| FTE | • 등록 거부율<br>- 시스템에서 시험인의 얼굴인식 등록을 거부하는 비율<br>- 등록 거부율 = (등록 실패 수 / 총 등록 시도 횟수) x 100 |
| FTA | • 인증 거부율<br>- 시스템에서 시험인의 얼굴인식 인증을 거부하는 비율<br>- 인증 거부율 = (인증 실패 수 / 총 인증 시도 횟수) x 100 |
| SDR | • 위조 검출률<br>- 위조 얼굴인식 등록·인증에 대해 위조로 판단하는 비율<br>- 위조 검출률 = (위조 판단 수 / 총 위조 입력 횟수) x 100 |
| SAR | • 위조 허용률<br>- 위조 얼굴인식 등록·인증에 대해 실제로 판단하는 비율<br>- 위조 허용률 = (실제 판단 수 / 총 위조 입력 횟수) x 100 |

### 2.4 위조 얼굴인식 성능평가 시스템

제안된 위조 얼굴인식 성능평가 시스템은 운영체제(OS)는 windows 10 이고, 출입인증 설비의 화면 인식을 위해 USB 타입 FHD 카메라를 사용하였다. 제안된 시스템은 출입인증 설비 제조사의 프로토콜에 종속되지 않고, 화면에 표시되는 내용을 분석하는 영상분석 방식으로 범용성을 제공한다. 본 시스템은 실시간 동영상 처리에 빠른 응답시간을 가져야 하며, 모든 입출력데이터를 저장 및 관리한다. 또한 중복 질의를 고속으로 처리하고, 인증 결과값에 대한 일반적인 DB 시스템의 제약 조건과 성능을 만족하도록 설계하였다. 그림 2는 위조 얼굴인식 성능평가 시스템 지그이며, ① 출입인증 설비 및 거치대, ② 출력화면 촬영용 카메라, ③ 성능분석시스템, ④ 결과모니터링 장치로 구성된다.

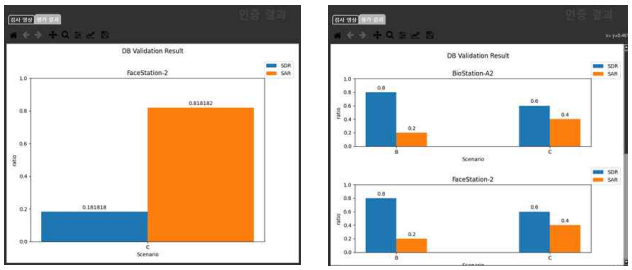



(그림 2) 위조 얼굴인식 성능평가 시스템.

성능평가는 그림 3과 같이 실험 결과를 직관적으로 모니터 화면과 메시지로 확인할 수 있다.


(그림 3) 성능평가 인증 결과 영상.

위조 얼굴인식 성능평가 결과값인 SAR, SDR를 그림 4와 같이 차트 형식으로 표현하였으며, 여러 제품 간의 성능 비교를 쉽게 확인할 수 있도록 결합 데이터 형식으로 시각화하였다.




(그림 4) 위조 얼굴인식 성능평가 결과 차트.

## Ⅲ. 결론

본 논문에서는 얼굴인식 출입인증 설비의 보안 적합성 성능평가를 위한 위조 얼굴인식 성능평가 시스템 개발과 테스트 환경 구축을 통하여 성능 검증을 수행하였다. 성능평가 실험을 통해 테스트에 사용된 출입인증 설비의 위조 얼굴인식 성능평가의 성능 비교를 위한 위조 허용률(SAR) 82%와 위조 검출율(SDR) 18%를 검출하고 시각화하는 결과를 확인할 수 있었다. 본 논문을 통해 주요 보안시설에 설치되는 얼굴인식 출입인증 설비에 위조 얼굴인식 공격에 대한 성능평가 방법이 필요함을 확인하였다. 향후, 얼굴인식 기술의 보급이 빨라짐에 따라 위조 얼굴을 이용한 침입 등 발생 되는 부작용을 방지하기 위한 성능평가 시스템으로 활용이 가능할 것으로 사료 된다.

## ACKNOWLEDGMENT

본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다.(No. 2106067)

## 참 고 문 헌

[1] 윤일영, “바이오와 보안의 융합, 생체인식 기술 융합 Weekly TIP”, 융합 연구정책센터, 제 110 권, 2018

[2] 김도현, “최근 생체인식 산업동향과 시사점, 이슈분석 188호”,https://now.k2base.re.kr, 2021

[3] 과학기술일자리진흥원. (2021). 신체적 특징을 이용한 바이오매트릭(생체인식) 기술동향. https://www.bioin.or.kr

[4] Zhang, Kaipeng, et al. (2016). Joint face detection and alignment using multitask cascaded convolutional networks. *IEEE Signal Processing Letters, 23*(10), 1499-1503.

[5] 한국인터넷진흥원. (2021). 바이오인식시스템 시험·인증 안내서.

[6] 한국인터넷진흥원. (2022). 위조 바이오인식 방어력 성능 시험 안내서.