(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년01월24일
(11) 등록번호 10-1941966
(24) 등록일자 2019년01월18일

(51) 국제특허분류(Int. Cl.)
H04B 1/40 (2015.01) *E05B 37/00* (2018.01)
E05B 47/00 (2018.01) *G05B 19/00* (2006.01)
G06K 9/18 (2006.01) *G06K 9/20* (2006.01)
H04W 12/06 (2009.01)
(52) CPC특허분류
H04B 1/40 (2013.01)
E05B 37/0072 (2013.01)
(21) 출원번호 10-2018-0083434(분할)
(22) 출원일자 2018년07월18일
심사청구일자 2018년07월18일
(65) 공개번호 10-2018-0084720
(43) 공개일자 2018년07월25일
(62) 원출원 특허 10-2014-0173064
원출원일자 2014년12월04일
심사청구일자 2017년10월26일
(56) 선행기술조사문헌
KR1020140020545 A*
KR101345018 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
에스케이텔레콤 주식회사
서울특별시 중구 을지로 65 (을지로2가)
(72) 발명자
김지훈
서울특별시 중구 을지로 65 (을지로2가) SK T-타워
강상철
서울특별시 중구 을지로 65 (을지로2가) SK T-타워
(74) 대리인
박종한

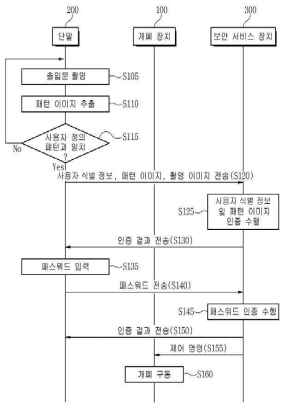
전체 청구항 수 : 총 14 항 심사관 : 손동현

(54) 발명의 명칭 **패턴 인식 기반의 출입 제어를 위한 장치, 방법 및 프로그램**

(57) 요 약

본 발명은 증강 현실 기술을 이용하여 개폐 장치의 촬영 이미지로부터 패턴 이미지를 인식하고, 인식된 패턴 이미지를 이용하여 개폐 장치 및 상기 개폐 장치를 통해 출입하는 사용자를 인증하는 패턴 인식 기반의 출입 제어를 위한 장치 및 방법에 관한 것으로서, 단말에서 개폐 장치를 촬영한 촬영 이미지로부터 인식된 패턴 이미지를 기 저장된 사용자 정의 패턴의 패턴 이미지와 상기 인식한 패턴 이미지가 매칭되는 지를 비교하여 1차 인증을 수행하고, 보안 서비스 장치가, 상기 단말로부터 사용자 식별 정보, 상기 촬영 이미지, 및 1차 인증된 패턴 이미지를 수신하고, 이를 기 등록된 계정 정보와 비교하여 2차 인증을 수행하고, 상기 보안 서비스 장치가, 상기 단말로부터 입력된 패스워드를 상기 계정 정보와 비교하여 3차 인증을 수행하도록 구현된다.

대 표 도 - 도4



(52) CPC특허분류
E05B 47/00 (2018.05)
G05B 19/00 (2013.01)
G06K 9/18 (2013.01)
G06K 9/20 (2013.01)
H04W 12/06 (2019.01)
E05B 2047/0071 (2013.01)
E05Y 2900/132 (2013.01)

명 세 서

청구범위

청구항 1

개폐장치를 촬영한 촬영 이미지를 획득하는 단계;

상기 개폐장치를 촬영한 촬영 이미지로부터 지정된 패턴 이미지를 인식하는 단계;

상기 인식된 패턴 이미지와 기 저장된 사용자 정의 패턴 이미지를 비교하는 단계;

상기 비교 결과를 개폐 장치를 제어하는 보안 서비스 장치에 전송하는 단계;를 실행시키는 것을 특징으로 하는 컴퓨터 판독 가능한 기록 매체에 기록된 프로그램.

청구항 2

제1항에 있어서,

상기 전송하는 단계에서, 상기 인식된 패턴 이미지 및 기 저장된 사용자 식별 정보를 상기 보안 서비스 장치에 전송하고,

상기 보안 서비스 장치로부터 상기 사용자 식별 정보에 대응되는 계정 정보에 연결된 패턴 이미지와 상기 전송된 패턴 이미지의 비교 결과를 수신하는 단계:를 더 포함하는 것을 특징으로 하는 컴퓨터 판독 가능한 기록 매체에 기록된 프로그램.

청구항 3

제1항에 있어서,

상기 전송하는 단계에서,

상기 촬영 이미지, 및 기 저장된 사용자 식별 정보를 상기 보안 서비스 장치에 전송하고,

상기 보안 서비스 장치로부터 상기 사용자 식별 정보에 대응되는 계정 정보에 연결된 패턴 이미지와 상기 보안 서비스 장치가 상기 촬영 이미지로부터 인식한 패턴 이미지의 비교 결과를 수신하는 단계;를 더 포함하는 것을 특징으로 하는 컴퓨터 판독 가능한 기록 매체에 기록된 프로그램.

청구항 4

제1항에 있어서,

패스워드 입력을 위한 사용자 인터페이스를 출력하는 단계;

상기 사용자 인터페이스를 통해 패스워드을 수신하는 단계;

상기 패스워드와 기 저장된 패스워드를 비교하여 인증 여부를 확인하는 단계;

상기 인증 결과를 상기 보안 서비스 장치로 전송하는 단계;를 더 포함하는 것을 특징으로 하는 컴퓨터 판독 가능한 기록 매체에 기록된 프로그램.

청구항 5

제1항에 있어서,

패스워드 입력을 위한 사용자 인터페이스를 출력하는 단계;

상기 사용자 인터페이스를 통해 패스워드를 수신하는 단계;

상기 패스워드를 상기 보안 서비스 장치로 전송하는 단계;

상기 보안 서비스 장치로부터 상기 사용자 입력에 대응하는 패스워드의 인증 결과를 수신하는 단계;를 더 포함

하는 것을 특징으로 하는 컴퓨터 판독 가능한 기록 매체에 기록된 프로그램.

청구항 6

제1항에 있어서,

상기 패턴 이미지는 증강 현실 기반으로 생성되는 것을 특징으로 하는 컴퓨터 판독 가능한 기록 매체에 기록된 프로그램.

청구항 7

카메라부;

사용자 인터페이스를 출력하는 출력부;

사용자 정의 패턴 이미지를 저장하는 저장부;

상기 저장부와 기능적으로 연결된 제어부;를 포함하고,

상기 제어부는

상기 카메라부를 이용하여 개폐 장치와 관련한 촬영 이미지를 획득하고,

상기 획득된 촬영 이미지로부터 지정된 패턴 이미지를 인식하고,

상기 인식된 패턴 이미지와 상기 저장부에 기 저장된 사용자 정의 패턴 이미지를 비교하고,

상기 비교 결과를 상기 개폐 장치 제어와 관련한 보안 서비스 장치에 전송하는 것을 특징으로 하는 단말 장치.

청구항 8

제7항에 있어서,

상기 제어부는

상기 인식된 패턴 이미지 및 기 저장된 사용자 식별 정보를 상기 보안 서비스 장치에 전송하고, 상기 보안 서비스 장치로부터 상기 사용자 식별 정보에 대응되는 계정 정보에 연결된 패턴 이미지와 상기 전송된 패턴 이미지의 비교 결과를 수신하거나,

상기 촬영 이미지 및 기 저장된 사용자 식별 정보를 상기 보안 서비스 장치에 전송하여, 상기 보안 서비스 장치로부터 상기 사용자 식별 정보에 대응되는 계정 정보에 연결된 패턴 이미지와 상기 보안 서비스 장치가 상기 촬영 이미지로부터 인식한 패턴 이미지의 비교 결과를 수신하는 것을 특징으로 하는 단말 장치.

청구항 9

제7항에 있어서,

상기 제어부는

상기 출력부를 통해 패스워드 입력을 위한 사용자 인터페이스를 출력하고,

상기 패스워드 입력 인터페이스를 통해 입력된 패스워드를 수신하고, 상기 입력된 패스워드와 상기 저장부에 기 저장된 패스워드를 비교하여 인증하거나, 상기 비교 결과를 상기 보안 서비스 장치로 전송하거나, 상기 입력된 패스워드를 상기 보안 서비스 장치로 전송하고, 상기 보안 서비스 장치로부터 패스워드에 대한 인증 결과를 수신하도록 설정된 것을 특징으로 하는 단말 장치.

청구항 10

사용자 식별 정보에 매칭되는 계정 정보, 상기 계정 정보에 연결된 패턴 이미지를 저장하는 저장부;

상기 저장부와 기능적으로 연결된 인증 처리부;를 포함하고,

상기 인증 처리부는

단말로부터 개폐 장치와 관련된 촬영 이미지 또는 상기 촬영 이미지로부터 인식한 패턴 이미지를 상기 단말에

관련된 사용자 식별 정보와 함께 수신하고,

상기 수신된 사용자 식별 정보와 매칭되는 계정 정보를 이용하여, 상기 계정 정보와 관련된 기 지정된 패턴 이미지를 획득하고,

상기 기 저장된 패턴 이미지와 상기 단말로부터 수신한 패턴 이미지 또는 상기 단말로부터 수신한 촬영 이미지로부터 인식한 패턴 이미지를 비교하고,

상기 패턴 이미지 비교 결과를 상기 단말 또는 상기 개폐 장치 중 적어도 하나에 송신하도록 설정된 것을 특징으로 하는 보안 서비스 장치.

청구항 11

제10항에 있어서,

상기 인증 처리부는

상기 패턴 이미지 비교 결과에 따른 상기 개폐 장치 개폐를 제어하는 제어 명령을 상기 단말 또는 상기 개폐 장치 중 적어도 하나에 송신하도록 설정된 것을 특징으로 하는 보안 서비스 장치.

청구항 12

제10항에 있어서,

상기 인증 처리부는

상기 단말로부터 패스워드 정보를 수신하고,

상기 수신된 패스워드 정보와 상기 저장부에 기 저장된 패스워드 정보를 비교하고,

상기 패스워드 정보 비교 결과 또는 상기 패스워드 정보 비교 결과에 따른 상기 개폐 장치 개폐를 제어하는 제어 명령을 상기 단말 또는 상기 개폐 장치 중 적어도 하나에 송신하도록 설정된 것을 특징으로 하는 보안 서비스 장치.

청구항 13

단말로부터 개폐 장치와 관련된 촬영 이미지 또는 상기 촬영 이미지로부터 인식한 패턴 이미지를 상기 단말에 관련된 사용자 식별 정보와 함께 수신하는 단계;

상기 수신된 사용자 식별 정보와 매칭되는 계정 정보를 이용하여, 상기 계정 정보와 관련된 기 저장된 패턴 이미지를 획득하는 단계;

상기 기 저장된 패턴 이미지와, 상기 단말로부터 수신한 패턴 이미지 또는 상기 단말로부터 수신한 촬영 이미지로부터 인식한 패턴 이미지를 비교하는 단계;

상기 패턴 이미지 비교 결과 또는 상기 패턴 이미지 비교 결과에 따른 상기 개폐 장치 개폐를 제어하는 제어 명령를 상기 단말 및 상기 개폐 장치 중 적어도 하나에 송신하는 단계;를 포함하는 보안 서비스 장치에 의한 패턴 인식 기반의 출입 제어를 위한 방법.

청구항 14

제13항에 있어서,

상기 단말로부터 패스워드 정보를 수신하는 단계;

상기 수신된 패스워드 정보와 기 저장된 패스워드 정보를 비교하는 단계;

상기 패스워드 정보 비교 결과 또는 상기 패스워드 정보 비교 결과에 따른 상기 개폐 장치 개폐를 제어하는 제어 명령을 상기 단말 또는 상기 개폐 장치 중 적어도 하나에 송신하는 단계:를 더 포함하는 보안 서비스 장치에 의한 패턴 인식 기반의 출입 제어를 위한 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 패턴 인식 기반의 출입 제어를 위한 장치, 방법 및 이를 위한 컴퓨터 판독 가능한 기록매체에 기록된 프로그램에 관한 것으로서, 더욱 상세하게는 증강 현실 기술을 이용하여 개폐 장치의 촬영 이미지로부터 패턴 이미지를 인식하고, 인식된 패턴 이미지를 이용하여 개폐 장치 및 상기 개폐 장치를 통해 출입하는 사용자를 인증하는 패턴 인식 기반의 출입 제어를 위한 장치, 방법 및 프로그램에 관한 것이다.

배 경 기 술

[0002] 최근에는 개방형 OS를 탑재함으로써, 휴대전화에 PC의 고기능을 결합시킨 스마트 폰(Smart Phone)이 대중화되면서, 고기능, 고성능의 스마트 폰의 활용 방향에 대한 다양한 시도가 이루어지고 있다.

[0003] 특히, 초소형 제작 기술의 발달과 함께 첨단 센서들이 더욱 소형화되고 저렴해지면서 스마트 폰에 더 많은 센서들이 탑재될 수 있으며, 이에 증강현실이나 3D 게임 등과 같이 이러한 센서들을 활용한 지능형 애플리케이션들이 많이 개발되고 있다.

[0004] 상기 증강현실(AR: Augmented Reality)은 카메라를 통해 실시간으로 촬영되는 실세계의 영상 정보에 실세계에서는 볼 수 없는 정적, 동적, 시각적, 청각적 요소가 포함된 컨텐츠를 융합하여 제공하는 기술로서, 촬영된 영상을 분석하여 영상 내에 포함된 기 설정된 객체(패턴 혹은 마크)를 인식하고, 인식된 객체(패턴 혹은 마크)를 기준으로 이미지, 동영상, 소리, 3D 모델 등의 디지털 컨텐츠를 상기 영상 위에 중첩하여 표시한다. 이러한 증강현실은 게임, 교육, 서비스 등 다양한 분야에 적용되고 있다.

[0005] 한편, 방범 및 보안 등을 목적으로, 출입하고자 하는 사람의 출입 권한을 확인하여 출입을 허용하는 보안 서비스가 이용되고 있는데, 이때, 출입자를 확인하기 위한 방법으로서, 기 설정된 패스워드를 입력하는 방식, 얼굴 인식 기술, 지문 인식 기술, 홍채 인식 기술 등의 생채 정보를 기반으로 한 사용자 인식 기술, NFC(Near Field Communication) 기술 등이 이용되고 있다.

[0006] 그러나, 아직 이러한 출입 통제 시스템에 증강현실을 적용하려는 시도는 이루어지지 않고 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 한국공개특허 제10-2005-0109338호, 2005년 11월 21일 공개 (명칭: 인체 인식을 이용한 출입문 도어락 보안 시스템)

발명의 내용

해결하려는 과제

[0008] 본 발명은 출입하고자 하는 사람의 출입 권한을 확인하여 출입을 제어하는데 있어서, 증강 현실 기술을 이용하여 개폐 장치의 촬영 이미지로부터 패턴 이미지를 인식하고, 인식된 패턴 이미지를 이용하여 개폐 장치 및 상기 개폐 장치를 통해 출입하는 사용자를 인증하는 패턴 인식 기반의 출입 제어를 위한 장치, 방법 및 프로그램을 제공하고자 한다.

과제의 해결 수단

[0009] 상술한 과제의 해결 수단으로서, 본 발명은 촬영 이미지를 획득하는 단계; 상기 획득된 촬영 이미지로부터 지정된 패턴 이미지를 인식하는 단계; 상기 인식된 패턴 이미지와 기 저장된 사용자 정의 패턴 이미지를 비교하는 단계; 상기 비교 결과를 개폐 장치를 제어하는 보안 서비스 장치에 전송하는 단계;를 포함하는 것을 특징으로 하는 컴퓨터 판독 가능한 기록매체에 기록된 프로그램을 제공한다.

[0010] 본 발명에 따른 프로그램은, 상기 전송하는 단계에서, 상기 인식된 패턴 이미지 및 기 저장된 사용자 식별 정보를 상기 보안 서비스 장치에 전송하고, 상기 보안 서비스 장치로부터 상기 사용자 식별 정보에 대응되는 계정 정보에 연결된 패턴 이미지와 상기 전송된 패턴 이미지의 비교 결과를 수신하는 단계:를 더 포함할 수 있다.

[0011] 본 발명에 따른 프로그램은, 상기 전송하는 단계에서, 상기 촬영 이미지, 상기 인식된 패턴 이미지 및 기 저장

된 사용자 식별 정보를 상기 보안 서비스 장치에 전송하고, 상기 보안 서비스 장치로부터 상기 사용자 식별 정보에 대응되는 계정 정보에 연결된 패턴 이미지와 상기 보안 서비스 장치가 상기 촬영 이미지로부터 인식한 패턴 이미지의 비교 결과를 수신하는 단계;를 더 포함할 수 있다.

[0012] 또한, 본 발명에 따른 프로그램은, 패스워드 입력을 위한 사용자 인터페이스를 출력하는 단계; 상기 사용자 인터페이스를 통해 패스워드을 수신하는 단계; 상기 패스워드와 기 저장된 패스워드를 비교하여 인증 여부를 확인하는 단계; 상기 인증 결과를 상기 보안 서비스 장치로 전송하는 단계;를 더 포함할 수 있다.

[0013] 또한, 본 발명에 따른 프로그램은, 패스워드 입력을 위한 사용자 인터페이스를 출력하는 단계; 상기 사용자 인터페이스를 통해 패스워드를 수신하는 단계; 상기 패스워드를 상기 보안 서비스 장치로 전송하는 단계; 상기 보안 서비스 장치로부터 상기 사용자 입력에 대응하는 패스워드의 인증 결과를 수신하는 단계;를 더 포함할 수 있다.

[0014] 상기에서, 패턴 이미지는 증강 현실 기반으로 생성될 수 있다.

[0015] 또한, 본 발명은 상술한 과제의 다른 해결 수단으로서, 카메라부; 사용자 인터페이스를 출력하는 출력부; 사용자 정의 패턴 이미지를 저장하는 저장부; 상기 저장부와 기능적으로 연결된 제어부;를 포함하고, 상기 제어부는 상기 카메라부를 이용하여 개폐 장치와 관련한 촬영 이미지를 획득하고, 상기 획득된 촬영 이미지로부터 지정된 패턴 이미지를 인식하고, 상기 인식된 패턴 이미지와 상기 저장부에 기 저장된 사용자 정의 패턴 이미지를 비교하고, 상기 비교 결과를 상기 개폐 장치 제어와 관련한 보안 서비스 장치에 전송하는 것을 특징으로 한다.

[0016] 본 발명에 따른 단말 장치에 있어서, 상기 제어부는, 상기 인식된 패턴 이미지 및 기 저장된 사용자 식별 정보를 상기 보안 서비스 장치에 전송하고, 상기 보안 서비스 장치로부터 상기 사용자 식별 정보에 대응되는 계정 정보에 연결된 패턴 이미지와 상기 전송된 패턴 이미지의 비교 결과를 수신하거나, 상기 촬영 이미지 및 기 저장된 사용자 식별 정보를 상기 보안 서비스 장치에 전송하여, 상기 보안 서비스 장치로부터 상기 사용자 식별 정보에 대응되는 계정 정보에 연결된 패턴 이미지와 상기 보안 서비스 장치가 상기 촬영 이미지로부터 인식한 패턴 이미지의 비교 결과를 수신할 수 있다.

[0017] 또한, 상기 제어부는, 상기 출력부를 통해 패스워드 입력을 위한 사용자 인터페이스를 출력하고, 상기 패스워드 입력 인터페이스를 통해 입력된 패스워드를 수신하고, 상기 입력된 패스워드와 상기 저장부에 기 저장된 패스워드를 비교하여 인증하거나, 상기 비교 결과를 상기 보안 서비스 장치로 전송하거나, 상기 입력된 패스워드를 상기 보안 서비스 장치로 전송하고, 상기 보안 서비스 장치로부터 패스워드에 대한 인증 결과를 수신할 수 있다.

[0018] 더하여, 본 발명은 상술한 과제의 다른 해결 수단으로서, 사용자 식별 정보에 매칭되는 계정 정보, 상기 계정 정보에 연결된 패턴 이미지를 저장하는 저장부; 상기 저장부와 기능적으로 연결된 인증 처리부;를 포함하고, 상기 인증 처리부는 단말로부터 개폐 장치와 관련된 촬영 이미지 또는 상기 촬영 이미지로부터 인식한 패턴 이미지를 상기 단말에 관련된 사용자 식별 정보와 함께 수신하고, 상기 수신된 사용자 식별 정보와 매칭되는 계정 정보를 이용하여, 상기 계정 정보와 관련된 기 지정된 패턴 이미지를 획득하고, 상기 기 저장된 패턴 이미지와 상기 단말로부터 수신한 패턴 이미지 또는 상기 단말로부터 수신한 촬영 이미지로부터 인식한 패턴 이미지를 비교하고, 상기 패턴 이미지 비교 결과를 상기 단말 또는 상기 개폐 장치 중 적어도 하나에 송신할 수 있다.

[0019] 상기 인증 처리부는, 상기 패턴 이미지 비교 결과에 따른 상기 개폐 장치 개폐를 제어하는 제어 명령을 상기 단말 또는 상기 개폐 장치 중 적어도 하나에 송신할 수 있으며, 상기 단말로부터 패스워드 정보를 수신하고, 상기 수신된 패스워드 정보와 상기 저장부에 기 저장된 패스워드 정보를 비교하고, 상기 패스워드 비교 결과 또는 상기 패스워드 비교 결과에 따른 상기 개폐 장치 개폐를 제어하는 제어 명령을 상기 단말 또는 상기 개폐 장치 중 적어도 하나에 송신할 수 있다.

[0020] 또한, 본 발명은 상술한 과제의 또 다른 해결 수단으로서, 단말로부터 개폐 장치와 관련된 촬영 이미지 또는 상기 촬영 이미지로부터 인식한 패턴 이미지를 상기 단말에 관련된 사용자 식별 정보와 함께 수신하는 단계; 상기 수신된 사용자 식별 정보와 매칭되는 계정 정보를 이용하여, 상기 계정 정보와 관련된 기 지정된 패턴 이미지를 획득하는 단계; 상기 기 저장된 패턴 이미지와, 상기 단말로부터 수신한 패턴 이미지 또는 상기 단말로부터 수신한 촬영 이미지로부터 인식한 패턴 이미지를 비교하는 단계; 상기 패턴 이미지 비교 결과 또는 상기 패턴 이미지 비교 결과에 따른 상기 개폐 장치 개폐를 제어하는 제어 명령를 상기 단말 및 상기 개폐 장치 중 적어도 하나에 송신하는 단계;를 포함하는 보안 서비스 장치에 의한 출입 제어 방법을 제공한다.

[0021] 상기 방법은, 상기 단말로부터 패스워드 정보를 수신하는 단계; 상기 수신된 패스워드 정보와 기 저장된 패스워드 정보를 비교하는 단계; 상기 패스워드 비교 결과 또는 상기 패스워드 비교 결과에 따른 상기 개폐 장치 개폐

를 제어하는 제어 명령을 상기 단말 또는 상기 개폐 장치 중 적어도 하나에 송신하는 단계:를 더 포함할 수 있다.

발명의 효과

[0022] 본 발명에 따른 패턴 인식 기반의 출입 제어 기술은, 증강현실과 같은, 영상 처리를 통해서 개폐 장치의 촬영 이미지로부터 그 패턴 이미지를 인식하고, 이를 기반으로 다단 인증을 수행함으로써, 보안성을 더 향상시킬 수 있다.

[0023] 구체적으로, 본 발명은 단말에서 촬영 이미지로부터 인식한 패턴 이미지를 기 등록된 사용자 정의 패턴의 패턴 이미지와 비교하여, 정당한, 즉, 출입 가능한 개폐 장치인지를 1차 인증하고, 1차 인증에 성공한 경우, 사용자 식별 정보와 함께 상기 인식한 패턴 이미지 및 촬영 이미지를 보안 서비스 장치로 전송하여, 상기 보안 서비스 장치를 통해서 사용자 확인 및 패턴 이미지를 재확인하는 2차 인증을 수행하고, 2차 인증에 성공한 경우, 단말을 통해 사용자로부터 입력 받은 패스워드를 기 등록된 패스워드와 비교하는 3차 인증을 수행함으로써, 정당한 사용자 및 상기 사용자가 출입할 개폐 장치를 함께 인증할 수 있으며, 그 결과 출입 통제의 신뢰성을 더 향상시킬 수 있다.

[0024] 또한, 본 발명은 증강현실을 출입 통제와 결합함으로써, 사용자 편의를 향상시킬 수 있을 뿐만 아니라, 사용자가 소지한 단말을 이용함으로써, 개폐 장치별 사용자 인식을 위한 장치의 설치 비용을 줄일 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명에 따른 출입 통제 시스템의 전체 구성을 개략적으로 나타낸 블럭도이다.

도 2는 본 발명에 따른 출입 통제 시스템에 있어서, 단말의 구성을 나타낸 블럭도이다.

도 3은 본 발명에 따른 출입 통제 시스템에 있어서, 보안 서비스 장치의 구성을 나타낸 블럭도이다.

도 4는 본 발명에 따른 출입 통제 시스템에 의한 패턴 인식 기반의 출입 제어 과정을 나타낸 순서도이다.

도 5는 본 발명에 따른 출입 통제 시스템에서, 단말에 의해 수행되는 패턴 인식 기반의 출입 제어 과정을 보다 구체적으로 나타낸 순서도이다.

도 6은 본 발명에 따른 출입 통제 시스템에서, 보안 서비스 장치에 의해 관리되는 계정 관리 테이블을 나타낸 도면이다.

도 7은 본 발명에 따른 출입 통제 시스템에서 이용되는 데이터 포맷을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0026] 이하 본 발명의 바람직한 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 도면 부호로 나타내고 있음에 유의하여야 한다.

[0027] 이하에서 설명되는 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이거나 사전적인 의미로 한정해서 해석되어서는 아니 되며, 발명자는 그 자신의 발명을 가장 최선의 방법으로 설명하기 위한 용어의 개념으로 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야만 한다. 따라서 본 명세서에 기재된 실시 예와 도면에 도시된 구성은 본 발명의 가장 바람직한 일 실시 예에 불과할 뿐이고, 본 발명의 기술적 사상을 모두 대변하는 것은 아니므로, 본 출원시점에 있어서 이들을 대체할 수 있는 다양한 균등물과 변형 예들이 있을 수 있음을 이해하여야 한다.

[0028] 더하여, 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급할 경우, 이는 논리적 또는 물리적으로 연결되거나, 접속될 수 있음을 의미한다. 다시 말해, 구성요소가 다른 구성요소에 직접적으로 연결되거나 접속되어 있을 수 있지만, 중간에 다른 구성요소가 존재할 수도 있으며, 간접적으로 연결되거나 접속될 수도 있다고 이해되어야 할 것이다.

[0029] 또한, 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 또한, 본 명세서에서 기술되는 "포함 한다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자,

단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0030] 도 1은 본 발명에 따른 출입 통제 시스템의 전체 구성을 개략적으로 나타낸 블럭도이다.

[0031] 도 1을 참조하면, 본 발명에 따른 출입 통제 시스템은, 개폐 장치(100)와, 단말(200)과, 보안 서비스 장치(300)를 포함한다.

[0032] 이때, 상기 단말(200)과 보안 서비스 장치(300)는 유무선 인터넷, Wi-Fi망, 이동통신망을 포함하는 유무선 통신망뿐만 아니라, 블루투스, Zigbee와 같은 유무선 근거리 통신 등 다양한 통신기술을 이용하여 연결될 수 있다.

[0033] 또한, 상기 보안 서비스 장치(300)와 개폐 장치(100)는 전용선을 통해 연결될 수 도 있고, 상기 상기 단말(200)과 보안 서비스 장치(300)와 마찬가지로, 유무선 인터넷, Wi-Fi망, 이동통신망을 포함하는 유무선 통신망뿐만 아니라, 블루투스, Zigbee와 같은 유무선 근거리 통신 등 다양한 통신기술을 이용하여 연결될 수 있다.

[0034] 상기 개폐 장치(100)는 보안 서비스 장치(300)로부터 전송된 제어 신호에 의해서 개폐되는 장치를 의미한다. 이러한 개폐 장치(100)는 열고 닫을 수 있도록 구현된 구조물과, 상기 구조물을 구동하는 구동 수단 및 상기 보안 서비스 장치(300)와 통신하여 상기 구동 수단을 제어하기 위한 제어 수단 등을 포함하여 이루어질 수 있다. 상기 구조물은 출입문, 창문 등이 될 수 있다.

[0035] 상기 단말(200)은 개폐 장치(100)를 이용하는 사용자가 휴대하는 장치로서, 휴대 가능한 사용자 장치라면 어떠한 것이든 이용 가능하다. 예를 들어, 상기 단말(200)은, 스마트 폰, 태블릿 PC 등이 될 수 도 있으며, 출입 제어를 위해 별도로 구현된 휴대장치일 수 도 있다. 전자의 경우, 상기 단말(200)은 하드웨어 혹은 소프트웨어 혹은 하드웨어와 소프트웨어의 조합으로 구현될 수 있는 본 발명에 따른 패턴 인식 기반의 출입 제어를 위한 장치를 구비함으로써, 본 발명에 따른 패턴 인식 기반의 출입 제어 기능을 수행할 수 있다. 사용자는 이러한 단말(200)을 이용하여 개폐 장치(100)를 촬영하여, 증강 현실 기술을 통해 상기 개폐 장치(100)의 촬영 이미지로부터 패턴 이미지를 인식하고, 이를 기반으로 보안 서비스 장치(200)와 연동하여 사용자 인증을 수행한다. 여기서, 패턴 이미지는 개폐장치(100)를 촬영한 영상으로부터 추출할 수 있는 패턴을 의미하는 것으로서, 바람직하게는 다른 개폐장치(100)와 구분할 수 있는 고유 패턴인 것이 바람직하다. 상기 패턴 이미지는 예를 들어, 개폐되는 구조물의 형상, 무늬, 구조물에 부착된 표식 등이 될 수 있다.

[0036] 보안 서비스 장치(200)는, 상기 단말(200)과의 연동을 통해 사용자를 인증하고 인증 결과에 따라서 상기 개폐 장치(100)를 제어하기 위한 서버 장치이다. 구체적으로, 보안 서비스 장치(200)는 사용자 별로 출입 제어를 위한 계정 정보를 관리하고, 상기 단말(200)과 연동하여 다단 인증을 통해 사용자의 출입 권한을 확인하고, 이를 기반으로 상기 개폐 장치(100)를 제어한다. 이때, 상기 계정 정보는, 사용자를 식별하기 위한 계정 식별 정보와, 상기 사용자가 이용 가능한 개폐 장치(100)와 관련된 패턴 이미지 정보 및 패스워드와 같은 인증 정보를 포함하고, 사이 보안 서비스 장치(200)는, 단말(200)에서 추출된 패턴 이미지와 계정 정보에 등록된 패턴 이미지 정보의 비교를 통한 인증 및 상기 단말(200)로부터 입력된 패스워드와 계정 정보로 등록된 패스워드의 비교를 통해 인증을 수행할 수 있다.

[0037] 본 발명에 따른 출입 통제 시스템의 구성 요소, 즉, 단말(200) 및 보안 서비스 장치(300)의 구성 및 기능을 도 2 및 도 3을 참조하여 더 구체적으로 설명한다.

[0038] 도 2는 본 발명에 따른 출입 통제 시스템에 있어서, 단말의 구성을 나타낸 블럭도이다.

[0039] 도 2를 참조하면, 단말(200)은 입력부(210)와, 출력부(220)와, 통신부(230)와, 카메라부(240)와, 저장부(250)와, 제어부(260)를 포함할 수 있다. 그리고, 상기 단말(200)은 본 발명에 따른 패턴 인식 기반의 출입 제어를 수행하기 위한 구성으로서, 영상 캡처 모듈(261), 영상 처리 모듈(262), 서버 연동 모듈(263) 및 사용자 인터페이스 모듈(264)를 포함할 수 있다. 본 발명에 따른 단말(200)에 포함된 '모듈'은 소프트웨어 혹은 하드웨어 혹은 소프트웨어와 하드웨어의 조합으로 구현되어 하기에서 설명하는 일정 기능을 수행하는 구성 요소를 의미한다.

[0040] 이하, 각 구성 요소에 대해서 보다 구체적으로 설명한다.

[0041] 상기 입력부(210)는 사용자 조작에 따라서, 문자, 숫자, 기호 혹은 명령어 중 어느 하나에 대응하는 사용자 입력 신호를 생성하여 상기 제어부(260)로 전달한다. 이러한 입력부(210)는 공지된 다양한 입력 수단으로 구현될 수 있으며, 예를 들어, 키보드, 키패드와 같은 키 입력 수단, 마우스, 조이스틱, 트랙볼, 터치패드와 같은 위치 지정 수단, 사용자의 움직임을 감지하여, 이에 대응하는 입력 신호를 생성하는 제스처 입력 수단 등이 이용될

수 있다. 특히, 본 발명에 있어서, 상기 입력부(210)는 개폐 장치(100)를 촬영하기 위한 카메라부(240)의 조작을 위한 명령, 패스워드 입력 등을 위해 이용될 수 있다.

[0042] 출력부(220)는 단말(200)의 동작 과정 혹은 동작 수행 결과를 사용자가 인식할 수 있는 형태로 출력하는 수단으로서, 예를 들어, LCD, LED, ELD, PDP, OLED, 레이저 TV, 프로젝터 등과 같은 디스플레이 장치가 될 수 있다. 본 발명에 있어서, 상기 출력부(220)는 카메라부(240)에서 촬영된 영상을 출력하거나, 사용자 인터페이스 모듈(264)에 의해 제공되는 패스워드 입력 및 인증 결과를 출력하기 위한 사용자 인터페이스 화면을 출력할 수 있다.

[0043] 통신부(230)는 상기 보안 서비스 장치(300)와 통신하기 위한 수단으로서, 상기 보안 서비스 장치(300)와의 연결 방식에 따라, 통신을 수행할 수 있다. 예를 들어, 상기 통신부(230)는 이동통신망 또는 Wi-Fi AP에 접속하여, 접속된 이동통신망을 통해서 보안 서비스 장치(300)로 데이터를 송신하거나, 보안 서비스 장치(300)로부터 전송된 데이터를 수신할 수 있다. 이외에도, 상기 통신부(230)는 공지된 다양한 통신 방식으로 구현될 수 있다.

[0044] 카메라부(240)는 빛을 이용하여 피사체의 형상 및 색채 등을 촬상하여 이미지로 기록하는 수단으로서, 상기 카메라부(240)는 이미지뿐만 아니라 동영상을 촬영할 수 있다. 본 발명에 있어서, 상기 카메라부(240)는 개폐 장치(100)를 촬영하는데 이용된다.

[0045] 저장부(250)는 제어부(260)에 의해 실행되는 프로그램 혹은 처리되는 데이터를 기록하기 위한 수단으로서, 주기억장치와 보조기억장치로 포함하는 개념이다. 예를 들어, 상기 저장부(250)는 롬(ROM), 램(ROM), 하드디스크, 블루레이디스크, 플래시 메모리, USB 메모리 등을 포함할 수 있다. 본 발명에 있어서, 상기 단말(200)의 저장부(250)는 출입 제어를 위한 이용되는 사용자 정의 패턴 정보(251)를 저장한다. 상기 사용자 정의 패턴 정보(251)는 사용자가 출입할 수 있는 개폐 장치(100)의 촬영 이미지로부터 인식될 수 있는 패턴 이미지로서, 사전에 등록되어 저장된다. 상기 사용자 정의 패턴 정보(251)는 보안 서비스 장치(300)로부터 수신되거나, 사전 등록 과정을 통해서 사용자가 촬영한 출입하고자 하는 개폐 장치(100)의 촬영 이미지로부터 추출될 수 있다.

[0046] 제어부(260)는 단말(200)에서 이루어지는 동작 전반을 제어하고 실행하는 구성요소로서, 프로세서(Processor)를 포함하여 이루어지고, 상기 프로세서를 통해 저장부(250)에 저장된 컴퓨터 프로그램을 로딩하여, 상기 컴퓨터 프로그램의 명령어를 해석하여 이에 따라서 상기 입력부(210), 출력부(220), 통신부(230), 카메라부(240), 저장부(250)를 제어함으로써, 소정의 기능을 수행한다. 이렇게 제어부(260)에서, 컴퓨터 프로그램 명령의 수행에 의해 이루어지는 기능을 모듈로 표현할 때, 상기 제어부(260)는, 본 발명에 따른 패턴 인식 기반의 출입 제어를 위하여, 영상 캡처 모듈(261), 영상 처리 모듈(262), 서버 연동 모듈(263) 및 사용자 인터페이스 모듈(264)를 포함할 수 있다.

[0047] 상기 영상 캡처 모듈(261)은 카메라부(240)로부터 출력되는 촬영 이미지를 캡처하여 영상 처리 모듈(262)로 전달하는 수단으로서, 이때, 상기 입력부(210)로부터 전송된 사용자 입력 신호에 따라서, 특정 시점에 촬영된 이미지를 캡처할 수 있다. 본 발명에 있어서, 캡처된 촬영 이미지는 개폐 장치(100)를 촬영한 이미지가 된다.

[0048] 상기 영상 처리 모듈(263)은 영상 캡처 모듈(261)에 의해 캡처된 촬영 이미지로부터 출입 제어를 위한 인증에 이용될 패턴 이미지를 인식하기 위한 수단으로서, 예를 들어, 촬영 이미지에 포함된 특정 패턴 혹은 객체 혹은 마크를 인식하고, 인식 결과에 따라서 상기 촬영 이미지에 디지털 컨텐츠를 중첩하여 출력하는 AR(Augmented Reality) 모듈이 될 수 있다. AR 모듈을 이용하는 경우, 촬영 이미지로부터 패턴 이미지를 인식하는 처리와 함께, 기 등록된 패턴 이미지에 대응하여 지정된 컨텐츠(예를 들어, 출입문 제어를 위한 사용자 인터페이스 화면)를 상기 촬영 이미지와 결합하여 증강현실로 나타낼 수 도 있다.

[0049] 그리고 상기 패턴 이미지는, 앞서 설명한 바와 같이, 촬영 이미지로부터 추출되는 것으로서, 예를 들어, 개폐 장치(100)의 표면에 나타나는 무늬, 개폐 장치(100)의 형상, 그에 부착되거나 그려진 표식 등이 될 수 있다.

[0050] 그리고, 상기 영상 처리 모듈(263)은 촬영 이미지로부터 인식된 패턴 이미지를 상기 저장부(250)에 저장된 사용자 정의 패턴 정보의 패턴 이미지와 비교하여 매칭되는 지를 판단한다. 이를 통해서 본 발명에 따른 출입 통제 시스템은, 단말(200)에서 촬영 이미지로부터 인식된 패턴 이미지를 기반으로 1차 인증을 수행함으로써, 상기 개폐 장치(100)가 사용자가 지정한 개폐 장치(100)인지를 먼저 판단할 수 있다. 상기 판단에서, 개폐 장치(100)의 촬영 이미지로부터 인식된 패턴 이미지가 기 저장된 사용자 정의 패턴 정보(251)의 패턴 이미지와 매칭되지 않으면, 상기 개폐 장치(100)가 출입 제어 대상이 아닌 것으로 간주할 수 있다.

[0051] 반대로, 상기 판단 결과, 개폐 장치(100)의 촬영 이미지로부터 인식된 패턴 이미지가 기 저장된 사용자 정의 패턴 정보(251)의 패턴 이미지와 매칭되면, 1차 인증에 성공한 것으로 간주하여, 서버 연동 모듈(263)을 통해서

출입을 위한 사용자 인증을 위해 필요한 정보, 구체적으로, 사용자 식별 정보와, 상기 카메라부(240)로부터 캡처한 촬영 이미지와, 상기 영상 처리 모듈(262)에서 매칭되는 것으로 판단된 패턴 이미지를 보안 서비스 장치(300)로 전송한다.

[0052] 상기 서버 연동 모듈(263)은 출입 통제를 위한 서버 장치, 즉, 보안 서비스 장치(300)와의 연동을 수행하기 위한 구성으로서, 통신부(230)를 제어하여, 상기 영상 처리 모듈(262) 및 사용자 인터페이스 모듈(264)로 보안 서비스 장치(300)로부터 전송된 메시지를 전달하거나, 역으로, 상기 영상 처리 모듈(262) 및 사용자 인터페이스 모듈(264)로부터 요청한 메시지를 보안 서비스 장치(300)로 전달한다.

[0053] 상기 사용자 인터페이스 모듈(264)는 출입 제어를 위한 사용자 인터페이스를 수행하는 구성으로서, 입력부(210) 및 출력부(220)를 제어하여, 인증 결과를 출력하여 사용자에게 안내하고, 사용자로부터 인증 수행에 필요한 정보, 예를 들어, 패스워드를 입력 받기 위한 사용자 인터페이스를 제공한다.

[0054] 상술한 바와 같이 구성된 단말(200)의 출입 제어를 위한 과정은 도 4 및 도 5를 참조하여 추후 구체적으로 설명하기로 한다.

[0055] 다음으로, 도 3은 본 발명에 따른 출입 통제 시스템에 있어서, 보안 서비스 장치(300)의 구성을 나타낸 블럭도이다.

[0056] 보안 서비스 장치(300)는, 단말(200)과 연동하여 본 발명에 따른 패턴 인식 기반의 출입 제어를 수행하기 위하여, 저장부(310), 영상 처리부(320), 인증 처리부(330) 및 개폐 장치 제어부(340)를 포함할 수 있다.

[0057] 상기 저장부(330)는, 보안 서비스 장치(300)에서 출입 제어를 위해 필요한 데이터를 저장하기 위한 구성으로서, NAS(Network Access Storage)를 포함하는 다양한 저장 수단으로 구현될 수 있다. 특히, 본 발명에 있어서, 상기 저장부(330)는, 계정 관리 DB를 저장한다. 상기 계정 관리 DB는 출입 제어를 이용하는 사용자의 계정 정보를 관리하는 데이터베이스이다. 여기서, 상기 계정 관리 DB는, 사용자 식별 정보, 3차 인증을 위한 패스워드 정보, 2차 인증을 위한 패턴 이미지 정보를 저장할 수 있다. 도 6은 상기 계정 관리 DB에서 관리되는 계정 정보를 예시한 테이블로서, 사용자 식별 정보(61)로서, 단말(200)에 대하여 할당되는 IMSI(International Mobile Station Identity), TMSI(Temporary Mobile Subscriber Identity), MIN(Mobile Identification Number), MSISDN(Mobile Station International ISDN Number), IMEI(International Mobile Equipment Identity), PIN(Personal Identification Number) 혹은 사용자에 의해 생성된 ID를 저장하여 관리할 수 있으며, 상술한 사용자 식별 정보(61)별로, 패스워드 정보(62)와, 패턴 이미지 정보(63)를 매칭하여 관리한다. 여기서, 패스워드 정보(62)는 계정 생성 시 사용자로부터 입력 받아 생성할 수 있으며, 패턴 이미지 정보(63)는 사용자에게 출입이 허용된 개폐 장치(100)로부터 인식될 수 있는 패턴 이미지로서, 이를 식별하기 위한 인식 이미지 ID, 상기 패턴 이미지 데이터가 저장된 인식 이미지 경로 정보를 포함하여 이루어질 수 있다. 특히, 상기 패스워드 정보(62)는 안전한 관리를 위하여 암호화되어 저장될 수 있다.

[0058] 영상 처리부(320)는 입력된 촬영 이미지로부터 패턴 이미지를 인식하기 위한 구성으로서, 예를 들어, 촬영 이미지에 포함된 특정 패턴 혹은 객체 혹은 마크를 인식하고, 인식 결과에 따라서 상기 촬영 이미지에 디지털 컨텐츠를 중첩하여 출력하는 AR(Augmented Reality) 엔진으로 구현될 수 있다

[0059] 인증 처리부(330)는 단말(200)과 연동하여 상기 단말(200)의 사용자가 출입하고자 하는 개폐 장치(100) 및 사용자가 정당한 지를 인증하기 위한 수단으로서, 구체적으로, 상기 인증 처리부(330)는 패턴 인식 기반의 2차 인증 및 패스워드 기반의 3차 인증을 수행한다.

[0060] 개폐 장치 제어부(340)는 개폐 장치(100)와 통신하여, 상기 개폐 장치(100)의 구동을 제어하기 위한 구성으로서, 상기 인증 처리부(330)의 인증 결과에 따라서 상기 개폐 장치(100)는 개폐시킬 수 있다.

[0061] 이하 상술한 바와 같이 구성된 단말(200) 및 보안 서비스 장치(300)의 연동에 따른 패턴 인식 기반의 출입 제어 과정을 도 4를 참조하여 설명한다.

[0062] 도 4는 본 발명에 따른 출입 통제 시스템에 의한 패턴 인식 기반의 출입 제어 과정을 나타낸 순서도이다.

[0063] 도 4를 참조하면, 단말(200)은 특정 개폐 장치(100)를 출입하고자 하는 사용자의 조작에 따라서, 카메라부(240)를 통해서 상기 개폐 장치(100)를 촬영한다(S105).

[0064] 그리고, 영상 캡처 모듈(261) 및 영상 처리 모듈(262)를 통해서 상기 개폐 장치(100)의 촬영 이미지를 캡처하여, 상기 촬영 이미지로부터 패턴 이미지를 인식한다(S110).

[0065] 그리고, 상기 단말(200)은 상기 인식된 패턴 이미지를 기반으로 정당한 개폐 장치인지를 판단하기 위한 1차 인증을 수행하는데, 이는, 상기 영상 처리 모듈(262)에 의해 촬영 이미지로부터 인식된 패턴 이미지가 기 등록된 사용자 정의 패턴의 패턴 이미지와 일치하는 지를 비교함에 의해 이루어진다(S115).

[0066] 비교 결과, 상기 인식한 패턴 이미지가 사용자 정의 패턴의 패턴 이미지와 일치하지 않으면, 상기 개폐 장치(100)가 사용자가 출입 가능한 개폐 장치 혹은 출입 제어 대상이 아니므로, 인증이 실패한 것으로 간주하고, 반대로, 사용자 정의 패턴의 패턴 이미지와 일치하면, 1차 인증이 성공된 것으로 간주하여, 사용자 식별 정보, 상기 단말(200)에서 인식한 패턴 이미지, 그리고, 개폐 장치(100)를 촬영한 촬영 이미지를 보안 서비스 장치(300)로 전송한다(S120). 상기 정보들은 도 7의 (a)과 같은 데이터 포맷으로 전송될 수 있다. 여기서, 타입은, 사용자 식별 정보의 종류를 정의하는 정보로서, 예를 들어, 사용자 식별 정보가 MSIDSN인지 ID인지를 구분하기 위한 것이다.

[0067] 이를 수신한 보안 서비스 장치(300)는 상기 수신한 사용자 식별 정보, 패턴 이미지, 촬영 이미지를 기반으로 2차 인증을 수행하는데, 구체적으로, 상기 사용자 식별 정보로 기 등록된 계정 정보를 비교하여, 정당한 사용자인지를 확인하고, 아울러, 상기 수신한 패턴 이미지를 통해 저장부(310)를 조회하여 상기 패턴 이미지 정보를 확인하고, 아울러, 상기 영상 처리부(320)를 통해서 상기 촬영 이미지로부터 패턴 이미지를 인식한 후, 인식된 패턴 이미지가 상기 매칭되는 지를 판단한다(S125). 여기서, 사용자 식별 정보가 기 등록되어 있지 않거나, 상기 패턴 이미지가 기 등록된 정보와 매칭되지 않는 경우, 2차 인증이 실패한 것으로 판단하고, 그 반대인 경우, 2차 인증이 성공한 것으로 판단한다.

[0068] 상기 보안 서비스 장치(300)는 이러한 2차 인증 결과를 단말(200)로 전송한다.

[0069] 이에 단말(200)은 사용자 인터페이스 모듈(264)을 통해서 상기 보안 서비스 장치(300)로부터 출력된 2차 인증 결과를 사용자가에게 안내할 수 있다.

[0070] 이때, 상기 2차 인증 결과가 성공적인 경우, 상기 단말(200)은 3차 인증을 위한 패스워드 입력을 위한 사용자 인터페이스 화면을 출력하고, 이를 통해 입력된 패스워드를 보안 서비스 장치(300)로 전송한다(S135. S140). 이때, 단말(200)은 도 7의 (b)과 같은 데이터 포맷으로 패스워드를 전송할 수 있다. 도 7의 (b)에서, 타입은 사용자 식별 정보의 종류를 정의하는 것이다. 아울러, 상기 사용자 인터페이스 화면은 카메라부(240)로 촬영된 촬영 이미지 위에 중첩되어 증강 현실로 표현될 수 있다. 아울러, 안전한 전송을 위하여, 상기 패스워드를 암호화하여 전송할 수 있다. 이때, 상기 패스워드의 암호화를 위하여, DES(data Encryption Standard), AES, SEED, MASK와 같은 대칭형 암호 방식 및 RSA(Rivest Shamir Adleman), DSS(Digital Signature Standard)와 같은 비대칭형 암호 방식 등, 기 공지된 다양한 암호화 알고리즘이 적용될 수 있다.

[0071] 2차 인증에 성공한 경우, 상기 보안 서비스 장치(300)는 상기 단말(200)로부터 3차 인증을 위한 패스워드를 전송 받고, 수신한 패스워드가 계정 정보로 등록된 패스워드와 일치하는 지를 판단하여 3차 인증을 수행한다(S145). 앞서 설명한 바와 같이, 상기 보안 서비스 장치(300)는 도 6에 도시된 바와 같이, 패스워드 정보(62)를 기 등록하여 관리함에 있어서, 개인 정보의 노출 위험을 최소화하기 위하여 상기 패스워드 정보를 암호화하여 저장할 수 있다. 이 경우, 상기 S145 단계는 상기 단말(200)로부터 암호화된 패스워드와 상기 기 등록된 패스워드 정보(62)를 기 설정된 유사도 판단 함수를 통해 연산함으로써, 복호화 과정없이 안전하게 3차 인증을 수행할 수 있으며, 이를 위해서 기 공지된 다양한 암호화 기법들을 참조할 수 있다.

[0072] 여기서, 패스워드가 계정 정보에 기 등록된 패스워드와 일치하면, 3차 인증에 성공한 것으로 판단하고, 그 반대인 경우, 3차 인증에 실패한 것으로 판단한다.

[0073] 보안 서비스 장치(300)는 3차 인증 결과를 단말(200)로 전송하여, 단말(200)이 3차 인증 결과를 사용자에게 안내할 수 있도록 한다(S150).

[0074] 이울러, 보안 서비스 장치(300)는 3차 인증에 성공한 경우, 최종적으로 해당 개폐 장치(100), 즉, 상기 패턴 이미지에 대응되는 개폐 장치(100)로 개폐를 제어하는 제어 명령을 전송하여(S155), 개폐 장치(100)가 구동되도록 제어한다(S160).

[0075] 상술한 과정 중, 단말(200)에 의해 수행되는 출입 제어를 위한 과정을 더 구체적으로 나타내면 도 5와 같다.

[0076] 도 5를 참조하여, 단말(200)의 패턴 인식 기반 출입 제어 과정을 보다 구체적으로 설명한다.

[0077] 단말(200)은 본 발명에 따른 패턴 인식 기반의 출입 제어를 수행하기 위하여, 먼저 사용자 정의 패턴을 등록하여야 한다(S205). 상기 사용자 정의 패턴은, 출입 제어 대상인 개폐 장치(100)에 매칭되는 패턴 이미지를 의미

하는 것으로서, 해당 개폐 장치(100)를 사전에 촬영한 후 촬영 이미지로부터 영상 처리 모듈(262)을 통해 인식된 패턴 이미지를 사용자 정의 패턴으로 등록할 수 있다.

[0078] 이후, 사용자가 출입을 위해 개폐 장치(100)의 촬영을 지시하면, 단말(200)은 카메라부(240)를 통해 상기 개폐 장치(100)를 촬영하고, 영상 캡처 모듈(261)이 상기 카메라부(240)에 의해 촬영된 이미지를 캡처하여 획득한다(S210).

[0079] 이어, 단말(200)의 영상 처리 모듈(262)이 캡처된 촬영 이미지로부터 출입 제어를 위한 인증에 이용될 패턴 이미지를 인식하고(S215), 인식한 패턴 이미지를 기 등록된 사용자 정의 패턴 정보의 패턴 이미지와 비교하여 1차 인증을 수행한다(S220). 여기서, 인식한 패턴 이미지가 사용자 정의 패턴의 패턴 이미지와 매칭되면, 1차 인증이 성공한 것으로 판단하고, 매칭되지 않으면, 1차 인증이 실패한 것으로 판단한다(S225).

[0080] 그리고, 1차 인증에 성공한 경우, 단말(200)은, 사용자 식별 정보와, 캡처한 촬영 이미지와, 인식한 패턴 이미지를 보안 서비스 장치(300)로 전송하여, 인증을 요청한다(S230). 이에, 보안 서비스 장치(300)는, 상기 수신한 사용자 식별 정보와, 캡처한 촬영 이미지와, 인식한 패턴 이미지와, 계정 정보를 비교하여 2차 인증을 수행한다.

[0081] 단말(200)은 보안 서비스 장치(300)로부터 2차 인증 결과를 수신하고(235), 수신된 2차 인증 결과가 성공인 경우(S240), 패스워드 입력을 위한 사용자 인터페이스 화면을 출력하여, 입력부(210)를 통해서 사용자로부터 패스워드를 입력 받는다(S245).

[0082] 그리고, 단말(200)은 입력된 패스워드를 보안 서비스 장치(300)로 전송한다(S250). 이때, 상기 단말(200)은 보안 서비스 장치(300)와의 사이에 기 설정된 암호화 설정에 따라서, 상기 패스워드를 암호화하여 전송할 수 있다.

[0083] 이후, 단말(200)은 3차 인증 결과를 대기하여, 보안 서비스 장치(300)로부터 3차 인증 결과가 수신되고(S255), 수신된 3차 인증 결과가 성공인 경우, 단말(200)은, 인증이 성공하여 개폐 장치(100)가 구동함을 안내하는 메시지를 출력부(220)로 출력할 수 있다(S265).

[0084] 반대로, 상기에서, 1차 인증, 2차 인증, 3차 인증 중 어느 하나에 실패한 경우, 단말(200)은 인증이 실패하여 개폐 장치(100)가 구동되지 않음을 안내하는 메시지를 출력한다(S270).

[0085] 상기 도 4 및 도 5에 도시한 과정은, 다양한 컴퓨터 수단을 통하여 판독 가능한 소프트웨어 형태로 구현되어 컴퓨터로 판독 가능한 기록매체에 기록될 수 있다. 여기서, 기록매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 기록매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 예컨대 기록매체는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 롬(ROM), 램(RAM, Random Access Memory), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함한다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 이러한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0086] 이상과 같이, 본 명세서와 도면에는 본 발명의 바람직한 실시 예에 대하여 개시하였으나, 여기에 개시된 실시 예외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 자명한 것이다. 또한, 본 명세서와 도면에서 특정 용어들이 사용되었으나, 이는 단지 본 발명의 기술 내용을 쉽게 설명하고 발명의 이해를 돕기 위한 일반적인 의미에서 사용된 것이지, 본 발명의 범위를 한정하고자 하는 것은 아니다.

[0087] 또한, 본 발명에 따른 보안 서비스 장치(300)나 단말(200)은 하나 이상의 프로세서로 하여금 앞서 설명한 기능들과 프로세스를 수행하도록 하는 명령에 의하여 구동될 수 있다. 예를 들어 그러한 명령으로는, 예컨대 JavaScript나 ECMAScript 명령 등의 스크립트 명령과 같은 해석되는 명령이나 실행 가능한 코드 혹은 컴퓨터로 판독 가능한 매체에 저장되는 기타의 명령이 포함될 수 있다. 여기서, 프로세서는, 싱글 쓰레드(Single-threaded) 프로세서일 수 있으며, 다른 구현예에서 본 프로세서는 멀티 쓰레드(Multithreaded) 프로세서일 수 있으며, 메모리 혹은 저장 장치 상에 저장된 명령을 처리하는 것이 가능하다.

[0088] 비록 본 명세서와 도면에서는 예시적인 장치 구성을 기술하고 있지만, 본 명세서에서 설명하는 기능적인 동작과 주제의 구현물들은 다른 유형의 디지털 전자 회로로 구현되거나, 본 명세서에서 개시하는 구조 및 그 구조적인 등가물들을 포함하는 컴퓨터 소프트웨어, 펌웨어 혹은 하드웨어로 구현되거나, 이들 중 하나 이상의 결합으로 구현 가능하다. 본 명세서에서 설명하는 주제의 구현물들은 하나 이상의 컴퓨터 프로그램 제품, 다시 말해 본 발명에 따른 장치의 동작을 제어하기 위하여 혹은 이것에 의한 실행을 위하여 유형의 프로그램 저장매체 상에 인코딩된 컴퓨터 프로그램 명령에 관한 하나 이상의 모듈로서 구현될 수 있다. 컴퓨터로 판독 가능한 매체는 기계로 판독 가능한 저장 장치, 기계로 판독 가능한 저장 기판, 메모리 장치, 기계로 판독 가능한 전파형 신호에 영향을 미치는 물질의 조성물 혹은 이들 중 하나 이상의 조합일 수 있다.

[0089] "처리 시스템", "처리 장치" 및 "하위시스템"이라는 용어는 예컨대 프로그래머블 프로세서, 컴퓨터 혹은 다중 프로세서나 컴퓨터를 포함하여 데이터를 처리하기 위한 모든 기구, 장치 및 기계를 포괄한다. 처리 시스템은, 하드웨어에 부가하여, 예컨대 프로세서 펌웨어를 구성하는 코드, 프로토콜 스택, 데이터베이스 관리 시스템, 운영 체제 혹은 이들 중 하나 이상의 조합 등 요청 시 컴퓨터 프로그램에 대한 실행 환경을 형성하는 코드를 포함할 수 있다.

[0090] 본 발명에 따른 장치에 탑재되고 본 발명에 따른 방법을 실행하는 컴퓨터 프로그램(프로그램, 소프트웨어, 소프트웨어 어플리케이션, 스크립트 혹은 코드로도 알려져 있음)은 컴파일 되거나 해석된 언어나 선험적 혹은 절차적 언어를 포함하는 프로그래밍 언어의 어떠한 형태로도 작성될 수 있으며, 독립형 프로그램이나 모듈, 컴포넌트, 서브루틴 혹은 컴퓨터 환경에서 사용하기에 적합한 다른 유닛을 포함하여 어떠한 형태로도 전개될 수 있다. 컴퓨터 프로그램은 파일 시스템의 파일에 반드시 대응하는 것은 아니다. 프로그램은 요청된 프로그램에 제공되는 단일 파일 내에, 혹은 다중의 상호 작용하는 파일(예컨대, 하나 이상의 모듈, 하위 프로그램 혹은 코드의 일부를 저장하는 파일) 내에, 혹은 다른 프로그램이나 데이터를 보유하는 파일의 일부(예컨대, 마크업 언어 문서 내에 저장되는 하나 이상의 스크립트) 내에 저장될 수 있다. 컴퓨터 프로그램은 하나의 사이트에 위치하거나 복수의 사이트에 걸쳐서 분산되어 통신 네트워크에 의해 상호 접속된 다중 컴퓨터나 하나의 컴퓨터 상에서 실행되도록 전개될 수 있다.

[0091] 본 명세서에서 설명한 주제의 구현물은 예컨대 데이터 서버와 같은 백엔드 컴포넌트를 포함하거나, 예컨대 어플리케이션 서버와 같은 미들웨어 컴포넌트를 포함하거나, 예컨대 사용자가 본 명세서에서 설명한 주제의 구현물과 상호 작용할 수 있는 웹 브라우저나 그래픽 유저 인터페이스를 갖는 클라이언트 컴퓨터와 같은 프론트엔드 컴포넌트 혹은 그러한 백엔드, 미들웨어 혹은 프론트엔드 컴포넌트의 하나 이상의 모든 조합을 포함하는 연산 시스템에서 구현될 수 있다. 시스템의 컴포넌트는 예컨대 통신 네트워크와 같은 디지털 데이터 통신의 어떠한 형태나 매체에 의해서도 상호 접속 가능하다.

[0092] 본 명세서는 다수의 특정한 구현물의 세부사항들을 포함하지만, 이들은 어떠한 발명이나 청구 가능한 것의 범위에 대해서도 제한적인 것으로서 이해되어서는 안되며, 오히려 특정한 발명의 특정한 실시형태에 특유할 수 있는 특징들에 대한 설명으로서 이해되어야 한다. 개별적인 실시형태의 문맥에서 본 명세서에 기술된 특정한 특징들은 단일 실시형태에서 조합하여 구현될 수도 있다. 반대로, 단일 실시형태의 문맥에서 기술한 다양한 특징들 역시 개별적으로 혹은 어떠한 적절한 하위 조합으로도 복수의 실시형태에서 구현 가능하다. 나아가, 특징들이 특정한 조합으로 동작하고 초기에 그와 같이 청구된 바와 같이 묘사될 수 있지만, 청구된 조합으로부터의 하나 이상의 특징들은 일부 경우에 그 조합으로부터 배제될 수 있으며, 그 청구된 조합은 하위 조합이나 하위 조합의 변형물로 변경될 수 있다.

[0093] 마찬가지로, 특정한 순서로 도면에서 동작들을 묘사하고 있지만, 이는 바람직한 결과를 얻기 위하여 도시된 그 특정한 순서나 순차적인 순서대로 그러한 동작들을 수행하여야 한다거나 모든 도시된 동작들이 수행되어야 하는 것으로 이해되어서는 안 된다. 특정한 경우, 멀티태스킹과 병렬 프로세싱이 유리할 수 있다. 또한, 상술한 실시형태의 다양한 시스템 컴포넌트의 분리는 그러한 분리를 모든 실시형태에서 요구하는 것으로 이해되어서는 안되며, 설명한 프로그램 컴포넌트와 시스템들은 일반적으로 단일의 소프트웨어 제품으로 함께 통합되거나 다중 소프트웨어 제품에 패키징될 수 있다는 점을 이해하여야 한다.

[0094] 본 명세서에서 설명한 주제의 특정한 실시형태를 설명하였다. 기타의 실시형태들은 이하의 청구항의 범위 내에 속한다. 예컨대, 청구항에서 인용된 동작들은 상이한 순서로 수행되면서도 여전히 바람직한 결과를 성취할 수 있다. 일 예로서, 첨부도면에 도시한 프로세스는 바람직한 결과를 얻기 위하여 반드시 그 특정한 도시된 순서나 순차적인 순서를 요구하지 않는다. 특정한 구현예에서, 멀티태스킹과 병렬 프로세싱이 유리할 수 있다.

[0095] 본 기술한 설명은 본 발명의 최상의 모드를 제시하고 있으며, 본 발명을 설명하기 위하여, 그리고 당업자가 본

발명을 제작 및 이용할 수 있도록 하기 위한 예를 제공하고 있다. 이렇게 작성된 명세서는 그 제시된 구체적인 용어에 본 발명을 제한하는 것이 아니다. 따라서, 상술한 예를 참조하여 본 발명을 상세하게 설명하였지만, 당업자라면 본 발명의 범위를 벗어나지 않으면서도 본 예들에 대해 개조, 변경 및 변형을 가할 수 있다.

[0096] 따라서 본 발명의 범위는 설명된 실시 예에 의하여 정할 것이 아니고 특허청구범위에 의해 정하여져야 한다.

산업상 이용가능성

[0097] 본 발명에 따른 패턴 인식 기반의 출입 제어 기술은, 증강현실과 같은, 영상 처리를 통해서 개폐 장치의 촬영 이미지로부터 그 패턴 이미지를 인식하고, 이를 기반으로 다단 인증을 수행함으로써, 보안성을 더 향상시킬 수 있다.

[0098] 구체적으로, 본 발명은 단말에서 촬영 이미지로부터 인식한 패턴 이미지를 기 등록된 사용자 정의 패턴의 패턴 이미지와 비교하여, 정당한, 즉, 출입 가능한 개폐 장치인지를 1차 인증하고, 1차 인증에 성공한 경우, 사용자 식별 정보와 함께 상기 인식한 패턴 이미지 및 촬영 이미지를 보안 서비스 장치로 전송하여, 상기 보안 서비스 장치를 통해서 사용자 확인 및 패턴 이미지를 재확인하는 2차 인증을 수행하고, 2차 인증에 성공한 경우, 단말을 통해 사용자로부터 입력 받은 패스워드를 기 등록된 패스워드와 비교하는 3차 인증을 수행함으로써, 정당한 사용자 및 상기 사용자가 출입할 개폐 장치를 함께 인증할 수 있으며, 그 결과 출입 통제의 신뢰성을 더 향상시킬 수 있다.

[0099] 또한, 본 발명은 증강현실을 출입 통제와 결합함으로써, 사용자 편의를 향상시킬 수 있을 뿐만 아니라, 사용자가 소지한 단말을 이용함으로써, 개폐 장치별 사용자 인식을 위한 장치의 설치 비용을 줄일 수 있다.

부호의 설명

[0100] 100: 개폐 장치 200: 단말

261: 영상 캡처 모듈 262: 영상 처리 모듈

263: 서버 연동 모듈 264: 사용자 인터페이스 모듈

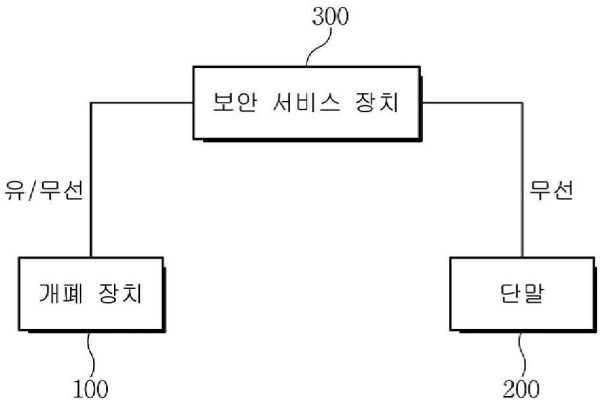
300: 보안 서비스 장치 310: 저장부

320: 영상 처리부 330: 인증 처리부

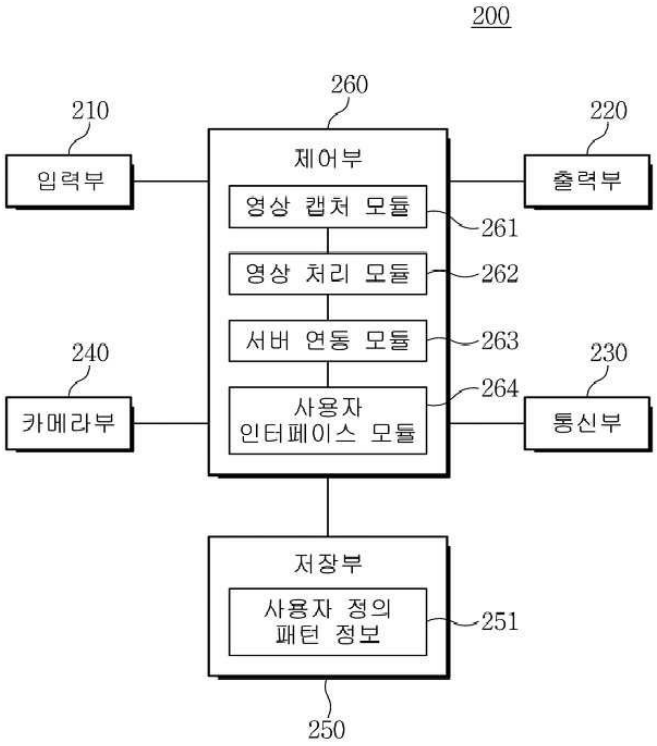
340: 개폐 장치 제어부

도면

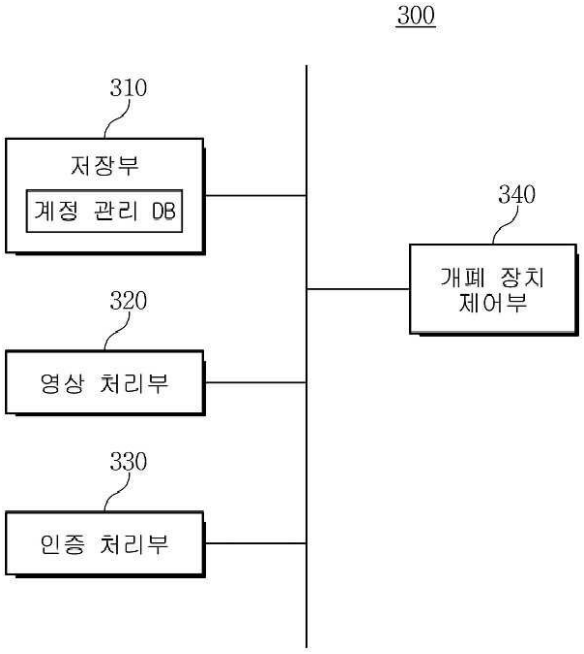
도면1



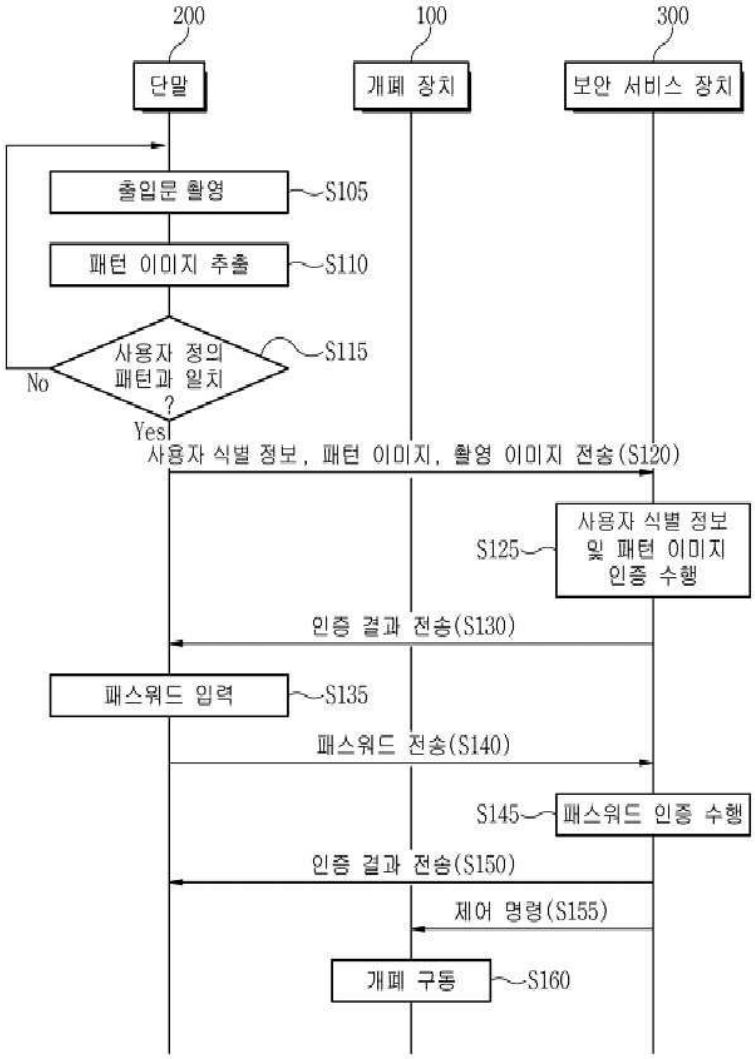
도면2


200
260
210
220
제어부
입력부
출력부
영상 캡처 모듈
261
영상 처리 모듈
262
서버 연동 모듈
263
240
230
264
카메라부
사용자
인터페이스 모듈
통신부
저장부
사용자 정의
패턴 정보
251
250

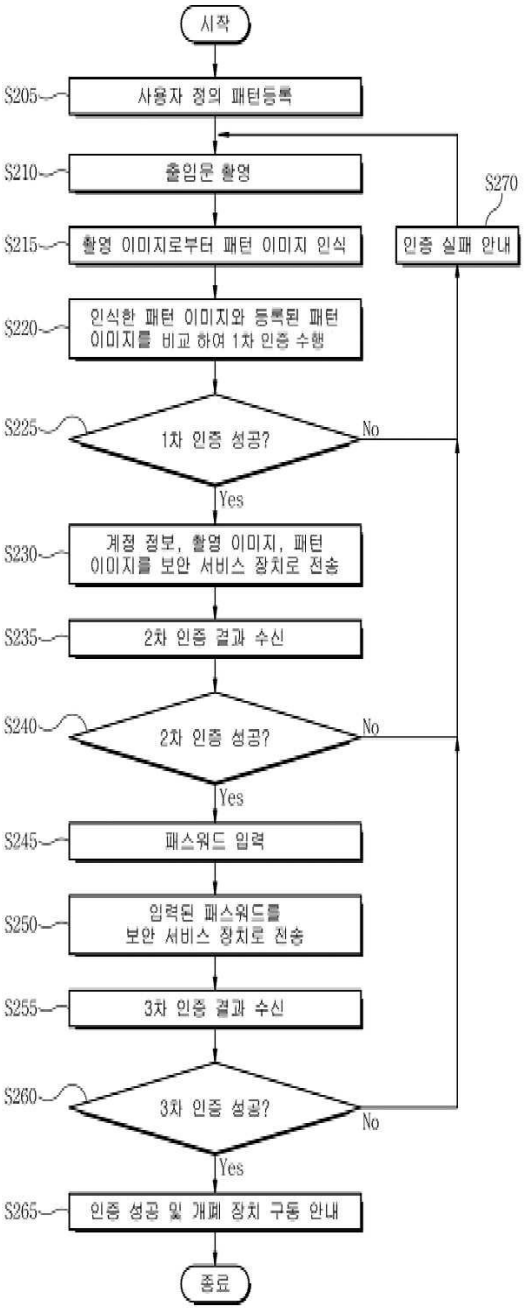
도면3


300
310
저장부
계정 관리 DB
340
개폐 장치
제어부
320
영상 처리부
330
인증 처리부

도면4


200
100
300
단말
개폐 장치
보안 서비스 장치
출입문 촬영
S105
패턴 이미지 추출
S110
사용자 정의 패턴과 일치 ?
S115
No
Yes
사용자 식별 정보, 패턴 이미지, 촬영 이미지 전송(S120)
S125
사용자 식별 정보 및 패턴 이미지 인증 수행
인증 결과 전송(S130)
패스워드 입력
S135
패스워드 전송(S140)
S145
패스워드 인증 수행
인증 결과 전송(S150)
제어 명령(S155)
개폐 구동
S160

도면5


시작
S205
사용자 정의 패턴등록
S210
출입문 촬영
S215
촬영 이미지로부터 패턴 이미지 인식
S220
인식한 패턴 이미지와 등록된 패턴 이미지를 비교 하여 1차 인증 수행
S225
1차 인증 성공?
No
Yes
S230
계정 정보, 촬영 이미지, 패턴 이미지를 보안 서비스 장치로 전송
S235
2차 인증 결과 수신
S240
2차 인증 성공?
No
Yes
S245
패스워드 입력
S250
입력된 패스워드를 보안 서비스 장치로 전송
S255
3차 인증 결과 수신
S260
3차 인증 성공?
No
Yes
S265
인증 성공 및 개폐 장치 구동 안내
종료
S270
인증 실패 안내

도면6

61 62 63

MSISDN	ID	P/W	인식 이미지 ID	인식 이미지 경로
010xxxxxxxx	Id_example1	37asnasn%D	Ne54CZQ_ng	user/Id_example1/door1/Ne54CZQ_ng.jpg
010xxxxxxxx	Id_example2	#<Kskd93ms	sk39Ksmf	user/Id_example2/door1/sk39Ksmf.jpg
⋮	⋮	⋮	⋮	⋮

도면7

(a)

타입	사용자 식별 정보	이미지 패턴 정보	촬영 이미지 데이터

(b)

타입	사용자 식별 정보	패스워드