



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0139100
(43) 공개일자 2012년12월27일

(51) 국제특허분류(Int. Cl.)
G06K 9/46 (2006.01)

(21) 출원번호 10-2011-0058671

(22) 출원일자 2011년06월16일

심사청구일자 없음

(71) 출원인

삼성전자주식회사

경기도 수원시 영통구 삼성로 129 (매탄동)

(72) 발명자

홍대화

서울특별시 구로구 신도림로 110, 301동 506호 (신도림동, 우성아파트)

김홍일

경기도 성남시 분당구 서현로 216, 오벨리스크오피스텔 308호 (서현동)

(뒷면에 계속)

(74) 대리인

이건주

전체 청구항 수 : 총 18 항

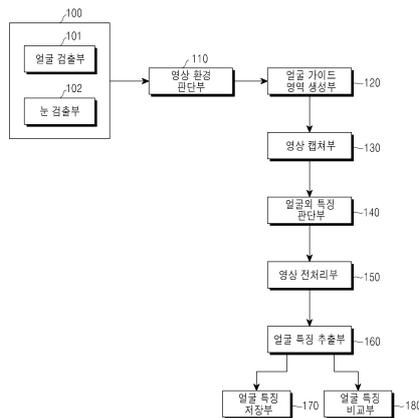
(54) 발명의 명칭 **얼굴 인증을 이용한 보안 장치 및 방법**

(57) 요약

본 발명은 문자 알림을 이용한 이미지 관리 장치 및 방법에 관한 것이다.

이를 위해 본 발명은 필기 데이터를 입력받고, 필기 데이터에 대한 획 순서 정보를 취득하며, 필기 데이터가 표시된 필기 화면을 캡처하여 캡처된 필기 화면을 입력 이미지로 저장한 후 취득된 획 순서 정보를 이용하여 입력 이미지에 대한 문자 인식을 수행하고, 문자 인식에 대한 결과에 따라 인식된 문자와 상기 입력 이미지를 대응시켜 저장함으로써 사용자가 직접 이미지에 대한 키워드를 직접 입력할 필요 없이 자동으로 필기 이미지에 대한 문자 인식을 통한 키워드 설정이 가능하다.

대표도 - 도1



(72) 발명자

손주영

경기도 수원시 권선구 권선동 현대아파트 210동
1202호

조성대

경기도 용인시 수지구 풍덕천동 664번지 동아아파
트 112동 1104호

김윤중

서울특별시 서초구 강남대로30길 48-2, 301호 (양
재동)

특허청구의 범위

청구항 1

얼굴 인증을 이용한 보안 장치에 있어서,
입력 영상으로부터 얼굴 영역을 검출하는 얼굴 검출부와,
상기 입력 영상 내에 얼굴 인증을 위한 얼굴 가이드 영역을 생성하여 화면에 표시하는 얼굴 가이드 영역 생성부와,
상기 검출된 얼굴 영역이 상기 얼굴 가이드 영역에 매치되면 상기 입력 영상을 캡처하는 영상 캡처부와,
상기 캡처 영상으로부터 얼굴 특징 정보를 추출하는 얼굴 특징 추출부와,
상기 추출된 얼굴 특징 정보를 저장하는 얼굴 특징 저장부를 포함하는 것을 특징으로 하는 보안 장치.

청구항 2

제1항에 있어서,
상기 얼굴 영역의 주변에 외부 환경이 얼굴 인증을 위해 미리 설정된 환경 조건에 만족하는지 여부를 판단하는 영상 환경 판단부를 더 포함하고,
상기 영상 환경 판단부는 상기 미리 설정된 환경 조건에 만족하지 않으면 다른 보안 인증 방식을 제공하는 것을 특징으로 하는 보안 장치.

청구항 3

제1항에 있어서,
사용자의 성별, 나이, 인종, 안경 착용 여부에 대한 정보를 포함하는 얼굴 외 특징 정보를 추출하는 얼굴 외 특징 추출부를 더 포함하고,
상기 얼굴 특징 저장부는 상기 추출된 얼굴 특징 정보와 함께 상기 추출된 얼굴 외 특징 정보를 포함하는 사용자 특징 정보를 저장하는 것을 특징으로 하는 보안 장치.

청구항 4

제1항에 있어서,
상기 얼굴 영역의 텍스처에 영향을 주는 외부 요소들을 최소화하기 위한 전처리를 수행하는 영상 전처리부를 더 포함하는 것을 특징으로 하는 보안 장치.

청구항 5

제1항에 있어서, 상기 영상 캡처부는,
상기 캡처된 영상의 눈의 위치, 눈 깜빡임 여부, 손떨림 정보를 확인하여 등록 영상으로 적합한지 여부를 판단하고, 판단 결과 상기 등록 영상으로 적합하지 않으면 영상 재촬영을 판단 결과로 출력하는 것을 특징으로 하는 보안 장치.

청구항 6

제1항에 있어서,
상기 영상 캡처부는 상기 캡처된 영상에 다양한 조명 변화 및 포즈 변화를 적용한 복수의 등록 영상을 생성하고,
상기 얼굴 특징 추출부는 상기 복수의 등록 영상으로부터 복수의 얼굴 특징 정보를 추출하며,
상기 얼굴 특징 저장부는 상기 추출된 복수의 얼굴 특징 정보를 저장하는 것을 특징으로 하는 보안 장치.

청구항 7

제6항에 있어서, 상기 영상 캡처부는,

보안 인증을 위한 얼굴 인증 요청이 있으면 상기 입력 영상을 캡처하고, 상기 캡처된 영상에 연속된 복수의 영상 프레임에 대한 정보를 획득하는 것을 특징으로 하는 보안 장치.

청구항 8

제7항에 있어서, 상기 얼굴 특징 추출부는,

상기 캡처된 영상 및 상기 연속된 복수의 영상 프레임에 대한 정보로부터 복수의 얼굴 특징 비교 정보를 추출하는 것을 특징으로 하는 보안 장치.

청구항 9

제8항에 있어서,

상기 얼굴 특징 저장부에 저장된 복수의 얼굴 특징 등록 정보와 상기 복수의 얼굴 특징 비교 정보를 서로 비교하는 얼굴 특징 비교부를 더 포함하고,

상기 얼굴 특징 비교부는 상기 얼굴 특징 등록 정보와 상기 얼굴 특징 비교 정보의 유사도 값을 산출하고, 상기 산출된 유사도 값이 미리 설정된 임계값 이상이면 보안 해제를 승인하는 비교 결과를 출력하고, 상기 산출된 유사도 값이 상기 미리 설정된 임계값 미만이면 상기 보안 해제를 거부하는 비교 결과를 출력하는 것을 특징으로 하는 보안 장치.

청구항 10

얼굴 인증을 이용한 보안 방법에 있어서,

입력 영상으로부터 얼굴 영역을 검출하는 과정과,

상기 입력 영상 내에 얼굴 인증을 위한 얼굴 가이드 영역을 생성하여 화면에 표시하는 과정과,

상기 검출된 얼굴 영역이 상기 얼굴 가이드 영역에 매치되면 상기 입력 영상을 캡처하는 과정과,

상기 캡처 영상으로부터 얼굴 특징 정보를 추출하는 과정과,

상기 추출된 얼굴 특징 정보를 저장하는 과정을 포함함을 특징으로 하는 보안 방법.

청구항 11

제10항에 있어서,

상기 얼굴 영역의 주변에 외부 환경이 얼굴 인증을 위해 미리 설정된 환경 조건에 만족하는지 여부를 판단하는 과정과,

상기 미리 설정된 환경 조건에 만족하지 않으면 다른 보안 인증 방식을 제공하는 과정을 더 포함함을 특징으로 하는 보안 방법.

청구항 12

제10항에 있어서,

사용자의 성별, 나이, 인종, 안경 착용 여부에 대한 정보를 포함하는 얼굴 외 특징 정보를 추출하는 과정과,

상기 추출된 얼굴 특징 정보와 함께 상기 추출된 얼굴 외 특징 정보를 포함하는 사용자 특징 정보를 저장하는 과정을 더 포함함을 특징으로 하는 보안 방법.

청구항 13

제10항에 있어서,

상기 얼굴 영역의 텍스처에 영향을 주는 외부 요소들을 최소화하기 위한 전처리를 수행하는 과정을 더 포함함을

특징으로 하는 보안 방법.

청구항 14

제10항에 있어서,

상기 캡처된 영상의 눈의 위치, 눈 깜빡임 여부, 손떨림 정보를 확인하여 등록 영상으로 적합한지 여부를 판단하는 과정과,

판단 결과 상기 등록 영상으로 적합하지 않으면 영상을 재촬영하는 과정을 더 포함함을 특징으로 하는 보안 방법.

청구항 15

제10항에 있어서,

상기 캡처된 영상에 다양한 조명 변화 및 포즈 변화를 적용한 복수의 등록 영상을 생성하는 과정과,

상기 복수의 등록 영상으로부터 복수의 얼굴 특징 등록 정보를 추출하는 과정과,

상기 추출된 복수의 얼굴 특징 등록 정보를 저장하는 과정을 더 포함함을 특징으로 하는 보안 방법.

청구항 16

제15항에 있어서,

보안 인증을 위한 얼굴 인증 요청이 있으면 상기 입력 영상을 캡처하는 과정과,

상기 캡처된 영상에 연속된 복수의 영상 프레임에 대한 정보를 획득하는 과정을 더 포함함을 특징으로 하는 보안 방법.

청구항 17

제16항에 있어서,

상기 캡처된 영상 및 상기 연속된 복수의 영상 프레임에 대한 정보로부터 복수의 얼굴 특징 비교 정보를 추출하는 과정을 더 포함함을 특징으로 하는 보안 방법.

청구항 18

제17항에 있어서,

상기 저장된 복수의 얼굴 특징 등록 정보와 상기 복수의 얼굴 특징 비교 정보를 서로 비교하는 과정과,

상기 얼굴 특징 등록 정보와 상기 얼굴 특징 비교 정보의 유사도 값을 산출하는 과정과,

상기 산출된 유사도 값이 미리 설정된 임계값 이상이면 보안 해제를 승인하는 과정과,

상기 산출된 유사도 값이 상기 미리 설정된 임계값 미만이면 상기 보안 해제를 거부하는 과정을 더 포함함을 특징으로 하는 보안 방법.

명세서

기술분야

[0001] 본 발명은 보안 장치에 관한 것으로, 특히 사용자의 얼굴 인증을 이용한 보안 장치 및 방법을 제공한다.

배경기술

[0002] 최근 스마트폰 또는 태블릿 PC 등의 개인용 장치의 보급에 따른 앱스토어의 활성화와 SNS(Social Networking Service)의 대중화 등 개인화된 콘텐츠의 관심이 증가되어 개인용 장치의 수요가 크게 증가하고 있는 실정이다.

[0003] 이러한 스마트 장치들은 장치 자체뿐만 아니라 개인화된 콘텐츠의 보안을 위해 다양한 보안 기능들을 제공하고

있다. 현존하는 보안 기능에는 전통적인 방식인 PIN(Personal Identification Number), 비밀번호(Password) 입력, 최근 주목받고 있는 패턴(Pattern) 입력 방식 등이 있다. 여기서, 패턴 입력 방식은 디바이스의 터치스크린과 같은 입력 장치를 통해서 입력된 패턴을 보안 인증으로 사용하는 기술이다. 예를 들어, 패턴 입력 방식은 터치 스크린상에 3x3으로 구성된 9개 노드와 같이 미리 설정된 개수의 노드가 배열되고, 배열된 노드를 터치한 순서와 모양으로 암호를 설정하는 방식을 사용한다.

[0004] 또한 최근 지문이나 얼굴과 같은 생체정보를 활용한 접근방식 또한 큰 각광을 받고 있으나 여러 가지 문제로 인해 쉽사리 상용화의 한계를 넘지 못하고 있는 실정이다.

발명의 내용

해결하려는 과제

[0005] 상기와 같이 현재 상용화된 휴대 장치에서 핀과 비밀번호의 경우 예를 들어, 4 ~ 16자리와 같이 특정 개수의 문자 또는 숫자를 입력하게 되어 있다.

[0006] 그러나 이러한 핀 번호와 비밀번호는 단지 사용자의 기억에만 의존하기 때문에 대부분의 사용자들은 짧은 자리수의 암호나 평소 다른 보안용으로 설정하던 암호들을 그대로 사용한다.

[0007] 이에 따라, 비밀번호 입력은 디스플레이 한계로 인해 자판을 디스플레이하고, 이를 누르는 데 불편함이 있기 때문에 숫자로만 구성할 수 있는 핀 번호 입력이 선호된다.

[0008] 그러나 핀 번호 입력은 단순히 숫자만의 조합으로 쉽게 기억하기 위한 추상적인 개념을 만들어 내기가 어렵기 때문에 비밀번호보다 훨씬 적은 자리수의 암호들이 주로 설정되어 노출의 위험을 증가시키게 된다.

[0009] 또한, 최근에 이용되고 있는 패턴 입력 방식의 경우 미리 설정된 개수의 노드 배열 및 순서에 대한 조합으로 암호를 설정하는데, 이것도 사용자의 기억에 의존을 하고, 사용자의 해제 편의성을 위해 단순한 구성들이 주로 선택되기 때문에 주변 지인들에게 쉽게 노출될 수 있어 보안성이 뛰어나다고 보기 어렵다.

[0010] 상기 방식들은 접촉식이고, 기억에 의존을 하기 때문에 최근 들어 생체인식 기술의 발전으로 인해 얼굴 및 지문 등의 인식기술들을 휴대 장치에 내장하는 방법들이 연구되고 있다. 생체인식의 경우 사용자의 편의성과 기억에 의존하지 않는다는 장점이 있지만 아직까지 환경변화에 변수가 많고, 그로 인한 정확도의 신뢰성이 떨어진다는 단점들이 있다. 특히, 지문의 경우 IR(Infrared Ray)과 같은 전용 센서가 필요하다는 단점이 있다.

[0011] 따라서, 본 발명은 사용자가 다양한 환경에서도 얼굴인식을 이용하여 편리하게 보안 인증을 하기 위한 보안 장치 및 방법을 제공한다.

과제의 해결 수단

[0012] 상술한 바를 달성하기 위한 본 발명은 얼굴 인증을 이용한 보안 장치에 있어서, 입력 영상으로부터 얼굴 영역을 검출하는 얼굴 검출부와, 상기 입력 영상 내에 얼굴 인증을 위한 얼굴 가이드 영역을 생성하여 화면에 표시하는 얼굴 가이드 영역 생성부와, 상기 검출된 얼굴 영역이 상기 얼굴 가이드 영역에 매치되면 상기 입력 영상을 캡처하는 영상 캡처부와, 상기 캡처 영상으로부터 얼굴 특징 정보를 추출하는 얼굴 특징 추출부와, 상기 추출된 얼굴 특징 정보를 저장하는 얼굴 특징 저장부를 포함하는 것을 특징으로 한다.

[0013] 또한, 본 발명은 얼굴 인증을 이용한 보안 방법에 있어서, 입력 영상으로부터 얼굴 영역을 검출하는 과정과, 상기 입력 영상 내에 얼굴 인증을 위한 얼굴 가이드 영역을 생성하여 화면에 표시하는 과정과, 상기 검출된 얼굴 영역이 상기 얼굴 가이드 영역에 매치되면 상기 입력 영상을 캡처하는 과정과, 상기 캡처 영상으로부터 얼굴 특징 정보를 추출하는 과정과, 상기 추출된 얼굴 특징 정보를 저장하는 과정을 포함함을 특징으로 한다.

발명의 효과

[0014] 본 발명은 다양한 환경을 반영한 얼굴 영상을 등록하고, 보안 인증 시 등록된 영상과 촬영된 영상을 비교하여 비교 결과에 따라 보안 유지 또는 해제를 수행함으로써 다양한 환경에서의 얼굴 인증 방식을 이용한 보안 장치를 상용화할 수 있어 사용자가 비밀번호 및 핀번호를 별도로 입력할 필요없이 촬영된 얼굴을 이용하여 편리하게 보안 설정 및 해제가 가능하다.

도면의 간단한 설명

- [0015] 도 1은 본 발명의 실시 예에 따른 보안 관리 장치에 대한 구성도,
- 도 2는 본 발명의 실시 예에 따라 저조도 또는 역광이 포함된 영상을 나타내는 예시도들,
- 도 3은 본 발명의 실시 예에 따른 얼굴 가이드 영역의 예시도들,
- 도 4는 본 발명의 실시 예에 따라 얼굴 착용 여부를 확인하기 위한 동작을 설명하기 위한 예시도들,
- 도 5 내지 도 6은 본 발명의 실시 예에 따라 보안 인증을 위한 얼굴 등록을 수행하는 과정을 나타내는 흐름도들,
- 도 7은 본 발명의 실시 예에 따라 보안 인증을 위한 얼굴 인증을 수행하는 과정을 나타내는 흐름도.

발명을 실시하기 위한 구체적인 내용

- [0016] 이하 본 발명의 바람직한 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 하기 설명 및 첨부 도면에서 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략한다.
- [0017] 본 발명은 얼굴 인식 기술을 이용한 휴대용 단말기의 보안 관리에 대한 발명이다.
- [0018] 얼굴 인증을 위해 본 발명에서는 전면 카메라가 내장된 단말기에서 사용자의 얼굴에 관련된 얼굴 특징 정보를 추출하여 등록하기 위한 구성과 보안이 필요한 상황에서 카메라가 자동으로 구동되어 얻어진 얼굴 영상으로부터 얼굴 특징 정보를 추출하여 등록된 얼굴 특징 정보들과 추출된 얼굴 특징 정보를 비교하는 구성을 포함한다.
- [0019] 휴대 단말기에서 보안을 설정하고, 이를 활용하기 위해서는 얼굴 등록 및 인증 과정을 수행하고, 얼굴 인식을 위한 카메라 구동, 얼굴 촬영, 얼굴 특징 추출 등과 같은 일련의 과정들을 수행하여야 한다. 본 발명에서는 각 단계의 과정별 얼굴인증 성능 향상을 위한 시나리오들로 구성되어 있다.
- [0020] 도 1은 본 발명의 실시 예에 따른 보안 관리 장치에 대한 구성도이다.
- [0021] 본 발명의 보안 관리 장치는 얼굴 검출부(101)와 눈 검출부(102)를 포함하는 검출부(100), 영상 환경 판단부(110), 얼굴 가이드 영역 생성부(120), 영상 캡처부(130), 얼굴 외 특징 판단부(140), 영상 전처리부(150), 얼굴 특징 추출부(160), 얼굴 특징 저장부(170), 얼굴 특징 비교부(170)를 포함한다.
- [0022] 얼굴 인증을 통한 단말기 보안 설정을 위한 요청 시 검출부(100)는 카메라를 통해서 입력된 영상이 카메라의 프리뷰 화면에 디스플레이되면 얼굴 및 눈을 검출한다.
- [0023] 구체적으로, 얼굴 검출부(101)는 입력 영상 내 얼굴의 위치를 검색하고, 검색된 얼굴 위치를 얼굴 영역으로 검출한다.
- [0024] 눈 검출부(102)는 검출된 얼굴 영역 내의 좌안 및 우안의 좌표를 검색하고, 검색된 두 눈의 좌표를 눈 위치로 검출한다.
- [0025] 영상 환경 판단부(110)는 촬영 시 사용자의 조명 환경과 같은 촬영 환경이 미리 설정된 촬영 환경 조건에 해당 하는지 여부를 판단한다. 구체적으로, 사용자가 얼굴 인증을 위한 촬영 시 저조도 또는 역광과 같은 조명이 좋지 않은 환경 조건에서 촬영을 할 경우에는 얼굴이 검출되기 어렵고, 검출된다고 하더라도 눈 검출의 성능을 보장하기 어렵기 때문에 인증 결과를 신뢰하기 어렵다.
- [0026] 이와 같은 경우 본 발명의 영상 환경 판단부(110)는 입력 영상이 저조도 또는 역광을 포함하는지 판단하고, 저조도 또는 역광이 포함되어 있다고 판단된 경우 비밀번호 설정 방법 또는 핀 번호 설정 방법과 같은 다른 보안 인증 방식을 제공한다.
- [0027] 도 2는 본 발명의 실시 예에 따라 저조도 또는 역광이 포함된 영상을 나타내는 예시도들이다.
- [0028] 영상 환경 판단부(110)는 도 2의 도면부호 200 또는 201과 같이 미리 설정된 개수의 블록 단위로 검출된 얼굴 영역과 그 주변의 밝기 값을 추출하고, 추출된 밝기 값을 이용하여 8단계의 밝기 히스토그램을 생성한다.
- [0029] 영상 환경 판단부(110)는 밝기 히스토그램의 하위 부에 수치가 집중되는 밝기 값과 얼굴 내부가 낮은 밝기 값이면 저조도가 포함된 영상으로 판단하고, 얼굴 영역 주변에 나타나는 빛의 포화(saturation) 현상 및 이로 인해 얼굴 영역의 음영 현상이 존재하면 역광이 포함된 영상으로 판단한다. 이때, 본 발명에서는 저조도의 판단 기준에서 사용한 히스토그램을 이용하여 밝기 히스토그램의 밝기 값 및 얼굴 내부의 밝기 값이 미리 설정된 임계값보다 작으면 저조도 영상으로 판단하고, 얼굴 영역의 밝기 값이 미리 설정된 임계값보다 작으면 역광 영상으로

판단할 수 있다.

- [0030] 본 발명에서는 촬영 환경 조건에 해당하면 영상 캡처부(130)가 입력 영상을 캡처하고, 촬영 환경 조건에 해당하지 않으면 얼굴 인증 외 다른 단말기 보안 설정을 제공한다.
- [0031] 얼굴 가이드 영역 생성부(120)는 검출된 두 눈의 좌표를 기반으로 하여 모든 얼굴에 동일하게 적용할 일정한 크기의 얼굴 가이드 영역과 두 눈의 가이드 영역을 프리뷰 화면에 디스플레이한다.
- [0032] 구체적으로, 사용자로부터 얼굴 등록을 위한 요청이 있으면 전면 셀프 카메라가 동작하고, 검출부(100)가 전면 셀프 카메라를 통해서 입력되는 사용자 이미지로부터 프리뷰 내에서 얼굴 영역의 위치와 눈의 좌표를 실시간으로 검출한다. 이후 얼굴 가이드 영역 생성부(120)가 검출된 얼굴 영역의 크기와 위치, 눈의 거리와 위치를 바탕으로 사용자와 카메라의 거리 및 가이드에 대한 최적화된 위치를 예측하여 얼굴 가이드 영역을 생성하여 프리뷰 화면에 디스플레이한다.
- [0033] 도 3는 본 발명의 실시 예에 따른 얼굴 가이드 영역의 예시도를 나타내는 도면들이다.
- [0034] 얼굴 가이드 영역 생성부(120)는 등록될 얼굴 특징 정보의 대표성을 보장하기 위해 도 3과 같은 얼굴 가이드 영역을 프리뷰 화면에 디스플레이하고, 디스플레이된 얼굴 가이드 영역 내에 얼굴 영역의 크기와 위치, 눈의 거리와 위치가 일치되는 정보를 판단하여 판단 결과에 따라 결과 메시지를 프리뷰 화면에 표시할 수 있다.
- [0035] 영상 캡처부(130)는 프리뷰 화면에 디스플레이된 입력 영상을 캡처한다. 이때, 영상 캡처부(130)는 미리 설정된 시간동안 영상 프레임의 연속성을 분석하여 분석된 연속성에 대한 값이 임계치 이상 되면 자동 또는 수동으로 입력 영상을 캡처한다. 수동으로 캡처하는 경우 영상 캡처부(130)는 동적인 신호를 출력하거나 영상 촬영 메시지를 화면에 디스플레이함으로써 사용자가 직접 촬영하도록 유도할 수 있다.
- [0036] 이러한 동작을 얼굴 위치 정규화라고 정의한다. 이와 같이 정규화된 얼굴들은 동일한 영상의 크기를 갖고 그 영상 내에 동일한 눈의 위치를 갖기 때문에 회전이나 얼굴크기의 변화로 인한 인식률의 저하를 방지할 수 있다.
- [0037] 영상 캡처부(130)는 얼굴 영상이 촬영되면 눈의 위치, 눈 깜빡임 여부, 손떨림 정보등과 같은 정보를 제공하여 대표 영상으로써 화질적인 문제가 없는지 여부를 확인하도록 유도할 수도 있다. 이때, 사용자가 촬영된 영상을 대표 영상으로 동의하지 않으면 카메라를 재동작하여 재촬영을 수행하도록 할 수 있다.
- [0038] 또한 본 발명에서는 보안 인증 단계에서 인증 요청자가 어떠한 조명 환경 등과 같은 외부 환경에서 인증 요청을 수행할지 예측이 하기 어렵기 때문에 영상 캡처부(130)에서 캡처한 하나의 영상에 조명 변화 및 포즈 변화를 수행하여 복수의 영상으로 더 생성할 수 있다.
- [0039] 예를 들어, 영상 캡처부(130)는 한 장의 영상을 캡처하고, 다양한 조명변화를 모델링하여 가상의 조명환경에서 촬영한 듯한 영상을 생성하거나, 포즈 변화에 대한 이슈들을 고려하여 워핑 기술들을 이용한 간단한 포즈 변화된 영상들을 생성할 수도 있다.
- [0040] 얼굴 외 특징 판단부(140)는 얼굴 자체의 모양이나 텍스처 뿐만 아니라 성별, 나이, 인종, 안경의 착용여부와 같은 얼굴 외 특징 정보를 판단하여 이를 추출한다. 본 발명에서는 이와 같이 추출된 얼굴 외 특징 정보도 함께 조합하여 사용자의 특징을 수치화하는데 이용할 수 있다.
- [0041] 사용자의 고유성은 입력 영상에서 추출된 얼굴 특징 정보뿐만 아니라 성별이나 안경 착용 여부 등과 같은 얼굴 외 특징 정보도 고유성을 표현하는 데 좋은 정보가 될 수 있다. 이러한 방식을 통해 인증 요청인의 성별 및 안경 착용 여부의 결과가 일치하지 않을 경우 얼굴 비교 시 감점의 요인으로 작용할 수 있다.
- [0042] 성별을 분석하기 위해 얼굴 외 특징 판단부(140)는 남성과 여성의 얼굴 데이터를 수집하고, 이를 구분할 수 있는 분류기를 통해서 학습하여 성별을 구분할 수 있다.
- [0043] 도 4는 본 발명의 실시 예에 따라 얼굴 착용 여부를 확인하기 위한 동작을 설명하기 위한 예시도들이다.
- [0044] 안경 착용 여부를 확인하기 위해 얼굴 외 특징 판단부(140)는 도 4의 도면부호 400과 같은 안경착용 얼굴과 도면부호 401과 같은 안경 미착용 얼굴들의 데이터를 수집하고, 이들의 평균 얼굴을 통해 데이터의 차이를 분석한다. 얼굴 외 특징 판단부(140)는 도면부호 403과 같은 얼굴 내 안경이 위치한다고 예측되는 영역인 R1, R2, R3를 선정하고, 선정된 영역에서의 에지의 분포를 분석하여 안경 착용 여부를 판단할 수 있다.
- [0045] 영상 전처리부(150)는 얼굴 영상에 조명과 같이 얼굴 텍스처에 영향을 주는 외부 요소들을 최소화하기 위한 전처리 과정을 수행한다.

- [0046] 얼굴 특징 추출부(160)는 전처리 과정이 완료된 얼굴 영상으로부터 얼굴 특징 정보를 추출한다. 이때, 얼굴 특징 추출부(160)는 영상 캡처부(130)에서 캡처한 하나의 영상에서 조명 및 포즈를 변화시켜 생성된 복수의 영상으로부터 얼굴 특징 정보를 추출한다.
- [0047] 얼굴 특징 저장부(170)는 추출된 얼굴 특징 정보를 저장한다.
- [0048] 이때, 얼굴 특징 저장부(170)는 추출된 얼굴 특징 정보와 함께 얼굴 외 특징 추출부(140)로부터 추출된 얼굴 외 특징 정보를 포함하는 사용자 특징 정보를 저장한다.
- [0049] 사용자로부터 보안 인증을 위한 얼굴 인증 요청이 있으면 검출부(100), 영상 환경 판단부(110), 얼굴 가이드 영역 생성부(120), 얼굴 캡처부(130), 얼굴 외 특징 추출부(140), 영상 전처리부(150), 얼굴 특징 추출부(160)는 기본적으로 얼굴 등록 과정 때와 유사한 동작을 수행한다.
- [0050] 특히, 영상 캡처부(130)는 상기와 같이 사용자 얼굴을 캡처하면서 연속된 몇몇 영상 프레임에 대한 정보들을 동시에 획득할 수 있다.
- [0051] 얼굴 특징 추출부(160)는 획득된 복수의 영상 프레임 정보로부터 복수의 영상 프레임 각각에 대응하는 얼굴 특징 정보를 추출한다.
- [0052] 얼굴 특징 비교부(180)는 보안 인증 요청이 있으면 얼굴 특징 저장부(170)에 저장된 복수의 사용자 특징 정보들과 얼굴 인증을 위해 얼굴 특징 추출부(160)로부터 추출된 얼굴 특징 정보와 얼굴 외 특징 추출부(140)로부터 추출된 얼굴 외 특징 정보를 포함하는 복수의 사용자 특징 정보를 비교한다.
- [0053] 즉, 저장된 사용자 특징 정보들과 인증을 위해 추출된 사용자 특징 정보들의 유사도 값을 서로 비교하여 비교 결과 두 사용자 특징 정보들간의 유사도 값이 미리 설정된 임계값 이상이면 얼굴 특징 비교부(180)는 보안 해제를 승인하는 결과값을 출력하고, 유사도값이 미리 설정된 임계값 미만이면 보안 해제를 거부하는 결과값을 출력하여 보안을 유지하도록 한다.
- [0054] 이와 같이 추출된 복수의 사용자 특징 정보와 저장된 복수의 사용자 특징 정보를 비교함으로써 인증 결과에 대한 신뢰성이 보장될 수 있다. 예를 들어, 만약 등록된 얼굴 특징 정보가 3개이고 획득된 얼굴 특징 정보가 2개이면 총 6쌍의 얼굴 정보들이 비교되므로 1개의 등록된 얼굴 특징 정보와 1개의 획득된 얼굴 특징 정보를 비교한 것보다는 신뢰성 높은 인증 결과가 출력될 수 있다.
- [0055] 본 발명에서는 사용자 얼굴 촬영 시 사진 위조 방지가 필요하기 때문에 얼굴 캡처 단계에서 사용자에게 웃는 표정, 놀란 표정, 눈 깜박임, 윙크등과 같은 얼굴 제스처를 설정하도록 할 수 있다. 이와 같이 사용자가 혼자만의 비밀로서 얼굴 제스처를 설정하여 얼굴 인증 시 등록된 제스처를 확인하도록 함으로써 사진 위조를 방지할 수 있다.
- [0056] 또한 본 발명에서는 시간이 흐를 수록 사용자의 외모나 스타일 등에 많은 변화가 생기기 때문에 얼굴 특징 저장부(170)가 저장된 얼굴 특징 정보 중 일부 또는 전체를 최근 인증에 성공된 얼굴 특징 정보들로 업데이트할 수 있다. 이러한 얼굴 정보의 교체조건은 인증 성공 조건 보다는 높은 임계치를 사용한다.
- [0057] 구체적으로, 본 발명은 최근의 사용자 외모나 스타일에 대한 변화를 반영한 사용자 특징 정보를 계속적으로 업데이트하기 위해서 유사도 판단을 위해 미리 설정된 비교 임계값보다 더 높은 임계치를 사용자 특징 정보를 교체하기 위해 사용되는 교체 임계값으로 설정한다.
- [0058] 이에 따라 특징 정보 저장부(170)는 비교 결과에 따라 두 사용자 특징 정보들간의 유사도 값이 교체 임계값 이상이면 인증 성공으로 판단할 뿐만 아니라 저장된 복수의 사용자 특징 정보들 중 적어도 하나를 교체 임계값 이상에 해당하는 사용자 특징 정보로 교체하여 저장한다.
- [0059] 이에 따라, 본 발명은 사용자의 최근 모습을 주기적으로 업데이트하도록 함으로써 보다 높은 인식률을 가질 수 있게 된다.
- [0060] 도 5 내지 도 6은 본 발명의 실시 예에 따라 보안 인증을 위한 얼굴 등록을 수행하는 과정을 나타내는 도면들이다.
- [0061] 500단계에서 카메라로부터 영상이 입력되면 501단계에서 검출부(100)가 얼굴 및 눈을 검출한다. 구체적으로, 얼굴 검출부(101)는 입력 영상 내 얼굴의 위치를 검색하고, 검색된 얼굴 위치를 얼굴 영역으로 검출한다. 눈 검출부(102)는 검출된 얼굴 영역 내의 좌안 및 우안의 좌표를 검색하고, 검색된 두 눈의 좌표를 눈 위치로

검출한다.

- [0062] 502단계에서 영상 환경 판단부(110)는 촬영 시 추출된 얼굴 영역 주변에 사용자의 조명 환경과 같은 촬영 환경이 미리 설정된 촬영 환경 조건에 해당하는지 여부를 판단한다.
- [0063] 503단계에서 영상 환경 판단부(110)는 입력 영상이 얼굴 인증 조건에 만족하는지 여부를 판단하여 만족하는 경우 505단계를 진행하고, 그렇지 않으면 504단계로 진행하여 다른 보안 인증 방식을 제공한다.
- [0064] 다시 말해서, 영상 환경 판단부(110)는 입력 영상이 저조도 또는 역광을 포함하는 영상인지 판단하여 판단 결과 저조도 또는 역광을 포함하는 영상인 경우 다른 보안 인증 방법을 제공하는 것이다.
- [0065] 505단계에서 얼굴 가이드 영역 생성부(120)는 검출된 얼굴 영역 및 두 눈의 좌표를 기반으로 하여 모든 얼굴에 동일하게 적용할 미리 설정된 크기의 얼굴 가이드 영역과 두 눈의 가이드 영역을 프리뷰 화면에 디스플레이한다.
- [0066] 506단계에서 얼굴 가이드 영역 생성부(120)는 검출된 얼굴 및 눈의 위치 정보가 디스플레이된 얼굴 가이드 영역 내 얼굴 영역의 크기와 위치, 눈의 거리와 위치와 같은 얼굴 영역 및 눈의 위치 정보가 일치되는지 여부를 판단하여 일치하면 508단계로 진행하고, 그렇지 않으면 507단계로 진행하여 일치하지 않음을 나타내는 안내 메시지를 프리뷰 화면에 표시한다.
- [0067] 508단계에서 영상 캡처부(130)는 프리뷰 화면에 디스플레이된 입력 영상을 캡처한다. 이때, 영상 캡처부(130)는 미리 설정된 시간동안 영상 프레임의 연속성을 분석하여 분석된 연속성에 대한 값이 미리 설정된 임계치 이상이면 자동 또는 수동으로 입력 영상을 캡처한다.
- [0068] 이후 508단계에서 도 6의 ㉔단계로 진행하여 설명하도록 한다.
- [0069] ㉔단계에서 600단계로 진행하여 얼굴 영상이 촬영되면 601단계에서 영상 캡처부(130)는 눈의 위치, 눈 깜빡임 여부, 손떨림 정보 등과 같은 얼굴 인증을 위한 조건에 만족하는지 여부를 판단하여 만족하면 602단계로 진행하고, 그렇지 않으면 도 5의 ㉕단계에서 507단계로 진행하여 영상을 다시 캡처한다.
- [0070] 602단계에서 얼굴 외 특징 판단부(140)는 얼굴 자체의 모양이나 텍스처 뿐만 아니라 성별, 나이, 인종, 안경의 착용여부와 같은 얼굴 외 특징 정보를 추출한다.
- [0071] 이와 같이 추출된 얼굴 외 특징 정보도 함께 조합하여 사용자의 특징을 수치화하는데 이용할 수 있다.
- [0072] 603단계에서 영상 전처리부(150)는 얼굴 영상에 조명과 같이 얼굴 텍스처에 영향을 주는 외부 요소들을 최소화하기 위한 전처리 과정을 수행한다.
- [0073] 604단계에서 얼굴 특징 추출부(160)는 전처리 과정이 완료된 얼굴 영상으로부터 얼굴 특징 정보를 추출한다.
- [0074] 605단계에서 얼굴 특징 저장부(170)는 추출된 얼굴 특징 정보와 함께 얼굴 외 특징 추출부(140)로부터 추출된 얼굴 외 특징 정보를 저장한다.
- [0075] 이와 같이 본 발명은 다양한 환경에서의 얼굴 인증 방식을 이용한 보안 장치를 상용화할 수 있어 사용자가 비밀번호 및 핀번호를 별도로 입력할 필요없이 촬영된 얼굴을 이용하여 편리하게 보안 설정 및 해제가 가능하다.
- [0076] 도 7은 본 발명의 실시 예에 따라 보안 인증을 위한 얼굴 인증을 수행하는 과정을 나타내는 흐름도이다.
- [0077] 본 발명의 실시 예에서는 도 5의 500단계~507단계 내지 도 6의 600단계~603단계와 유사한 과정을 수행한 후 도 7의 700단계를 수행한다.
- [0078] 700단계에서 얼굴 특징 추출부(160)는 영상 캡처부(130)로부터 캡처된 영상에서 사용자 특징 정보를 추출한다.
- [0079] 701단계에서 얼굴 특징 비교부(180)는 저장된 사용자 특징 정보들과 추출된 사용자 특징 정보들을 비교한다.
- [0080] 702단계에서 얼굴 특징 비교부(180)는 비교 결과 일치하는지 여부를 판단하여 일치하면 704단계를 진행하여 보안 해제 승인을 비교 결과로 출력하고, 일치하지 않으면 703단계로 진행하여 보안 해제 거부를 비교 결과로 출력한다.
- [0081] 705단계에서 얼굴 특징 저장부(170)는 저장된 얼굴 특징 정보 중 일부 또는 전체를 최근 인증에 성공된 얼굴 특징 정보들로 업데이트한다.
- [0082] 상기에서는 얼굴 특징 정보를 업데이트하는 것을 예로 들어 설명하였으나, 얼굴 외 특징 정보도 함께 업데이트

할 수 있다.

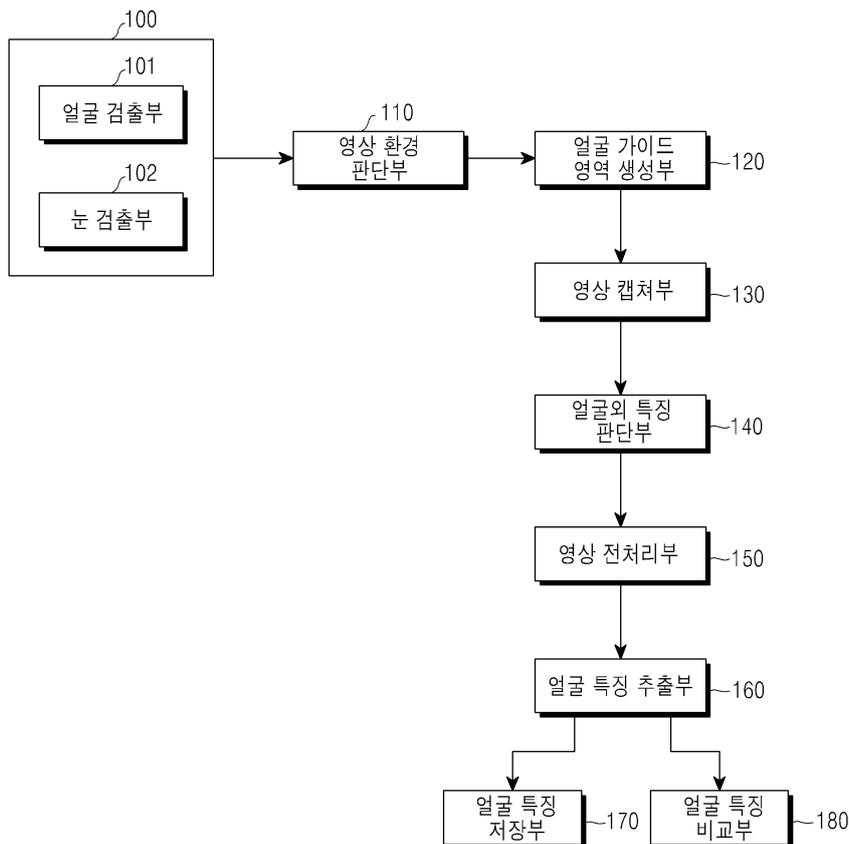
[0083] 이와 같이 본 발명은 다양한 환경에서의 얼굴 인증 방식을 이용한 보안 장치를 상용화할 수 있어 사용자가 비밀번호 및 핀번호를 별도로 입력할 필요없이 촬영된 얼굴을 이용하여 편리하게 보안 설정 및 해제가 가능하다.

부호의 설명

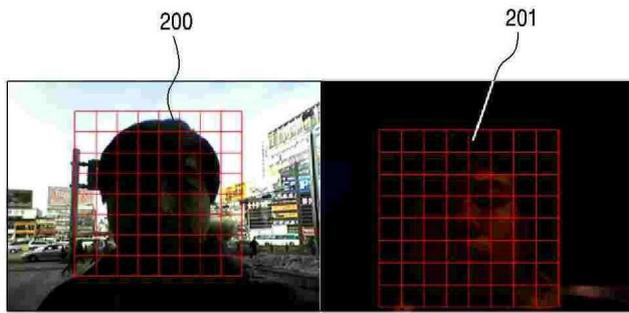
- [0084] 100: 검출부
- 101: 얼굴 검출부
- 102: 눈 검출부
- 110: 영상 환경 판단부
- 120: 얼굴 가이드 영역 생성부
- 130: 영상 캡처부
- 140: 얼굴 외 특징 판단부
- 150: 영상 전처리부
- 160: 얼굴 특징 추출부
- 170: 얼굴 특징 저장부
- 180: 얼굴 특징 비교부

도면

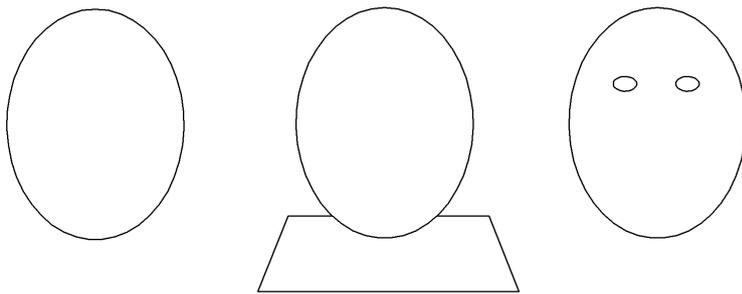
도면1



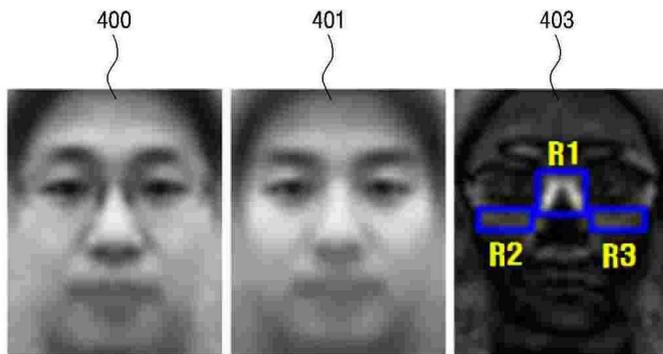
도면2



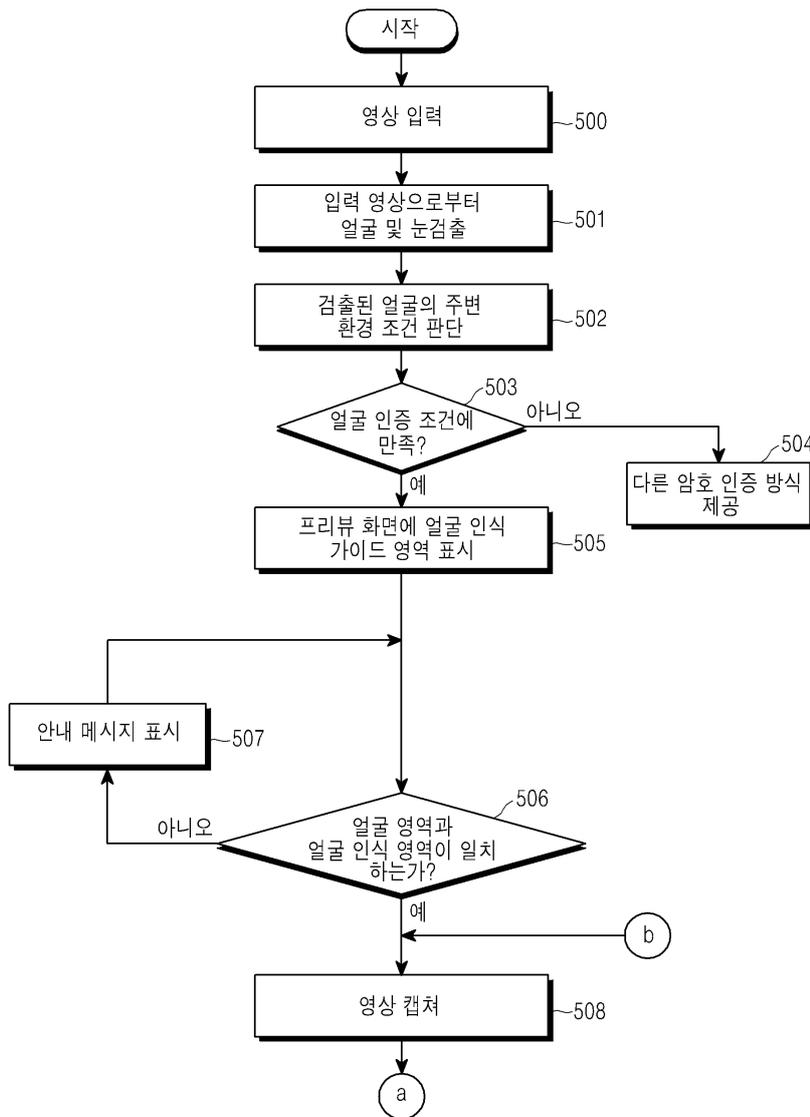
도면3



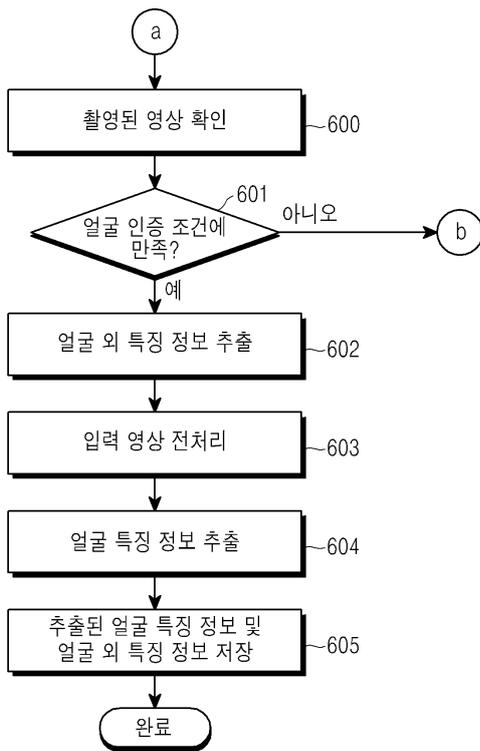
도면4



도면5



도면6



도면7

