



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년09월24일
(11) 등록번호 10-2708688
(24) 등록일자 2024년09월13일

(51) 국제특허분류(Int. Cl.)
G06F 21/32 (2013.01) G06F 21/45 (2013.01)
(52) CPC특허분류
G06F 21/32 (2013.01)
G06F 21/45 (2013.01)
(21) 출원번호 10-2019-7020766
(22) 출원일자(국제) 2019년03월21일
심사청구일자 2022년03월16일
(85) 번역문제출일자 2019년07월16일
(65) 공개번호 10-2021-0130856
(43) 공개일자 2021년11월02일
(86) 국제출원번호 PCT/KR2019/003280
(87) 국제공개번호 WO 2020/189827
국제공개일자 2020년09월24일
(56) 선행기술조사문헌
KR1020070019363 A*
KR1020160117129 A*
KR1020080092789 A
US20120087549 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
엘지전자 주식회사
서울특별시 영등포구 여의대로 128 (여의도동)
(72) 발명자
심수영
서울특별시 서초구 양재대로11길 19
김고근
서울특별시 서초구 양재대로11길 19
(뒷면에 계속)
(74) 대리인
박장원

전체 청구항 수 : 총 10 항

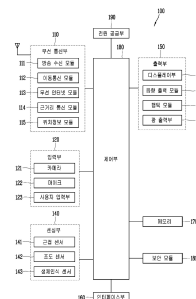
심사관 : 정성훈

(54) 발명의 명칭 전자 장치 및 그 제어 방법

(57) 요약

본 발명은 복합생체 인증이 가능한 전자 장치 및 그 제어 방법에 관한 것으로, 생체 정보를 감지하도록 형성된 적어도 하나의 센서를 포함하는 센서부와, 사용자 등록시, 감지된 생체 정보로부터 진정 점수(genuine score)를 추출하고, 추출된 진정 점수에 근거하여 인증 임계 점수를 결정하기 위한 생체 인증 모델을 생성하며, 사용자 인증시, 감지된 생체 정보로부터 획득되는 특징점들과 상기 생체 인증 모델에 근거하여 사용자 인증을 수행하는 보안 모듈 및, 상기 사용자 인증 결과에 근거하여 상기 전자 장치의 동작을 제어하는 제어부를 포함하며, 상기 보안 모듈은, 상기 사용자 인증 결과 사용자 인증에 실패한 경우, 사용자 인증에 사용된 생체 정보가 진정 사용자로부터 획득된 생체 정보인지 여부를 판단하고, 진정 사용자로부터 획득된 생체 정보인 경우 획득된 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 것을 특징으로 한다.

대표도



(72) 발명자

김범오

서울특별시 서초구 양재대로11길 19

김성진

서울특별시 서초구 양재대로11길 19

김지혜

서울특별시 서초구 양재대로11길 19

명세서

청구범위

청구항 1

복합생체인증을 수행하는 전자 장치에 있어서,

생체 정보를 감지하도록 형성된 적어도 하나의 센서를 포함하는 센서부;

사용자 등록시, 감지된 생체 정보로부터 진정 점수(genuine score)를 추출하고, 추출된 진정 점수에 근거하여 인증 임계 점수를 결정하기 위한 생체 인증 모델을 생성하며,

사용자 인증시, 감지된 생체 정보로부터 획득되는 특징점들과 상기 생체 인증 모델에 근거하여 사용자 인증을 수행하는 보안 모듈; 및,

상기 사용자 인증 결과에 근거하여 상기 전자 장치의 동작을 제어하는 제어부를 포함하며,

상기 보안 모듈은,

상기 사용자 인증 결과 사용자 인증에 실패한 경우, 사용자 인증에 사용된 생체 정보가 진정 사용자로부터 획득된 생체 정보인지 여부를 판단하고, 진정 사용자로부터 획득된 생체 정보인 경우 획득된 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하고,

상기 보안 모듈은,

상기 진정 사용자 여부를 판단한 결과, 진정 사용자가 아닌 경우 상기 사용자 인증에 사용된 생체 정보를 위조 생체 정보로 저장하며, 동일한 위조 생체 정보가 기 설정된 횟수 이상 반복하여 저장되는 경우 상기 위조 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 것을 특징으로 하는 전자 장치.

청구항 2

제1항에 있어서,

상기 생체 인증 모델은,

상기 사용자 인증을 위해 획득된 생체 정보가 진정 사용자인지 여부를 판단할 수 있는 기준값인 인증 임계 점수(threshold score)를 결정하기 위한 모델이며,

상기 인증 임계 점수는,

상기 생체 인증 모델의 업데이트에 따라 변경되는 것을 특징으로 하는 전자 장치.

청구항 3

제1항에 있어서,

상기 보안 모듈은,

사용자 인증에 실패한 진정 사용자의 생체 정보를 저장하며,

동일한 생체 정보가 기 설정된 횟수 이상 반복하여 저장되는 경우 상기 사용자 인증에 실패한 진정 사용자의 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 것을 특징으로 하는 전자 장치.

청구항 4

제1항에 있어서,

상기 보안 모듈은,

사용자 등록을 위한 생체 정보가 획득되는 경우, 획득된 생체 정보로부터 센싱되는 정보들 중 일부를 등록 데이

터로, 나머지 일부를 인증 데이터로 설정하며, 분류된 등록 데이터와 인증 데이터에 근거하여 상기 진정 점수를 추출하는 것을 특징으로 하는 전자 장치.

청구항 5

제1항에 있어서,

상기 보안 모듈은,

상기 사용자 인증 결과 사용자 인증에 성공한 경우, 사용자 인증에 사용된 생체 정보로부터 산출된 매칭 점수가, 인증 임계 점수로부터 기 설정된 수준 이내인지 여부를 체크하고,

상기 체크 결과에 근거하여 상기 사용자 인증에 사용된 생체 정보에 대응하는 사용자가 진정 사용자인지 여부를 판단하고, 판단 결과에 따라 상기 사용자 인증에 사용된 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 것을 특징으로 하는 전자 장치.

청구항 6

삭제

청구항 7

제1항에 있어서,

상기 보안 모듈은,

기 설정된 비밀번호 방식 또는 적어도 하나의 다른 생체 정보에 따른 사용자 인증 방식을 통해 상기 사용자 인증에 사용된 생체 정보가 진정 사용자로부터 획득된 생체 정보인지 여부를 판단하는 것을 특징으로 하는 전자 장치.

청구항 8

복합생체인증을 수행하는 전자 장치의 제어 방법에 있어서,

사용자 등록을 위한 생체 정보를 획득하는 단계;

획득된 생체 정보로부터 진정 점수(genuine score)를 추출하고, 추출된 진정 점수에 근거하여 인증 임계 점수를 결정하기 위한 생체 인증 모델을 생성하는 단계;

사용자로부터 사용자 인증을 위한 생체 정보를 획득하고 획득된 생체 정보와 상기 생체 인증 모델에 근거하여 사용자 인증을 수행하는 단계;

사용자 인증이 실패한 경우, 상기 사용자 인증을 위해 획득된 생체 정보가 진정 사용자로부터 획득된 생체 정보인지 여부를 판단하는 단계;

상기 판단 결과에 따라 상기 사용자 인증에 실패한 생체 정보로부터 진정 점수를 추출하는 단계; 및,

추출된 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 제6 단계를 포함하고,

상기 생체 인증 모델에 근거하여 사용자 인증을 수행하는 단계는,

상기 진정 사용자 여부를 판단한 결과, 진정 사용자가 아닌 경우 상기 사용자 인증에 사용된 생체 정보를 위조 생체 정보로 저장하는 단계; 및

동일한 위조 생체 정보가 기 설정된 횟수 이상 반복하여 저장되는 경우 상기 위조 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 단계를 포함하는 것을 특징으로 하는 전자 장치의 제어 방법.

청구항 9

제8항에 있어서,

획득된 생체 정보인지 여부를 판단하는 단계는,

상기 생체 인증 모델에 근거하여 사용자 인증을 수행하는 것과 다른 인증 방식에 근거하여 사용자 인증을 수행하는 단계를 더 포함하며,

상기 다른 인증 방식은,

기 설정된 비밀번호 방식 또는 다른 생체 정보를 이용하는 생체 인증 방식임을 특징으로 하는 전자 장치의 제어 방법.

청구항 10

제8항에 있어서,

상기 생체 정보로부터 진정 점수를 추출하는 단계는,

상기 판단 결과에 따라, 사용자 인증에 실패한 진정 사용자의 생체 정보를 저장하는 단계와,

동일한 생체 정보가 저장된 횟수를 검출하는 단계와;

검출된 횟수가 기 설정된 횟수 이상인 경우, 사용자 인증에 실패한 진정 사용자의 생체 정보로부터 진정 점수를 추출하는 단계를 더 포함하는 것을 특징으로 하는 전자 장치의 제어 방법.

청구항 11

제8항에 있어서,

상기 생체 인증 모델에 근거하여 사용자 인증을 수행하는 단계는,

상기 사용자 인증 결과 사용자 인증에 성공한 경우, 사용자 인증에 사용된 생체 정보로부터 산출된 매칭 점수가, 인증 임계 점수로부터 기 설정된 수준 이내인지 여부를 체크하는 단계와;

상기 체크 결과에 근거하여 상기 사용자 인증에 사용된 생체 정보가 진정 사용자로부터 획득된 생체 정보인지 여부를 판단하는 단계와; 그리고,

상기 획득된 생체 정보인지 여부를 판단 결과에 따라 상기 사용자 인증에 사용된 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 단계를 더 포함하는 것을 특징으로 하는 전자 장치의 제어 방법.

발명의 설명

기술 분야

[0001] 본 발명은 복합생체인증이 가능한 전자 장치에 관한 것이다.

배경 기술

[0002] 기술 발전과 함께 전자 장치의 기능이 다양화되고 있다. 예를 들면, 데이터와 음성통신, 카메라를 통한 사진촬영 및 비디오 촬영, 음성녹음, 스피커 시스템을 통한 음악파일 재생 그리고 디스플레이부에 이미지나 비디오를 출력하는 기능이 있다. 일부 전자 장치는 전자게임 플레이 기능이 추가되거나, 멀티미디어 플레이어 기능을 수행한다. 특히 최근의 전자 장치는 방송과 비디오나 텔레비전 프로그램과 같은 시각적 콘텐츠를 제공하는 멀티캐스트 신호를 수신할 수 있다.

[0003] 이와 같은 전자 장치의 기능이 다양화됨에 따라 예를 들어, 사진이나 동영상의 촬영, 음악이나 동영상 파일의 재생, 게임, 방송의 수신 등의 복합적인 기능들을 갖춘 멀티미디어 기기(Multimedia player) 형태로 구현되고 있다.

[0004] 이러한 전자 장치의 기능 지지 및 증대를 위해, 단말기의 구조적인 부분 및/또는 소프트웨어적인 부분을 개량하는 것이 고려될 수 있다.

[0005] 전자 장치의 기능이 다양화됨에 따라 보안성 강화를 위한 사용자 인증에 대한 중요성이 증대되고 있다. 사용자 인증에는 개인 식별 번호(Personal Identification Number: PIN)와 같은 비밀번호 방식, 및 생체 인증 정보를 이용하는 생체 인식 방식 등 다양한 방식이 사용될 수 있다.

- [0006] 생체 인식은 보안 인증의 일 방식으로, 사용자의 지문, 얼굴, 음성, 홍채, 망막, 혈관 등과 같은 고유의 신체적 특징을 이용하여, 사용자 인증을 수행하는 기술이다. 이러한 생체 인식 기술 분야는 도용 또는 모방의 위험성이 적고, 사용 편의성이 높다.
- [0007] 한편, 최근에는 보안성 강화를 위하여, 단일의 생체 정보를 이용하여 생체 인증을 수행하는 단일모드 생체 인증(Unimodal Biometric)에서 복수의 생체 인식 정보를 이용하여 생체 인증을 수행하는 다중모드 생체 인증(Multimodal Biometric) 또는 복합생체 인증으로 기술 발전이 이루어지고 있다.
- [0008] 이러한 생체 인증 방식의 경우, 사용자로부터 획득된 생체 정보로부터 획득되는 등록 데이터와 인증 데이터로부터 추출되는 진정(genuine) 점수에 근거하여 생체 인증 모델을 생성하고, 생성된 생체 인증 모델에 근거하여 인증을 위해 획득된 생체 정보의 특징점을 매칭하여 사용자의 인증을 수행할 수 있다.
- [0009] 한편 이러한 생체 인증 모델의 경우 통계적으로 일반화된 인체 생체 정보의 특징을 기반으로 생성되는 고정된 모델이므로, 생체 정보의 진정 점수 분포 또는 위조 점수의 분포가 일반적이지 않은 사용자의 경우, 진정 사용자로부터 획득된 생체 정보라고 할지라도 사용자 인증이 이루어지지 않을 확률이 높아질 수 있다는 문제가 있다.

발명의 내용

해결하려는 과제

- [0010] 본 발명은 전술한 문제 및 다른 문제를 해결하는 것을 목적으로 하는 것으로, 사용자의 생체적 특징에 따라 최적화된 생체 인증 모델을 통해 사용자 인증을 수행할 수 있는 전자 장치 및 그 전자 장치의 제어 방법을 제공하는 것이다.

과제의 해결 수단

- [0011] 상기 또는 다른 목적을 달성하기 위해 본 발명의 일 측면에 따르면, 본 발명의 실시 예에 따른 전자 장치는, 생체 정보를 감지하도록 형성된 적어도 하나의 센서를 포함하는 센서부와, 사용자 등록시, 감지된 생체 정보로부터 진정 점수(genuine score)를 추출하고, 추출된 진정 점수에 근거하여 인증 임계 점수를 결정하기 위한 생체 인증 모델을 생성하며, 사용자 인증시, 감지된 생체 정보로부터 획득되는 특징점들과 상기 생체 인증 모델에 근거하여 사용자 인증을 수행하는 보안 모듈 및, 상기 사용자 인증 결과에 근거하여 상기 전자 장치의 동작을 제어하는 제어부를 포함하며, 상기 보안 모듈은, 상기 사용자 인증 결과 사용자 인증에 실패한 경우, 사용자 인증에 사용된 생체 정보가 진정 사용자로부터 획득된 생체 정보인지 여부를 판단하고, 진정 사용자로부터 획득된 생체 정보인 경우 획득된 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 것을 특징으로 한다.
- [0012] 일 실시 예에 있어서, 상기 생체 인증 모델은, 상기 사용자 인증을 위해 획득된 생체 정보가 진정 사용자인지 여부를 판단할 수 있는 기준값인 인증 임계 점수(threshold score)를 결정하기 위한 모델이며, 상기 인증 임계 점수는, 상기 생체 인증 모델의 업데이트에 따라 변경되는 것을 특징으로 한다.
- [0013] 일 실시 예에 있어서, 상기 보안 모듈은, 사용자 인증에 실패한 진정 사용자의 생체 정보를 저장하며, 동일한 생체 정보가 기 설정된 횟수 이상 반복하여 저장되는 경우 상기 사용자 인증에 실패한 진정 사용자의 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 것을 특징으로 한다.
- [0014] 일 실시 예에 있어서, 상기 보안 모듈은, 사용자 등록을 위한 생체 정보가 획득되는 경우, 획득된 생체 정보로부터 센싱되는 정보들 중 일부를 등록 데이터로, 나머지 일부를 인증 데이터로 설정하며, 분류된 등록 데이터와 인증 데이터에 근거하여 상기 진정 점수를 추출하는 것을 특징으로 한다.
- [0015] 일 실시 예에 있어서, 상기 보안 모듈은, 상기 사용자 인증 결과 사용자 인증에 성공한 경우, 사용자 인증에 사용된 생체 정보로부터 산출된 매칭 점수가, 인증 임계 점수로부터 기 설정된 수준 이내인지 여부를 체크하고, 상기 체크 결과에 근거하여 상기 사용자 인증에 사용된 생체 정보에 대응하는 사용자가 진정 사용자인지 여부를 판단하고, 판단 결과에 따라 상기 사용자 인증에 사용된 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 것을 특징으로 한다.
- [0016] 일 실시 예에 있어서, 상기 보안 모듈은, 상기 진정 사용자 여부를 판단한 결과, 진정 사용자가 아닌 경우 상기 사용자 인증에 사용된 생체 정보를 위조 생체 정보로 저장하며, 동일한 위조 생체 정보가 기 설정된 횟수 이상

반복하여 저장되는 경우 상기 위조 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 것을 특징으로 한다.

[0017] 일 실시 예에 있어서, 상기 보안 모듈은, 기 설정된 비밀번호 방식 또는 적어도 하나의 다른 생체 정보에 따른 사용자 인증 방식을 통해 상기 사용자 인증에 사용된 생체 정보가 진정 사용자로부터 획득된 생체 정보인지 여부를 판단하는 것을 특징으로 한다.

[0018] 상기 또는 다른 목적을 달성하기 위해 본 발명의 일 측면에 따르면, 본 발명의 실시 예에 따른 전자 장치의 제어 방법은,

[0019] 사용자 등록을 위한 생체 정보를 획득하는 제1 단계와, 획득된 생체 정보로부터 진정 점수(genuine score)를 추출하고, 추출된 진정 점수에 근거하여 인증 임계 점수를 결정하기 위한 생체 인증 모델을 생성하는 제2 단계와, 사용자로부터 사용자 인증을 위한 생체 정보를 획득하고 획득된 생체 정보와 상기 생체 인증 모델에 근거하여 사용자 인증을 수행하는 제3 단계와, 사용자 인증이 실패한 경우, 상기 사용자 인증을 위해 획득된 생체 정보가 진정 사용자로부터 획득된 생체 정보인지 여부를 판단하는 제4 단계와, 상기 판단 결과에 따라 상기 사용자 인증에 실패한 생체 정보로부터 진정 점수를 추출하는 제5 단계 및, 추출된 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 제6 단계를 포함하는 것을 특징으로 한다.

[0020] 일 실시 예에 있어서, 상기 제4 단계는, 상기 제3 단계의 사용자 인증 방식과 다른 인증 방식에 근거하여 사용자 인증을 수행하는 제4-1 단계를 더 포함하며, 상기 다른 인증 방식은, 기 설정된 비밀번호 방식 또는 상기 제3 단계의 사용자 인증에 사용된 생체 정보와 다른 생체 정보를 이용하는 생체 인증 방식임을 특징으로 한다.

[0021] 일 실시 예에 있어서, 상기 제5 단계는, 상기 제4 단계의 판단 결과에 따라, 사용자 인증에 실패한 진정 사용자의 생체 정보를 저장하는 제5-1 단계와, 동일한 생체 정보가 저장된 횟수를 검출하는 제5-2 단계와, 상기 제5-2 단계에서 검출된 횟수가 기 설정된 횟수 이상인 경우, 상기 사용자 인증에 실패한 진정 사용자의 생체 정보로부터 진정 점수를 추출하는 제5-3 단계를 포함하는 것을 특징으로 한다.

[0022] 일 실시 예에 있어서, 상기 제3 단계는, 상기 사용자 인증 결과 사용자 인증에 성공한 경우, 사용자 인증에 사용된 생체 정보로부터 산출된 매칭 점수가, 인증 임계 점수로부터 기 설정된 수준이내인지 여부를 체크하는 제3-1 단계와, 상기 체크 결과에 근거하여 상기 사용자 인증에 사용된 생체 정보가 진정 사용자로부터 획득된 생체 정보인지 여부를 판단하는 제3-2 단계 및, 상기 제3-2 단계의 판단 결과에 따라 상기 사용자 인증에 사용된 생체 정보로부터 추출되는 진정 점수에 근거하여 상기 생체 인증 모델을 업데이트하는 제3-3 단계를 더 포함하는 것을 특징으로 한다.

발명의 효과

[0023] 본 발명에 따른 전자 장치 및 그 제어 방법의 효과에 대해 설명하면 다음과 같다.

[0024] 본 발명의 실시 예들 중 적어도 하나에 의하면, 본 발명은 진정 사용자로부터 획득되었음에도 불구하고 사용자 인증에 실패한 생체 정보가 있는 경우, 그 생체 정보로부터 추출된 인증 데이터를 반영하여 생체 인증 모델을 업데이트함으로써 사용자에게 최적화된 생체 인증 모델을 생성할 수 있으며, 이에 따라 진정 사용자로부터 획득된 생체 정보에 따른 사용자 인증의 인증 실패 가능성을 보다 낮출 수 있다는 효과가 있다.

[0025] 또한, 본 발명의 실시 예들 중 적어도 하나에 의하면, 본 발명은 사용자에게 최적화된 생체 인증 모델을 제공함으로써, 진정 사용자가 아닌 사용자로부터 획득되었음에도 진정 사용자로 인증될 수 있는 인증 오류 가능성을 보다 낮출 수 있다는 효과가 있다.

도면의 간단한 설명

[0026] 도 1은 본 발명과 관련된 전자 장치를 설명하기 위한 블록도이다.

도 2는 단일생체 인증 방식을 설명한 개념도이다.

도 3a 내지 도 3d는 복합생체 인증 방식을 설명한 개념도들이다.

도 4a 및 도 4b는 생체 인증 판단의 오차율과 관련된 그래프들이다.

도 5는 본 발명의 실시 예에 따른 전자 장치에서, 인증에 실패한 진정 사용자의 인증 데이터에 근거하여 생체 인증 모델을 업데이트하는 동작 과정을 도시한 흐름도이다.

도 6a는 본 발명의 실시 예에 따른 전자 장치에서, 사용자로부터 획득된 생체 정보로부터 진정 점수를 추출하는 동작 과정을 도시한 흐름도이다.

도 6b는 본 발명의 실시 예에 따른 전자 장치에서, 사용자에게 개인화된 초기 생체 인증 모델을 생성하는 과정을 도시한 개념도이다.

도 7은 본 발명의 실시 예에 따른 전자 장치에서, 사용자 인증을 수행한 결과에 따라 인증에 실패한 진정 사용자의 인증 데이터를 저장하는 동작 과정을 도시한 흐름도이다.

도 8은 본 발명의 실시 예에 따른 전자 장치에서, 인증에 실패한 진정 사용자의 인증 데이터에 근거하여 생체 인증 모델을 업데이트하는 과정을 도시한 개념도이다.

도 9는 본 발명의 실시 예에 따른 전자 장치에서, 생체 인증 모델의 업데이트에 따라 인증 임계 점수(Threshold score) 분포가 변경되는 예를 도시한 예시도이다.

도 10은 본 발명의 실시 예에 따른 전자 장치에서, 사용자 인증을 수행한 결과에 따라 위조 생체 정보를 검출 및 저장하는 동작 과정을 도시한 흐름도이다.

도 11은 본 발명의 실시 예에 따른 전자 장치에서, 생체 인증 모델의 업데이트에 따라 인증 임계 점수(Threshold score) 분포가 변경되는 다른 예를 도시한 예시도이다.

발명을 실시하기 위한 구체적인 내용

- [0027] 이하, 첨부된 도면을 참조하여 본 명세서에 개시된 실시 예를 상세히 설명하되, 도면 부호에 관계없이 동일하거나 유사한 구성요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 이하의 설명에서 사용되는 구성요소에 대한 접미사 "모듈" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서, 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다. 또한, 본 명세서에 개시된 실시 예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시 예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시 예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않으며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.
- [0028] 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되지는 않는다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.
- [0029] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.
- [0030] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.
- [0031] 본 출원에서, "포함한다" 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.
- [0032] 본 명세서에서 설명되는 휴대 전자장치에는 휴대폰, 스마트 폰(smart phone), 노트북 컴퓨터(laptop computer), 디지털방송용 단말기, PDA(personal digital assistants), PMP(portable multimedia player), 네비게이션, 슬레이트 PC(slate PC), 태블릿 PC(tablet PC), 울트라북(ultrabook), 웨어러블 디바이스(wearable device, 예를 들어, 위치형 단말기 (smartwatch), 글래스형 단말기 (smart glass), HMD(head mounted display)), 스마트 자동차 등이 포함될 수 있다.
- [0033] 그러나, 본 명세서에 기재된 실시 예에 따른 구성은 휴대 전자장치에만 적용 가능한 경우를 제외하면, 디지털 TV, 데스크탑 컴퓨터, 디지털 사이니지 등과 같은 고정 단말기에도 적용될 수도 있음을 본 기술분야의 당업자라면 쉽게 알 수 있을 것이다.
- [0034] 도 1은 본 발명과 관련된 전자 장치를 설명하기 위한 블록도이다.

- [0035] 도 1을 참조하면, 입력부(120), 감지부(140), 출력부(150), 인터페이스부(160), 메모리(170), 제어부(180), 보안모듈(181) 및 전원 공급부(190) 등을 포함할 수 있다. 도 1에 도시된 구성요소들은 전자 장치를 구현하는데 있어서 필수적인 것은 아니어서, 본 명세서 상에서 설명되는 전자 장치는 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다.
- [0036] 보다 구체적으로, 상기 구성요소들 중 무선 통신부(110)는, 전자 장치(100)와 무선 통신 시스템 사이, 전자 장치(100)와 다른 전자 장치(100) 사이, 또는 전자 장치(100)와 외부서버 사이의 무선 통신을 가능하게 하는 하나 이상의 모듈을 포함할 수 있다. 또한, 상기 무선 통신부(110)는, 전자 장치(100)를 하나 이상의 네트워크에 연결하는 하나 이상의 모듈을 포함할 수 있다.
- [0037] 이러한 무선 통신부(110)는, 방송 수신 모듈(111), 이동통신 모듈(112), 무선 인터넷 모듈(113), 근거리 통신 모듈(114), 위치정보 모듈(115) 중 적어도 하나를 포함할 수 있다.
- [0038] 입력부(120)는, 영상 신호 입력을 위한 카메라(121) 또는 영상 입력부, 오디오 신호 입력을 위한 마이크로폰(microphone, 122), 또는 오디오 입력부, 사용자로부터 정보를 입력받기 위한 사용자 입력부(123, 예를 들어, 터치키(touch key), 푸시키(mechanical key) 등)를 포함할 수 있다. 입력부(120)에서 수집한 음성 데이터나 이미지 데이터는 분석되어 사용자의 제어명령으로 처리될 수 있다.
- [0039] 센싱부(140)는 전자 장치 내 정보, 전자 장치를 둘러싼 주변 환경 정보 및 사용자 정보 중 적어도 하나를 센싱하기 위한 하나 이상의 센서를 포함할 수 있다. 예를 들어, 센싱부(140)는 근접센서(141, proximity sensor), 조도 센서(142, illumination sensor), 터치 센서(touch sensor), 가속도 센서(acceleration sensor), 자기 센서(magnetic sensor), 중력 센서(G-sensor), 자이로스코프 센서(gyroscope sensor), 모션 센서(motion sensor), RGB 센서, 적외선 센서(IR 센서: infrared sensor), 지문인식 센서(finger scan sensor), 초음파 센서(ultrasonic sensor), 광 센서(optical sensor, 예를 들어, 카메라(121 참조)), 마이크로폰(microphone, 122 참조), 배터리 게이지(battery gauge), 환경 센서(예를 들어, 기압계, 습도계, 온도계, 방사능 감지 센서, 열 감지 센서, 가스 감지 센서 등), 화학 센서(예를 들어, 전자 코, 헬스케어 센서, 생체 인식 센서 등) 중 적어도 하나를 포함할 수 있다. 생체 인식 센서(143)는, 홍채 센서, 얼굴인식 센서, PPG 센서, 음성 센서 등이 포함될 수 있다. 한편, 본 명세서에 개시된 전자 장치는, 이러한 센서들 중 적어도 둘 이상의 센서에서 센싱되는 정보들을 조합하여 활용할 수 있다.
- [0040] 출력부(150)는 시각, 청각 또는 촉각 등과 관련된 출력을 발생시키기 위한 것으로, 디스플레이부(151), 음향 출력부(152), 햅틱 모듈(153), 광 출력부(154) 중 적어도 하나를 포함할 수 있다. 디스플레이부(151)는 터치 센서와 상호 레이어 구조를 이루거나 일체형으로 형성됨으로써, 터치 스크린을 구현할 수 있다. 이러한 터치 스크린은, 전자 장치(100)와 사용자 사이의 입력 인터페이스를 제공하는 사용자 입력부(123)로써 기능함과 동시에, 전자 장치(100)와 사용자 사이의 출력 인터페이스를 제공할 수 있다.
- [0041] 인터페이스부(160)는 전자 장치(100)에 연결되는 다양한 종류의 외부 기기와의 통로 역할을 수행한다. 이러한 인터페이스부(160)는, 유/무선 헤드셋 포트(port), 외부 충전기 포트(port), 유/무선 데이터 포트(port), 메모리 카드(memory card) 포트, 식별 모듈이 구비된 장치를 연결하는 포트(port), 오디오 I/O(Input/Output) 포트(port), 비디오 I/O(Input/Output) 포트(port), 이어폰 포트(port) 중 적어도 하나를 포함할 수 있다. 전자 장치(100)에서는, 상기 인터페이스부(160)에 외부 기기가 연결되는 것에 대응하여, 연결된 외부 기기와 관련된 적절한 제어를 수행할 수 있다.
- [0042] 또한, 메모리(170)는 전자 장치(100)의 다양한 기능을 지원하는 데이터를 저장한다. 메모리(170)는 전자 장치(100)에서 구동되는 다수의 응용 프로그램(application program 또는 애플리케이션(application)), 전자 장치(100)의 동작을 위한 데이터들, 명령어들을 저장할 수 있다. 이러한 응용 프로그램 중 적어도 일부는, 무선 통신을 통해 외부 서버로부터 다운로드 될 수 있다. 또한 이러한 응용 프로그램 중 적어도 일부는, 전자 장치(100)의 기본적인 기능(예를 들어, 전화 착신, 발신 기능, 메시지 수신, 발신 기능)을 위하여 출고 당시부터 전자 장치(100)상에 존재할 수 있다. 한편, 응용 프로그램은, 메모리(170)에 저장되고, 전자 장치(100) 상에 설치되어, 제어부(180)에 의하여 상기 전자 장치의 동작(또는 기능)을 수행하도록 구동될 수 있다.
- [0043] 제어부(180)는 상기 응용 프로그램과 관련된 동작 외에도, 통상적으로 전자 장치(100)의 전반적인 동작을 제어한다. 제어부(180)는 위에서 살펴본 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 메모리(170)에 저장된 응용 프로그램을 구동함으로써, 사용자에게 적절한 정보 또는 기능을 제공 또는 처리할 수 있다.

- [0044] 또한, 제어부(180)는 메모리(170)에 저장된 응용 프로그램을 구동하기 위하여, 도 1a와 함께 살펴본 구성요소들 중 적어도 일부를 제어할 수 있다. 나아가, 제어부(180)는 상기 응용 프로그램의 구동을 위하여, 전자 장치(100)에 포함된 구성요소들 중 적어도 둘 이상을 서로 조합하여 동작시킬 수 있다.
- [0045] 전원공급부(190)는 제어부(180)의 제어 하에서, 외부의 전원, 내부의 전원을 인가 받아 전자 장치(100)에 포함된 각 구성요소들에 전원을 공급한다. 이러한 전원공급부(190)는 배터리를 포함하며, 상기 배터리는 내장형 배터리 또는 교체가능한 형태의 배터리가 될 수 있다.
- [0046] 상기 각 구성요소들 중 적어도 일부는, 이하에서 설명되는 다양한 실시 예들에 따른 전자 장치의 동작, 제어, 또는 제어방법을 구현하기 위하여 서로 협력하여 동작할 수 있다. 또한, 상기 전자 장치의 동작, 제어, 또는 제어방법은 상기 메모리(170)에 저장된 적어도 하나의 응용 프로그램의 구동에 의하여 전자 장치 상에서 구현될 수 있다.
- [0047] 이하에서는, 위에서 살펴본 전자 장치(100)를 통하여 구현되는 다양한 실시 예들을 살펴보기에 앞서, 위에서 열거된 구성요소들에 대하여 도 1a를 참조하여 보다 구체적으로 살펴본다.
- [0048] 먼저, 무선 통신부(110)에 대하여 살펴보면, 무선 통신부(110)의 방송 수신 모듈(111)은 방송 채널을 통하여 외부의 방송 관리 서버로부터 방송 신호 및/또는 방송 관련된 정보를 수신한다. 상기 방송 채널은 위성 채널, 지상파 채널을 포함할 수 있다. 적어도 두 개의 방송 채널들에 대한 동시 방송 수신 또는 방송 채널 스위칭을 위해 둘 이상의 상기 방송 수신 모듈이 상기 이동단말기(100)에 제공될 수 있다.
- [0049] 이동통신 모듈(112)은, 이동통신을 위한 기술표준들 또는 통신방식(예를 들어, GSM(Global System for Mobile communication), CDMA(Code Division Multi Access), CDMA2000(Code Division Multi Access 2000), EV-DO(Enhanced Voice-Data Optimized or Enhanced Voice-Data Only), WCDMA(Wideband CDMA), HSDPA(High Speed Downlink Packet Access), HSUPA(High Speed Uplink Packet Access), LTE(Long Term Evolution), LTE-A(Long Term Evolution-Advanced) 등)에 따라 구축된 이동 통신망 상에서 기지국, 외부의 단말, 서버 중 적어도 하나와 무선 신호를 송수신한다.
- [0050] 상기 무선 신호는, 음성 호 신호, 화상 통화 호 신호 또는 문자/멀티미디어 메시지 송수신에 따른 다양한 형태의 데이터를 포함할 수 있다.
- [0051] 무선 인터넷 모듈(113)은 무선 인터넷 접속을 위한 모듈을 말하는 것으로, 전자 장치(100)에 내장되거나 외장될 수 있다. 무선 인터넷 모듈(113)은 무선 인터넷 기술들에 따른 통신망에서 무선 신호를 송수신하도록 이루어진다.
- [0052] 무선 인터넷 기술로는, 예를 들어 WLAN(Wireless LAN), Wi-Fi(Wireless-Fidelity), Wi-Fi(Wireless Fidelity) Direct, DLNA(Digital Living Network Alliance), WiBro(Wireless Broadband), WiMAX(World Interoperability for Microwave Access), HSDPA(High Speed Downlink Packet Access), HSUPA(High Speed Uplink Packet Access), LTE(Long Term Evolution), LTE-A(Long Term Evolution-Advanced) 등이 있으며, 상기 무선 인터넷 모듈(113)은 상기에서 나열되지 않은 인터넷 기술까지 포함한 범위에서 적어도 하나의 무선 인터넷 기술에 따라 데이터를 송수신하게 된다.
- [0053] WiBro, HSDPA, HSUPA, GSM, CDMA, WCDMA, LTE, LTE-A 등에 의한 무선인터넷 접속은 이동통신망을 통해 이루어진다는 관점에서 본다면, 상기 이동통신망을 통해 무선인터넷 접속을 수행하는 상기 무선 인터넷 모듈(113)은 상기 이동통신 모듈(112)의 일종으로 이해될 수도 있다.
- [0054] 근거리 통신 모듈(114)은 근거리 통신(Short range communication)을 위한 것으로서, 블루투스(Bluetooth™), RFID(Radio Frequency Identification), 적외선 통신(Infrared Data Association; IrDA), UWB(Ultra Wideband), ZigBee, NFC(Near Field Communication), Wi-Fi(Wireless-Fidelity), Wi-Fi Direct, Wireless USB(Wireless Universal Serial Bus) 기술 중 적어도 하나를 이용하여, 근거리 통신을 지원할 수 있다. 이러한, 근거리 통신 모듈(114)은, 근거리 무선 통신망(Wireless Area Networks)을 통해 전자 장치(100)와 무선 통신 시스템 사이, 전자 장치(100)와 다른 전자 장치(100) 사이, 또는 전자 장치(100)와 다른 전자 장치(100, 또는 외부서버)가 위치한 네트워크 사이의 무선 통신을 지원할 수 있다. 상기 근거리 무선 통신망은 근거리 무선 개인 통신망(Wireless Personal Area Networks)일 수 있다.
- [0055] 여기에서, 다른 전자 장치(100)는 본 발명에 따른 전자 장치(100)와 데이터를 상호 교환하는 것이 가능한(또는 연동 가능한) 웨어러블 디바이스(wearable device, 예를 들어, 스마트워치(smartwatch), 스마트 글래스(smart

glass), HMD(head mounted display))가 될 수 있다. 근거리 통신 모듈(114)은, 전자 장치(100) 주변에, 상기 전자 장치(100)와 통신 가능한 웨어러블 디바이스를 감지(또는 인식)할 수 있다. 나아가, 제어부(180)는 상기 감지된 웨어러블 디바이스가 본 발명에 따른 전자 장치(100)와 통신하도록 인증된 디바이스인 경우, 전자 장치(100)에서 처리되는 데이터의 적어도 일부를, 상기 근거리 통신 모듈(114)을 통해 웨어러블 디바이스로 전송할 수 있다. 따라서, 웨어러블 디바이스의 사용자는, 전자 장치(100)에서 처리되는 데이터를, 웨어러블 디바이스를 통해 이용할 수 있다. 예를 들어, 이에 따르면 사용자는, 전자 장치(100)에 전화가 수신된 경우, 웨어러블 디바이스를 통해 전화 통화를 수행하거나, 전자 장치(100)에 메시지가 수신된 경우, 웨어러블 디바이스를 통해 상기 수신된 메시지를 확인하는 것이 가능하다.

[0056] 위치정보 모듈(115)은 전자 장치의 위치(또는 현재 위치)를 획득하기 위한 모듈로서, 그의 대표적인 예로는 GPS(Global Positioning System) 모듈 또는 WiFi(Wireless Fidelity) 모듈이 있다. 예를 들어, 전자 장치는 GPS 모듈을 활용하면, GPS 위성에서 보내는 신호를 이용하여 전자 장치의 위치를 획득할 수 있다. 다른 예로서, 전자 장치는 Wi-Fi모듈을 활용하면, Wi-Fi모듈과 무선신호를 송신 또는 수신하는 무선 AP(Wireless Access Point)의 정보에 기반하여, 전자 장치의 위치를 획득할 수 있다. 필요에 따라서, 위치정보모듈(115)은 치환 또는 부가적으로 전자 장치의 위치에 관한 데이터를 얻기 위해 무선 통신부(110)의 다른 모듈 중 어느 기능을 수행할 수 있다. 위치정보모듈(115)은 전자 장치의 위치(또는 현재 위치)를 획득하기 위해 이용되는 모듈로, 전자 장치의 위치를 직접적으로 계산하거나 획득하는 모듈로 한정되지는 않는다.

[0057] 다음으로, 입력부(120)는 영상 정보(또는 신호), 오디오 정보(또는 신호), 데이터, 또는 사용자로부터 입력되는 정보의 입력을 위한 것으로서, 영상 정보의 입력을 위하여, 전자 장치(100)는 하나 또는 복수의 카메라(121)를 구비할 수 있다. 카메라(121)는 화상 통화모드 또는 촬영 모드에서 이미지 센서에 의해 얻어지는 정지영상 또는 동영상 등의 화상 프레임을 처리한다. 처리된 화상 프레임은 디스플레이부(151)에 표시되거나 메모리(170)에 저장될 수 있다. 한편, 전자 장치(100)에 구비되는 복수의 카메라(121)는 매트릭스 구조를 이루도록 배치될 수 있으며, 이와 같이 매트릭스 구조를 이루는 카메라(121)를 통하여, 전자 장치(100)에는 다양한 각도 또는 초점을 갖는 복수의 영상정보가 입력될 수 있다. 또한, 복수의 카메라(121)는 입체영상을 구현하기 위한 좌 영상 및 우 영상을 획득하도록, 스테레오 구조로 배치될 수 있다.

[0058] 마이크로폰(122)은 외부의 음향 신호를 전기적인 음성 데이터로 처리한다. 처리된 음성 데이터는 전자 장치(100)에서 수행 중인 기능(또는 실행 중인 응용 프로그램)에 따라 다양하게 활용될 수 있다. 한편, 마이크로폰(122)에는 외부의 음향 신호를 입력 받는 과정에서 발생하는 잡음(noise)을 제거하기 위한 다양한 잡음 제거 알고리즘이 구현될 수 있다.

[0059] 사용자 입력부(123)는 사용자로부터 정보를 입력받기 위한 것으로서, 사용자 입력부(123)를 통해 정보가 입력되면, 제어부(180)는 입력된 정보에 대응되도록 전자 장치(100)의 동작을 제어할 수 있다. 이러한, 사용자 입력부(123)는 기계식 (mechanical) 입력수단(또는, 메커니컬 키, 예를 들어, 전자 장치 (100)의 전·후면 또는 측면에 위치하는 버튼, 돔 스위치(dome switch), 조그 휠, 조그 스위치 등) 및 터치식 입력수단을 포함할 수 있다. 일 예로서, 터치식 입력수단은, 소프트웨어적인 처리를 통해 터치스크린에 표시되는 가상 키(virtual key), 소프트 키(soft key) 또는 비주얼 키(visual key)로 이루어지거나, 상기 터치스크린 이외의 부분에 배치되는 터치 키(touch key)로 이루어질 수 있다. 한편, 상기 가상키 또는 비주얼 키는, 다양한 형태를 가지면서 터치스크린 상에 표시되는 것이 가능하며, 예를 들어, 그래픽(graphic), 텍스트(text), 아이콘(icon), 비디오(video) 또는 이들의 조합으로 이루어질 수 있다.

[0060] 한편, 센싱부(140)는 전자 장치 내 정보, 전자 장치를 둘러싼 주변 환경 정보 및 사용자 정보 중 적어도 하나를 센싱하고, 이에 대응하는 센싱 신호를 발생시킨다. 제어부(180)는 이러한 센싱 신호에 기초하여, 전자 장치(100)의 구동 또는 동작을 제어하거나, 전자 장치(100)에 설치된 응용 프로그램과 관련된 데이터 처리, 기능 또는 동작을 수행할 수 있다. 센싱부(140)에 포함될 수 있는 다양한 센서 중 대표적인 센서들의 대하여, 보다 구체적으로 살펴본다.

[0061] 먼저, 근접 센서(141)는 소정의 검출면에 접근하는 물체, 혹은 근방에 존재하는 물체의 유무를 전자계의 힘 또는 적외선 등을 이용하여 기계적 접촉이 없이 검출하는 센서를 말한다. 이러한 근접 센서(141)는 위에서 살펴본 터치 스크린에 의해 감싸지는 전자 장치의 내부 영역 또는 상기 터치 스크린의 근처에 근접 센서(141)가 배치될 수 있다.

[0062] 근접 센서(141)의 예로는 투과형 광전 센서, 직접 반사형 광전 센서, 미러 반사형 광전 센서, 고주파 발진형 근접 센서, 정전 용량형 근접 센서, 자기형 근접 센서, 적외선 근접 센서 등이 있다. 터치 스크린이 정전식인 경

우에, 근접 센서(141)는 전도성을 갖는 물체의 근접에 따른 전계의 변화로 상기 물체의 근접을 검출하도록 구성될 수 있다. 이 경우 터치 스크린(또는 터치 센서) 자체가 근접 센서로 분류될 수 있다.

[0063] 한편, 설명의 편의를 위해, 터치 스크린 상에 물체가 접촉되지 않으면서 근접되어 상기 물체가 상기 터치 스크린 상에 위치함이 인식되도록 하는 행위를 "근접 터치(proximity touch)"라고 명명하고, 상기 터치 스크린 상에 물체가 실제로 접촉되는 행위를 "접촉 터치(contact touch)"라고 명명한다. 상기 터치 스크린 상에서 물체가 근접 터치 되는 위치라 함은, 상기 물체가 근접 터치될 때 상기 물체가 상기 터치 스크린에 대해 수직으로 대응되는 위치를 의미한다. 상기 근접 센서(141)는, 근접 터치와, 근접 터치 패턴(예를 들어, 근접 터치 거리, 근접 터치 방향, 근접 터치 속도, 근접 터치 시간, 근접 터치 위치, 근접 터치 이동 상태 등)을 감지할 수 있다. 한편, 제어부(180)는 위와 같이, 근접 센서(141)를 통해 감지된 근접 터치 동작 및 근접 터치 패턴에 상응하는 데이터(또는 정보)를 처리하며, 나아가, 처리된 데이터에 대응하는 시각적인 정보를 터치 스크린상에 출력시킬 수 있다. 나아가, 제어부(180)는, 터치 스크린 상의 동일한 지점에 대한 터치가, 근접 터치인지 또는 접촉 터치인지에 따라, 서로 다른 동작 또는 데이터(또는 정보)가 처리되도록 전자 장치(100)를 제어할 수 있다.

[0064] 터치 센서는 저항막 방식, 정전용량 방식, 적외선 방식, 초음파 방식, 자기장 방식 등 여러 가지 터치방식 중 적어도 하나를 이용하여 터치 스크린(또는 디스플레이부(151))에 가해지는 터치(또는 터치입력)를 감지한다.

[0065] 일 예로서, 터치 센서는, 터치 스크린의 특정 부위에 가해진 압력 또는 특정 부위에 발생하는 정전 용량 등의 변화를 전기적인 입력신호로 변환하도록 구성될 수 있다. 터치 센서는, 터치 스크린 상에 터치를 가하는 터치 대상체가 터치 센서 상에 터치 되는 위치, 면적, 터치 시의 압력, 터치 시의 정전 용량 등을 검출할 수 있도록 구성될 수 있다. 여기에서, 터치 대상체는 상기 터치 센서에 터치를 인가하는 물체로서, 예를 들어, 손가락, 터치펜 또는 스타일러스 펜(Stylus pen), 포인터 등이 될 수 있다.

[0066] 이와 같이, 터치 센서에 대한 터치 입력이 있는 경우, 그에 대응하는 신호(들)는 터치 제어기로 보내진다. 터치 제어기는 그 신호(들)를 처리한 다음 대응하는 데이터를 제어부(180)로 전송한다. 이로써, 제어부(180)는 디스플레이부(151)의 어느 영역이 터치 되었는지 여부 등을 알 수 있게 된다. 여기에서, 터치 제어기는, 제어부(180)와 별도의 구성요소일 수 있고, 제어부(180) 자체일 수 있다.

[0067] 한편, 제어부(180)는, 터치 스크린(또는 터치 스크린 이외에 구비된 터치키)을 터치하는, 터치 대상체의 종류에 따라 서로 다른 제어를 수행하거나, 동일한 제어를 수행할 수 있다. 터치 대상체의 종류에 따라 서로 다른 제어를 수행할지 또는 동일한 제어를 수행할 지는, 현재 전자 장치(100)의 동작상태 또는 실행 중인 응용 프로그램에 따라 결정될 수 있다.

[0068] 한편, 위에서 살펴본 터치 센서 및 근접 센서는 독립적으로 또는 조합되어, 터치 스크린에 대한 숏(또는 탭) 터치(short touch), 롱 터치(long touch), 멀티 터치(multi touch), 드래그 터치(drag touch), 플릭 터치(flick touch), 핀치-인 터치(pinch-in touch), 핀치-아웃 터치(pinch-out 터치), 스와이프(swipe) 터치, 호버링(hovering) 터치 등과 같은, 다양한 방식의 터치를 센싱할 수 있다.

[0069] 초음파 센서는 초음파를 이용하여, 감지대상의 위치정보를 인식할 수 있다. 한편 제어부(180)는 광 센서와 복수의 초음파 센서로부터 감지되는 정보를 통해, 파동 발생원의 위치를 산출하는 것이 가능하다. 파동 발생원의 위치는, 광이 초음파보다 매우 빠른 성질, 즉, 광이 광 센서에 도달하는 시간이 초음파가 초음파 센서에 도달하는 시간보다 매우 빠름을 이용하여, 산출될 수 있다. 보다 구체적으로 광을 기준 신호로 초음파가 도달하는 시간과의 시간차를 이용하여 파동 발생원의 위치가 산출될 수 있다.

[0070] 한편, 입력부(120)의 구성으로 살펴본, 카메라(121)는 카메라 센서(예를 들어, CCD, CMOS 등), 포토 센서(또는 이미지 센서) 및 레이저 센서 중 적어도 하나를 포함한다.

[0071] 카메라(121)와 레이저 센서는 서로 조합되어, 3차원 입체영상에 대한 감지대상의 터치를 감지할 수 있다. 포토 센서는 디스플레이 소자에 적층될 수 있는데, 이러한 포토 센서는 터치 스크린에 근접한 감지대상의 움직임을 스캐닝하도록 이루어진다. 보다 구체적으로, 포토 센서는 행/열에 Photo Diode와 TR(Transistor)를 실장하여 Photo Diode에 인가되는 빛의 양에 따라 변화되는 전기적 신호를 이용하여 포토 센서 위에 올려지는 내용물을 스캔한다. 즉, 포토 센서는 빛의 변화량에 따른 감지대상의 좌표 계산을 수행하며, 이를 통하여 감지대상의 위치정보가 획득될 수 있다.

[0072] 디스플레이부(151)는 전자 장치(100)에서 처리되는 정보를 표시(출력)한다. 예를 들어, 디스플레이부(151)는 전자 장치(100)에서 구동되는 응용 프로그램의 실행화면 정보, 또는 이러한 실행화면 정보에 따른 UI(User

Interface), GUI(Graphic User Interface) 정보를 표시할 수 있다.

- [0073] 또한, 상기 디스플레이부(151)는 입체영상을 표시하는 입체 디스플레이부로서 구성될 수 있다.
- [0074] 상기 입체 디스플레이부에는 스테레오스코픽 방식(안경 방식), 오토 스테레오스코픽 방식(무안경 방식), 프로젝션 방식(홀로그래픽 방식) 등의 3차원 디스플레이 방식이 적용될 수 있다.
- [0075] 음향 출력부(152)는 호 신호 수신, 통화모드 또는 녹음 모드, 음성인식 모드, 방송수신 모드 등에서 무선 통신부(110)로부터 수신되거나 메모리(170)에 저장된 오디오 데이터를 출력할 수 있다. 음향 출력부(152)는 전자 장치(100)에서 수행되는 기능(예를 들어, 호신호 수신음, 메시지 수신음 등)과 관련된 음향 신호를 출력하기도 한다. 이러한 음향 출력부(152)에는 리시버(receiver), 스피커(speaker), 버저(buzzer) 등이 포함될 수 있다.
- [0076] 햅틱 모듈(haptic module)(153)은 사용자가 느낄 수 있는 다양한 촉각 효과를 발생시킨다. 햅틱 모듈(153)이 발생시키는 촉각 효과의 대표적인 예로는 진동이 될 수 있다. 햅틱 모듈(153)에서 발생하는 진동의 세기와 패턴 등은 사용자의 선택 또는 제어부의 설정에 의해 제어될 수 있다. 예를 들어, 상기 햅틱 모듈(153)은 서로 다른 진동을 합성하여 출력하거나 순차적으로 출력할 수도 있다.
- [0077] 햅틱 모듈(153)은, 진동 외에도, 접촉 피부면에 대해 수직 운동하는 핀 배열, 분사구나 흡입구를 통한 공기의 분사력이나 흡입력, 피부 표면에 대한 스침, 전극(electrode)의 접촉, 정전기력 등의 자극에 의한 효과와, 흡열이나 발열 가능한 소자를 이용한 냉온감 재현에 의한 효과 등 다양한 촉각 효과를 발생시킬 수 있다.
- [0078] 햅틱 모듈(153)은 직접적인 접촉을 통해 촉각 효과를 전달할 수 있을 뿐만 아니라, 사용자가 손가락이나 팔 등의 근 감각을 통해 촉각 효과를 느낄 수 있도록 구현할 수도 있다. 햅틱 모듈(153)은 전자 장치(100)의 구성 태양에 따라 2개 이상이 구비될 수 있다.
- [0079] 광출력부(154)는 전자 장치(100)의 광원의 빛을 이용하여 이벤트 발생을 알리기 위한 신호를 출력한다. 전자 장치(100)에서 발생 되는 이벤트의 예로는 메시지 수신, 호 신호 수신, 부재중 전화, 알람, 일정 알림, 이메일 수신, 애플리케이션을 통한 정보 수신 등이 될 수 있다.
- [0080] 광출력부(154)가 출력하는 신호는 전자 장치가 전면이나 후면으로 단색이나 복수색의 빛을 발광함에 따라 구현된다. 상기 신호 출력은 전자 장치가 사용자의 이벤트 확인을 감지함에 의하여 종료될 수 있다.
- [0081] 인터페이스부(160)는 전자 장치(100)에 연결되는 모든 외부 기기와의 통로 역할을 한다. 인터페이스부(160)는 외부 기기로부터 데이터를 전송받거나, 전원을 공급받아 전자 장치(100) 내부의 각 구성요소에 전달하거나, 전자 장치(100) 내부의 데이터가 외부 기기로 전송되도록 한다. 예를 들어, 유/무선 헤드셋 포트(port), 외부 충전기 포트(port), 유/무선 데이터 포트(port), 메모리 카드(memory card) 포트(port), 식별 모듈이 구비된 장치를 연결하는 포트(port), 오디오 I/O(Input/Output) 포트(port), 비디오 I/O(Input/Output) 포트(port), 이어폰 포트(port) 등이 인터페이스부(160)에 포함될 수 있다.
- [0082] 한편, 식별 모듈은 전자 장치(100)의 사용 권한을 인증하기 위한 각종 정보를 저장한 칩으로서, 사용자 인증 모듈(user identify module; UIM), 가입자 인증 모듈(subscriber identity module; SIM), 범용 사용자 인증 모듈(universal subscriber identity module; USIM) 등을 포함할 수 있다. 식별 모듈이 구비된 장치(이하 '식별 장치')는, 스마트 카드(smart card) 형식으로 제작될 수 있다. 따라서 식별 장치는 상기 인터페이스부(160)를 통하여 단말기(100)와 연결될 수 있다.
- [0083] 또한, 상기 인터페이스부(160)는 전자 장치(100)가 외부 크래들(cradle)과 연결될 때 상기 크래들로부터의 전원이 상기 전자 장치(100)에 공급되는 통로가 되거나, 사용자에게 의해 상기 크래들에서 입력되는 각종 명령 신호가 상기 전자 장치(100)로 전달되는 통로가 될 수 있다. 상기 크래들로부터 입력되는 각종 명령 신호 또는 상기 전원은 상기 전자 장치(100)가 상기 크래들에 정확히 장착되었음을 인지하기 위한 신호로 동작될 수 있다.
- [0084] 메모리(170)는 제어부(180)의 동작을 위한 프로그램을 저장할 수 있고, 입/출력되는 데이터들(예를 들어, 폰북, 메시지, 정지영상, 동영상 등)을 임시 저장할 수도 있다. 상기 메모리(170)는 상기 터치 스크린 상의 터치 입력시 출력되는 다양한 패턴의 진동 및 음향에 관한 데이터를 저장할 수 있다.
- [0085] 메모리(170)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), SSD 타입(Solid State Disk type), SDD 타입(Silicon Disk Drive type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(random access memory; RAM), SRAM(static random access memory), 롬(read-only memory; ROM), EEPROM(electrically erasable

programmable read-only memory), PROM(programmable read-only memory), 자기 메모리, 자기 디스크 및 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 전자 장치(100)는 인터넷(internet)상에서 상기 메모리(170)의 저장 기능을 수행하는 웹 스토리지(web storage)와 관련되어 동작될 수도 있다.

- [0086] 한편, 앞서 살펴본 것과 같이, 제어부(180)는 응용 프로그램과 관련된 동작과, 통상적으로 전자 장치(100)의 전반적인 동작을 제어한다. 예를 들어, 제어부(180)는 상기 전자 장치의 상태가 설정된 조건을 만족하면, 애플리케이션들에 대한 사용자의 제어 명령의 입력을 제한하는 잠금 상태를 실행하거나, 해제할 수 있다.
- [0087] 또한, 제어부(180)는 음성 통화, 데이터 통신, 화상 통화 등과 관련된 제어 및 처리를 수행하거나, 터치 스크린 상에서 행해지는 필기 입력 또는 그림 그리기 입력을 각각 문자 및 이미지로 인식할 수 있는 패턴 인식 처리를 행할 수 있다. 나아가 제어부(180)는 이하에서 설명되는 다양한 실시 예들을 본 발명에 따른 전자 장치(100) 상에서 구현하기 위하여, 위에서 살펴본 구성요소들을 중 어느 하나 또는 복수를 조합하여 제어할 수 있다.
- [0088] 보안모듈(181)은 전자 장치의 동작 중 보안과 관련된 동작을 제어한다. 예를 들어, 보안 모듈(181)은 생체 인증 기능이 실행되면, 생체 인증과 관련된 제어를 수행할 수 있다. 예를 들어, 보안모듈(181)은 생체 인증을 위한 알고리즘인 인공신경망 알고리즘, SVM 알고리즘을 이용하여, 생체 인증을 수행할 수 있다. 이 밖에도 보안모듈(181)은 생체 인증을 위한 알고리즘인 Fuzzy logic, Dempster-Shafer theory, SVM, RVM(relevance vector machine) Mean rule, Monte carlo approach, Phase stretch transform(PST), 신경 회로망, Principal Component Analysis, Fisherfaces, Wavelet and Elastic Matching 등을 동작시킬 수 있다.
- [0089] 보안모듈(181)은 제어부(180)와 통신을 통하여, 데이터를 송수신할 수 있으며, 이를 통하여 전자 장치의 전반적인 동작을 제어할 수 있다. 예를 들어, 제어부(180)는 보안모듈(181)로부터 사용자 인증 결과 데이터를 수신하고, 이를 기반으로 전자 장치의 동작을 제어할 수 있다. 또한, 보안 모듈(181)은 제어부(180)로부터 생체 인증을 수행하기 위한 제어 명령을 수신하고, 이에 따라 생체 인증을 수행할 수 있다.
- [0090] 한편, 도 1에서는, 보안 모듈(181)과 제어부(180)가 별개의 구성인 것으로 도시하였으나, 본 발명은 이에 한정하지 아니하고, 보안 모듈(181)이 제어부(180)의 일 구성으로 구성될 수도 있다.
- [0091] 전원 공급부(190)는 제어부(180)의 제어에 의해 외부의 전원, 내부의 전원을 인가 받아 각 구성요소들의 동작에 필요한 전원을 공급한다. 전원공급부(190)는 배터리를 포함하며, 배터리는 충전 가능하도록 이루어지는 내장형 배터리가 될 수 있으며, 충전 등을 위하여 단말기 바디에 착탈 가능하게 결합될 수 있다.
- [0092] 또한, 전원공급부(190)는 연결포트를 구비할 수 있으며, 연결포트는 배터리의 충전을 위하여 전원을 공급하는 외부 충전기가 전기적으로 연결되는 인터페이스(160)의 일 예로서 구성될 수 있다.
- [0093] 다른 예로서, 전원공급부(190)는 상기 연결포트를 이용하지 않고 무선방식으로 배터리를 충전하도록 이루어질 수 있다. 이 경우에, 전원공급부(190)는 외부의 무선 전력 전송장치로부터 자기 유도 현상에 기초한 유도 결합(Inductive Coupling) 방식이나 전자기적 공진 현상에 기초한 공진 결합(Magnetic Resonance Coupling) 방식 중 하나 이상을 이용하여 전력을 전달받을 수 있다.
- [0094] 한편, 이하에서 다양한 실시 예는 예를 들어, 소프트웨어, 하드웨어 또는 이들의 조합된 것을 이용하여 컴퓨터 또는 이와 유사한 장치로 읽을 수 있는 기록매체 내에서 구현될 수 있다.
- [0095] 이하에서는 도 1에서 설명한 전자 장치에서 생체인증을 수행하는 방법에 대하여 구체적으로 설명한다. 도 2는 단일생체인증 방식을 설명한 개념도이다.
- [0096] 도 2를 참조하면, 단일생체인증은 획득(210), 특징점 추출(220), 매칭(230) 및 결정(240) 단계를 포함할 수 있다.
- [0097] 획득(210, acquisition) 단계에서는, 생체 인식 센서를 통하여 생체인식 정보를 획득할 수 있다. 생체인식 정보에는, 지문, 얼굴, 음성, 정맥, 홍채 등 사용자의 고유 생체정보가 포함될 수 있다.
- [0098] 특징점 추출(220, Feature extraction) 단계에서는, 생체인식 정보의 특징점들을 추출할 수 있다. 특징점은 사람마다 다른 사람의 고유 특징을 인지할 수 있는 정보이다. 예를 들어, 지문의 경우, 지문의 특이한 모양을 나타내는 점을 특징점으로 설정할 수 있다. 이러한 특징점은 생체인증방식마다 서로 다르게 설정되어 있다.
- [0099] 매칭(230, Matching) 단계에서는, 기 등록된 사용자 정보와 감지된 생체인식 정보 간의 매칭 점수를 산출할 수 있다. 기 등록된 사용자 정보는, 생체인증 수행 전, 사용자에게 의하여 미리 저장된 생체 정보이다. 사용자는 지문 정보, 얼굴 정보, 음성 정보, 정맥 정보, 홍채 정보 등을 템플릿(template) 형태로 메모리(170)에 미리 저장

할 수 있다.

- [0100] 상기 매칭 점수는, 기 등록된 사용자 정보와 생체인식 정보 간의 유사도를 점수로 나타낸 것이다. 매칭 점수를 산출하는 알고리즘은 종래에 알려진 다양한 알고리즘이 사용될 수 있다.
- [0101] 결정(240, decision) 단계에서는, 매칭 점수와 결정 함수를 이용하여 사용자 인증을 수행할 수 있다. 결정 함수는 생체인식 정보를 입력한 사용자가 진정(genuine) 사용자인지 또는 위조(imposter) 사용자인지 여부를 판단하는 기준이 되는 함수이다. 결정 함수는 특정 임계값으로 설정될 수도 있고, 다차원 함수로 설정될 수도 있다.
- [0102] 상기 결정 함수는, 생체인증기능의 제조사에 의하여 초기 설정값(default)이 설정될 수 있다. 또한 결정 함수는, 생체인식 센서를 통하여 감지된 사용자의 생체인식 정보들을 이용하여 초기 설정값을 변경할 수 있다. 따라서, 전자 장치는 생체인식 동작을 많이 진행될수록 생체인식의 속도 및 정확도를 향상시킬 수 있다.
- [0103] 또한, 결정 함수는 결정함수를 생성하는데 사용된 정보에 따라 서로 다르게 생성될 수 있다. 그리고, 서로 다르게 생성된 결정함수는 메모리(170)에 복수로 저장될 수 있다. 예를 들어, 결정 함수는 매칭 점수만으로 생성되거나, 매칭 점수와 스푸핑 점수를 이용하여 생성될 수 있다. 이 경우, 메모리(170)에는 두 개의 결정 함수가 모두 저장될 수 있으며, 필요에 따라 어느 하나의 결정 함수를 이용하여 생체인증을 수행할 수 있다.
- [0104] 이상에서는 단일생체인증 방법에 대하여 설명하였다. 이하에서는 복합생체인증 방법에 대하여 설명한다. 도 3a 내지 도 3d는 복합생체인증 방식을 설명한 개념도들이다.
- [0105] 복합생체인증은 복수의 생체인식 정보를 퓨전(fusion)하는 시점에 따라 4가지 방식으로 구분될 수 있다. 여기에서 퓨전은 복수의 정보들을 기 설정된 알고리즘에 따라 결합하여, 하나의 정보로 산출하는 동작을 의미하는 것으로, 결합, 조합, 융합, 정합 등의 용어로도 사용될 수 있다.
- [0106] 도 3a는 센서 퓨전 방식(310)을 나타내었다. 센서 퓨전 방식(310)은 생체인식정보의 획득 단계에서, 서로 다른 센서에서 획득된 복수의 생체인식정보들을 결합하는 방식이다. 구체적으로, 센서 퓨전 방식은 서로 다른 생체인식 센서로부터 감지된 생체인식 정보를 퓨전하고, 퓨전된 정보로부터 특징점을 추출하는 방식이다.
- [0107] 도 3b는 특징점 퓨전 방식(320)을 나타내었다. 특징점 퓨전 방식(320)은 생체인식정보의 특징점 추출 단계에서, 서로 다른 생체인식센서로부터 획득된 복수의 생체인식정보로부터 각각 특징점을 추출하고, 각각 추출된 특징점들을 결합하는 방식이다.
- [0108] 도 3c는 스코어 퓨전 방식(330)을 나타내었다. 스코어 퓨전 방식(330)은 생체인식정보의 매칭 단계에서, 복수의 생체인식 정보 별로 산출된 매칭 점수들을 결합하는 방식이다.
- [0109] 도 3d는 결정 퓨전 방식(340)을 나타내었다. 결정 퓨전 방식(340)은 생체인식 정보의 결정 단계에서, 복수의 생체인식 정보 별로 산출된 결정 결과를 결합하는 방식이다.
- [0110] 이상에서는 복합생체인증의 여러가지 방식에 대하여 설명하였다. 이하에서는 생체인증을 통한 사용자 인증 시, 결정 함수와 관련된 생체인식의 오차율을 설명한다. 도 4a 및 도 4b는 생체인증 판단의 오차율과 관련된 그래프들이다.
- [0111] 도 4a의 그래프 a는 생체인증 시의 진정 사용자의 생체 정보와 기 등록된 사용자 정보 간의 유사도 분포를 나타낸 그래프이고, 도 4a의 그래프 b는 위조 사용자의 생체 정보와 기 등록된 사용자 정보 간의 유사도 분포를 나타낸 그래프이다.
- [0112] 그래프 a와 그래프 b는 서로 겹치는 부분이 존재하며, 전자 장치(100)는 점선 aa'으로 도시된 임계값보다 높은 유사도를 갖는 경우, 진정 사용자로 판단하고, 임계값보다 낮은 유사도를 갖는 경우, 위조 사용자로 판단할 수 있다. 여기에서, 임계값은 생체인증기능을 제공하는 제공사에 의하여 결정된 값일 수 있으며, 앞서 설명한 결정 함수를 의미한다.
- [0113] 한편, 도 4a에 도시된 FRR(False rejection rate)은 진정 사용자이지만, 위조 사용자로 판단되는 비율을 나타낸다. FRR이 높을수록 임계값이 높아지고, 이에 따라 생체인식정보를 입력한 사용자가 진정 사용자로 판단될 확률이 낮아지기 때문에, 생체인증의 보안성은 높아질 수 있다.
- [0114] FRR이 낮을수록 임계값이 낮아지고, 이에 따라 생체인식정보를 입력한 사용자가 진정 사용자로 판단될 확률이 높아지기 때문에, 생체인증의 보안성은 낮아질 수 있다.
- [0115] FAR(False acceptance rate)은 위조 사용자이지만 진정 사용자로 판단되는 오차를 나타낸다. FAR은 FRR과 상반

되는 개념으로, FAR이 높을수록 임계값이 낮아지고, 이에 따라 생체인식정보를 입력한 사용자가 진정 사용자로 판단될 확률이 높아지기 때문에, 생체인증의 보안성은 낮아질 수 있다.

- [0116] 도 4b는 FRR과 FAR 과의 관계를 나타낸 그래프이다. FRR과 FAR은 서로 반비례할 수 있다.
- [0117] FRR이 높고, FAR이 낮은 d의 영역에 해당하는 임계값은 인증 속도가 느리나 높은 보안성을 요하는 애플리케이션들이 사용될 수 있다. 예를 들어, 진정 사용자를 엄격하게 판단하는 결제 애플리케이션, 은행 애플리케이션에서 이러한 영역의 임계값이 설정될 수 있다.
- [0118] 반대로, FRR이 낮고, FAR이 높은 c의 영역에 해당하는 임계값은 인증 속도를 빠르게 하며 낮은 보안성을 요하는 애플리케이션들에 사용될 수 있다. 예를 들어, 잠금 해제 기능 등에 이러한 영역에 해당하는 임계값이 사용될 수 있다.
- [0119] 이렇게 생체인증 기능의 임계값(즉, 결정함수)는 생체인증을 통하여 실행하고자 하는 기능들의 보안 수준을 고려하여, 결정될 수 있다. 이상에서는, 생체인증 시의 오차와 관계된 파라미터들에 대하여 설명하였다.
- [0120] 한편, 본 발명은 복합생체인증의 스코어 퓨전 방식의 인증 정확도를 향상시키기 위한 방법에 관한 것이다. 이하에서는 복합생체인증 방식 중 스코어 퓨전 방식에서 사용될 수 있는 알고리즘에 대하여 설명한다.
- [0121] 스코어 퓨전 방식에서는, 매칭 점수들을 결합하는 다양한 인공지능 알고리즘이 사용될 수 있다. 스코어 퓨전 방식에서 사용될 수 있는 알고리즘에는 combination-based score fusion 알고리즘, classifier-based score fusion 알고리즘, density-based score fusion 알고리즘 등이 사용될 수 있다.
- [0122] Combination-based score fusion 알고리즘에는 statical rule, dynamic weighting, triangular norms 등이 포함될 수 있다. Classifier-based score fusion 알고리즘에는, SVM(support vector machine), AdaBoost(RS-ADA), Dampster-Shafer(DS) 등이 포함될 수 있다. density-based score fusion 알고리즘에는, Liklihood feature(LF) 등이 포함될 수 있다.
- [0123] 이 밖에도 본 발명은 스코어 퓨전 방식에서 종래 알려진 다양한 알고리즘 등이 사용될 수 있으며, 본 발명의 취지를 벗어나지 않기 위하여, 그 구체적인 설명은 생략한다.
- [0124] 이하에서는 이와 같이 구성된 전자 장치에서 구현될 수 있는 제어 방법과 관련된 실시 예들에 대해 첨부된 도면을 참조하여 살펴보겠다. 본 발명은 본 발명의 정신 및 필수적 특징을 벗어나지 않는 범위에서 다른 특정한 형태로 구체화될 수 있음은 당업자에게 자명하다.
- [0125] 먼저 도 5는 본 발명의 실시 예에 따른 전자 장치(100)에서, 인증에 실패한 진정 사용자의 인증 데이터에 근거하여 생체 인증 모델을 업데이트하는 동작 과정을 도시한 흐름도이다.
- [0126] 도 5를 참조하여 살펴보면, 본 발명의 실시 예에 따른 전자 장치(100)의 보안 모듈(181)은, 사용자로부터 사용자 등록을 위한 생체 정보를 획득할 수 있다(S500). 일 예로 보안 모듈(181)은 생체 인식 센서(143)를 통해 지문 정보, 얼굴 이미지, 음성 정보, 정맥 또는 홍채 이미지 등 사용자의 고유한 생체 정보를 획득할 수 있다.
- [0127] 그리고 보안 모듈(181)은 획득된 생체 정보에 근거하여 진정(genuine) 점수를 추출할 수 있다(S502). 그리고 추출된 진정 점수에 근거하여 생체 인증을 위한 생체 인증 모델을 생성할 수 있다(S504). 일 예로 상기 생체 인증 모델은, 사용자 인증을 위해 획득된 생체 정보가 진정 사용자인지 여부를 판단할 수 있는 기준값, 즉 인증 임계점수(threshold score)를 결정하기 위한 모델일 수 있다.
- [0128] 이를 위해 보안 모듈(181)은 획득된 생체 정보를 등록 데이터와 인증 데이터로 분류할 수 있으며, 분류된 등록 데이터와 인증 데이터에 근거하여 상기 진정 점수를 추출할 수 있다.
- [0129] 이하 하기 도 6a 내지 도 6b를 참조하여 획득된 생체 점수로부터 진정 점수를 추출 및 사용자의 생체 인증 모델이 생성되는 과정을 살펴보기로 한다.
- [0130] 한편 초기 생체 인증 모델이 생성되면, 보안 모듈(181)은 상기 초기 생체 인증 모델에 근거하여 사용자 인증을 수행할 수 있다. 그리고 사용자 인증 수행 결과에 따라 진정 사용자로부터 획득된 생체 정보임에도 불구하고 사용자 인증에 실패한 생체 정보가 있는지 여부를 검출할 수 있다(S506).
- [0131] 한편 상기 S506 단계에서, 보안 모듈(181)은 사용자 인증 수행 결과 사용자 인증이 실패하는 경우, 사용자 인증을 위해 획득된 생체 정보가 진정 사용자로부터 획득된 것인지 여부를 판단할 수 있다. 그리고 판단 결과에 따라 사용자 인증에 실패한 진정 사용자의 생체 정보가 있는지 여부를 검출할 수 있다. 이하 도 7을 참조하여, 상

기 S506 단계의 동작 과정을 보다 자세하게 살펴보기로 한다.

- [0132] 한편 상기 S506 단계의 검출 결과, 사용자 인증에 실패한 진정 사용자의 생체 정보가 있는 경우, 보안 모듈(181)은 획득된 생체 정보로부터 진정 점수를 추출할 수 있다(S508). 그리고 보안 모듈(181)은 상기 S508 단계에서 추출된 진정 점수를 반영하여 사용자의 생체 인증 모델을 업데이트할 수 있다(S510).
- [0133] 그러면 생체 인증 모델이 변경될 수 있으며, 변경된 생체 인증 모델에 따라, 획득되는 생체 정보가 진정 사용자 인지 여부를 판단하기 위한 인증 임계 점수가 변경될 수 있다. 이 경우 상기 S510 단계의 생체 인증 모델 업데이트에 따라, 상기 S506 단계에서 검출된 생체 정보 즉, 사용자 인증에 실패한 진정 사용자의 생체 정보에 근거하여 사용자의 인증이 이루어질 수 있도록 상기 인증 임계 점수가 변경될 수 있다.
- [0134] 따라서 본 발명의 실시 예에 따른 전자 장치(100)에서는, 통상적인 생체 인증 모델에서 사용자 인증에 실패하는 경우라도, 진정 사용자로부터 획득된 생체 정보인 경우에는 사용자의 인증이 성공할 수 있는, 진정 사용자에게 대해 최적화된 생체 인증 모델이 생성될 수 있다.
- [0135] 한편 도 6a는 본 발명의 실시 예에 따른 전자 장치(100)에서, 사용자로부터 획득된 생체 정보로부터 진정 점수를 추출하는 동작 과정을 도시한 흐름도이다. 그리고 도 6b는 본 발명의 실시 예에 따른 전자 장치에서, 사용자에게 개인화된 초기 생체 인증 모델을 생성하는 과정을 도시한 개념도이다.
- [0136] 도 6a와 도 6b를 참조하여 살펴보면, 보안 모듈(181)은 상기 S500 단계에서 사용자 등록을 위한 생체 정보가 획득되는 경우, 획득된 생체 정보(650)로부터 센싱되는 정보들 중 일부를 등록 데이터(662)로, 나머지 일부를 인증 데이터(664)로 설정할 수 있다.
- [0137] 즉, 생체 정보로부터 획득된 데이터들(650)을 등록 데이터(662)와 인증 데이터(664)로 분류할 수 있다(S600). 그리고 보안 모듈(181)은 분류된 등록 데이터(662)와 인증 데이터(664)에 근거하여 진정 점수(genuine score)(670)를 추출할 수 있다(S602).
- [0138] 여기서 상기 인증 데이터와 등록 데이터는 사용자의 인증을 위해 사용되는 특징을 포함하고 있는지 여부에 따라 결정될 수 있다. 즉, 인체의 신체적 특징에 따라 사람들이 공통적으로 가지고 있는 특징점인 경우 등록 데이터로 분류될 수 있다. 반면 다른 사람들과 차별화될 수 있는 해당 사용자만의 고유한 특징인 경우 인증 데이터로 분류될 수 있다.
- [0139] 한편 상기 S602 단계에서 진정 점수가 추출되면, 보안 모듈(181)은 도 5의 S504 단계로 진행하여 사용자의 생체 인증 모델(680)을 생성할 수 있다. 여기서 상기 생체 인증 모델(680)은 상술한 바와 같이, 사용자 인증 시, 사용자 인증을 위해 획득된 생체 정보가 진정 사용자인지 여부를 판단할 수 있는 기준값, 즉 인증 임계 점수(threshold score)를 결정하기 위한 모델일 수 있다.
- [0140] 이와 같이 생체 인증 모델이 생성되면, 본 발명의 실시 예에 따른 전자 장치(100)의 보안 모듈(181)은 생성된 생체 인증 모델에 근거하여 사용자 인증을 수행할 수 있다. 즉 보안 모듈(181)은 사용자의 인증을 위해 생체 정보를 획득할 수 있으며, 획득된 생체 정보로부터 특징점을 추출할 수 있다.
- [0141] 그리고 추출된 특징점과 기 등록된 인증 데이터를 매칭하여 매칭 점수를 산출할 수 있다. 그리고 산출된 매칭 점수와, 상기 생체 인증 모델에 의해 결정되는 인증 임계 점수에 근거하여 사용자의 인증을 수행할 수 있다.
- [0142] 도 7은 이러한 본 발명의 실시 예에 따른 전자 장치(100)에서, 사용자 인증을 수행한 결과에 따라 인증에 실패한 진정 사용자의 인증 데이터를 저장하는 동작 과정을 도시한 흐름도이다.
- [0143] 그리고 도 8은 본 발명의 실시 예에 따른 전자 장치에서, 인증에 실패한 진정 사용자의 인증 데이터에 근거하여 생체 인증 모델을 업데이트하는 과정을 도시한 개념도이다.
- [0144] 먼저 본 발명의 실시 예에 따른 전자 장치(100)의 제어부(180)는 사용자 인증이 필요한 기능의 수행을 요청받을 수 있다. 일 예로 결제 기능이나 사용자의 개인 정보 조회 등과 같은 기능이 상기 사용자의 인증이 필요한 기능일 수 있다.
- [0145] 그러면 본 발명의 실시 예에 따른 전자 장치(100)의 보안 모듈(181)은, 먼저 사용자 인증을 위해 생체 인식 센서(143)를 제어하여, 사용자로부터 생체 정보를 획득할 수 있다(S700). 그리고 획득된 생체 정보의 특징점에 근거하여 사용자의 인증을 수행할 수 있다(S702).
- [0146] 그리고 보안 모듈(181)은 상기 S702 단계의 사용자 인증이 성공하였는지 실패하였는지 여부를 판단할 수 있다

(S704). 상기 S704 단계의 판단 결과 사용자 인증이 성공한 경우라면 보안 모듈(181)은 도 7에서 도시한 사용자 인증 과정을 종료할 수 있다. 그러면 본 발명의 실시 예에 따른 제어부(180)는 현재 전자 장치(100)에 요구된 기능이 수행되도록 전자 장치(100)의 동작을 제어할 수 있다.

[0147] 한편 상기 S702 단계에서 사용자 인증이 실패하는 경우라면, 보안 모듈(181)은 현재 획득된 생체 정보에 대응하는 사용자가 진정 사용자인지 여부를 확인할 수 있다. 이를 위해 보안 모듈(181)은 적어도 하나의 다른 인증 수단을 통해 사용자의 인증을 수행할 수 있다(S706).

[0148] 상기 S706 단계의 인증은 다양한 방식을 통해 이루어질 수 있다. 일 예로 인증은 기 설정된 개인 식별 정보(PIN 정보)와 같은 비밀번호 인증 방식을 통해 이루어질 수 있다. 또는 상기 S706 단계의 인증은 현재 획득된 생체 정보와 다른 종류의 생체 정보로부터 수행되는 생체 인증 방식에 따라 이루어질 수 있다.

[0149] 그리고 상기 S706 단계의 사용자 확인을 위한 사용자 인증 결과, 사용자 인증이 실패하는 경우라면, 보안 모듈(181)은 현재 생체 정보를 입력한 사용자가 진정 사용자가 아닌 것으로 판단할 수 있다. 그러면 보안 모듈(181)은 사용자 인증이 실패하였음을 표시하고 도 7에서 도시한 과정을 종료할 수 있다.

[0150] 반면, 상기 S706 단계의 사용자 인증 결과, 사용자 인증이 성공하는 경우라면, 보안 모듈(181)은 현재 생체 정보를 입력한 사용자가 진정 사용자인 것으로 판단할 수 있다. 그러면 보안 모듈(181)은 상기 S700 단계에서 획득된 생체 정보가 진정 사용자로부터 획득된 생체 정보라고 판단할 수 있다. 그리고 획득된 생체 정보를, 진정 사용자의 생체 정보로서 저장할 수 있다(S710).

[0151] 한편, 상기 S710 단계에서 진정 사용자의 생체 정보가 저장되면, 보안 모듈(181)은 상기 도 5의 S506 단계에서 사용자 인증에 실패한 진정 인증 데이터가 있는 것으로 판단할 수 있다.

[0152] 이에 따라 도 8에서 보이고 있는 바와 같이, 도 5의 S508 단계로 진행하여 인증에 실패한 진정 사용자의 생체 정보로부터 진정 점수를 추출할 수 있다(810). 그리고 도 5의 S510 단계로 진행하여, 상기 진정 사용자의 생체 정보로부터 추출된 진정 점수가 반영되도록 생체 인증 모델을 업데이트할 수 있다(S820).

[0153] 한편 보안 모듈(181)은 보다 정확한 생체 인증 모델의 업데이트를 위해, 동일한 생체 정보가 상기 S710 단계에서 기 설정된 횟수 이상 반복하여 저장되는 경우에 한하여 상기 도 5의 S508 단계 및 S510 단계를 수행할 수도 있음은 물론이다.

[0154] 일 예로 보안 모듈(181)은 도 7에서 도시한 바와 같이 사용자 인증을 수행하면서 사용자 인증에 실패한 진정 사용자의 생체 정보가 저장되는 경우(S710 단계), 기 저장된 진정 사용자의 생체 정보(사용자 인증에 실패한 생체 정보)가 있는지 여부를 검출할 수 있다.

[0155] 그리고, 현재 검출된 진정 사용자의 생체 정보와 동일한 생체 정보가 저장되어 있는 경우, 해당 생체 정보의 저장이 반복된 횟수를 체크할 수 있다.

[0156] 그리고 반복된 횟수가 기 설정된 횟수 이상인 경우라면, 상기 도 5의 S508 단계 및 S510 단계로 진행하여 현재 검출된 진정 사용자의 생체 정보로부터 진정 점수를 추출하고 추출된 진정 점수가 반영되도록 생체 인증 모델을 업데이트 할 수 있다.

[0157] 한편 상술한 설명에 따르면, 생체 인증 모델은 인증 임계 점수를 결정하기 위한 것으로, 생체 인증 모델이 업데이트를 통해 변경되는 경우 상기 인증 임계 점수가 변경될 수 있음을 설명한 바 있다.

[0158] 도 9는 이러한 경우에 본 발명의 실시 예에 따른 전자 장치(100)에서, 생체 인증 모델의 업데이트에 따라 인증 임계 점수(Threshold score) 분포가 변경되는 예를 도시한 예시도이다.

[0159] 도 9를 참조하여 살펴보면, 도 9의 X축과 Y축은 각각 인증 수단으로부터 획득되는 매칭 점수를 의미할 수 있다. 그리고 제1 분포(900)는 진정 사용자의 생체 정보에 대해 인증 수단으로부터 산출된 매칭 점수의 분포를 나타낼 수 있다. 또한 제2 분포(910)는 진정 사용자가 아닌 사용자(이하 위조 사용자라고 하기로 한다)의 생체 정보에 대해 인증 수단으로부터 산출된 매칭 점수의 분포를 나타낼 수 있다. 즉, 진정 사용자의 생체 정보일수록 높은 매칭 점수를 가질 수 있으며, 위조 사용자의 생체 정보일수록 낮은 매칭 점수를 가질 수 있다.

[0160] 한편, 매칭 점수 데이터(920)들은, 비록 제1 분포(900)의 영역을 벗어났지만, 진정 사용자로부터 획득된 생체 정보에 대해 인증 수단으로부터 산출된 매칭 점수들을 의미할 수 있다.

[0161] 도 9의 제1 인증 임계 점수 분포(950a)는 업데이트가 이루어지기 전의 초기 생체 인증 모델에 의해 결정되는 인

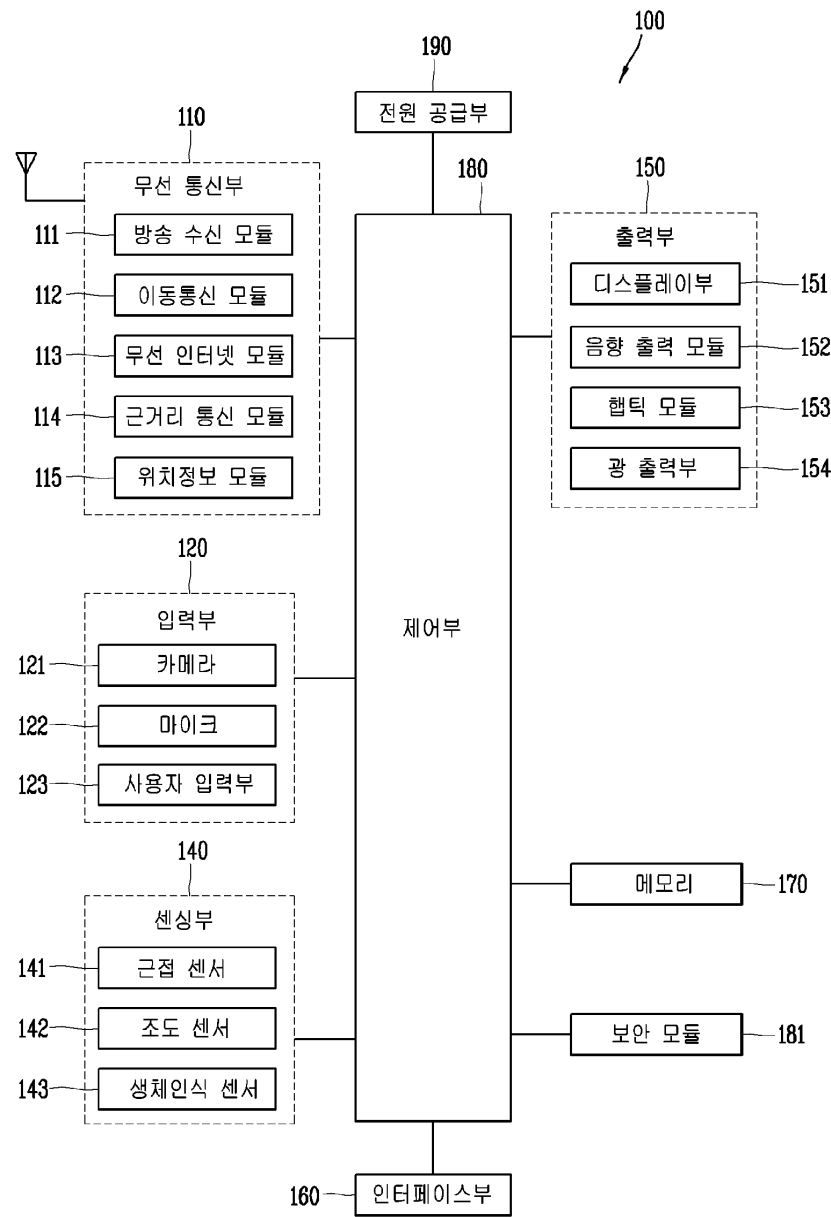
증 임계 점수들을 의미할 수 있다.

- [0162] 이 경우, 제1 인증 임계 점수 분포(950a)에 의해 도 9에서 도시하고 있는 매칭 점수 분포 영역은 사용자 인증이 이루어지는 영역과 사용자 인증이 실패하는 영역으로 구분될 수 있다.
- [0163] 사용자 인증이 이루어지는 영역(제1 영역 : 930)은 제1 분포(900)가 형성된 영역일 수 있으며, 사용자 인증이 실패하는 영역(제2 영역 : 940)은 제2 분포(910)가 형성된 영역일 수 있다.
- [0164] 이에 따라 제1 인증 임계 점수 분포(950a)에서 보이고 있는 바와 같이 인증 임계 점수가 형성되는 경우, 매칭 점수 데이터(920)들의 일부가 제2 영역(940)에 포함됨으로써 진정 사용자로부터 획득된 생체 정보임에도 불구하고 사용자 인증이 실패할 수 있다는 문제가 있다.
- [0165] 한편 이러한 경우 본 발명의 실시 예에 따른 전자 장치(100)의 제어부(180)는 사용자 인증에 실패한 생체 정보가 진정 사용자로부터 획득된 생체 정보인 경우, 그 생체 정보에 근거하여 생체 인증 모델을 업데이트할 수 있다.
- [0166] 이에 따라 생체 인증 모델이 변경되면, 제2 인증 임계 점수 분포(950)에서 보이고 있는 바와 같이 인증 임계 점수가 변경될 수 있다. 따라서 매칭 점수 데이터(920)들이 모두 제1 영역(930)에 포함됨으로써 그 생체 정보에 따른 사용자 인증이 이루어질 수 있다.
- [0167] 상술한 설명에서는 진정 사용자로부터 획득되는 생체 정보임에도 불구하고 사용자 인증이 실패하는 경우에, 상기 진정 사용자로부터 획득되는 생체 정보에 따라 사용자 인증이 이루어질 수 있도록 생체 인증 모델을 변경하는 동작 과정을 설명하였다.
- [0168] 한편 본 발명의 실시 예에 따른 보안 모듈(181)은 상술한 설명과 상반되도록 생체 인증 모델을 업데이트 할 수도 있음은 물론이다. 즉, 위조 사용자임에도 불구하고 사용자 인증이 이루어지는 경우 보안 모듈(181)은 해당 생체 데이터에 의해 사용자 인증이 이루어지지 않도록 생체 인증 모델을 업데이트 할 수도 있음은 물론이다.
- [0169] 도 10은 이러한 경우에 본 발명의 실시 예에 따른 전자 장치(100)에서, 사용자 인증을 수행한 결과에 따라 위조 생체 정보를 검출 및 저장하는 동작 과정을 도시한 흐름도이다.
- [0170] 도 10을 참조하여 살펴보면, 본 발명의 실시 예에 따른 전자 장치(100)의 보안 모듈(181)은, 먼저 사용자 인증을 위해 생체 인식 센서(143)를 제어하여, 사용자로부터 생체 정보를 획득할 수 있다(S1000). 그리고 획득된 생체 정보의 특징점에 따른 매칭 점수에 근거하여 사용자의 인증을 수행할 수 있다(S1002).
- [0171] 그리고 보안 모듈(181)은 상기 S1002 단계의 사용자 인증이 성공하였는지 실패하였는지 여부를 판단할 수 있다(S1004). 상기 S1004 단계의 판단 결과 사용자 인증이 실패한 경우라면 보안 모듈(181)은 사용자 인증이 실패하였음을 표시하고 사용자 인증 과정을 종료할 수 있다(S1012).
- [0172] 그러나 상기 S1004 단계에서 사용자 인증이 성공하는 경우라면, 보안 모듈(181)은 사용자 인증에 사용된 매칭 점수가, 인증 임계 점수로부터 기 설정된 오차 수준 이내인지 여부를 판단할 수 있다(S1006).
- [0173] 그리고 상기 S1006 단계의 검출 결과, 매칭 점수가 인증 임계 점수로부터 기 설정된 오차 수준을 벗어난 경우라면 보안 모듈(181)은 사용자 인증 과정을 종료할 수 있다. 그러면 본 발명의 실시 예에 따른 제어부(180)는 현재 전자 장치(100)에 요구된 기능이 수행되도록 전자 장치(100)의 동작을 제어할 수 있다.
- [0174] 한편 상기 S1006 단계의 검출 결과, 매칭 점수가 인증 임계 점수로부터 기 설정된 오차 수준 이내인 경우라면, 보안 모듈(181)은 현재 획득된 생체 정보에 대응하는 사용자가 진정 사용자인지 여부를 확인할 수 있다(S1008). 이를 위해 보안 모듈(181)은 적어도 하나의 다른 인증 수단을 통해 사용자의 인증을 수행할 수 있다.
- [0175] 상기 S1008 단계의 사용자 확인은 다양한 방식을 통해 이루어질 수 있다. 일 예로 인증은 기 설정된 개인 식별 정보(PIN 정보)와 같은 비밀번호 인증 방식을 통해 이루어질 수 있다. 또는 상기 S1008 단계의 사용자 확인은 현재 획득된 생체 정보와 다른 종류의 생체 정보로부터 수행되는 생체 인증 방식에 따라 이루어질 수 있다.
- [0176] 그리고 보안 모듈(181)은 상기 S1008 단계의 사용자 확인 결과에 따라 현재 인증된 사용자가 진정 사용자인지 여부를 판단할 수 있다. 그리고 진정 사용자가 아닌 경우, 즉 위조 사용자인 경우 현재의 사용자 인증을 취소할 수 있다.
- [0177] 이 경우 보안 모듈(181)은 사용자 인증이 실패하였음을 표시하고 사용자 인증 과정을 종료할 수 있다. 그리고 상기 S1000 단계에서 획득된 생체 정보를 위조 생체 정보로 저장할 수 있다(S1010).

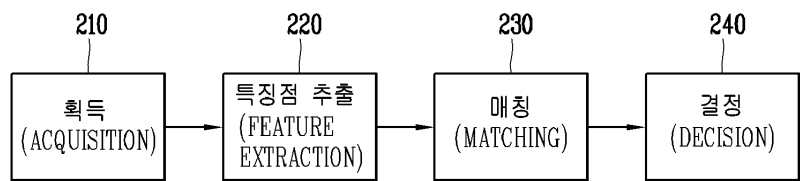
- [0178] 한편 상기 S1010 단계에서 위조 사용자의 생체 정보, 즉 위조 생체 정보가 저장되면, 보안 모듈(181)은 위조 생체 정보에 근거하여 생체 인증 모델을 업데이트 할 수 있다. 일 예로, 보안 모듈(181)은 현재 저장된 위조 생체 정보로부터 진정 점수를 추출하고, 추출된 진정 점수가 반영되도록 생체 인증 모델을 업데이트할 수 있다.
- [0179] 한편 보안 모듈(181)은 보다 정확한 생체 인증 모델의 업데이트를 위해, 동일한 위조 생체 정보가 기 설정된 횟수 이상 반복하여 저장되는 경우에 한하여 생체 인증 모델을 업데이트할 수도 있음은 물론이다.
- [0180] 일 예로, 보안 모듈(181)은 도 10에서 도시한 바와 같이 위조 생체 정보가 저장되는 경우, 기 저장된 위조 생체 정보가 있는지 여부를 검출할 수 있다. 그리고, 현재 검출된 위조 생체 정보와 동일한 위조 생체 정보가 저장되어 있는 경우, 그 생체 정보의 저장이 반복된 횟수를 체크할 수 있다. 그리고 보안 모듈(181)은 반복된 횟수가 기 설정된 횟수 이상인 경우에 한하여 현재 저장된 위조 생체 정보에 따라 생체 인증 모델을 업데이트 할 수 있다.
- [0181] 도 11은 본 발명의 실시 예에 따른 전자 장치(100)에서, 이처럼 위조 생체 정보를 반영하여 생체 인증 모델의 업데이트 되는 경우의 예를 도시한 예시도이다.
- [0182] 도 11을 참조하여 살펴보면, 도 11의 X축과 Y축은 도 9와 마찬가지로 각각 인증 수단으로부터 획득되는 매칭 점수를 의미할 수 있다.
- [0183] 그리고, 제1 분포(900)는 진정 사용자의 생체 정보에 대해 인증 수단으로부터 산출된 매칭 점수의 분포를 나타낼 수 있다. 또한, 제2 분포(910)는 진정 사용자가 아닌 사용자(이하 위조 사용자라고 하기로 한다)의 생체 정보에 대해 인증 수단으로부터 산출된 매칭 점수의 분포를 나타낼 수 있다.
- [0184] 한편, 도 11의 제1 인증 임계 점수 분포(950b)는 업데이트가 이루어지기 전의 초기 생체 인증 모델에 의해 결정되는 인증 임계 점수들을 의미할 수 있다. 이 경우 제1 인증 임계 점수 분포(950b)에 의해 도 11에서 도시하고 있는 매칭 점수 분포 영역은 사용자 인증이 이루어지는 제1 영역(930)과 사용자 인증이 실패하는 제2 영역(940)으로 구분될 수 있다.
- [0185] 이러한 경우 본 발명의 실시 예에 따른 전자 장치(100)의 제어부(180)는 위조 생체 정보에 근거하여 생체 인증 모델을 업데이트할 수 있다. 이에 따라 생체 인증 모델이 변경되면, 제2 인증 임계 점수 분포(950)에서 보이고 있는 바와 같이 인증 임계 점수가 변경될 수 있다.
- [0186] 따라서, 도 11에서 보이고 있는 바와 같이 인증 임계 점수 분포의 변경에 따라 제1 영역(930)이 보다 축소되고 제2 영역(940)이 보다 확장될 수 있다. 즉, 위조 생체 정보에 따른 사용자 인증이 방지될 수 있도록 인증 임계 점수가 상향 조정될 수 있다.
- [0187] 이상에서 살펴본 바와 같이, 본 발명의 실시 예들 중 적어도 하나에 의하면, 본 발명은 진정 사용자로부터 획득되었음에도 불구하고 사용자 인증에 실패한 생체 정보가 있는 경우, 그 생체 정보로부터 추출된 인증 데이터를 반영하여 생체 인증 모델을 업데이트함으로써 사용자에게 최적화된 생체 인증 모델을 생성할 수 있으며, 이에 따라 진정 사용자로부터 획득된 생체 정보에 따른 사용자 인증의 인증 실패 가능성을 보다 낮출 수 있다는 효과가 있다. 또한, 본 발명의 실시 예들 중 적어도 하나에 의하면, 본 발명은 사용자에게 최적화된 생체 인증 모델을 제공함으로써, 진정 사용자가 아닌 사용자로부터 획득되었음에도 진정 사용자로 인증될 수 있는 인증 오류 가능성을 보다 낮출 수 있다는 효과가 있다.
- [0188] 전술한 본 발명은, 프로그램이 기록된 매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 매체는, 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 매체의 예로는, HDD(Hard Disk Drive), SSD(Solid State Disk), SDD(Silicon Disk Drive), ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광 데이터 저장 장치 등이 있으며, 또한 캐리어 웨이브(예를 들어, 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한, 상기 컴퓨터는 단말기의 제어부(180)를 포함할 수도 있다. 따라서, 상기의 상세한 설명은 모든 면에서 제한적으로 해석되어서는 아니되고 예시적인 것으로 고려되어야 한다. 본 발명의 범위는 첨부된 청구항의 합리적 해석에 의해 결정되어야 하고, 본 발명의 등가적 범위 내에서의 모든 변경은 본 발명의 범위에 포함된다.

도면

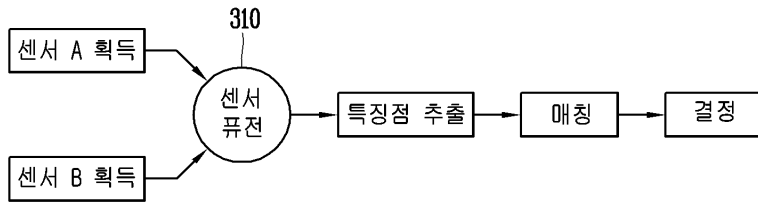
도면1



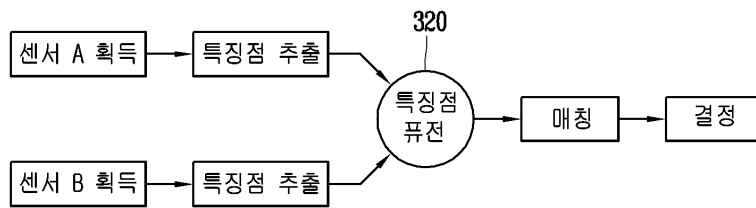
도면2



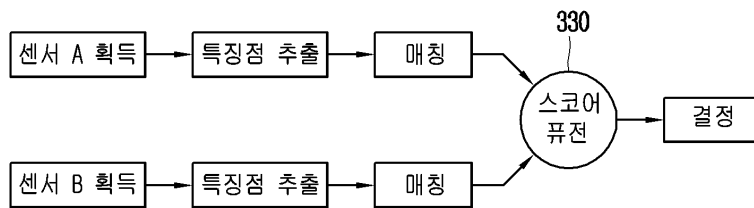
도면3a



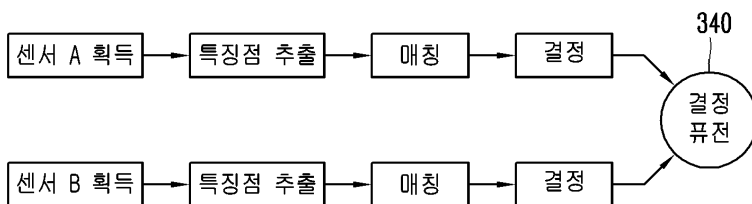
도면3b



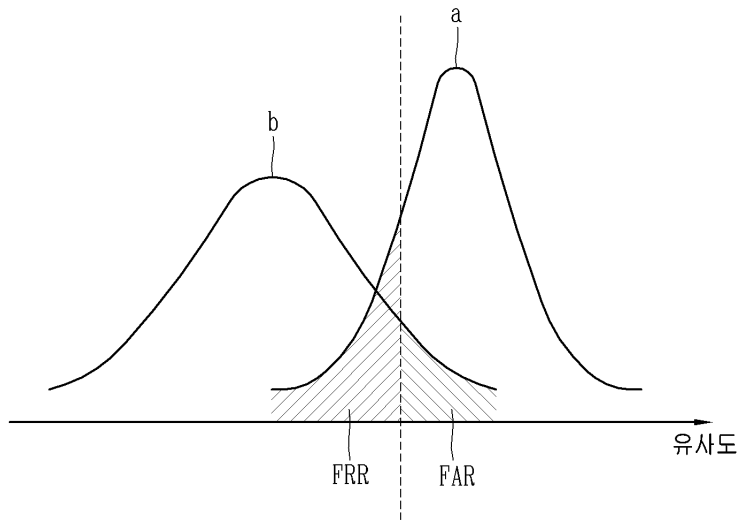
도면3c



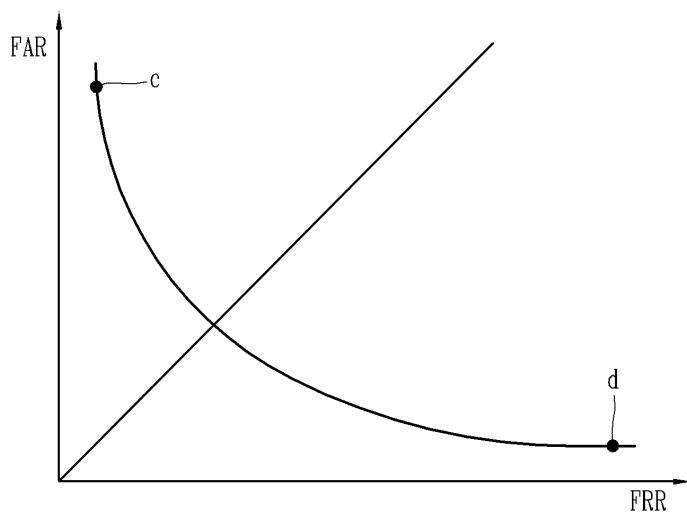
도면3d



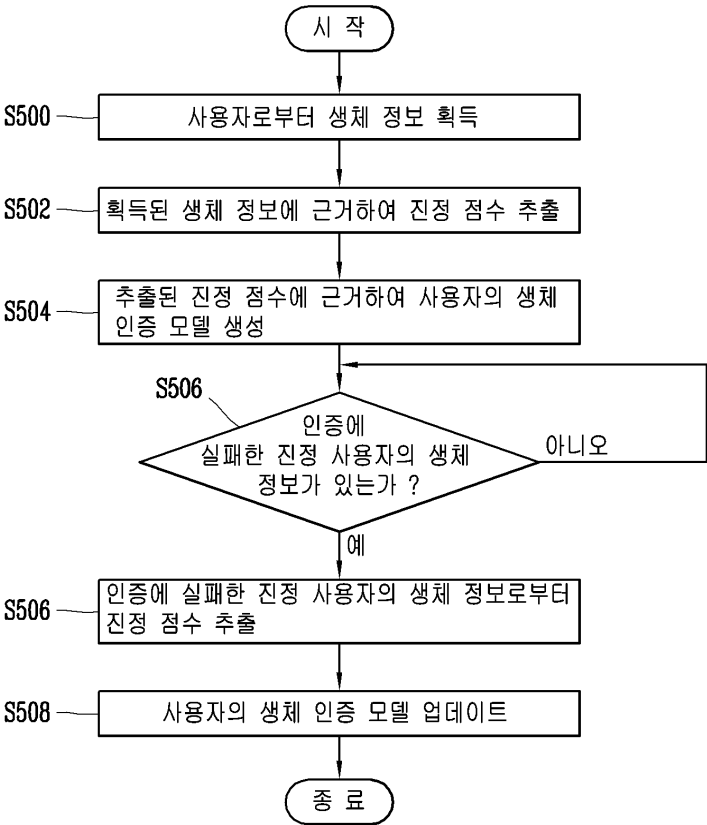
도면4a



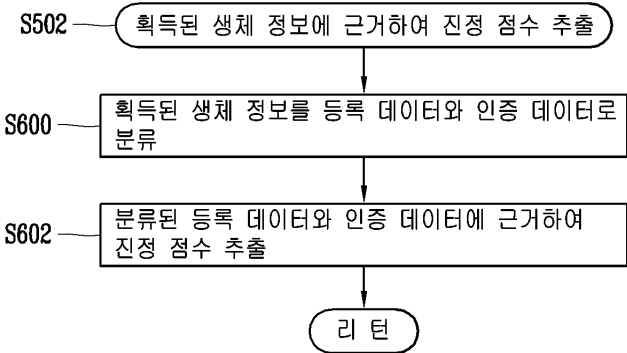
도면4b



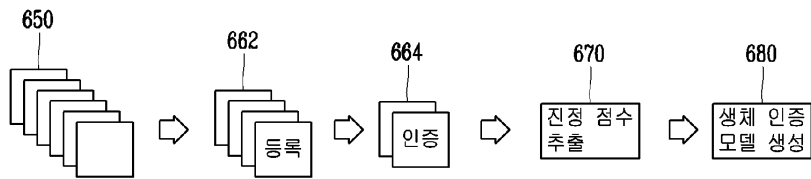
도면5



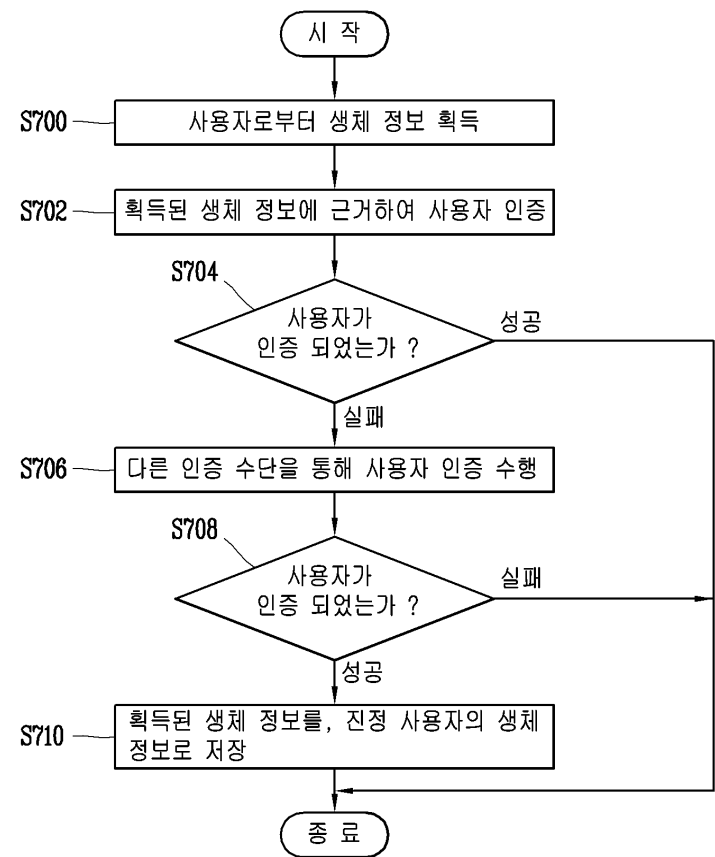
도면6a



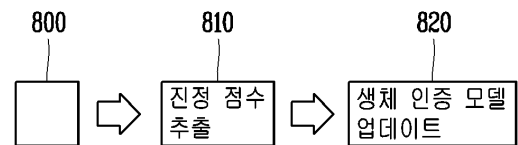
도면6b



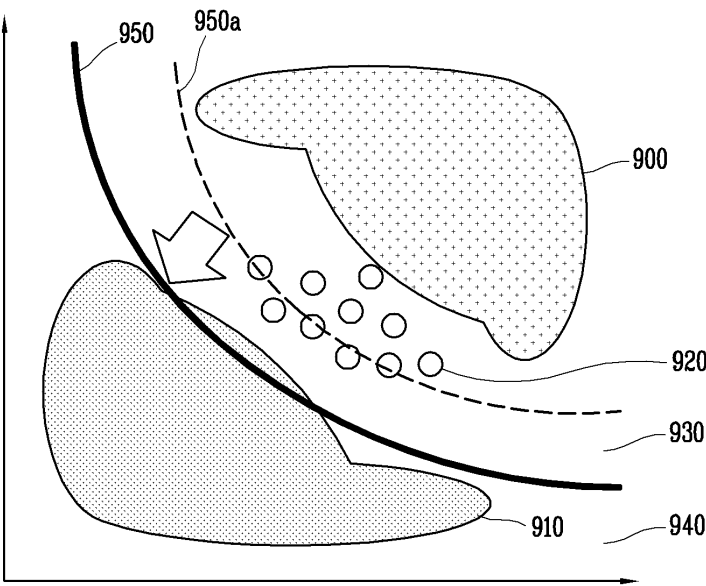
도면7



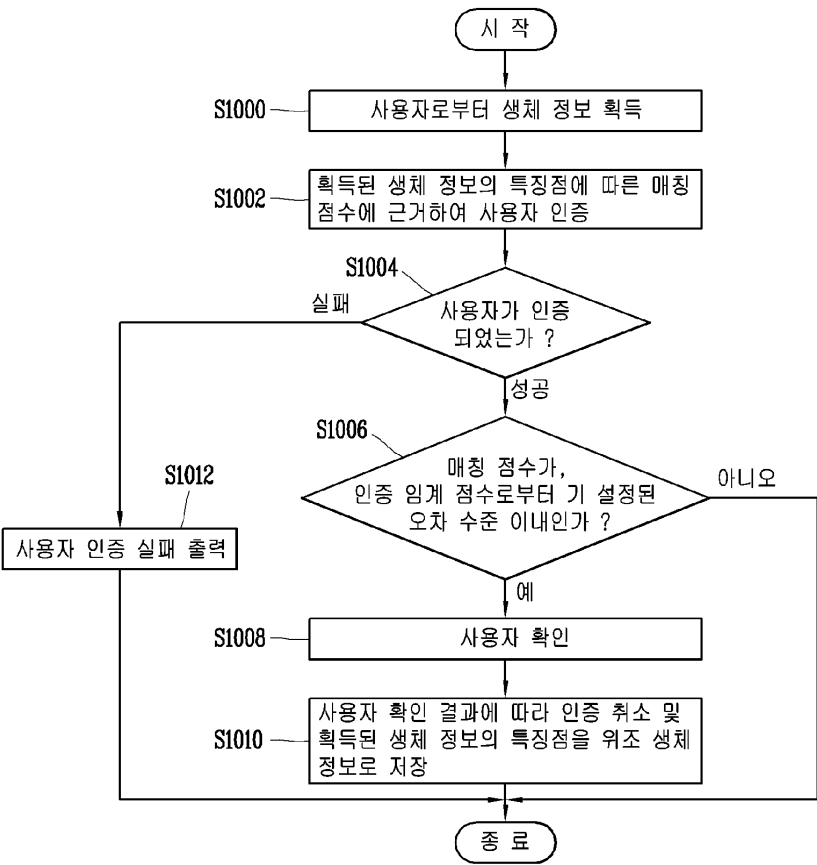
도면8



도면9



도면10



도면11

