



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0052345
(43) 공개일자 2018년05월18일

(51) 국제특허분류(Int. Cl.)
G06F 21/31 (2013.01) G06F 21/46 (2013.01)
H04L 9/32 (2006.01) H04M 1/02 (2006.01)
(52) CPC특허분류
G06F 21/31 (2013.01)
G06F 21/46 (2013.01)
(21) 출원번호 10-2016-0149549
(22) 출원일자 2016년11월10일
심사청구일자 2016년11월10일

(71) 출원인
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대현
서울특별시 서초구 서초중앙로 200, 17동 901호(서초동, 삼풍아파트)
(74) 대리인
양성보

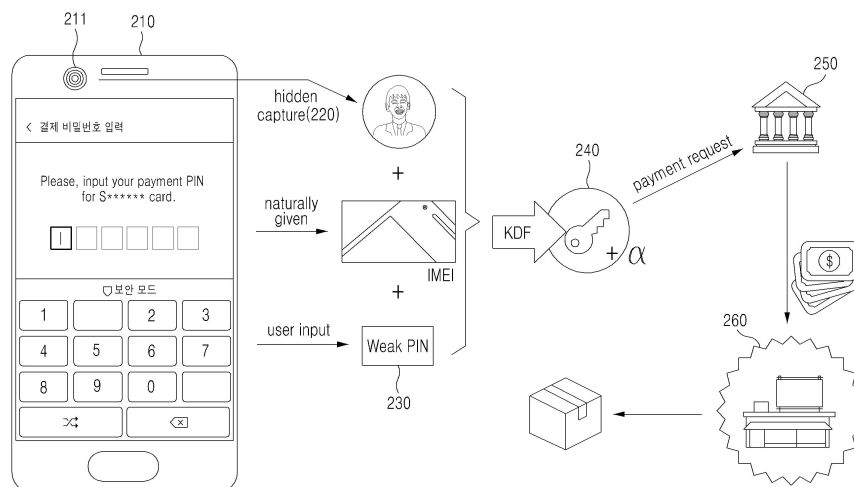
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 숨김 정보 및 사용자 인증 정보를 결합하여 사용자 인증을 수행하는 방법 및 장치

(57) 요약

2가지 요소를 결합한 사용자 인증 방법 및 장치가 개시된다. 일 실시예에 따른 전자 장치를 통한 사용자 인증 방법은, 인증 대상의 사용자로부터 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는 인증 정보를 수신하는 단계; 상기 전자 장치의 카메라를 사용하여 상기 사용자를 히든 캡처하는 단계; 및 상기 히든 캡처에 의해 획득된 사용자의 이미지 및 상기 인증 정보와 기 저장된 사용자 인증 정보와의 비교에 기반하여 상기 사용자의 인증을 수행하는 단계를 포함하고, 상기 히든 캡처는 상기 카메라에 의한 상기 인증 대상의 사용자에 대한 촬영이 상기 사용자에 의해 인식되지 않도록 상기 전자 장치 및 카메라를 제어함으로써 수행될 수 있다.

대표도



(52) CPC특허분류

H04L 9/3226 (2013.01)

H04M 1/0264 (2013.01)

명세서

청구범위

청구항 1

전자 장치를 통한 사용자 인증 방법에 있어서,

인증 대상의 사용자로부터 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는 인증 정보를 수신하는 단계;

상기 전자 장치의 카메라를 사용하여 상기 사용자를 히든 캡처하는 단계; 및

상기 히든 캡처에 의해 획득된 사용자의 이미지 및 상기 인증 정보와 기 저장된 사용자 인증 정보와의 비교에 기반하여 상기 사용자의 인증을 수행하는 단계

를 포함하고,

상기 히든 캡처는 상기 카메라에 의한 상기 인증 대상의 사용자에게 대한 촬영이 상기 사용자에게 의해 인식되지 않도록 상기 전자 장치 및 카메라를 제어함으로써 수행되는 사용자 인증 방법.

청구항 2

제1항에 있어서,

인증 대상의 사용자의 이미지와 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는 사용자 인증 정보를 등록하는 단계

를 더 포함하고,

상기 등록하는 단계는,

상기 카메라를 사용하여, 상기 인증 대상의 사용자의 얼굴의 측면 및 정면 중 적어도 하나를 촬영함으로써 상기 사용자의 이미지를 획득하는 단계

를 포함하는 사용자 인증 방법.

청구항 3

제2항에 있어서,

상기 사용자의 이미지는 상기 카메라의 스폿 측광 모드를 사용하여 상기 사용자의 얼굴의 측면 및 정면 중 적어도 하나를 촬영함으로써 획득되는, 사용자 인증 방법.

청구항 4

제1항에 있어서,

상기 히든 캡처는 상기 카메라의 촬영 음성을 오프(Off) 모드로 제어하여 수행되는 사용자 인증 방법.

청구항 5

제1항에 있어서,

상기 히든 캡처는 상기 카메라의 라이브 뷰 모드를 오프(Off) 모드로 제어하여 수행되는 사용자 인증 방법.

청구항 6

제1항에 있어서,

상기 히든 캡처하는 단계는,

상기 카메라를 사용하여 상기 인증 대상의 사용자의 얼굴의 정면 및 측면 중 적어도 하나를 히든 캡처하는

사용자 인증 방법.

청구항 7

제1항에 있어서,

상기 기 저장된 사용자 인증 정보는 상기 인증 대상의 사용자의 인증을 위한 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보와 연관된 제1 사용자 인증 정보 및 상기 사용자의 이미지와 연관된 제2 사용자 인증 정보를 포함하고,

상기 인증 정보와 상기 제1 사용자 인증 정보와의 비교에 기반하여 상기 사용자에게 대한 1차 인증을 수행하는 단계

를 더 포함하고,

상기 히든 캡처는 상기 1차 인증이 완료된 경우에만 수행되고,

상기 사용자의 인증을 수행하는 단계는,

상기 히든 캡처에 의해 획득된 사용자의 이미지와 상기 제2 사용자 인증 정보와의 비교에 기반하여 상기 사용자의 인증을 완료하는 단계

를 포함하는 사용자 인증 방법.

청구항 8

제1항에 있어서,

상기 사용자의 인증을 수행하는 단계는,

상기 히든 캡처에 의해 획득된 사용자의 이미지 및 상기 인증 정보를 상기 전자 장치의 고유키를 이용하여 암호화하고, 상기 암호화된 암호화값과 기 저장된 사용자 인증 정보가 매칭됨에 따라 사용자 인증을 수행하는 단계

를 포함하는 사용자 인증 방법.

청구항 9

전자 장치를 통한 사용자 인증을 수행하기 위한 사용자 인증 장치에 있어서,

인증 대상의 사용자로부터 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는 인증 정보를 수신하는 수신부;

상기 전자 장치의 카메라를 사용하여 상기 사용자를 히든 캡처하는 캡처부; 및

상기 히든 캡처에 의해 획득된 사용자의 이미지 및 상기 인증 정보와 기 저장된 사용자 인증 정보와의 비교에 기반하여 상기 사용자의 인증을 수행하는 수행부

를 포함하고,

상기 히든 캡처는 상기 카메라에 의한 상기 인증 대상의 사용자에게 대한 촬영이 상기 사용자에게 의해 인식되지 않도록 상기 전자 장치 및 상기 카메라를 제어함으로써 수행되는 사용자 인증 장치.

발명의 설명

기술 분야

[0001] 아래의 설명은 사용자 인증 기술에 관한 것으로, 2가지 요소를 이용하여 사용자 인증을 수행하는 방법 및 장치에 관한 것이다.

배경 기술

- [0002] 멀티미디어 기기의 형태로 구현된 모바일 기기는, 복잡한 기능을 구현하기 위해 하드웨어나 소프트웨어적 측면에서 새로운 시도들이 다양하게 적용되고 있다. 모바일 기기를 이용하여 단순한 문자 송수신, 음성통화뿐 아니라 영상통화, 웹 서비스, 앱 다운로드 등의 유료 서비스가 가능해지면서, 다양한 유료서비스가 타인에 의해 사용되지 않도록 보호될 필요성이 증가하였다. 또한, 모바일 기기가 일상 생활과 밀접한 관계를 갖게 되면서, 타인의 모바일 기기에 포함된 정보에 대한 접근을 제한할 필요성도 증가하였다. 또한 현대 사회는 사생활 보호가 더욱 중요해지고 있으며, 이에 따라 모바일 기기뿐만 아니라 다른 전자 기기에서도 보안기능의 강화가 중요한 화두가 되고 있다.
- [0003] 전자 기기의 보안 기능을 위하여 종래에는 키패드를 이용한 패스워드 입력수단이 다양한 방법으로 실시되었다. 예를 들면, 일반적인 방법으로는 사용자와 시스템 간에 미리 공유되어 있는 비밀 정보를 기반으로 하며 사용자가 비밀 정보인 패스워드 또는 PIN을 직접 키패드나 터치패드 등을 통해 입력함으로써 사용자 인증을 수행할 수 있다.
- [0004] 또한 극도의 보안을 유지하기 위하여 인간의 신체정보를 이용한 인증 방법이 존재한다. 상기 방법은, 사용자의 화상, 지문, 홍채 등을 분석함으로써 생성한 사용자 특성 정보를 미리 저장하고, 저장된 사용자 특성 정보와 입력된 사용자 특정 정보를 비교함으로써 사용자 인증이 수행된다. 하지만, 인간의 신체정보를 이용한 인증 방법 중 화상 인식을 인증에 따르면, 얼굴데이터는 촬영시마다 촬영각도, 촬영조도, 안경착용여부, 모자 착용여부, 머리염색여부 등의 다양한 인자들이 변할 수 있기 때문에 다른 인증과는 달리 인식 오류가 발생할 확률이 높다는 문제점이 있다.

발명의 내용

해결하려는 과제

- [0005] 이미지 및 사용자 인증 정보를 결합한 사용자 인증 과정을 수행하는 방법 및 장치를 제공할 수 있다. 다시 말해서, 사용자가 인증 화면을 통하여 인증 정보를 입력할 때, 히든 캡처를 통하여 획득된 사용자의 이미지에 기초하여 인증을 수행함으로써 사용자 인증 정보가 노출되더라도 보안을 유지하는 방법을 제공할 수 있다.

과제의 해결 수단

- [0006] 전자 장치를 통한 사용자 인증 방법은, 인증 대상의 사용자로부터 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는 인증 정보를 수신하는 단계; 상기 전자 장치의 카메라를 사용하여 상기 사용자를 히든 캡처하는 단계; 및 상기 히든 캡처에 의해 획득된 사용자의 이미지 및 상기 인증 정보와 기 저장된 사용자 인증 정보와의 비교에 기반하여 상기 사용자의 인증을 수행하는 단계를 포함하고, 상기 히든 캡처는 상기 카메라에 의한 상기 인증 대상의 사용자에 대한 촬영이 상기 사용자에 의해 인식되지 않도록 상기 전자 장치 및 카메라를 제어함으로써 수행될 수 있다.
- [0007] 상기 사용자 인증 방법은, 인증 대상의 사용자의 이미지와 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는 사용자 인증 정보를 등록하는 단계를 더 포함하고, 상기 등록하는 단계는, 상기 카메라를 사용하여, 상기 인증 대상의 사용자의 얼굴의 측면 및 정면 중 적어도 하나를 촬영함으로써 상기 사용자의 이미지를 획득하는 단계를 포함할 수 있다.
- [0008] 상기 사용자의 이미지는 상기 카메라의 스팟 측광 모드를 사용하여 상기 사용자의 얼굴의 측면 및 정면 중 적어도 하나를 촬영함으로써 획득될 수 있다.
- [0009] 상기 히든 캡처는 상기 카메라의 촬영 음성을 오프(Off) 모드로 제어하여 수행될 수 있다.
- [0010] 상기 히든 캡처는 상기 카메라의 라이브 뷰 모드를 오프(Off) 모드로 제어하여 수행될 수 있다.
- [0011] 상기 히든 캡처하는 단계는, 상기 카메라를 사용하여 상기 인증 대상의 사용자의 얼굴의 정면 및 측면 중 적어도 하나를 히든 캡처할 수 있다.
- [0012] 상기 기 저장된 사용자 인증 정보는 상기 인증 대상의 사용자의 인증을 위한 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보와 연관된 제1 사용자 인증 정보 및 상기 사용자의 이미지와 연관된 제2 사용자 인증 정보를

포함하고, 상기 인증 정보와 상기 제1 사용자 인증 정보와의 비교에 기반하여 상기 사용자에게 대한 1차 인증을 수행하는 단계를 더 포함하고, 상기 히든 캡처는 상기 1차 인증이 완료된 경우에만 수행되고, 상기 사용자의 인증을 수행하는 단계는, 상기 히든 캡처에 의해 획득된 사용자의 이미지와 상기 제2 사용자 인증 정보와의 비교에 기반하여 상기 사용자의 인증을 완료하는 단계를 포함할 수 있다.

[0013] 상기 사용자의 인증을 수행하는 단계는, 상기 히든 캡처에 의해 획득된 사용자의 이미지 및 상기 인증 정보를 상기 전자 장치의 고유키를 이용하여 암호화하고, 상기 암호화된 암호화값과 기 저장된 사용자 인증 정보가 매칭됨에 따라 사용자 인증을 수행하는 단계를 포함할 수 있다.

[0014] 전자 장치를 통한 사용자 인증을 위한 사용자 인증 장치는, 인증 대상의 사용자로부터 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는 인증 정보를 수신하는 수신부; 상기 전자 장치의 카메라를 사용하여 상기 사용자를 히든 캡처하는 캡처부; 및 상기 히든 캡처에 의해 획득된 사용자의 이미지 및 상기 인증 정보와 기 저장된 사용자 인증 정보와의 비교에 기반하여 상기 사용자의 인증을 수행하는 수행부를 포함하고, 상기 히든 캡처는 상기 카메라에 의한 상기 인증 대상의 사용자에게 대한 촬영이 상기 사용자에게 의해 인식되지 않도록 상기 전자 장치 및 상기 카메라를 제어함으로써 수행될 수 있다.

발명의 효과

[0015] 일 실시예에 따른 사용자 인증 장치는, 사용자가 인증 화면을 통하여 인증 정보를 입력할 때, 무음으로 사용자의 이미지를 연속적으로 촬영하기 때문에 사용자는 이미지를 촬영하는 것을 인지할 수 없으며, 인증 정보가 해킹되더라도 사용자의 이미지 정보에 대한 인식을 수행함으로써 보안을 유지할 수 있다.

[0016] 일 실시예에 따른 사용자 인증 장치는, 사용자로부터 입력된 인증 정보 및 히든 캡처를 통해 획득된 이미지를 고유키를 이용하여 암호화한 암호화값과 데이터베이스에 저장된 템플릿 정보를 복호화하지 않고 암호화된 상태에서 서로 비교하기 때문에 암호화값이 노출되더라도 이미지 정보 및 인증 정보의 보안을 유지할 수 있다.

[0017] 일 실시예에 따른 사용자 인증 장치는, 사용자 인증을 수행하기 위한 등록 과정에서 스냅 측광 모드에 기초하여 촬영된 이미지 정보를 저장함으로써, 추후에 사용자 인증이 수행되었을 경우 촬영되는 사용자의 이미지를 인식하는 인식률을 높일 수 있다.

[0018] 일 실시예에 따른 사용자 인증 장치는, 사용자가 인증 화면을 통하여 인증 정보를 입력함에 따라 실시간으로 사용자의 이미지를 인식하기 때문에 보다 빠르게 사용자 인증을 수행할 수 있다.

도면의 간단한 설명

[0019] 도 1은 일 실시예에 따른 사용자 인증 과정의 개략적인 동작을 설명하기 위한 도면이다.

도 2 및 도3은 일 실시예에 따른 사용자 인증 장치에서 사용자 인증 과정을 설명하기 위한 도면이다.

도 4는 일 실시예에 따른 사용자 인증 장치의 구성을 설명하기 위한 블록도이다.

도 5는 일 실시예에 따른 사용자 인증 장치의 사용자 인증 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0021] 아래의 실시예들은 복수의 요소를 결합한 사용자 인증 기술에 관한 것으로, 사용자의 모습 및 사용자로부터 입력되는 인증 정보에 기초하여 사용자 인증을 수행하는 방법에 대하여 설명하기로 한다. 더욱 상세하게는, 전자 장치의 카메라를 이용하여 인증 대상의 사용자를 식별하기 위하여 무음 모드로 사용자를 계속적으로 촬영할 수 있다. 이때, 사용자 인증 장치는 전자 장치의 카메라를 통하여 사용자를 히든 캡처하면서 사용자로부터 패스워드 정보 또는 패스워드 패턴 정보를 포함하는 인증 정보를 입력받을 수 있다. 이를 통하여 사용자가 느끼기에는 사용자의 인증 정보만을 입력하면 사용자 인증이 수행되는 것처럼 느껴지지만, 실제로는 전자 장치의 카메라를 통하여 사용자를 실시간으로 히든 캡처하여 사용자의 모습을 식별하기 때문에 사용자의 인증 정보가 노출되

더라도 보안을 유지할 수 있다. 상기 사용자 인증 방법에 대하여 아래의 설명에서 더욱 상세하게 설명하기로 한다.

- [0022] 도 1은 일 실시예에 따른 사용자 인증 과정의 개략적인 동작을 설명하기 위한 도면이다.
- [0023] 전자 장치(110)는 컴퓨터 장치로 구현되는 고정형 단말이거나 이동형 단말일 수 있다. 전자 장치(110)는 예를 들면, 스마트폰(smart phone), 휴대폰, 내비게이션, 컴퓨터, 노트북, 디지털방송용 단말, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 태블릿 PC 등이 있다. 일례로 전자 장치(110)는 무선 또는 유선 통신 방식을 이용하여 네트워크(120)를 통해 다른 단말들 및/또는 서버(예를 들면, 사용자 인증 장치)(100)와 통신할 수 있다.
- [0024] 통신 방식은 제한되지 않으며, 네트워크(120)가 포함할 수 있는 통신망(일례로, 이동통신망, 유선 인터넷, 무선 인터넷, 방송망)을 활용하는 통신 방식뿐만 아니라 기기들간의 근거리 무선 통신 역시 포함될 수 있다. 예를 들어, 네트워크(170)는, PAN(personal area network), LAN(local area network), CAN(campus area network), MAN(metropolitan area network), WAN(wide area network), BBN(broadband network), 인터넷 등의 네트워크 중 하나 이상의 임의의 네트워크를 포함할 수 있다. 또한, 네트워크는 버스 네트워크, 스타 네트워크, 링 네트워크, 메쉬 네트워크, 스타-버스 네트워크, 트리 또는 계층적(hierarchical) 네트워크 등을 포함하는 네트워크 토폴로지 중 임의의 하나 이상을 포함할 수 있으나, 이에 제한되지 않는다.
- [0025] 서버(100)는 전자 장치(110)와 네트워크(120)를 통해 통신하여 명령, 코드, 파일, 콘텐츠, 서비스 등을 제공하는 컴퓨터 장치 또는 복수의 컴퓨터 장치들로 구현될 수 있다. 일례로, 서버(100)는 네트워크(120)를 통해 접속한 전자 장치(110)로 사용자 인증을 수행하도록 제공하는 사용자 인증 장치일 수 있다.
- [0026] 도 2 및 도3은 일 실시예에 따른 사용자 인증 장치에서 사용자 인증 과정을 설명하기 위한 도면이다.
- [0027] 사용자 인증 장치는 전자 장치(210, 310)로 사용자 인증을 수행하기 위한 인증 화면을 제공할 수 있다. 예를 들면, 전자 장치(210, 310)에 사용자 인증 장치로부터 제공되는 사용자 인증을 수행하기 위한 인증 화면이 연동됨으로써 사용자 인증을 수행할 수 있으며, 전자 장치(210, 310)에 사용자 인증을 수행하기 위한 어플리케이션(App)이 설치되어 구동될 수도 있다.
- [0028] 사용자 인증 장치는 전자 장치(210, 310)의 인증 화면에 사용자로부터 입력된 인증 정보를 입출력하기 위한 인터페이스를 제공할 수 있다. 이때, 인증 정보를 입출력하기 위한 인터페이스는 사용자 인터페이스일 수 있다. 예를 들면, 사용자는 전자 장치(210, 310)에 표시된 인증 화면에 체크, 터치&드래그, 터치 등을 통하여 패스워드 정보 또는 패스워드 패턴 정보를 포함하는 인증 정보를 입력할 수 있다. 이때, 전자 장치(210, 310)는 표시된 인증 화면에 사용자의 인증 정보를 보다 편리하게 입력할 수 있도록 키펀드를 제공할 수도 있다.
- [0029] 사용자는 사용자 인증을 수행하기 전에, 인증 대상의 사용자의 이미지와 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는 사용자 인증 정보를 사전에 사용자 인증 장치에 등록할 수 있다. 사용자 인증 장치는 전자 장치(210, 310)에 사용자 인증을 위한 정보를 등록할 수 있도록 제공할 수 있다. 사용자가 전자 장치(210)를 통하여 인증 정보를 입력하는 동안, 전자 장치(210, 310)는 사용자의 이미지를 촬영할 수 있다. 전자 장치(210, 310)는 다양한 각도(예를 들면, 0도~360 범위 이내)의 사용자의 이미지를 촬영할 수 있다. 예를 들면, 전자 장치(210, 310)는 사용자의 정면 얼굴 또는 측면 얼굴을 촬영할 수 있다. 사용자 인증 장치는 복수의 이미지에 대하여 행렬을 생성하여 특정 값으로 변환할 수 있다. 이때, 사용자 인증 장치는 사용자 정면 얼굴 또는 측면 얼굴을 획득함으로써 사용자 이미지의 인식률을 높일 수 있다.
- [0030] 사용자 인증 장치는 전자 장치(210, 310)를 통하여 사용자의 이미지를 보다 뚜렷하게 획득하기 위하여 스폿(Spot) 측광 모드에 기초하여 사용자의 이미지(예를 들면, 사용자의 얼굴의 측면 또는 정면)를 촬영하도록 할 수 있다. 이때, 전자 장치(210, 310)의 카메라가 스폿 측광 모드로 동작됨으로써 사용자의 이미지를 촬영할 수 있고, 카메라의 음성이 온(On)/오프(Off)되어 촬영될 수 있다.
- [0031] 스폿 측광 모드란 디스플레이 화면의 정중앙의 좁은 부분(기 설정된 크기 이하의 범위)에서 들어오는 빛을 측정하는 방법이다. 같은 색이라도 각각의 위치에 따른 빛의 반사가 다르기 때문에 노출값이 다르다. 이에 따라 세밀하게 각각의 위치에 따른 노출을 찾기 위하여 사용될 수 있다. 스폿 측광 모드는 노출 차이가 클 때 사용하여, 의도적으로 밝은 부분을 스폿 측광할 경우, 나머지 부분이 어둡게 표현되므로 명암이 확실한 사용자의 이미지를 획득할 수 있다. 상기 스폿 측광 모드를 이용하여 사용자의 이미지를 추출함에 있어서, 조명에 따라 사용자의 이미지를 인식하는 인식률이 다른 문제점을 해결할 수 있게 된다.

- [0032] 사용자 인증 장치는 사용자 이미지의 인식률을 높이기 위하여 전자 장치(210, 310)의 스냅 측광 모드에 기초하여 사용자의 이미지를 촬영하는 것으로 예를 들어 설명한 것 일뿐, 이에 한정되는 것은 아니다.
- [0033] 사용자 인증 장치는 전자 장치(210, 310)로부터 획득된 사용자 인증 정보를 필터링하여 데이터베이스에 저장할 수 있다. 예를 들면, 사용자 인증 장치는 이미지를 행렬을 생성하여 특정 값으로 변환하여 데이터베이스에 저장할 수 있다. 또는 사용자 인증 장치는 이미지 및 전자 장치의 국제모바일기기 식별코드에 기초하여 특정 값으로 변환하여 데이터베이스에 저장할 수도 있다.
- [0034] 또한, 사용자 인증 장치는 전자 장치(210, 310)를 통하여 사용자의 이미지를 촬영하여 사용자 이미지를 획득함에 따라 사용자가 입력한 인증 정보를 수신할 수 있다. 이때, 인증 정보는 패스워드 정보 또는 패스워드 패턴 정보를 포함할 수 있다. 예를 들면, 인증 정보는 문자, 숫자 및 패턴 중 적어도 하나로 설정된 패스워드 정보일 수 있고, 설정된 패스워드에 따라 입력되는 패스워드 패턴 정보를 더 포함할 수도 있다.
- [0035] 사용자 인증 장치는 전자 장치(210, 310)를 통하여 획득된 사용자의 이미지 정보 및 사용자의 인증 정보를 전자 장치(210, 310)의 국제모바일기기 식별 코드에 기초하여 암호화할 수 있다. 사용자 인증 장치는 암호화된 암호화값을 데이터베이스에 사용자 인증을 수행하기 위한 템플릿 정보로 저장할 수 있다. 이때, 데이터베이스에 저장된 템플릿 정보는 사용자로부터 입력될 때마다 또는 주기적으로(예를 들면, 1달) 업데이트될 수 있다. 또한, 사용자 인증 장치는 전자 장치의 고유키를 이용하여 생성된 소정의 변환 매트릭스에 의해 치환되어 데이터베이스에 저장할 수 있다.
- [0036] 이와 같은 과정을 통하여 인증 대상의 사용자의 이미지와 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는 사용자 인증 정보를 등록하는 등록 과정이 수행될 수 있다. 예를 들면, 종래의 지문 인식을 위한 등록 과정에서는 사용자의 손가락을 전자 장치에 다양한 면적을 접촉시킴으로써 등록이 이루어졌지만, 일 실시예에 따른 사용자 인증 장치는 전자 장치의 카메라를 이용하여 실시간으로 연속적인 이미지를 촬영하여 등록하기 때문에 지문 인식을 통한 등록 과정보다 빠르게 등록 과정이 수행될 수 있다.
- [0037] 사용자가 전자 장치(210, 310)를 통하여 사용자 인증을 수행한다고 가정하자. 일례로, 전자 장치에서 지불 처리 과정이 수행될 경우, 사용자 인증을 수행하는 과정을 도 2를 참고하여 설명하기로 한다.
- [0038] 전자 장치(210)에 사용자 인증을 수행하기 위한 인증 화면이 표시될 수 있다. 사용자는 전자 장치(210)를 통하여 패스워드 정보 또는 패스워드 패턴 정보를 포함하는 인증 정보(230)를 입력할 수 있고, 카메라(211)는 촬영 음성을 오프(Off) 모드(예를 들면, 무음 모드)로 사용자의 모습을 실시간으로 촬영할 수 있고, 카메라(211)의 라이브 뷰 모드를 오프 모드로 촬영할 수 있다. 사용자 인증 장치는 전자 장치의 카메라를 사용하여 사용자를 히든 캡처할 수 있다. 이때, 히든 캡처(220)는 카메라(211)가 사용자를 촬영하고 있다는 것을 사용자에게 의해 인식되지 않도록 전자 장치(210) 및 카메라를 제어함으로써 수행될 수 있다. 사용자 인증 장치는 카메라(211)를 이용하여 인증 대상 사용자의 얼굴의 정면 및 측면 중 적어도 하나를 히든 캡처할 수 있다.
- [0039] 사용자 인증 장치는 전자 장치(210)로부터 촬영된 히든 캡처(220)를 통하여 사용자의 모습을 실시간으로 획득할 수 있다. 예를 들면, 사용자 인증 장치는 전자 장치(210)로부터 히든 캡처(220)를 획득함에 따라 데이터베이스에 저장된 이미지 정보를 비교함으로써 히든 캡처(220)에 대한 템플릿 정보를 추출할 수 있다.
- [0040] 사용자 인증 장치는 획득된 히든 캡처에 의해 획득된 사용자의 이미지 및 인증 정보를 전자 장치(210)의 고유키(예를 들면, 국제모바일기기 식별코드)를 이용하여 암호화할 수 있다(240).
- [0041] 국제모바일기기 식별코드(international mobile equipment identity)는 휴대 단말에 부여되는 고유 식별 번호로서, 예를 들면, 도난 단말기에 대한 통화차단 등을 관리할 수 있다. 국제모바일기기 식별코드는 제조사가 휴대 단말을 출고할 때 부여되며 형식 승인코드 8자리, 모델 일련번호 6자리, 검증용 숫자 1자리 등 총 15자리로 구성될 수 있다.
- [0042] 사용자 인증 장치는 히든 캡처에 의해 획득된 사용자의 이미지 및 인증 정보를 고유키를 이용하여 암호화한 암호화값과 데이터베이스에 저장된 템플릿 정보와 비교할 수 있다. 이때, 데이터베이스는 인증 대상의 사용자의 이미지, 패스워드 정보 또는 패스워드 패턴 정보를 포함하는 사용자 인증 정보를 저장하고 있을 수 있으며, 이러한 사용자 인증 정보를 암호화하여 저장할 수 있다.
- [0043] 사용자 인증 장치는 고유키에 기초하여 암호화된 값에 기초하여 데이터베이스에 저장된 템플릿 정보를 추출할 수 있다. 사용자 인증 장치는 암호화값을 복호화하여 비교하지 않고, 각각의 암호화값을 비교함으로써 사용자 인증을 수행할 수 있다. 다시 말해서, 사용자의 인증 정보 및 히든 캡처를 통해 획득된 이미지에 대한 정보를

고유키를 이용한 암호화값과 데이터베이스에 암호화되어 저장된 템플릿 정보를 비교함으로써 보안을 유지할 수 있다는 장점이 있다.

[0044] 또한, 사용자 인증 장치는 사용자로부터 입력된 인증 정보에 기초하여 기저장된 사용자 인증 정보와 1차적으로 인증을 수행한 후, 사용자로부터 입력된 인증 정보가 일치할 경우 히든 캡처를 통한 사용자 인증을 수행할 수 있다. 이때, 기 저장된 사용자 인증 정보는 인증 대상의 사용자의 인증을 위한 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보와 연관된 제1 사용자 인증 정보 및 사용자의 이미지와 연관된 제2 사용자 인증 정보를 포함할 수 있다. 이때, 인증 정보와 제1 사용자 인증 정보와의 비교에 기반하여 사용자에게 대한 1차 인증을 수행한 후, 1차 인증이 완료된 경우 히든 캡처에 의해 획득된 이미지와 제2 사용자 인증 정보와의 비교에 기반하여 사용자의 인증을 완료할 수 있다. 예를 들면, 사용자 인증 장치는 사용자로부터 입력된 패스워드 정보 또는 패스워드 패턴 정보와 기 저장된 사용자 인증 정보를 비교한 후, 1차 인증이 완료된 경우, 히든 캡처에 의해 획득된 이미지와 기 저장된 사용자 인증 정보를 비교하여 사용자 인증을 수행할 수 있다.

[0045] 예를 들면, 사용자 인증 장치는 사용자 인증을 수행함에 따라 은행(결제 서버)으로 지불을 수행하기 위한 지불 요청을 전송할 수 있다. 은행은 지불 요청을 수락함에 따라 사용자의 지불 요청에 대한 결제를 처리할 수 있고, 사용자가 구입하고자 하는 물건에 대한 값을 판매자에게 전달할 수 있다. 판매자는 사용자로부터 주문된 물건에 대한 값이 지불됨을 확인한 후, 사용자에게 물건을 배송할 수 있다.

[0046] 또 다른 실시예로서 전자 장치의 Unlock 처리 과정이 수행될 경우, 사용자 인증 과정을 도 3을 참고하여 설명하기로 한다.

[0047] 전자 장치(310)에 사용자 인증을 수행하기 위한 인증 화면이 표시될 수 있다. 사용자는 전자 장치(310)를 통하여 인증 정보(330)를 입력할 수 있고, 카메라(311)는 히든 캡처를 통하여 사용자를 촬영할 수 있다. 예를 들면, 사용자는 전자 장치(310)를 통하여 인증 정보(330)로서 패스워드 정보 또는 패스워드 패턴 정보를 입력할 수 있다. 이때, 히든 캡처는 카메라에 의한 인증 대상의 사용자에게 대한 촬영이 사용자에게 의해 인식되지 않도록 상기 전자 장치 및 카메라를 제어함으로써 수행될 수 있다. 히든 캡처는 카메라의 촬영 음성을 오프 모드로 제어하여 수행될 수 있으며, 카메라의 라이브 뷰 모드를 오프 모드로 제어하여 수행될 수 있다. 사용자 인증 장치는 전자 장치(310)의 카메라를 사용하여 인증 대상의 사용자의 얼굴의 정면 및 측면 중 적어도 하나를 히든 캡처할 수 있다.

[0048] 사용자 인증 장치는 히든 캡처를 통해 획득된 이미지(320)를 통하여 사용자의 모습을 실시간으로 탐지할 수 있다. 예를 들면, 사용자 인증 장치는 히든 캡처를 통하여 획득된 이미지에 대하여 행렬을 생성하여 이미지 값으로 변환할 수 있다. 사용자 인증 장치는 변환된 이미지 값 및 사용자로부터 입력된 입력 정보를 전자 장치(310)의 고유키를 이용하여 암호화할 수 있다(340). 사용자 인증 장치는 암호화된 암호화값을 템플릿 정보로서 저장할 수 있다.

[0049] 사용자 인증 장치는 암호화된 암호화값과 데이터베이스에 저장된 템플릿 정보와 비교할 수 있다. 사용자 인증 장치는 고유키에 기초하여 암호화값에 대응하는 데이터베이스에 저장된 템플릿 정보를 추출할 수 있다. 사용자 인증 장치는 데이터베이스에 저장된 템플릿 정보도 암호화되어 있을 수 있다. 사용자 인증 장치는 각각의 암호화값을 비교함으로써 사용자 인증을 수행할 수 있다.

[0050] 일 실시예에 따른 사용자 인증 장치는 사용자 인증을 수행함에 따라 전자 장치(310)로 액세스 권한(Access Privilege)을 부여할 수 있다. 예를 들면, 전자 장치(310)는 보안 폴더, 전화 서비스 등 다양한 분야에 접근할 수 있게 된다.

[0051] 도 4는 일 실시예에 따른 사용자 인증 장치의 구성을 설명하기 위한 블록도이고, 도 5는 일 실시예에 따른 사용자 인증 장치의 사용자 인증 방법을 설명하기 위한 흐름도이다.

[0052] 사용자 인증 장치(400)는 사용자 인증 정보 및 히든 캡처로부터 획득된 이미지 정보에 기초하여 사용자 인증을 수행하기 위한 것으로, 수신부(410), 캡처부(420) 및 수행부(430)를 포함할 수 있다. 수신부(410), 캡처부(420) 및 수행부(430)는 도 5의 사용자 인증 방법이 포함하는 단계들을 수행하도록 사용자 인증 장치를 제어할 수 있다.

[0053] 등록부(도시되지 않음)는 인증 대상의 사용자의 이미지와 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는 사용자 인증 정보를 등록하는 과정이 이루어질 수 있도록 할 수 있다. 등록부는 사용자의 이미지 정보 및 인증 정보를 포함하는 사용자 인증 정보를 고유키를 이용하여 암호화하여 템플릿 정보를 데이터베이스에 저장할 수 있다. 등록부는 전자 장치의 카메라의 스냅 측광 모드에 기초하여 연속적으로 촬영된 사용자의

얼굴의 정면 또는 측면 중 적어도 하나 이상의 이미지를 획득하고, 획득된 이미지를 필터링하여 데이터베이스에 저장할 수 있다.

[0054] 단계(510)에서 수신부(410)는 인증 대상의 사용자로부터 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는 인증 정보를 수신할 수 있다. 이때, 전자 장치에 사용자 인증을 위한 인증 화면이 표시될 수 있다.

[0055] 단계(520)에서 캡처부(420)는 전자 장치의 카메라를 사용하여 상기 사용자를 히든 캡처할 수 있다. 캡처부(420)는 카메라의 촬영 음성이 오프(Off) 모드로 제어될 수 있고, 카메라의 라이브 뷰 모드가 오프(Off) 모드로 제어될 수 있다. 이때, 히든 캡처는 상기 카메라에 의한 상기 인증 대상의 사용자에 대한 촬영이 상기 사용자에게 의해 인식되지 않도록 상기 전자 장치 및 카메라를 제어함으로써 수행될 수 있다. 캡처부(420)는 카메라를 사용하여 인증 대상의 사용자의 얼굴의 정면 및 측면 중 적어도 하나를 히든 캡처할 수 있다.

[0056] 단계(530)에서 수행부(430)는 히든 캡처에 의해 획득된 사용자의 이미지 및 인증 정보와 기 저장된 사용자 인증 정보와의 비교에 기반하여 사용자의 인증을 수행할 수 있다. 수행부(430)는 히든 캡처에 의해 획득된 사용자의 이미지 및 인증 정보를 전자 장치의 고유키를 이용하여 암호화하고, 암호화된 암호화값과 기 저장된 사용자 인증 정보가 매칭됨에 따라 사용자 인증을 수행할 수 있다. 이때, 기 저장된 사용자 인증 정보는 암호화되어 템플릿 정보로서 저장되어 있을 수 있다. 수행부(430)는 암호화값과 데이터베이스에 저장된 템플릿 정보를 복호화하지 않고 암호화된 상태에서 서로 비교할 수 있다.

[0057] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0058] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 영구적으로, 또는 일시적으로 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0059] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0060] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태

로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

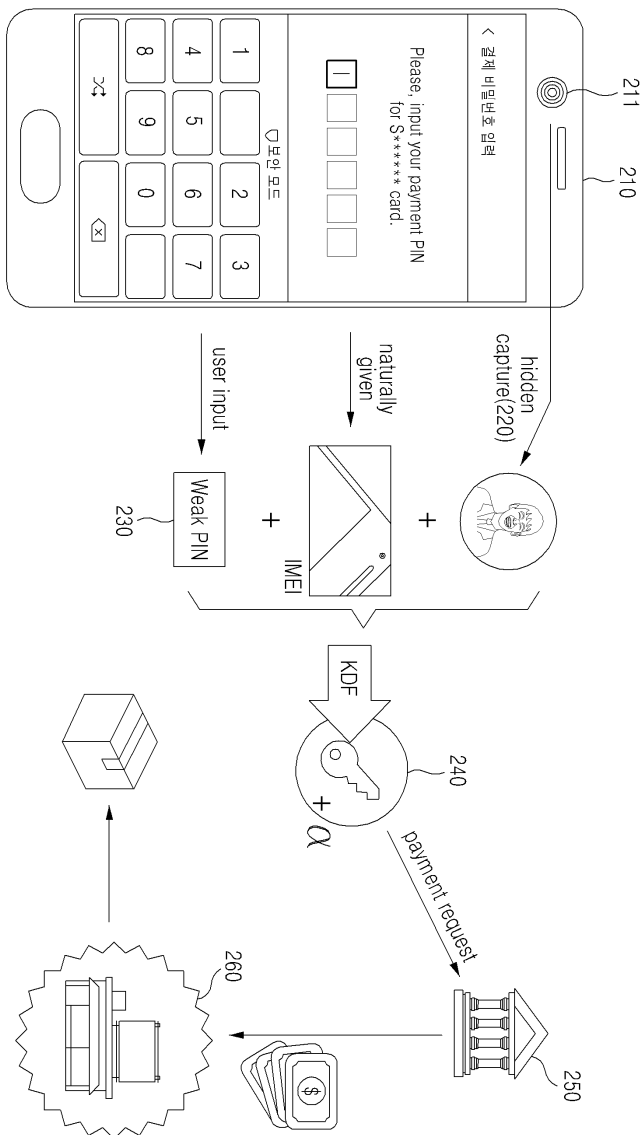
[0061] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

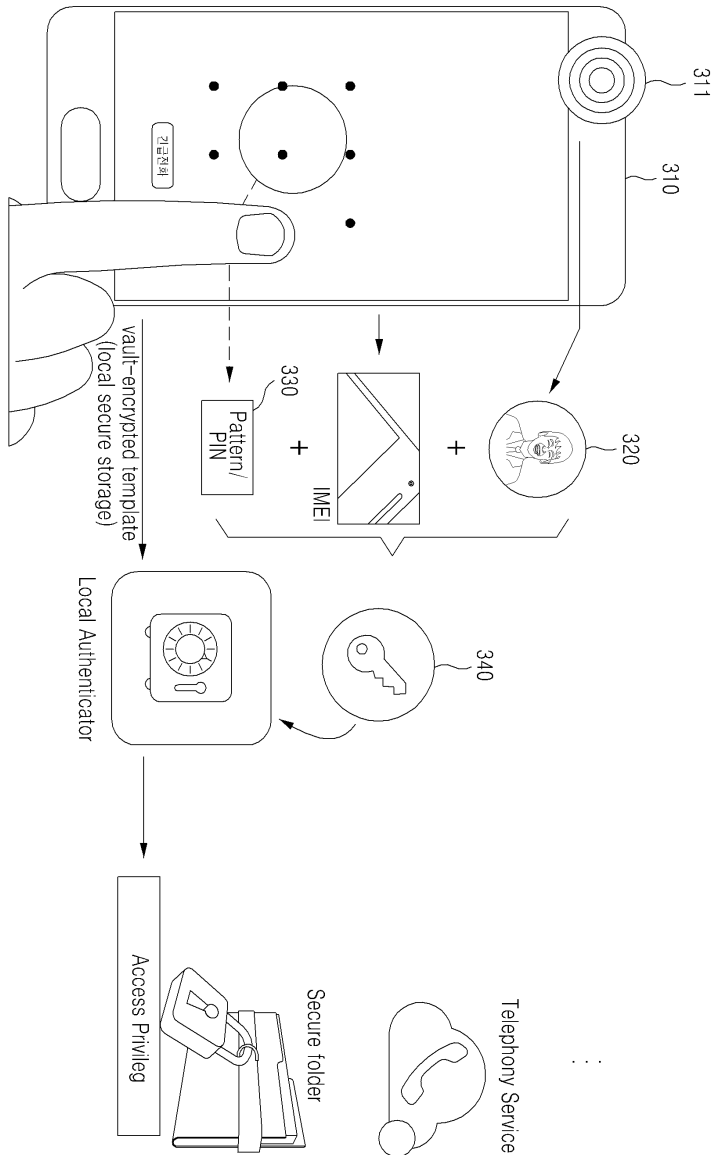
도면1



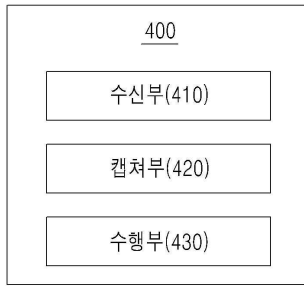
도면2



도면3



도면4



도면5

