(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년07월05일
(11) 등록번호 10-1997371
(24) 등록일자 2019년07월01일

(51) 국제특허분류(Int. Cl.)
G06F 21/32 (2013.01) *G06F 21/45* (2013.01)
G06F 3/01 (2006.01) *G06K 9/00* (2006.01)
(52) CPC특허분류
G06F 21/32 (2013.01)
G06F 21/45 (2013.01)
(21) 출원번호 10-2017-7005848
(22) 출원일자(국제) 2015년08월27일
심사청구일자 2018년07월12일
(85) 번역문제출일자 2017년03월02일
(65) 공개번호 10-2017-0047255
(43) 공개일자 2017년05월04일
(86) 국제출원번호 PCT/CN2015/088215
(87) 국제공개번호 WO 2016/034069
국제공개일자 2016년03월10일
(30) 우선권주장
201410446657.0 2014년09월03일 중국(CN)
(56) 선행기술조사문헌
KR1020070034327 A
KR1020070080066 A
WO2007105193 A1

(73) 특허권자
알리바바 그룹 홀딩 리미티드
케이만군도, 그랜드 케이만, 피오박스 847, 원 캐피탈 플레이스 4층
(72) 발명자
두 지준
중국 제지앙 311121 항조우 유 항 디스트릭트 웨스트 웬 위 로드 넘버969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5/에프
(74) 대리인
제일특허법인(유)

전체 청구항 수 : 총 15 항 심사관 : 문남두

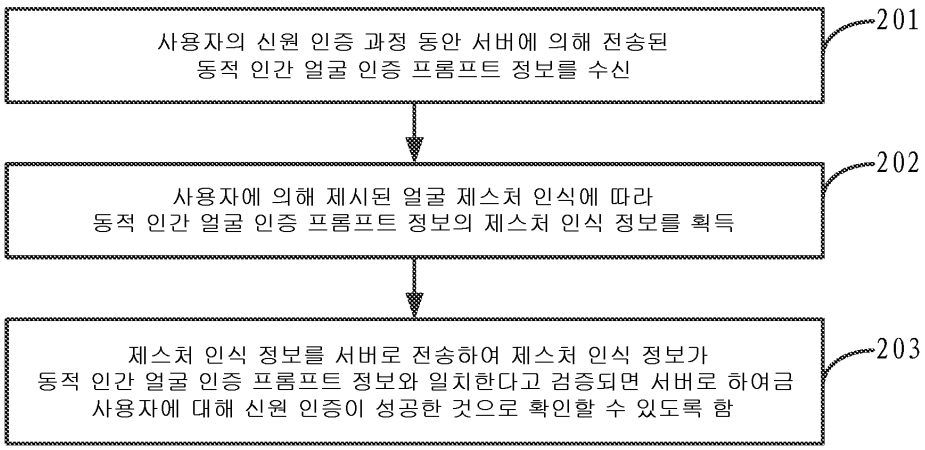
(54) 발명의 명칭 **신원 인증 방법 및 장치, 단말기 및 서버**

(57) 요 약

본 출원은 신원 인증을 위한 방법, 장치, 단말기 및 서버에 관한 것이다. 본 방법은 사용자의 신원 인증 과정 동안 서버에 의해 전송된 동적 얼굴 인증 프롬프트 정보를 수신하는 단계와, 사용자에 의해 제시된 얼굴 제스처를 인식하여 동적 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 획득하는 단계 및 제스처 인식 정보가 서버로

(뒷면에 계속)

대 표 도 - 도2a



전송되어 제스처 인식 정보가 동적 얼굴 인증 프롬프트 정보와 일치한다고 검증되면 서버로 하여금 신원 인증이 성공한 것으로 확인하도록 하는 단계를 포함한다. 본 출원의 실시예를 사용하여, 동적 얼굴 인증을 통해 사용자의 신원에 대해 매우 안전한 인증이 수행될 수 있다. 인증 암호를 사용하는 기존 인증 방법과 비교하면 악의적인 제3자에 의해 인증 정보를 도용당하지 않으므로 인증의 신뢰성이 향상된다. 게다가, 사용자는 동적 얼굴 인증을 통해 실제 사용자로 인식될 수 있으므로 인증 과정 동안 신원 인증의 정확성을 더 향상시키고 잠재적인 보안 위험을 감소시킨다.

(52) CPC특허분류
G06F 3/017 (2013.01)
G06K 9/00268 (2013.01)
G06K 9/00335 (2013.01)

명 세 서

청구범위

청구항 1

신원 인증 방법(identity authentication method)으로서,

사용자의 얼굴 특징 정보(facial feature information)를 획득하는 단계- 상기 사용자의 상기 얼굴 특징 정보를 획득하는 단계는,

상기 사용자의 얼굴이 검출되면 상기 사용자의 상기 얼굴을 추적하는 단계와,

상기 얼굴을 추적하는 경우 미리 설정된 시간 간격(preset time interval)에 따라 얼굴 이미지를 획득하는 단계와,

상기 얼굴 이미지가 미리 설정된 특징 추출 조건(preset feature extraction condition)을 만족시키는지를 판정하는 단계와,

상기 미리 설정된 특징 추출 조건이 만족되면 상기 얼굴 이미지로부터 상기 사용자의 상기 얼굴 특징 정보를 추출하는 단계를 포함함 -와,

상기 얼굴 특징 정보를 상기 사용자의 제1 얼굴 특징 정보로서 사용하는 단계와,

상기 사용자의 상기 제1 얼굴 특징 정보를 서버로 전송하여, 상기 제1 얼굴 특징 정보가 저장된 상기 사용자의 제2 얼굴 특징 정보와 일치한다고 검증되면, 상기 서버로 하여금 동적 얼굴 인증 프롬프트 정보(dynamic face authentication prompt information)를 전송하게 하는 단계와,

상기 사용자의 신원 인증 동안 상기 서버에 의해 전송된 상기 동적 얼굴 인증 프롬프트 정보를 수신하는 단계와,

상기 사용자에 의해 제시된 얼굴 제스처(facial gesture)를 인식함으로써 상기 동적 얼굴 인증 프롬프트 정보의 제스처 인식 정보(gesture recognition information)를 획득하는 단계와,

상기 제스처 인식 정보를 상기 서버로 전송하여, 상기 제스처 인식 정보가 상기 동적 얼굴 인증 프롬프트 정보와 일치한다고 검증되면, 상기 서버로 하여금 상기 사용자에 대한 신원 인증이 성공한 것으로 확인(confirm)하도록 하는 단계

를 포함하는 신원 인증 방법.

청구항 2

제1항에 있어서,

상기 사용자가 등록(registration)을 수행하는 경우 상기 사용자의 얼굴 특징 정보를 획득하고, 상기 등록 동안 획득된 상기 얼굴 특징 정보를 상기 사용자의 상기 제2 얼굴 특징 정보로서 사용하는 단계와,

상기 제2 얼굴 특징 정보를 상기 서버로 전송하여, 상기 서버로 하여금 상기 사용자의 사용자 이름과 상기 제2 얼굴 특징 정보 간의 대응 관계(correspondence)를 저장할 수 있게 하는 단계

를 더 포함하는 신원 인증 방법.

청구항 3

제1항에 있어서,

상기 얼굴 이미지가 상기 미리 설정된 특징 추출 조건을 만족시키는지를 판정하는 단계는,

상기 얼굴 이미지의 해상도가 미리 설정된 해상도 임계값(preset resolution threshold)을 만족시키는지를 판정하는 단계와,

상기 해상도 임계값이 만족되면 상기 얼굴 이미지로부터 머리 제스처 정보를 추출하는 단계- 상기 머리 제스처 정보는 머리 내리기/들기 각도, 얼굴 회전 각도 및 머리 기울기(head leaning) 각도 중 적어도 하나를 포함하는 것임 - 와,

상기 머리 제스처 정보에 포함된 각각의 각도가 각각의 미리 설정된 각도 범위 내에 속하는지를 판정하는 단계와,

상기 각각의 각도가 상기 각각의 미리 설정된 각도 범위 내에 속하는 경우 상기 얼굴 이미지가 상기 미리 설정된 특징 추출 조건을 만족시킨다고 판정하는 단계

를 포함하는 신원 인증 방법.

청구항 4

제1항에 있어서,

상기 사용자에 의해 제시된 얼굴 제스처를 인식함으로써 상기 동적 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 획득하는 단계는,

상기 사용자가 상기 동적 얼굴 인증 프롬프트 정보에 따라 얼굴 제스처를 제시하는 경우 상기 사용자의 상기 얼굴을 추적함으로써 얼굴 추적 정보(face tracking information)를 획득하는 단계와,

상기 얼굴 추적 정보를 분석하여 상기 사용자의 상기 제스처 인식 정보를 획득하는 단계

를 포함하는 신원 인증 방법.

청구항 5

제4항에 있어서,

상기 얼굴 추적 정보를 분석하여 상기 사용자의 상기 제스처 인식 정보를 획득하는 단계는,

상기 얼굴 추적 정보가 얼굴의 주요 지점 위치 정보(facial key point position information)인 경우, 상기 얼굴의 주요 지점 위치 정보를 분석함으로써 상기 사용자의 표정(expression) 제스처 인식 정보를 획득하는 단계, 또는

상기 얼굴 추적 정보가 머리 제스처 정보인 경우, 상기 머리 제스처 정보를 분석함으로써 상기 사용자의 머리 회전(head turning) 인식 정보를 획득하는 단계

를 포함하는 신원 인증 방법.

청구항 6

제1항 내지 제5항 중 어느 한 항에 있어서,

상기 동적 얼굴 인증 프롬프트 정보는 표정 동작 프롬프트 정보(expression action prompt information) 및 음성 판독 프롬프트 정보(voice read prompt information) 중 적어도 하나를 포함하는

신원 인증 방법.

청구항 7

제6항에 있어서,

상기 동적 얼굴 인증 프롬프트 정보는 상기 음성 판독 프롬프트 정보를 포함하고,

상기 제스처 인식 정보를 획득하는 단계는,

상기 사용자의 입 모양(mouth shapes)과 음성 정보(audio information)를 획득하는 단계와,

상기 음성 판독 프롬프트 정보를 판독하는 경우 상기 사용자의 하나 이상의 입 모양을 인식하고, 음성 인식을 통해 상기 음성 정보로부터 상기 사용자의 음성 정보를 획득하는 단계를 포함하되,

상기 하나 이상의 입 모양을 인식하고 상기 음성 정보를 획득하는 단계는 상기 제스처 인식 정보를 검증하는 경우 상기 서버로 하여금 상기 음성 정보가 상기 음성 판독 프롬프트 정보와 일치하는지를 판정하게 하고, 상기 음성 정보가 상기 음성 판독 프롬프트 정보와 일치하고 상기 제스처 인식 정보가 상기 동적 얼굴 인증 프롬프트 정보와 일치하는 것으로 검증되면 상기 사용자에 대한 상기 신원 인증이 성공한 것으로 판정되도록 하는

신원 인증 방법.

청구항 8

신원 인증 장치로서,

사용자의 얼굴 특징 정보를 획득하고, 신원 인증 동안 획득된 상기 얼굴 특징 정보를 상기 사용자의 제1 얼굴 특징 정보로서 사용하도록 구성된 획득 유닛(acquisition unit)- 상기 획득 유닛은,

상기 사용자의 얼굴이 검출되는 경우 상기 사용자의 상기 얼굴을 추적하도록 구성된 얼굴 추적 서브유닛(face tracking subunit)과,

상기 얼굴이 추적되는 경우 미리 설정된 시간 간격에 따라 얼굴 이미지를 획득하도록 구성된 이미지 획득 서브유닛(image acqusicion subunit)과,

상기 얼굴 이미지가 미리 설정된 특징 추출 조건을 만족하는지를 판정하도록 구성된 조건 판정 서브유닛(condition determination subunit)과,

상기 미리 설정된 특징 추출 조건이 만족되는 경우, 상기 얼굴 이미지로부터 상기 사용자의 상기 얼굴 특징 정보를 추출하도록 구성된 특징 추출 서브유닛(feature extraction subunit)을 포함함 -과,

상기 사용자의 신원 인증 동안 서버에 의해 전송된 동적 얼굴 인증 프롬프트 정보를 수신하도록 구성된 수신 유닛(receiving unit)과,

상기 사용자에 의해 제시된 얼굴 제스처를 인식함으로써 상기 동적 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 획득하도록 구성된 인식 유닛(recognition unit)과,

전송 유닛(sending unit)을 포함하되,

상기 전송 유닛은,

상기 사용자의 상기 제1 얼굴 특징 정보를 상기 서버로 전송하여, 상기 제1 얼굴 특징 정보가 저장된 상기 사용자의 제2 얼굴 특징 정보와 일치한다고 검증되면, 상기 서버로 하여금 상기 동적 얼굴 인증 프롬프트 정보를 전송하게 하고,

상기 제스처 인식 정보를 상기 서버로 전송하여, 상기 제스처 인식 정보가 상기 동적 얼굴 인증 프롬프트 정보와 일치한다고 검증되면, 상기 서버로 하여금 상기 사용자에 대한 신원 인증이 성공한 것으로 확인하게 하도록 구성되는

신원 인증 장치.

청구항 9

제8항에 있어서,

상기 인식 유닛은,

상기 동적 얼굴 인증 프롬프트 정보에 따라 상기 사용자가 상기 얼굴 제스처를 제시하는 경우 상기 사용자의 얼굴을 추적함으로써 얼굴 추적 정보를 획득하도록 구성된 얼굴 정보 획득 서브유닛(face information obtaining subunit)과,

상기 얼굴 추적 정보를 분석하여 상기 사용자의 상기 제스처 인식 정보를 획득하도록 구성된 얼굴 정보 분석 서브유닛(face information analysis subunit)

을 포함하는 신원 인증 장치.

청구항 10

제9항에 있어서,

상기 얼굴 정보 분석 서브유닛은,

상기 얼굴 추적 정보가 얼굴의 주요 지점 위치 정보(facial key point position information)인 경우 상기 얼굴의 주요 지점 위치 정보를 분석함으로써 상기 사용자의 표정 제스처 인식 정보(expression gesture recognition information)를 획득하도록 더 구성되거나,

상기 얼굴 추적 정보가 머리 제스처 정보인 경우 상기 머리 제스처 정보를 분석함으로써 상기 사용자의 머리 회전 인식 정보(head turning recognition information)를 획득하도록 더 구성되는

신원 인증 장치.

청구항 11

제8항에 있어서,

상기 획득 유닛은 사용자 등록 동안 상기 사용자의 얼굴 특징 정보를 획득하고, 상기 등록 동안 획득된 상기 얼굴 특징 정보를 상기 사용자의 상기 제2 얼굴 특징 정보로서 사용하도록 더 구성되며,

상기 전송 유닛은 상기 제2 얼굴 특징 정보를 상기 서버로 전송하여 상기 서버로 하여금 상기 사용자의 사용자 이름과 상기 제2 얼굴 특징 정보 간의 대응 관계를 저장하게 하도록 더 구성되는

신원 인증 장치.

청구항 12

제8항에 있어서,

상기 조건 판정 서브유닛은,

상기 얼굴 이미지의 해상도가 미리 설정된 해상도 임계값을 만족시키는지를 판정하도록 구성된 해상도 판정 모듈(resolution determination module)과,

상기 해상도 임계값이 만족되는 경우 상기 얼굴 이미지로부터 머리 제스처 정보를 추출하도록 구성된 제스처 정보 추출 모듈(gesture information extraction module)- 상기 머리 제스처 정보는 머리 내리기/들기 각도, 얼굴 회전 각도 및 머리 기울기 각도 중 적어도 하나를 포함함 - 과,

상기 머리 제스처 정보에 포함된 각각의 각도가 각각의 미리 설정된 각도 범위 내에 속하는지를 판정하도록 구성된 각도 판정 모듈(angle determination module)과,

상기 각각의 각도가 상기 각각의 미리 설정된 각도 범위 내에 속하는 경우, 상기 얼굴 이미지는 상기 특징 추출 조건을 만족시킨다고 판정하도록 구성된 판단 판정 모듈(judgement determination module)

을 포함하는 신원 인증 장치.

청구항 13

단말기로서,

하나 이상의 프로세서와,

상기 하나 이상의 프로세서에 의해 실행 가능한 명령어를 저장하도록 구성된 메모리를 포함하되,

상기 하나 이상의 프로세서는,

사용자의 얼굴 특징 정보를 획득하고- 상기 사용자의 상기 얼굴 특징 정보를 획득하는 것은,

상기 사용자의 얼굴이 검출되면 상기 사용자의 상기 얼굴을 추적하는 것과,

상기 얼굴을 추적하는 경우 미리 설정된 시간 간격에 따라 얼굴 이미지를 획득하는 것과,

상기 얼굴 이미지가 미리 설정된 특징 추출 조건(preset feature extraction condition)을 만족시키는지를 판정하는 것과,

상기 미리 설정된 특징 추출 조건이 만족되면 상기 얼굴 이미지로부터 상기 사용자의 상기 얼굴 특징 정보를 추출하는 것을 포함함 -,

상기 얼굴 특징 정보를 상기 사용자의 제1 얼굴 특징 정보로서 사용하며,

상기 사용자의 상기 제1 얼굴 특징 정보를 서버로 전송하여, 상기 제1 얼굴 특징 정보가 저장된 상기 사용자의 제2 얼굴 특징 정보와 일치한다고 검증되면 상기 서버로 하여금 동적 얼굴 인증 프롬프트 정보를 전송하도록 하고,

상기 사용자의 신원 인증 동안 상기 서버에 의해 전송된 상기 동적 얼굴 인증 프롬프트 정보를 수신하며,

상기 사용자에 의해 제시된 얼굴 제스처를 인식함으로써 상기 동적 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 획득하며,

상기 제스처 인식 정보를 상기 서버로 전송하여 상기 제스처 인식 정보가 상기 동적 얼굴 인증 프롬프트 정보와 일치한다고 검증되면, 상기 서버로 하여금 상기 사용자가 신원 인증을 통과한 것으로 확인하도록 구성되는

단말기.

청구항 14

제13항에 있어서,

상기 얼굴 이미지가 상기 미리 설정된 특징 추출 조건을 만족시키는지를 판정하는 것은,

상기 얼굴 이미지의 해상도가 미리 설정된 해상도 임계값을 만족시키는지를 판정하는 것과,

상기 해상도 임계값이 만족되면 상기 얼굴 이미지로부터 머리 제스처 정보를 추출하는 것 - 상기 머리 제스처 정보는 머리 내리기/들기 각도, 얼굴 회전 각도 및 머리 기울기(head leaning) 각도 중 적어도 하나를 포함함 - 과,

상기 머리 제스처 정보에 포함된 각각의 각도가 각각의 미리 설정된 각도 범위 내에 속하는지를 판정하는 것과,

상기 각각의 각도가 상기 각각의 미리 설정된 각도 범위 내에 속하는 경우 상기 얼굴 이미지가 상기 특징 추출 조건을 만족시킨다고 판정하는 것을 포함하는

단말기.

청구항 15

제13항에 있어서,

상기 동적 얼굴 인증 프롬프트 정보는 음성 판독 프롬프트 정보를 포함하고,

상기 제스처 인식 정보를 획득하는 것은,

상기 사용자의 입 모양과 음성 정보를 획득하는 것과,

상기 음성 판독 프롬프트 정보를 판독하는 경우 상기 사용자의 하나 이상의 입 모양을 인식하고 음성 인식을 통해 상기 음성 정보로부터 상기 사용자의 음성 정보를 획득하는 것을 포함하되,

상기 하나 이상의 입 모양을 인식하고 상기 음성 정보를 획득하는 것은 상기 제스처 인식 정보를 검증하는 경우 상기 서버로 하여금 상기 음성 정보가 상기 음성 판독 프롬프트 정보와 일치하는지를 판정하도록 하고, 상기 음성 정보가 상기 음성 판독 프롬프트 정보와 일치하고 상기 제스처 인식 정보가 상기 동적 얼굴 인증 프롬프트 정보와 일치하는 것으로 검증되면 상기 사용자에 대한 상기 신원 인증이 성공한 것으로 판정되도록 하는

단말기.

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

발명의 설명

기 술 분 야

[0001] 본 출원은 통신 기술 분야에 관한 것으로서, 특히 신원(identity) 인증(authentication) 방법 및 장치(apparatuses), 단말기 및 서버에 관한 것이다.

배 경 기 술

[0002] 지능형 단말기의 성장 및 네트워크 애플리케이션의 발전에 따라, 사용자는 단말기에 설치된 다양한 유형의 애플리케이션 클라이언트 단말기를 통해 소셜형(social-type) 인스턴트 통신 애플리케이션 및 쇼핑형(shopping-type) 애플리케이션과 같이 다양한 유형의 네트워크 애플리케이션에 액세스할 수 있다. 액세스하는 동안, 일반적으로 사용자의 신원이 인증되어야 하므로, 사용자는 신원 인증이 성공한 후에 다양한 애플리케이션 기능을 사용할 수 있게 된다.

[0003] 종래의 기술에서 사용자는 신원 인증 과정 동안 통상적으로 인증 인터페이스에 인증 암호를 입력해야 했고, 서버는 사용자 등록 과정 동안 입력된 인증 암호가 인증 암호와 동일하다는 것이 검증(verifying)되면 사용자가 신원 인증을 통과한 것으로 확인한다(confirm). 그러나 인증 암호는 일반적으로 숫자와 문자의 간단한 조합이며 악의적인 제3자에 의해 쉽게 도용당한다. 따라서, 신원 인증 모드의 종래의 방법은 신뢰성이 비교적 낮고 사용자 정보를 도용당하기 쉬워서 취약한 인증 보안을 초래한다.

발명의 내용

[0004] 본 출원은 신원 인증을 위한 방법, 장치, 단말기 및 서버를 제공하여, 종래의 기술에서 신원 인증 방법의 취약한 신뢰성과 낮은 보안성이라는 문제점을 해결하고자 한다.

[0005] 본 출원의 실시예의 제1 양태(aspect)에 따르면, 신원 인증 방법이 제공된다. 해당 방법은, 사용자의 신원 인증이 수행되는 경우 서버에 의해 전송된 동적 인간 얼굴 인증 프롬프트 정보를 수신하는 단계, 사용자에 의해 제시된 얼굴 제스처를 인식하여 동적 인간 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 획득하는 단계, 제스처 인식정보를 서버로 전송하여 제스처 인식 정보가 동적 인간 얼굴 인증 프롬프트 정보와 일치한다고 검증(verifying)되면, 서버로 하여금 사용자의 신원 인증이 성공한 것으로 확인할 수 있도록 하는 단계를 포함한다.

[0006] 본 출원의 실시예의 제2 양태에 따르면, 신원 인증 방법이 제공된다. 해당 방법은, 사용자의 신원 인증이 수행되는 경우 동적 인간 얼굴 인증 프롬프트 정보를 단말기로 전송하는 단계와, 단말기에 의해 전송된 제스처 인식 정보를 수신하는 단계(제스처 인식 정보는 동적 인간 얼굴 인증 프롬프트 정보에 따라 사용자에 의해 제시된 얼굴 제스처 인식을 통해 단말기에 의해 획득된 제스처 인식 정보임)와, 제스처 인식 정보가 동적 인간 얼굴 인증 프롬프트 정보와 일치한다고 검증되면, 사용자의 신원 인증이 성공한 것으로 판정하는 단계를 포함한다.

[0007] 본 출원의 실시예의 제3 양태에 따르면, 신원 인증 장치가 제공된다. 해당 장치는, 사용자의 신원 확인이 수행되는 경우 서버에 의해 전송된 동적 인간 얼굴 인증 프롬프트 정보를 수신하도록 구성되는 수신 유닛과, 사용자에 의해 제시된 얼굴 제스처를 인식하여 동적 인간 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 획득하도록 구성되는 인식 유닛과, 제스처 인식 정보를 서버로 전송하여 제스처 인식 정보가 동적 인간 얼굴 인증 프롬프트 정보와 일치한다고 검증되면, 서버로 하여금 사용자의 신원 인증이 성공한 것으로 확인할 수 있도록 구성되는 전송 유닛을 포함한다.

[0008] 본 출원의 실시예의 제4 양태에 따르면, 신원 인증 장치가 제공된다. 해당 장치는, 사용자의 신원 인증이 수행되는 경우 동적 인간 얼굴 인증 프롬프트 정보를 단말기로 전송하도록 구성된 전송 유닛과, 단말기에 의해 획득된 제스처 인식 정보를 수신하도록 구성되는 수신 유닛(제스처 인식 정보는 동적 인간 얼굴 인증 프롬프트 정보에 따라 사용자에 의해 제시되는 얼굴 제스처를 인식하여 단말기에 의해 획득된 제스처 인식 정보임)과, 제스처 인식 정보가 동적 인물 얼굴 인증 프롬프트 정보와 일치한다고 검증되면, 사용자의 신원 인증이 성공한 것으로 판정하도록 구성된 판정 유닛을 포함한다.

[0009] 본 출원의 실시예의 제5 양태에 따르면, 단말기가 제공되는데, 해당 단말기는, 프로세서(들) 및 프로세서(들)에 의해 실행 가능한 명령을 저장하도록 구성된 메모리를 포함하며, 프로세서(들)는 사용자의 신원 확인이 수행되는 경우 서버에 의해 전송된 동적 인간 얼굴 인증 프롬프트 정보를 수신하고, 사용자의 얼굴 제스처를 인식하여 동적 인물 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 획득하며, 제스처 인식 정보를 서버로 전송하여 제스처 인식 정보가 동적 인간 얼굴 인증 프롬프트 정보와 일치한다고 검증되면, 서버로 하여금 사용자의 신원 인증이 성공한 것으로 확인할 수 있도록 구성된다.

[0010] 본 출원의 실시예의 제6 양태에 따르면, 서버가 제공되는데, 해당 서버는, 프로세서(들) 및 프로세서(들)에 의해 실행 가능한 명령을 저장하도록 구성된 메모리를 포함하며, 프로세서(들)는 사용자의 신원 인증이 수행되는 경우 단말기로 동적 인간 얼굴 인증 프롬프트 정보를 전송하고, 제스처 인식 정보를 단말기로부터 수신하며(제스처 인식 정보는 동적 인간 얼굴 인증 프롬프트 정보에 따라 사용자가 제시한 얼굴 제스처를 인식하여 단말기

에 의해 획득된 제스처 인식 정보임), 제스처 인식 정보가 동적 얼굴 인증 프롬프트 정보와 일치한다고 검증하는 즉시 사용자의 신원 인증이 성공한 것으로 판정하도록 구성된다.

[0011] 본 출원의 실시예에서, 사용자에 대해 신원 인증이 수행되는 경우, 서버는 단말기에 동적 인증 프롬프트 정보를 전송한다. 단말기는 사용자가 제시하는 얼굴 제스처를 인식하여 동적 인간 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 획득하고, 제스처 인식 정보를 서버로 전송한다. 서버는 제스처 인식 정보가 동적 인간 얼굴 인증 프롬프트 정보와 일치함을 확인하면 사용자 신원의 인증이 성공한 것으로 판정한다. 본 출원의 실시예를 사용함으로써, 동적 인간 얼굴 인증을 사용하여 높은 보안성을 갖는 사용자 인증을 수행할 수 있다. 인증 암호를 사용하는 기존 인증 방법과 비교하면 악의적인 제3자에 의해 인증 정보를 도용당하지 않으므로 인증의 신뢰성을 향상시킨다. 또한, 사용자는 동적 인간 얼굴 인증을 통해 실제 사용자로 인식될 수 있으므로 인증 과정 동안 신원 인증의 정확성을 향상시키고 잠재적인 보안 위험을 감소시킨다.

도면의 간단한 설명

[0012] 도 1은 본 출원의 실시예에 따른 신원 인증 시나리오의 개략도이다.

도 2a는 본 출원에 따른 신원 인증 방법의 예시적인 흐름도이다.

도 2b는 본 출원에 따른 다른 예시적인 신원 인증 방법의 흐름도이다.

도 3a는 본 출원에 따른 다른 예시적인 신원 인증 방법의 흐름도이다.

도 3b는 본 출원의 실시예에서 인간 얼굴 인증 과정 동안 인간 머리 제스처의 개략도이다.

도 4a는 본 출원에 따른 다른 예시적인 신원 인증 방법의 흐름도이다.

도 4b와 도 4c는 본 출원의 실시예에서 얼굴의 주요 지점의 개략도이다.

도 5는 본 출원에 따른 신원 인증 장치가 위치하는 디바이스의 하드웨어를 도시하는 구조도이다.

도 6은 본 출원에 따른 예시적인 신원 인증 장치의 블록도이다.

도 7은 본 출원에 따른 다른 예시적인 신원 인증 장치의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 예시적인 실시예들이 본 명세서에서 상세히 설명될 것이며, 그 예들은 첨부 도면들에 표정된다. 다음 설명이 첨부 도면을 포함하는 경우, 다르게 특정되지 않는 한, 상이한 첨부 도면에서 동일한 번호는 동일하거나 유사한 요소를 나타낸다. 다음의 예시적인 실시예들에서 설명된 구현들은 본 출원과 일치하는 모든 구현을 나타내는 것은 아니다. 오히려 구현들은 단지 첨부된 청구범위에서 상세히 설명된 대로 본 출원의 일부 양태와 일치하는 장치 및 방법의 예들에 불과하다.

[0014] 본 출원에 사용된 용어는 본 출원을 한정하는 것이 아니라 특정 실시예를 설명하기 위해 사용된 것이다. 본 출원 및 첨부된 청구범위에서 사용된 단수 형태 "한", "그" 및 "상기"는 문맥상 다른 의미를 명확히 나타내지 않는 한 복수 형태를 포함하도록 의도된다. 이에 더해 본 명세서에서 사용된 "및/또는"이라는 용어는 열거된 하나 이상의 관련 항목의 임의의 또는 모든 가능한 조합을 가리키고 포함하는 것으로 이해해야 한다.

[0015] "제1", "제2" 및 "제3"과 같은 용어가 본 출원의 다양한 유형의 정보를 설명하는 데 사용될 수 있지만, 이러한 정보는 이들 용어에 의해 제한되지 않는다는 것을 이해해야 한다. 이러한 용어들은 동일한 유형의 정보를 서로 구별하기 위해 사용된다. 예를 들어, 본 출원의 범위를 벗어나지 않으면서, 제1 정보는 제2 정보로 지칭될 수 있고, 유사하게, 제2 정보는 대신 제1 정보로 지칭될 수 있다. 문맥에 따라, 본문에 사용된 "~한다면(if)"은 "~하는 경우(when)", "~하는 동안(while)" 또는 "~라는 판정에 응답하여(in response to determining that)"로 해석될 수 있다.

[0016] 인터넷 기반(internet-based) 통신 시나리오에서, 사용자는 자신의 단말기에 설치된 다양한 유형의 애플리케이션 단말기를 통해 다양한 유형의 네트워크 애플리케이션에 액세스할 수 있다. 액세스 프로세스 중에 사용자의 신원은 통상적으로 인증되어야 한다. 그러나 종래의 기술에서 사용자의 신원은 일반적으로 인증 암호를 통해 인증되며 인증 암호는 일반적으로 숫자와 문자의 간단한 조합이어서 악의적인 제3자에 의해 쉽게 도용당한다. 그러므로 기존의 신원 인증 방법은 상대적으로 신뢰성이 떨어지며 보안이 취약하다. 따라서, 본 출원의 실시예에 따른 신원 인증을 구현하기 위한 응용 시나리오의 개략도인 도 1을 참조하여, 사용자에 대한 신원 인증은 사

용자에 의해 보유된 단말기와 서버 간의 상호 작용을 통해 완료된다. 단말기와 서버 간의 통신은 네트워크에 기초하여 완료될 수 있다. 네트워크는 다양한 형태의 무선 네트워크나 유선 네트워크를 포함하며, 본 출원의 실시예에 한정되지 않는다. 단말기는 이동 전화, 태블릿 컴퓨터, 개인용 컴퓨터 등일 수 있다. 도 1에 도시된 애플리케이션 시나리오에서, 서버에는 두 데이터베이스, 인간 얼굴 특징 정보 데이터베이스 및 동적 인간 얼굴 인증 프롬프트 정보 데이터베이스가 각각 배치될 수 있다.

[0017] 얼굴 등록 단계에서, 단말기는 등록된 사용자의 인간 얼굴 특징 정보를 획득할 수 있으며, 이는 서버에 전송된다. 서버는 등록된 사용자의 인간 얼굴 특징 정보를 얼굴 특징 정보 데이터베이스에 저장한다. 신원 인증 단계에서는 인간 얼굴 인증이 먼저 수행될 수 있다. 이 시점에서 사용자는 획득된 인간 얼굴 특징 정보를 서버로 전송한다. 해당 인간 얼굴 특징 정보가 얼굴 특징 정보 데이터에 저장된 사용자의 인간 얼굴 특징 정보와 일치한다고 검증되면, 서버는 사용자 본인에 대해 현재 신원 인증이 수행되고 있음을 예비적으로 판정할 수 있다. 그 후 동적 인간 얼굴 인증이 수행된다. 이 시점에서, 서버는 동적 인간 얼굴 인증 프롬프트 정보 데이터베이스로부터 획득된 동적 인간 얼굴 인증 프롬프트 정보를 사용자에게 반환할 수 있다. 단말기는 동적 인간 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 얻기 위해 사용자가 제시한 인간 얼굴 제스처를 인식하여 제스처 인식 정보를 서버로 전송한다. 제스처 인식 정보가 동적 인간 얼굴 인증 프롬프트 정보와 일치한다고 확인되면, 서버는 현재 인증되는 사용자가 실제 사용자임을 알게 되고, 그로 인해 마침내 사용자의 신원 인증이 성공한 것으로 판정한다. 설명의 편의상, 본 출원의 실시예에서는, 얼굴 등록 단계에서 획득된 사용자의 인간 얼굴 특징 정보를 제2 인간 얼굴 특징 정보라고 하고, 얼굴 인증 단계에서 획득한 사용자의 인간 얼굴 특징 정보를 제1 인간 얼굴 특징 정보라고 한다. 본 출원의 실시예들이 아래에서 상세하게 설명된다.

[0018] 도 2a는 본 출원에 따른 신원 인증 방법의 실시예의 흐름도이다. 해당 실시예는 신원 인증을 구현하는 단말기의 관점에서 설명된다.

[0019] 단계(201)는 사용자의 신원 인증 과정 동안 서버에 의해 전송된 동적 인간 얼굴 인증 프롬프트 정보를 수신한다.

[0020] 본 출원의 실시예에서, 서버는 동적 인간 얼굴 인증 프롬프트 정보 데이터로부터 동적 인간 얼굴 인증 프롬프트 정보를 무작위로 추출하고, 동적 인간 얼굴 인증 프롬프트 정보를 단말기로 반환할 수 있다. 동적 인간 얼굴 인증 프롬프트 정보는 눈(들) 감기, 입 벌리기나 머리 돌리기와 같은 표정 동작 프롬프트 정보 또는 "20달러를 지불하라"와 같은 음성 판독(voice read) 프롬프트 정보 중 적어도 한 유형을 포함할 수 있다.

[0021] 또는, 서버로부터 동적 인간 얼굴 인증 프롬프트 정보를 수신하기에 앞서, 단말기는 먼저 사용자의 인간 얼굴 특징 정보를 획득하고, 신원 인증 과정 동안 획득된 인간 얼굴 특징 정보를 사용자의 제1 인간 얼굴 정보로서 사용할 수 있다. 사용자의 제1 인간 얼굴 특징 정보가 서버로 전송된 후, 서버는 저장된 제2 얼굴 특징 정보와 제1 인간 얼굴 특징 정보가 일치한다고 검증되면 동적 인간 얼굴 인증 프롬프트 정보를 단말기로 전송한다.

[0022] 사용자의 인간 얼굴 특징 정보를 획득하는 경우, 단말기는 카메라와 같이 그에 부착된 통합 이미징 디바이스를 시동하여 사용자의 인간 얼굴을 검출하고, 인간 얼굴이 검출되는 경우에 사용자의 인간 얼굴을 추적할 수 있다. 인간 얼굴 추적 과정 동안, 단말기는 미리 설정된 시간 간격에 따라 인간 얼굴 이미지를 획득하고, 획득된 각각의 얼굴 이미지에 대해 각각의 얼굴 이미지가 미리 설정된 특징 추출 조건을 충족시키는지를 판정하며, 그 얼굴 이미지가 특징 추출 조건을 충족시키는 경우에 그 얼굴 이미지로부터 사용자의 인간 얼굴 특징 정보를 추출한다.

[0023] 사용자의 제1 인간 얼굴 특징 정보를 수신한 후, 서버는 사용자의 사용자 이름에 기초하여 얼굴 특징 정보 데이터베이스를 검색하여 사용자 이름에 대응하는 제2 얼굴 특징 정보를 획득할 수 있고, 그 후 사전 정의된 비교 접근법을 사용하여 제1 인간 얼굴 특징 정보를 제2 인간 얼굴 특징 정보와 비교할 수 있다. 특징 비교 값이 미리 설정된 유사도 범위 내에 속하면, 제1 인간 얼굴 특징 정보가 제2 얼굴 특징 정보와 일치하는 것으로 판정될 수 있다. 제1 인간 얼굴 특징 정보가 제2 인간 얼굴 특징 정보와 일치한다는 판정에 응답하여, 사용자에 대해 인간 얼굴 인증이 성공한 것으로 판정될 수 있다. 이 경우, 서버는 동적 인간 얼굴 인증 프롬프트 정보를 단말기로 전송한다.

[0024] 단계(202)는 사용자에 의해 제시된 얼굴 제스처를 인식하여 동적 인간 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 획득한다.

[0025] 본 발명의 실시예에서, 단말기는 동적 인간 얼굴 인증 프롬프트 정보를 수신한 후에, 신원 인증 인터페이스에 동적 인간 얼굴 인증 프롬프트 정보를 디스플레이한다. 사용자는 정보에 따라 대응하는 인간 얼굴 제스처를 제

시할 수 있다. 인간 얼굴 제스처를 인식하는 경우, 단말기는 사용자의 인간 얼굴을 추적하여 인간 얼굴 추적 정보를 획득할 수 있다. 인간 얼굴 추적 정보는 얼굴의 주요 지점 위치 정보(facial key point position information)와 인간 머리 제스처 정보(human head gesture information) 중 적어도 하나를 포함할 수 있다. 그 후 단말기는 인간 얼굴 추적 정보를 분석하여 사용자의 제스처 인식 정보를 획득한다. 예를 들어, 얼굴의 주요 지점 위치 정보를 통해, 표정 동작 프롬프트 정보에 따라 사용자가 눈을 감을지 입을 열지 여부를 알 수 있거나, 음성 판독 프롬프트 정보를 읽는 경우 사용자의 입 모양을 알 수 있다(각 단어의 발음과 입 모양의 대응 관계가 존재하고, 입 모양에 기초하여 사용자의 제스처 인식 정보가 판정될 수 있다). 또한, 머리 제스처 정보를 통해 사용자가 머리를 돌리는지, 머리를 내리는지 등을 알 수 있다.

[0026] 단계(203)는 제스처 인식 정보를 서버로 전송하여, 제스처 인식 정보가 동적 인간 얼굴 인증 프롬프트 정보와 일치한다고 검증되면, 서버로 하여금 사용자에 대해 신원 인증이 성공한 것으로 확인하도록 할 수 있다.

[0027] 서버는 한 번에 여러 사용자에 대해 신원 인증을 수행해야 할 수 있다. 타인의 동적 인증 프롬프트 정보 일부가 다른 사용자에게 전송된 경우, 서버는 단계(201)에서 그 동적 인간 얼굴 인증 프롬프트 정보를 단말기로 전송한 후 사용자의 사용자 이름과 동적 인간 얼굴 인증 프롬프트 정보 간의 대응 관계를 기록할 수 있다. 이 단계에서 단말기가 제스처 인식 정보를 서버로 전송한 후 서버는 사용자의 사용자 이름에 따라 대응하는 동적 인간 얼굴 인증 프롬프트 정보를 획득하고 제스처 인식 정보가 동적 인간 얼굴 인증 프롬프트 정보와 일치한다고 검증한다. 이는 사용자가 실제 사용자임을 나타내며, 이 경우 사용자에 대해 신원 인증이 성공한 것으로 판정된다.

[0028] 또한, 단계(201)에서 동적 인간 얼굴 인증 프롬프트 정보가 음성 판독 프롬프트 정보인 경우, 단말기는 사용자의 입 모양뿐만 아니라 사용자의 음성 정보도 획득할 수 있다. 음성 정보의 음성 인식을 통해 사용자에 의해 판독된 음성 정보를 얻음으로써 서버는 음성 정보가 음성 판독 프롬프트 정보와 일치하는지를 비교할 수 있고, 이들이 일치한다면 사용자에 대해 신원 인증이 성공한 것으로 판정할 수 있다.

[0029] 도 2b는 본 출원에 따른 신원 인증 방법의 다른 실시예의 흐름도이다. 해당 실시예는 신원 인증을 구현하는 서버의 관점에서 설명된다.

[0030] 단계(211)는 사용자의 신원 인증이 수행될 때 동적 인간 얼굴 인증 프롬프트 정보를 단말기로 전송한다.

[0031] 단계(212)는 단말기에 의해 전송된 제스처 인식 정보를 수신하며, 해당 제스처 인식 정보는 동적 인간 얼굴 인증 프롬프트 정보에 따라 사용자에 의해 제시된 인간 얼굴 제스처 인식을 통해 단말기에 의해 획득된 제스처 인식 정보이다.

[0032] 단계(213)는 제스처 인식 정보가 동적 인간 얼굴 인증 프롬프트 정보와 일치한다고 검증되면, 사용자의 신원 인증이 성공한 것으로 판정한다.

[0033] 도 2b에 도시된 신원 인증 프로세스와 도 2a에 도시된 신원 인증 프로세스 간의 유일한 차이점은 실행 개체(entities)의 차이이다. 구체적으로, 도 2a는 단말기의 관점에서 설명되고, 도 2b는 서버의 관점에서 설명된다. 따라서, 도 2b의 실시예에서 관련된 구현 프로세스는 전술한 도 2a의 설명이 참조될 수 있으며, 본 명세서에서 반복하여 설명되지는 않는다.

[0034] 전술한 실시예에서 알 수 있듯이, 해당 실시예는 동적 인간 얼굴 인증에 의해 높은 보안성을 갖는 사용자 신원 인증을 수행할 수 있다. 인증 암호를 사용하는 기존 인증 방법과 비교하면 악의적 제3자에 의해 인증 정보를 도용당하지 않으므로 인증의 신뢰도가 향상된다. 또한, 사용자가 동적 인간 얼굴 인증을 통해 실제 사용자로 인식됨으로써 인증 과정 동안 신원 인증의 정확성을 더 향상시키고 잠재적 보안 위험을 감소시킬 수 있다.

[0035] 도 3a는 본 출원에 따른 신원 인증 방법의 또 다른 실시예이다. 해당 실시예는 인간 얼굴 등록 프로세스를 상세히 설명한다.

[0036] 단계(301): 사용자는 단말기를 통해 서버에 등록한다.

[0037] 단계(302): 단말기는 사용자의 인간 얼굴이 검출될 때 사용자의 인간 얼굴을 추적한다.

[0038] 통상적으로 카메라와 같은 이미징 디바이스는 단말기에 통합되어 있다. 해당 실시예에서, 이미징 디바이스는 자동으로 시작하도록 설정되어 사용자 등록 과정 동안 사용자의 인간 얼굴을 검출할 수 있다. 일반적으로, 사용자는 단말기를 손으로 들고 이미징 디바이스를 사용자의 얼굴과 정렬시킬 수 있다. 이미징 디바이스를 통해 얼굴이 검출되면, 단말기는 인간 얼굴 추적 알고리즘에 따라 사용자의 얼굴을 추적할 수 있다. 본 출원의 이러

한 실시예는 본 명세서에서 상세히 설명되지 않은 다양한 유형의 종래의 얼굴 추적 알고리즘을 사용할 수도 있음에 주의해야 한다.

[0039] 단계(303): 단말기는 얼굴 추적 과정 동안 미리 설정된 시간 간격에 따라 얼굴 이미지를 획득한다.

[0040] 얼굴 추적 과정 동안, 단말기는 이미징 디바이스를 사용하여 미리 설정된 시간 간격에 따라 얼굴 이미지를 획득한다. 시간 간격은 실질적으로 동일한 얼굴 이미지의 추출을 방지하도록 설정된다. 예를 들어, 미리 설정된 시간 간격은 3초일 수 있다.

[0041] 단계(304): 얼굴 이미지의 해상도가 미리 설정된 해상도 임계값을 만족시키는지에 대한 판정이 이루어진다. 만족시키면, 단계(305)가 수행된다. 그렇지 않으면 현재 프로세스가 종료된다.

[0042] 단계(303)에서 획득된 얼굴 이미지의 해상도는 불충분한 해상도를 갖는 얼굴 이미지를 제거하기 위해 먼저 검사될 수 있다. 이 경우, 단말기는 미리 설정된 퍼지 판정 기능을 작동하여 해당 얼굴 이미지의 해상도가 해상도 임계값을 만족시키는지를 판정할 수 있다. 이 퍼지 판정 기능에는 종래의 이미지 인식 프로세싱 기술에서의 퍼지 판정 기능이 사용될 수 있지만, 본 출원의 실시예에서는 이에 한정되지 않는다. 해상도 임계값을 만족시키는 얼굴 이미지에 대해, 단계(305)가 수행된다. 해상도 임계값을 만족시키지 못하는 얼굴 이미지는 바로 폐기되고, 그 후 단계(303)로 되돌아간다.

[0043] 단계(305): 단말기는 얼굴 이미지로부터 머리 제스처 정보를 추출한다.

[0044] 단계(304)에서, 획득된 얼굴 이미지가 깨끗한 얼굴 이미지라고 판정한 후, 단말기는 얼굴 이미지로부터 머리 제스처 정보를 추출한다. 도 3b는 본 출원의 실시예의 머리 제스처의 개략도를 도시한다. 본 실시예의 머리 제스처 정보는 머리 내리기/들기 각도, 얼굴 돌리기 각도 및 머리 기울기 각도 중 적어도 하나를 포함할 수 있다.

[0045] 단계(306): 단말기는 제스처 정보에 포함된 각각의 각도가 각각의 미리 설정된 각도 범위 내에 속하는지를 판정한다. 속한다면, 단계(307)가 수행된다. 그렇지 않으면 현재 프로세스가 종료된다.

[0046] 본 출원의 실시예에서, 머리 제스처 정보를 통해 얼굴 이미지가 사용자의 얼굴 전면부 이미지인지 여부에 대한 판정이 이루어질 수 있다. 이 시점에서, 단말기는 머리 제스처 정보에 포함된 각각의 각도가 각각의 미리 설정된 각도 범위 내에 속하는지를 판정할 수 있다. 예를 들어 미리 설정된 각도 범위는 0 ~ 10도이다. 판정 결과가 긍정인(positive) 머리 제스처 정보에 대응하는 얼굴 이미지에 대해, 단계(307)이 수행된다. 판정 결과가 부정인(negative) 머리 제스처 정보에 대응하는 얼굴 이미지는 바로 폐기되고, 그 후 단계(303)로 되돌아간다.

[0047] 단계(307): 단말기는 얼굴 이미지로부터 사용자의 얼굴 특징 정보를 추출한다.

[0048] 본 출원의 해당 실시예에서, LBP(Linear Back Projection) 특징 추출 알고리즘이 사용되어 사용자의 얼굴 특징(들) 정보로서 얼굴 이미지로부터 얼굴 특징 벡터 값(들)을 추출할 수 있다. 명백하게, 본 출원의 이러한 실시예는 얼굴 특징 추출을 위한 특정 알고리즘에 어떠한 제한도 부과하지 않는다. 윈도우 푸리에 변환(windowed Fourier transform) 등에서의 가버(Gabor) 특징 추출 알고리즘과 같이, 임의의 기존 이미지 프로세싱 기술에 사용되는 임의의 얼굴 특징 추출 알고리즘이 본 출원의 실시예에 적용될 수 있다.

[0049] 얼굴 인증의 후속 단계에서 얼굴 인증의 정확성을 보장하기 위해, 얼굴 등록 단계 동안 등록된 동일 사용자에 대한 복수의 얼굴 이미지로부터 사용자의 얼굴 특징 정보가 추출될 수 있다. 얼굴 이미지의 수는 예컨대 5일 수 있다. 이에 응답하여, 설정된 얼굴 이미지의 수에 따라, 전술한 단계(303) 내지 단계(307)를 반복 수행하여, 미리 설정된 수를 만족시키는 여러 얼굴 이미지를 획득하고, 그로부터 얼굴 특징 정보를 추출할 수 있다.

[0050] 단계(308): 단말기는 얼굴 특징(들) 정보를 서버로 전송한다.

[0051] 단계(309): 서버는 등록된 사용자의 사용자 이름과 얼굴 특징(들) 사이의 대응 관계를 저장하고, 현재의 프로세스는 종료된다.

[0052] 해당 실시예에서, 서버는 단말기로부터 얼굴 특징(들) 정보를 수신한 후에, 등록된 사용자의 사용자 이름과 얼굴 특징(들) 사이의 대응 관계를 얼굴 특징 정보 데이터베이스에 저장하고, 복수의 얼굴 특징 정보를 수신하는 경우 사용자 이름과 복수의 얼굴 특징 정보 사이의 대응 관계를 저장한다.

[0053] 도 4a는 본 출원에 따른 신원 인증 방법의 다른 실시예이다. 해당 실시예는 도 3에 도시된 바와 같이 얼굴 등록 프로세스에 기초하여 사용자의 신원을 상세하게 인증하는 프로세스를 설명한다.

[0054] 단계(401): 사용자의 신원 인증이 시작된다.

[0055] 단계(402): 단말기는 사용자의 제1 얼굴 특징 정보를 획득한다.

[0056] 신원 인증 과정 동안, 단말기는 전술한 도 3에 도시된 바와 같이 얼굴 등록 프로세스에서 얼굴 특징 정보를 획득하는 접근법과 동일한, 그리고 구체적으로는 도 3에 도시된 바와 같이 단계(302)에서 단계(307)까지와 동일한 접근법을 사용하여 사용자의 얼굴 특징 정보를 획득한다. 그 상세한 설명은 본 명세서에서 반복하여 기술되지는 않는다.

[0057] 이 단계에서, 단말기는 적어도 하나의 제1 얼굴 특징 정보를 획득할 수 있다.

[0058] 단계(403): 단말기는 사용자의 제1 얼굴 특징 정보를 서버로 전송한다.

[0059] 단계(404): 서버는 저장된 사용자의 제2 얼굴 특징 정보와 제1 얼굴 특징 정보가 일치하는지를 검증한다. 일치하면, 단계(405)가 수행된다. 그렇지 않으면 현재 프로세스가 종료된다.

[0060] 본 출원의 해당 실시예에서, 서버는 사용자의 제1 얼굴 특징 정보를 수신한 후 사용자의 사용자 이름에 기초해서 얼굴 특징 정보 데이터베이스를 검색하여 사용자 이름에 대응하는 제2 얼굴 특징 정보를 얻고, 그 후 제1 얼굴 특징 정보와 제2 얼굴 특징 정보를 미리 설정된 비교 방식으로 비교할 수 있다. 특징 비교 값이 미리 설정된 유사도 범위 내에 속하는 경우, 제1 얼굴 특징 정보가 제2 얼굴 특징 정보와 일치한다고 판정될 수 있다.

[0061] 본 출원의 해당 실시예에서 얼굴 특징 정보는 예컨대 LBP 알고리즘을 통해 추출된 얼굴 특징 벡터라고 한다.

[0062] 일례로, 제1 얼굴 특징 정보 및 제2 얼굴 특징을 비교를 위해 유클리드 거리(Euclidean distances) 비교법이 사용될 수 있다. 이 경우, 제2 얼굴 특징 벡터와 제1 얼굴 특징 벡터 간의 차의 제곱의 합이 계산된다. 제곱의 합이 미리 설정된 임계값보다 작은 경우, 신원 인증이 사용자 본인에 대해 수행되는 것으로 판정될 수 있다.

[0063] 다른 예에서, 제1 얼굴 특징 정보와 제2 얼굴 특징을 비교를 위해 코사인 거리 비교법이 사용될 수 있다. 제1 얼굴 특징 벡터가 V1이고 제2 얼굴 특징 벡터가 V2인 경우, V2*V1 / (|V1|*|V2|)라는 수식 값(formula value)이 계산될 수 있다. 수식 값이 미리 설정된 임계값보다 크면, 신원 인증이 사용자 본인에 대해 수행되는 것으로 판정될 수 있다.

[0064] 단계(405): 서버는 동적 얼굴 인증 프롬프트 정보를 단말기로 전송한다.

[0065] 제1 얼굴 특징 정보가 제2 얼굴 특징 정보와 일치한다고 검증되면, 서버는 사용자 본인에 대해 신원 인증이 수행된 것을 확인하고, 이 시점에서 동적 얼굴 인증 프로세스 수행을 시작한다. 서버는 동적 얼굴 인증 프롬프트 정보 데이터베이스로부터 동적 얼굴 인증 프롬프트 정보를 무작위로 추출할 수 있다.

[0066] 본 실시예에서, 동적 얼굴 인증 프롬프트 정보는 표정 동작 프롬프트 정보(expression action prompt information)나 음성 판독 프롬프트 정보(voice read prompt information)를 포함할 수 있다. 표정 동작 프롬프트 정보에 의해 프롬프트되는 동작은 일반적으로 사용자가 입을 벌리고, 눈을 감고, 머리를 돌리는 등의 얼굴 제스처를 통해 쉽게 표정할 수 있는 동작이다. 음성 판독 프롬프트 정보의 경우에 정보가 통상적으로 짧아서 사용자가 인증 과정 동안 쉽게 읽을 수 있고, 단말기는 사용자가 음성 판독 프롬프트 정보를 읽어 낼 때 얼굴 제스처를 쉽게 인식할 수 있다.

[0067] 단계(406): 단말기는 사용자의 얼굴을 추적하여 얼굴 추적 정보를 획득한다.

[0068] 단말기는 동적 얼굴 인증 프롬프트 정보를 수신한 후, 인증 인터페이스상에 동적 얼굴 인증 프롬프트 정보를 출력할 수 있다. 사용자는 정보에 따라 대응하는 얼굴 제스처를 제시할 수 있다. 제시 과정 동안, 단말기는 얼굴 추적 알고리즘을 통해 사용자의 얼굴 추적 정보를 획득한다. 얼굴 추적 정보는 얼굴의 주요 지점 위치 정보와 머리 제스처 정보 중 적어도 하나의 유형에 대한 정보를 포함할 수 있다.

[0069] 단계(407): 단말기는 얼굴 추적 정보를 분석하여 사용자의 제스처 인식 정보를 획득한다.

[0070] 예를 들어, 동적 얼굴 인증 프롬프트 정보가 "입을 벌리시오"인 경우, 사용자는 이에 대응하여 입을 벌리는 동작을 취한다. 단말기는 사용자의 얼굴을 추적하여 얼굴의 주요 지점 위치 정보, 특히 입의 주요 지점 위치 정보를 획득할 수 있다. 도 4b 및 도 4c는 본 출원의 본 실시예의 얼굴의 주요 지점 위치 정보의 개략도이다. 도 4b는 정상 상태에서 사용자 입의 주요 지점 위치(들)의 추출된 정보를 도시한다. 도 4c는 사용자가 입을 벌리는 제스처를 제시한 후 사용자의 입의 주요 지점 위치의 추출된 정보를 도시한다. 도 4c 및 도 4c의 주요 지점 위치(들) 각각의 추출된 정보를 비교하여, 즉 입의 상부와 하부 주요 지점 위치 사이의 각 좌표 거리를 비교

함으로써, 사용자의 제스처 인식 정보는 "입을 벌리시오"로서 획득된다.

[0071] 다른 예에서, 동적 얼굴 인증 프롬프트 정보가 "머리를 돌리시오"인 경우, 사용자는 이에 대응하여 머리를 돌리는 행동을 취한다. 단말기는 사용자의 얼굴을 추적함으로써, 특히 도 3b에 도시된 바와 같이 3개의 각도를 포함할 수 있는, 머리 제스처 정보를 획득할 수 있다. 3개의 각도의 각도 값이 "머리를 돌리시오"에 의해 정의된 각각의 각도 값 범위를 충족시키면, 사용자의 제스처 인식 정보는 "머리를 돌리시오"로서 획득될 수 있다.

[0072] 단계(408): 단말기는 제스처 인식 정보를 서버로 전송한다.

[0073] 단계(409): 서버는 제스처 인식 정보가 동적 얼굴 인증 프롬프트 정보와 일치하는지를 검증한다. 일치하면, 단계(410)이 실행된다. 그렇지 않으면 현재 프로세스가 종료된다.

[0074] 단계(410): 서버는 사용자에 대해 신원 인증이 성공한 것으로 판정하고, 현재 프로세스는 종료된다.

[0075] 위 실시예에서 볼 수 있듯이, 본 실시예는 얼굴 인증을 동적 인증과 결합하여 사용자의 신원에 대해 매우 안전한 인증을 수행하고, 얼굴 인증을 통해 사용자 본인인지를 사전에 검증할 수 있다. 인증 암호를 사용하는 기존 인증 방법과 비교하면 악의적인 제3자에 의해 인증 정보를 쉽게 도용당하지 않으므로 인증의 신뢰성이 향상된다. 또한, 사용자가 확인된 후에는 동적 얼굴 인증을 통해 실제 사용자로 인식될 수 있어서 인증 과정 동안 신원 인증의 정확도를 더 향상시키고 잠재적인 보안 위험을 감소시킬 수 있다.

[0076] 본 출원의 신원 인증 방법의 실시예에 상응하여, 본 출원은 신원 인증을 위한 장치, 단말기 및 서버의 실시예를 더 제공한다.

[0077] 본 출원의 신원 인증 장치의 실시예는 단말기와 서버에 개별적으로 적용될 수 있다. 장치 실시예는 소프트웨어에 의해 구현될 수 있거나 하드웨어 또는 소프트웨어와 하드웨어의 조합에 의해 구현될 수 있다. 소프트웨어 구현이 일례로 사용된다. 논리 장치로서, 본 장치는 실행을 위해 비휘발성 저장기기(non-volatile storage)로부터 메모리로의 컴퓨터 프로그램 명령에 대응하여 판독하도록 장치가 배치된 디바이스의 프로세서(들)에 의해 구성된다. 도 5는 하드웨어 레벨의 관점에서 본 출원에 따라 예시적인 신원 인증 장치가 배치된 디바이스의 하드웨어 구성도를 도시한다. 장치가 배치된 디바이스는 도 5에 도시된 바와 같은 프로세서(들), 메모리, 네트워크 인터페이스 및 비휘발성 저장기기에 더하여, 디바이스의 실제 기능에 따라 다른 추가적인 하드웨어 컴포넌트를 통상적으로 포함할 수 있다. 예를 들어, 단말기는 카메라, 터치 스크린, 통신 컴포넌트 등을 포함할 수 있다. 서버는 패킷 프로세싱 등을 담당하는 순방향 칩(forward chip)을 포함할 수 있다.

[0078] 도 6은 본 출원에 따른 신원 인증 장치의 실시예의 블록도를 도시한다. 신원 인증 장치는 단말기에 적용될 수 있다. 장치는 수신 유닛(610), 인식 유닛(620) 및 전송 유닛(630)을 포함한다.

[0079] 수신 유닛(610)은 사용자의 신원 인증 과정 동안 서버에 의해 전송된 동적 얼굴 인증 프롬프트 정보를 수신하도록 구성된다.

[0080] 인식 유닛(620)은 사용자에 의해 제시된 얼굴 제스처를 인식하여 동적 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 획득하도록 구성된다.

[0081] 전송 유닛(630)은 제스처 인식 정보를 서버에 전송하여 서버가 제스처 인식 정보가 동적 얼굴 인증 프롬프트 정보와 일치한다고 검증되면, 사용자에 대해 신원 인증이 성공한 것으로 확인할 수 있도록 구성될 수 있다.

[0082] 선택적 구현에서, 인식 유닛(620)은, 사용자가 얼굴 인증 프롬프트 정보에 따라 얼굴 제스처를 제시할 때 사용자의 얼굴을 추적하여 얼굴 추적 정보를 획득하는 얼굴 정보 획득 서브유닛과, 얼굴 추적 정보를 분석하여 사용자의 제스처 인식 정보를 획득하는 얼굴 정보 분석 서브유닛을 포함할 수 있다(도 6에 도시되지 않음).

[0083] 얼굴 정보 분석 서브유닛은 특히 얼굴 추적 정보가 얼굴의 주요 지점 위치 정보인 경우 얼굴의 주요 지점 위치 정보를 분석하여 사용자의 표정 제스처 인식 정보를 획득하거나, 얼굴 추적 정보가 머리 제스처 정보인 경우 머리 제스처 정보를 분석하여 사용자의 머리 회전 인식 정보를 획득하도록 구성될 수 있다.

[0084] 동적 얼굴 인증 프롬프트 정보는 표정 동작 프롬프트 정보나 음성 판독 프롬프트 정보 중 적어도 한 유형의 정보를 포함할 수 있다.

[0085] 다른 선택적 구현에서, 장치는 사용자의 얼굴 특징 정보를 획득하도록 구성된 획득 유닛을 더 포함하고, 신원 인증 과정 동안 획득된 얼굴 특징 정보를 사용자의 제1 얼굴 특징 정보로서 사용할 수 있다(도 6에는 도시되지 않음).

[0086] 전송 유닛(630)은 사용자의 제1 얼굴 특징 정보를 서버로 전송하여 저장된 사용자의 제2 얼굴 특징 정보와 제1 얼굴 특징 정보가 일치한다고 검증되면 서버로 하여금 동적 얼굴 인증 프롬프트 정보를 전송하게 하도록 더 구성될 수 있다.

[0087] 선택적으로, 획득 유닛은 사용자가 등록을 수행하는 경우 사용자의 얼굴 특징 정보를 획득하여, 등록 과정 동안 획득된 얼굴 특징 정보를 사용자의 제2 얼굴 특징 정보로서 사용하도록 더 구성될 수 있다. 전송 유닛(630)은 제2 얼굴 특징 정보를 서버로 전송하여 서버로 하여금 사용자의 사용자 이름과 제2 얼굴 특징 간의 대응 관계를 저장할 수 있게 하도록 더 구성될 수 있다.

[0088] 선택적으로, 획득 유닛은 사용자의 얼굴이 검출되는 경우 사용자의 얼굴을 추적하도록 구성된 얼굴 추적 서브유닛, 얼굴 추적 과정 동안 미리 설정된 시간 간격에 따라 얼굴 이미지를 획득하도록 구성된 이미지 획득 서브유닛, 얼굴 이미지가 미리 설정된 특징 추출 조건을 충족시키는지를 판정하도록 구성된 조건 판정 서브유닛, 특징 추출 조건이 충족되는 경우 얼굴 이미지로부터 사용자의 얼굴 특징 정보를 추출하도록 구성된 특징 추출 서브유닛을 포함할 수 있다.

[0089] 조건 판정 서브유닛은, 얼굴 이미지의 해상도가 미리 설정된 해상도 임계값을 만족시키는지를 판정하도록 구성된 해상도 판정 모듈과, 해상도 임계값이 충족되면 얼굴 이미지로부터 머리 제스처 정보를 추출하도록 구성된 제스처 정보 추출 모듈(머리 제스처 정보는 머리 내리기/들기 각도, 얼굴 회전 각도 또는 머리 기울기 각도 중 적어도 하나의 각도를 포함함)과, 머리 제스처 정보에 포함된 각각의 각도가 미리 설정된 각도 범위 내에 속하는지를 판정하는 각도 판정 모듈과, 각각의 각도가 미리 설정된 각도 범위 내에 속하는 경우, 얼굴 이미지가 특징 추출 조건을 충족시키는 것으로 판정하도록 구성된 판단(judgment) 판정(determination) 모듈을 포함한다.

[0090] 특징 추출 서브유닛은 특히 미리 설정된 특징 추출 알고리즘을 사용하여 사용자의 얼굴 특징 정보로서 얼굴 이미지로부터 얼굴 특징 벡터 값을 추출하도록 구성될 수 있으며, 미리 설정된 특징 추출 알고리즘은 LBP(Linear Back Projection) 추출 알고리즘이나 윈도우 푸리에 변환에서의 가버(Gabor) 특징 추출 알고리즘을 포함할 수 있다.

[0091] 도 7은 본 출원에 따른 신원 인증 장치의 다른 실시예의 블록도를 도시한다. 신원 인증 장치는 서버상에 적용될 수 있다. 장치는 전송 유닛(710), 수신 유닛(720) 및 판정 유닛(730)를 포함한다.

[0092] 전송 유닛(710)은 사용자의 신원 인증 과정 동안 동적 얼굴 인증 프롬프트 정보를 단말기로 전송하도록 구성된다.

[0093] 수신 유닛(720)은 단말기에 의해 전송된 제스처 인식 정보를 수신하도록 구성되며, 제스처 인식 정보는 동적 얼굴 인증 프롬프트 정보에 따라 사용자에 의해 제시된 얼굴 제스처 인식을 통해 단말기에 의해 획득된 제스처 인식 정보이다.

[0094] 판정 유닛(730)은 제스처 인식 정보가 동적 얼굴 인증 프롬프트 정보와 일치한다고 검증되면 사용자의 신원 인증이 성공한 것으로 판정하도록 구성된다.

[0095] 선택적 구현에서, 수신 유닛(720)은 단말기에 의해 전송된 사용자의 제1 얼굴 특징 정보를 수신하도록 더 구성될 수 있다.

[0096] 장치는 저장된 사용자의 제2 얼굴 특징 정보와 제1 얼굴 특징 정보가 일치하는지를 검증하도록 구성된 검증 유닛을 더 포함할 수 있다(도 7에는 도시되지 않음).

[0097] 전송 유닛(710)은 특히 제1 얼굴 특징 정보와 제2 얼굴 특징 정보가 일치하면 동적 얼굴 인증 프롬프트 정보를 단말기로 전송하도록 구성될 수 있다.

[0098] 선택적으로, 수신 유닛(720)은 또한 사용자가 등록을 수행하는 경우 단말기에 의해 전송된 사용자의 제2 얼굴 특징 정보를 수신하도록 더 구성될 수 있다. 또한, 장치는 사용자의 사용자 이름과 제2 얼굴 특징 정보 간의 대응 관계를 저장하는 저장 유닛을 더 포함할 수 있다(도 7에는 도시되지 않음).

[0099] 또한, 검증 유닛은 사용자의 사용자 이름에 기초한 대응 관계를 검색하여 사용자 이름에 대응하는 제2 얼굴 특징 정보를 획득하도록 구성된 특징 검색 서브유닛과, 제1 얼굴 특징 정보와 제2 얼굴 특징 정보를 미리 설정된 비교 방식으로 비교하도록 구성된 특징 비교 서브유닛과, 특징 비교 값이 미리 설정된 유사도 범위 내에 속하는 경우에 제1 얼굴 특징 정보가 제2 얼굴 특징 정보와 일치함을 판정하도록 구성된 매칭 판정 서브유닛을 포함할 수 있다. 특징 비교 서브유닛에 의해 사용되는 미리 설정된 비교 방식은 유클리드 거리(Euclidean distance)

비교법 또는 코사인 거리 비교법을 포함할 수 있다.

[0100] 전술한 장치(apparatus)에서의 각종 유닛의 기능과 효과의 구현 프로세스의 세부 사항은 전술한 방법(method)에 상응하는 단계의 구현 프로세스를 참조할 수 있으며, 본 명세서에서 반복적으로 설명되지는 않는다.

[0101] 장치 실시예는 기본적으로 방법 실시예에 상응하기 때문에, 관련된 부분은 방법 실시예의 설명의 각 부분이 참조될 수 있다. 전술한 장치 실시예는 단지 예시적일 뿐이다. 개별 컴포넌트로 설명된 유닛은 물리적으로 분리되어 있을 수도 있고 그렇지 않을 수도 있다. 하나의 유닛으로 표시된 컴포넌트는 물리적 유닛일 수도 있고 아닐 수도 있는데, 즉, 단일 위치에 배치되거나 여러 네트워크 유닛으로 분산될 수 있다. 모듈의 일부 또는 전부는 본 출원의 해결방안의 목적을 달성하기 위한 실제 요구사항에 따라 선택될 수 있다. 통상의 기술자는 창의적인 노력을 기울이지 않고도 본 출원을 이해하고 구현할 수 있다.

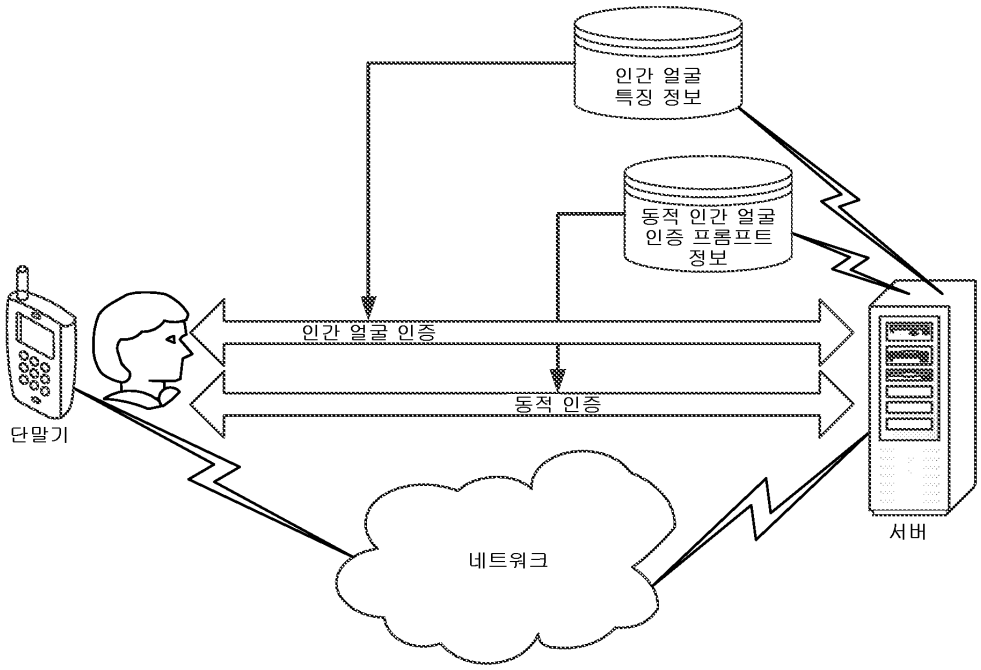
[0102] 전술한 실시예에서 볼 수 있듯이, 사용자의 신원 인증 과정 동안 동적 얼굴 인증을 통해 사용자의 신원에 대해 매우 안전한 인증이 수행될 수 있다. 인증 암호를 사용하는 기존의 인증 방법과 비교하면 악의적인 제3자에 의해 인증 정보를 쉽게 도용당하지 않으므로 인증의 신뢰성이 향상된다. 또한, 사용자는 동적 얼굴 인증을 통해 실제 사용자로 인식될 수 있으므로 인증 과정 동안 신원 인증의 정확성을 향상시키고 잠재적인 보안 위험을 감소시킨다.

[0103] 통상의 기술자는 본 서면에 개시된 명세서를 참작하여 발명을 실시한 후에 본 출원의 다른 구현법(implementation solutions)을 쉽게 찾아낼 수 있다. 본 출원은 본 출원에 대한 임의의 변형(variations), 사용(usages) 또는 적응적 변경(adaptive change)을 포함하도록 의도된다. 이러한 변형, 용도 또는 적응적 변경은 본 출원의 통상적인 원리들을 따르며 본 출원에 개시되지 않은 해당 기술 분야에서의 보편적인 지식이나 통상의 기술적 수단을 포함한다. 명세서와 실시예는 단지 예시적인 것으로 간주되며, 본 출원의 실제 범위와 사상은 본 명세서의 청구범위에 의해 구체화된다.

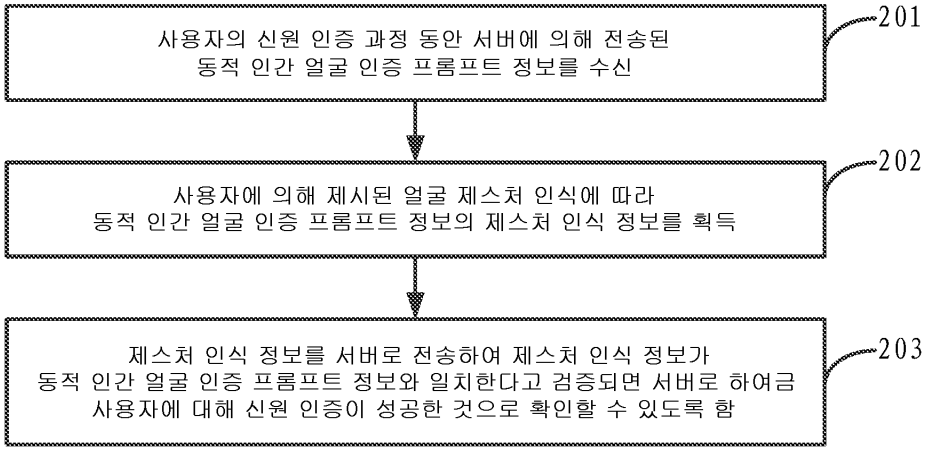
[0104] 본 출원은 전술된 내용과 첨부 도면에 도시된 그 구조에 한정되지는 않는다는 것에 주의해야 한다. 본 출원의 범위를 벗어나지 않으면서 다양한 수정 및 변경이 본 출원에 행해질 수 있다. 본 출원의 범위는 첨부된 청구범위에 의해서만 한정된다.

도면

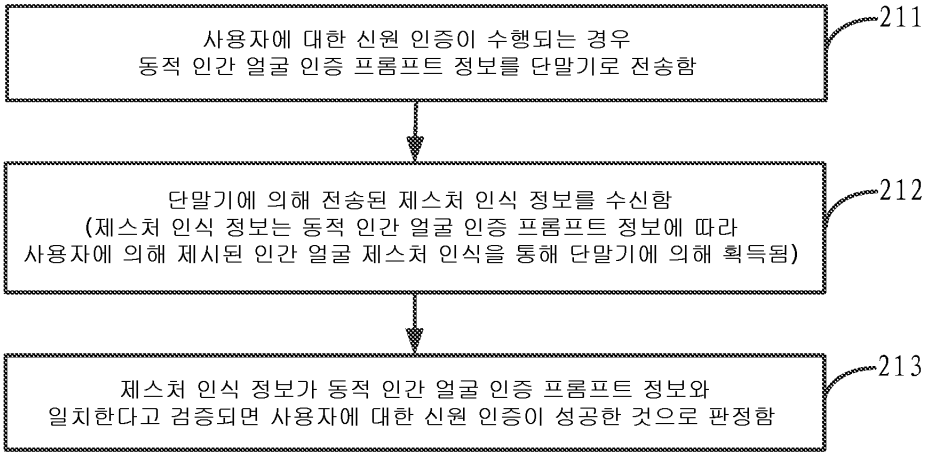
도면1



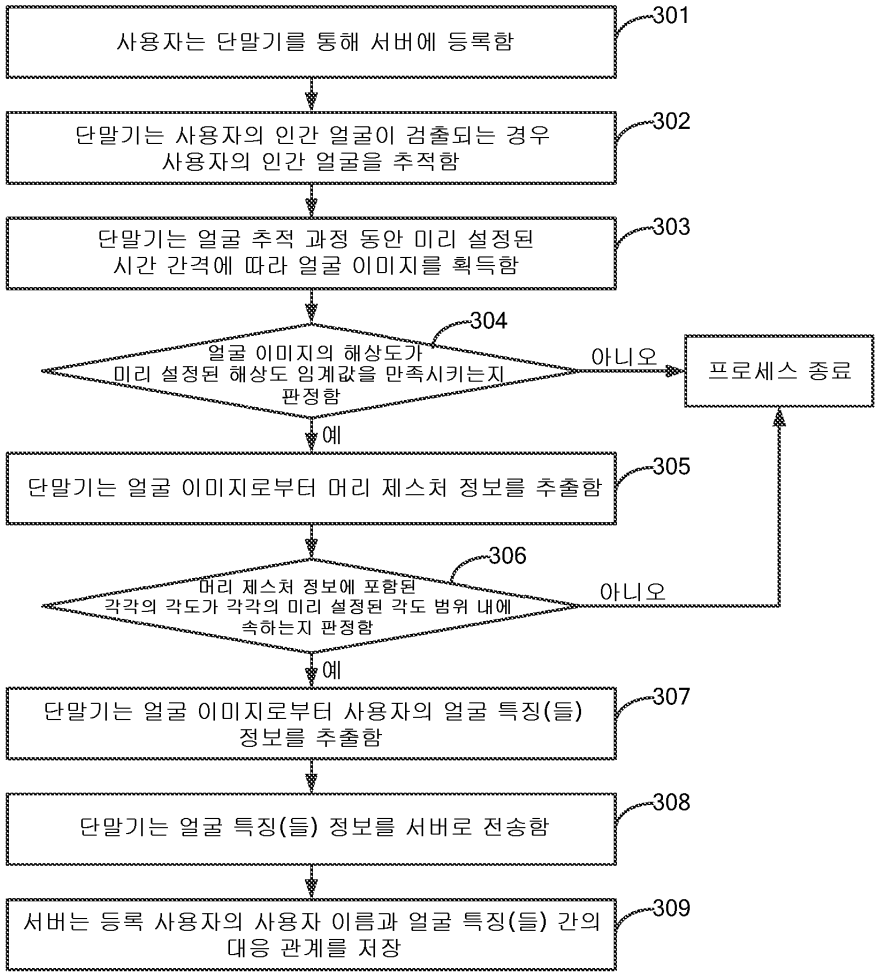
도면2a


사용자의 신원 인증 과정 동안 서버에 의해 전송된
동적 인간 얼굴 인증 프롬프트 정보를 수신
201
사용자에 의해 제시된 얼굴 제스처 인식에 따라
동적 인간 얼굴 인증 프롬프트 정보의 제스처 인식 정보를 획득
202
제스처 인식 정보를 서버로 전송하여 제스처 인식 정보가
동적 인간 얼굴 인증 프롬프트 정보와 일치한다고 검증되면 서버로 하여금
사용자에 대해 신원 인증이 성공한 것으로 확인할 수 있도록 함
203

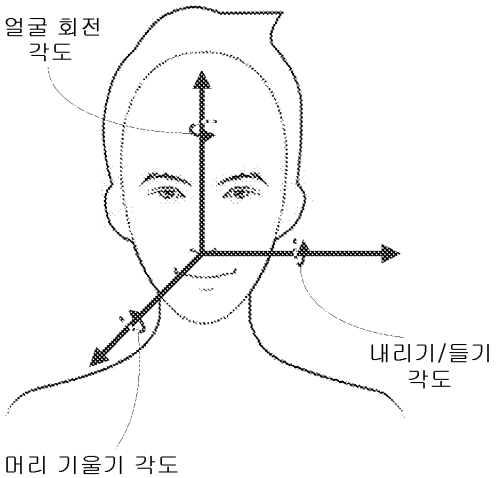
도면2b


사용자에 대한 신원 인증이 수행되는 경우
동적 인간 얼굴 인증 프롬프트 정보를 단말기로 전송함
211
단말기에 의해 전송된 제스처 인식 정보를 수신함
(제스처 인식 정보는 동적 인간 얼굴 인증 프롬프트 정보에 따라
사용자에 의해 제시된 인간 얼굴 제스처 인식을 통해 단말기에 의해 획득됨)
212
제스처 인식 정보가 동적 인간 얼굴 인증 프롬프트 정보와
일치한다고 검증되면 사용자에 대한 신원 인증이 성공한 것으로 판정함
213

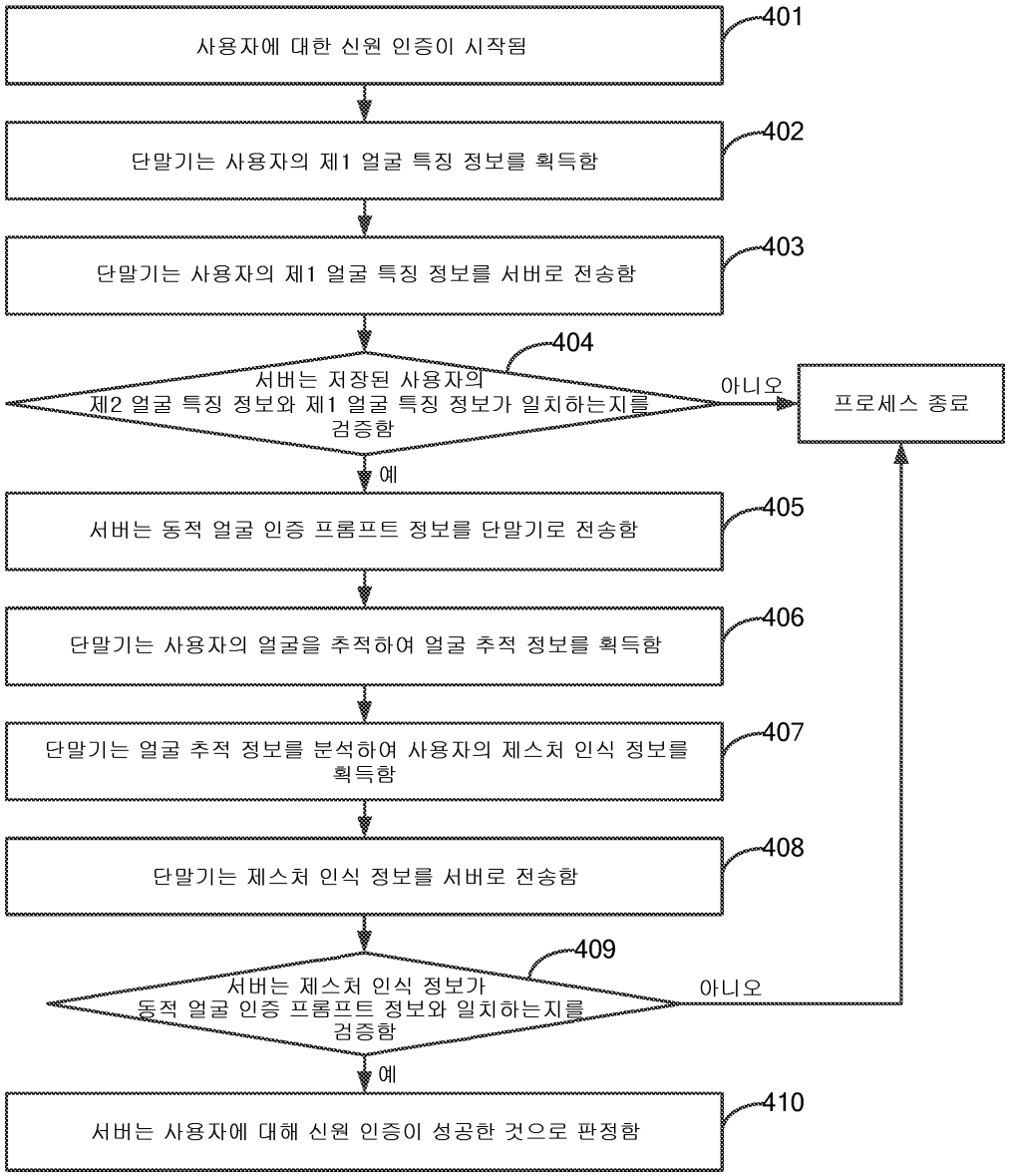
도면3a


사용자는 단말기를 통해 서버에 등록함
301
단말기는 사용자의 인간 얼굴이 검출되는 경우 사용자의 인간 얼굴을 추적함
302
단말기는 얼굴 추적 과정 동안 미리 설정된 시간 간격에 따라 얼굴 이미지를 획득함
303
얼굴 이미지의 해상도가 미리 설정된 해상도 임계값을 만족시키는지 판정함
304
아니오
프로세스 종료
예
단말기는 얼굴 이미지로부터 머리 제스처 정보를 추출함
305
머리 제스처 정보에 포함된 각각의 각도가 각각의 미리 설정된 각도 범위 내에 속하는지 판정함
306
아니오
예
단말기는 얼굴 이미지로부터 사용자의 얼굴 특징(들) 정보를 추출함
307
단말기는 얼굴 특징(들) 정보를 서버로 전송함
308
서버는 등록 사용자의 사용자 이름과 얼굴 특징(들) 간의 대응 관계를 저장
309

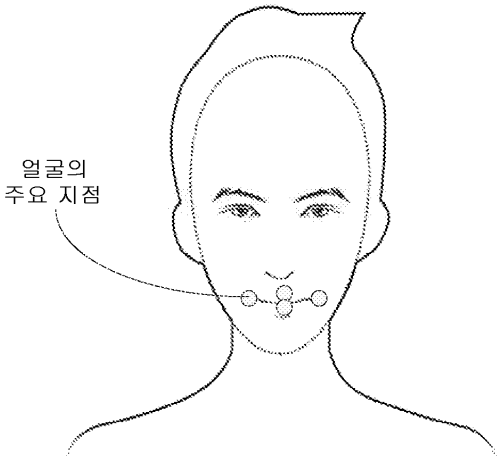
도면3b


얼굴 회전 각도
내리기/들기 각도
머리 기울기 각도

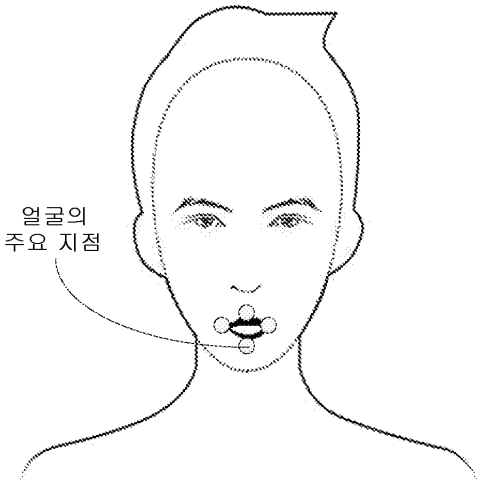
도면4a


사용자에 대한 신원 인증이 시작됨
401
단말기는 사용자의 제1 얼굴 특징 정보를 획득함
402
단말기는 사용자의 제1 얼굴 특징 정보를 서버로 전송함
403
서버는 저장된 사용자의 제2 얼굴 특징 정보와 제1 얼굴 특징 정보가 일치하는지를 검증함
404
아니오
프로세스 종료
예
서버는 동적 얼굴 인증 프롬프트 정보를 단말기로 전송함
405
단말기는 사용자의 얼굴을 추적하여 얼굴 추적 정보를 획득함
406
단말기는 얼굴 추적 정보를 분석하여 사용자의 제스처 인식 정보를 획득함
407
단말기는 제스처 인식 정보를 서버로 전송함
408
서버는 제스처 인식 정보가 동적 얼굴 인증 프롬프트 정보와 일치하는지를 검증함
409
아니오
예
서버는 사용자에 대해 신원 인증이 성공한 것으로 판정함
410

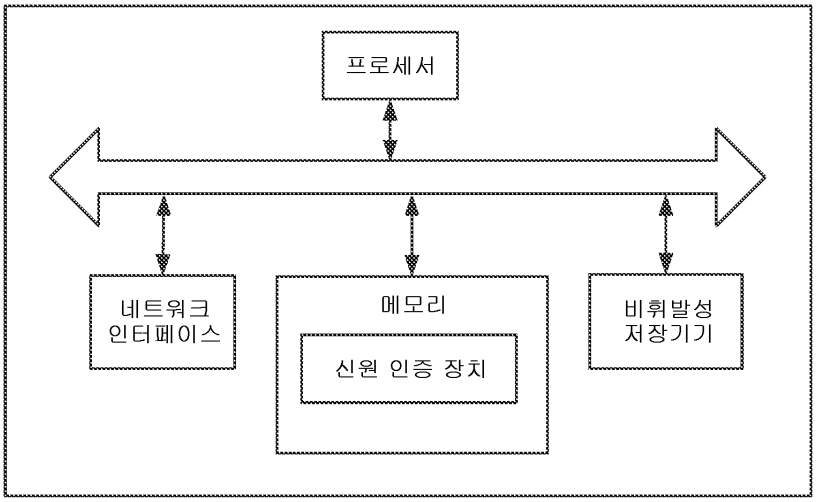
도면4b


얼굴의
주요 지점

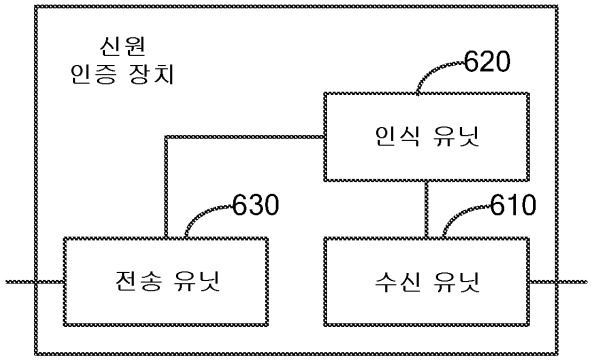
도면4c


얼굴의
주요 지점

도면5


프로세서
네트워크
인터페이스
메모리
신원 인증 장치
비휘발성
저장기기

도면6


신원
인증 장치
620
인식 유닛
630
610
전송 유닛
수신 유닛

도면7