(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년11월01일
(11) 등록번호 10-2596783
(24) 등록일자 2023년10월27일

(51) 국제특허분류(Int. Cl.)
G06F 21/32 (2013.01) *H04L 9/40* (2022.01)
(52) CPC특허분류
G06F 21/32 (2013.01)
H04L 63/0861 (2013.01)
(21) 출원번호 10-2021-7022290
(22) 출원일자(국제) 2019년12월13일
심사청구일자 2021년07월15일
(85) 번역문제출일자 2021년07월15일
(65) 공개번호 10-2021-0103517
(43) 공개일자 2021년08월23일
(86) 국제출원번호 PCT/CN2019/125377
(87) 국제공개번호 WO 2020/135114
국제공개일자 2020년07월02일
(30) 우선권주장
201811608040.9 2018년12월26일 중국(CN)
(56) 선행기술조사문헌
CN105847253 A*
CN108243495 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
쉔텅 (광동) 테크놀러지 컴퍼니., 리미티드.
중국 510000 광동, 광저우 하이-테크 존, 사이언스 시티, 커쉬에 에비뉴, 황신 빌딩 넘버. 182, 빌딩 C2, 그라운드 플로어, 유닛 103
(72) 발명자
지엔, 웨이밍
중국 510000 광동, 광저우 하이-테크 존, 사이언스 시티, 커쉬에 에비뉴, 황신 빌딩 넘버. 182, 빌딩 C2, 그라운드 플로어, 유닛 103
피, 아이핑
중국 510000 광동, 광저우 하이-테크 존, 사이언스 시티, 커쉬에 에비뉴, 황신 빌딩 넘버. 182, 빌딩 C2, 그라운드 플로어, 유닛 103
(뒷면에 계속)
(74) 대리인
김진환, 박지하, 김민철

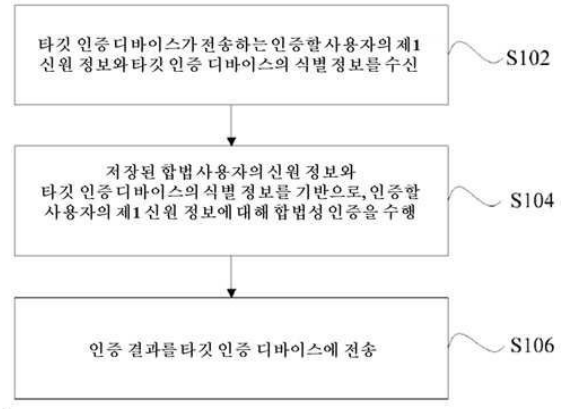
전체 청구항 수 : 총 11 항 심사관 : 문남두

(54) 발명의 명칭 **신원 정보의 인증 방법, 장치 및 서버**

(57) 요 약

신원 정보의 인증 방법, 장치 및 서버에 있어서, 이는 신원 인증 기술 분야에 관한 것이다. 상기 방법은 서버에 의해 실행된다. 서버는 각각 타깃 인증 디바이스 및 사용자 단말과 통신 연결된다. 상기 방법은 타깃 인증 디바이스가 전송하는 인증할 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 수신하는 단계(S102); 저장된 합법 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 기반으로, 인증할 사용자의 신원 정보에 대해 합법성 인증을 수행하는 단계(S104); 및 인증 결과를 타깃 인증 디바이스에 전송하는 단계(S106)를 포함한다. 상기 방법은 개인 신원 정보를 효과적으로 보호하고, 신원 인증의 안전성, 신뢰성 및 간편성을 향상시키며, 사용자 체험도를 강화할 수 있다.

대 표 도 - 도1



(72) 발명자

리앙, 화궈이

중국 510000 광동, 광저우 하이-테크 존, 사이언스 시티, 커쉬에 에비뉴, 촹신 빌딩 넘버. 182, 빌딩 C2, 그라운드 플로어, 유닛 103

황, 페잉

중국 510000 광동, 광저우 하이-테크 존, 사이언스 시티, 커쉬에 에비뉴, 촹신 빌딩 넘버. 182, 빌딩 C2, 그라운드 플로어, 유닛 103

천, 치우룽

중국 510000 광동, 광저우 하이-테크 존, 사이언스 시티, 커쉬에 에비뉴, 촹신 빌딩 넘버. 182, 빌딩 C2, 그라운드 플로어, 유닛 103

명 세 서

청구범위

청구항 1

신원 정보의 인증 방법에 있어서,

상기 방법은 서버에 의해 실행되며, 상기 서버는 각각 타깃 인증 디바이스 및 사용자 단말과 통신 연결되고, 상기 방법은,

상기 타깃 인증 디바이스가 전송하는 인증할 사용자의 제1 신원 정보와 상기 타깃 인증 디바이스의 식별 정보를 수신하는 단계-여기에서 상기 인증할 사용자의 제1 신원 정보는 상기 인증할 사용자의 현재 생물 특징을 포함하고, 상기 현재 생물 특징은 현재 얼굴 특징을 포함하고, 상기 타깃 인증 디바이스의 식별 정보는 상기 타깃 인증 디바이스의 계정 정보와 상기 타깃 인증 디바이스의 위치 정보를 포함함-;

저장된 합법 사용자의 제1 신원 정보와 상기 타깃 인증 디바이스의 식별 정보를 기반으로, 상기 인증할 사용자의 제1 신원 정보에 대해 합법성 인증을 수행하는 단계; 및

인증 결과를 상기 타깃 인증 디바이스에 전송하는 단계를 포함하고,

상기 타깃 인증 디바이스가 전송한 인증할 사용자의 제1 신원 정보를 수신하는 단계 전에, 상기 방법은,

상기 사용자 단말이 전송한 상기 사용자 단말의 위치 정보를 수신하는 단계; 및

상기 사용자 단말의 위치 정보에 대해 동적 래스터화 처리를 수행하여, 상기 사용자 단말의 위치 정보가 위치한 래스터를 확정하는 단계를 더 포함하는 것을 특징으로 하는 신원 정보의 인증 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

저장된 합법 사용자의 제1 신원 정보와 상기 타깃 인증 디바이스의 식별 정보를 기반으로, 상기 인증할 사용자의 제1 신원 정보에 대해 합법성 인증을 수행하는 단계는,

상기 타깃 인증 디바이스의 위치 정보에 대해 동적 래스터화 처리를 수행하여, 상기 타깃 인증 디바이스의 위치 정보가 위치한 래스터를 확정하는 단계;

상기 타깃 인증 디바이스의 위치 정보가 위치한 래스터와 상기 타깃 인증 디바이스의 위치 정보가 위치한 래스터로부터 소정의 범위 내에 떨어진 래스터를 타깃 래스터로 사용하는 단계;

저장된 합법 사용자의 제1 신원 정보를 기반으로, 각 상기 사용자 단말의 위치 정보가 상기 타깃 래스터에 위치한 각 사용자가 저장한 생물 특징을 조회하는 단계; 및

상기 인증할 사용자의 현재 생물 특징과 조회한 각 상기 사용자가 저장한 생물 특징을 매칭시켜, 상기 인증할 사용자의 제1 신원 정보에 대한 합법성 인증을 수행하는 단계를 포함하는 것을 특징으로 하는 신원 정보의 인증 방법.

청구항 4

제3항에 있어서,

상기 인증할 사용자의 현재 생물 특징과 조회한 각 상기 사용자가 저장한 생물 특징을 매칭시키는 단계는,

상기 현재 생물 특징이 생체의 생물 특징인지 여부를 판단하는 단계;

그러한 경우, 상기 인증할 사용자의 현재 생물 특징과 조회한 각 상기 사용자가 저장한 생물 특징을 일대일 비

교하는 단계;

비교하여 획득한 하나의 상기 저장된 생물 특징과 상기 현재 생물 특징의 유사도가 소정의 유사도 임계값보다 큰 경우, 상기 유사도가 소정의 유사도 임계값보다 큰 저장된 생물 특징에 대응하는 계정을 현재 사용자 계정으로 확정하는 단계;

비교하여 획득한 복수의 상기 저장된 생물 특징과 상기 현재 생물 특징의 유사도가 소정의 유사도 임계값보다 큰 경우, 각 상기 유사도가 소정의 유사도 임계값보다 큰 저장된 생물 특징에 각각 대응하는 사용자를 복수의 상기 인증할 사용자로 확정하는 단계; 및

복수의 상기 인증할 사용자에 대해 다시 신원 확인을 수행하는 단계를 포함하고, 여기에서 상기 신원 확인은 신분증의 소정의 자릿수의 숫자 및 생물 인식 매칭 중 적어도 하나를 포함하는 것을 특징으로 하는 신원 정보의 인증 방법.

청구항 5

제4항에 있어서,

상기 인증할 사용자의 사용자 단말은 사용자 계정을 포함하고, 상기 다시 신원 확인을 수행하는 상기 인증할 사용자의 사용자 계정은 현재 사용자 계정이고, 상기 방법은,

상기 현재 사용자 계정의 사용자 단말에 사용자의 제2 신원 정보를 획득하는 요청을 전송하는 단계-여기에서 상기 사용자 단말에는 상기 사용자의 제2 신원 정보가 있고, 상기 사용자의 제2 신원 정보에는 사용자의 성명, 사용자의 신분증 번호 및 상기 사용자가 저장한 생물 특징 정보가 포함됨-;

상기 현재 사용자 계정의 사용자 단말이 전송한 상기 사용자의 제2 신원 정보를 수신한 경우, 상기 사용자 단말이 상기 요청에 대한 응답을 허용하도록 설정되었는지 여부를 판단하는 단계;

그러한 경우, 상기 제2 신원 정보의 합법성에 대해 검증을 수행하는 단계;

상기 제2 신원 정보가 합법적인 것으로 검증된 경우, 상기 제2 신원 정보를 상기 타깃 인증 디바이스에 전송하고, 신원 정보 인증 로그를 생성하는 단계; 및

상기 신원 정보 인증 로그를 상기 사용자 계정의 사용자 단말에 전송하는 단계를 더 포함하는 것을 특징으로 하는 신원 정보의 인증 방법.

청구항 6

제5항에 있어서,

상기 현재 사용자 계정의 사용자 단말에 사용자의 제2 신원 정보를 획득하는 요청을 전송하는 단계 이후, 상기 방법은,

상기 현재 사용자 계정의 사용자 단말을 통해 상기 제2 신원 정보의 합법성에 대해 검증을 수행하는 단계; 및

상기 제2 신원 정보가 합법적인 경우, 상기 현재 사용자 계정의 사용자 단말을 통해 상기 제2 신원 정보를 상기 서버에 전송하는 단계를 더 포함하는 것을 특징으로 하는 신원 정보의 인증 방법.

청구항 7

제5항에 있어서,

상기 서버는 또한 신원 인증 시스템과 통신 연결되고, 상기 방법은,

상기 신원 정보의 인증이 2차 신원 인증 요청인 경우, 상기 제2 신원 정보의 합법성을 검증한 후, 상기 제2 신원 정보를 상기 신원 인증 시스템에 전송하는 단계;

상기 신원 인증 시스템을 통해 상기 제2 신원 정보에 대해 신원 검증을 수행하여, 신원 검증 결과를 획득하는 단계;

상기 신원 인증 시스템을 통해 상기 신원 검증 결과를 상기 서버에 전송하는 단계;

상기 신원 검증 결과에 상기 제2 신원 정보가 합법적이라는 정보가 포함되면, 상기 제2 신원 정보를 상기 타깃

인증 디바이스에 전송하고, 신원 정보 인증 로그를 생성하는 단계; 및

상기 신원 정보 인증 로그를 상기 사용자 계정의 사용자 단말에 전송하는 단계를 더 포함하는 것을 특징으로 하는 신원 정보의 인증 방법.

청구항 8

제5항에 있어서,

상기 서버는 또한 신원 인증 시스템과 통신 연결되고, 상기 방법은,

상기 신원 인증 시스템을 통해 상기 사용자 단말에 대해 상기 제2 신원 정보의 등록을 수행하는 단계를 더 포함하는 것을 특징으로 하는 신원 정보의 인증 방법.

청구항 9

제8항에 있어서,

상기 신원 인증 시스템을 통해 상기 사용자 단말에 대해 상기 제2 신원 정보의 등록을 수행하는 단계는,

상기 사용자 단말이 전송한 상기 제2 신원 정보를 수신하는 단계;

상기 제2 신원 정보를 상기 신원 인증 시스템에 전송하는 단계;

상기 신원 인증 시스템을 통해 상기 제2 신원 정보에 대해 신원 검증을 수행하는 단계;

상기 신원 인증 시스템을 통해 상기 제2 신원 정보의 신원 검증 결과를 상기 서버에 전송하는 단계;

상기 신원 검증 결과에 상기 제2 신원 정보가 합법적이라는 정보가 포함되면, 상기 제2 신원 정보 중의 상기 사용자가 저장한 생물 특징과 상기 사용자 계정을 연관 짓는 단계;

상기 제2 신원 정보가 합법적이라는 신원 검증 결과를 상기 사용자 단말에 전송하는 단계; 및

상기 사용자 단말이 상기 제2 신원 정보가 합법적이라는 신원 검증 결과를 수신한 후, 상기 제2 신원 정보를 암호화 처리하고, 암호화 처리된 상기 제2 신원 정보를 상기 사용자 단말에 저장하는 단계를 포함하는 것을 특징으로 하는 신원 정보의 인증 방법.

청구항 10

신원 정보의 인증 장치에 있어서,

상기 장치는 서버에 의해 실행되며, 상기 서버는 각각 타깃 인증 디바이스 및 사용자 단말과 통신 연결되고, 상기 장치는,

상기 타깃 인증 디바이스가 전송하는 인증할 사용자의 제1 신원 정보와 상기 타깃 인증 디바이스의 식별 정보를 수신하도록 구성되는 수신 모듈-여기에서 상기 인증할 사용자의 제1 신원 정보는 상기 인증할 사용자의 현재 생물 특징을 포함하고, 상기 현재 생물 특징은 현재 얼굴 특징을 포함하고, 상기 타깃 인증 디바이스의 식별 정보는 상기 타깃 인증 디바이스의 계정 정보와 상기 타깃 인증 디바이스의 위치 정보를 포함함-;

저장된 합법 사용자의 제1 신원 정보와 상기 타깃 인증 디바이스의 식별 정보를 기반으로, 상기 인증할 사용자의 제1 신원 정보에 대해 합법성 인증을 수행하도록 구성되는 인증 모듈; 및

인증 결과를 상기 타깃 인증 디바이스에 전송하도록 구성되는 전송 모듈을 포함하고,

상기 수신 모듈은,

상기 사용자 단말이 전송하는 상기 사용자 단말의 위치 정보를 수신하고,

상기 사용자 단말의 위치 정보에 대해 동적 래스터화 처리를 수행하여, 상기 사용자 단말의 위치 정보가 위치한 래스터를 확정하도록 구성되는 것을 특징으로 하는 신원 정보의 인증 장치.

청구항 11

삭제

청구항 12

서버에 있어서,

프로세서 및 메모리를 포함하고,

상기 메모리에 컴퓨터 프로그램이 저장되고, 상기 컴퓨터 프로그램이 상기 프로세서에 의해 실행될 때 제1항, 또는 제3항 내지 제9항 중 어느 한 항에 따른 방법을 실행하는 것을 특징으로 하는 서버.

청구항 13

칩에 있어서,

상기 칩에 프로그램이 저장되고, 상기 프로그램은 프로세서에 의해 실행될 때 제1항, 또는 제3항 내지 제9항 중 어느 한 항에 따른 방법의 단계를 실행하는 것을 특징으로 하는 칩.

발명의 설명

기 술 분 야

[0001] 본 출원은 2018년 12월 26일 중국 특허국에 제출된 출원번호 CN201811608040.9, 발명의 명칭 "신원 정보의 인증 방법, 장치 및 서버"의 중국 특허 출원에 대한 우선권을 요청하며, 이는 본 출원에 전체로써 인용되었다.

[0002] 본 발명은 신원 인증 기술 분야에 관한 것으로, 더욱 상세하게는 신원 정보의 인증 방법, 장치 및 서버에 관한 것이다.

배 경 기 술

[0003] 네트워크 기술이 빠르게 발전하고 모바일 결제와 같은 편리한 수단이 출현하면서 현금 휴대는 점차 역사가 되고 있다. 머지않아 실체 신분증도 기존 기술에 의해 대체되어 실체 신분증을 휴대하지 않고도 편리하게 외출할 수 있으며, 이는 일종의 트렌드가 될 것이다.

[0004] 생물 특징 인식 기반의 신원 인증은 이미 많은 상황에 응용되고 있다. 그러나 종래의 생물 특징 인식 기술은 얼굴 이미지와 같은 생물 특징을 수집할 때 촬영 각도, 촬영 거리, 빛 조사 방향, 빛 조사 각도, 광선 명암, 광선 컬러 등 조건의 영향을 받아 얼굴 비교 결과에 비교적 큰 편차가 발생한다. 또한 형제, 자매, 쌍둥이 또는 혈연 관계가 없으나 두 사람이 매우 닮은 경우가 있으므로, 생물 특징 인식 기술의 신뢰성은 개설될 필요가 있다.

[0005] 시민의 개인 신원 정보는 개인의 사생활에 속하며 법으로 보호된다. 어떠한 개인, 단체, 기업도 시민의 개인 신원 정보를 저장할 수 없다. 개인 신원 정보의 불법 저장은 시민의 프라이버시를 침해하고 심지어 개인 정보 유출을 유발하며 각종 사회 문제를 일으킬 수 있다. 따라서 신원 인증의 안전성은 강화되어야 한다.

발명의 내용

[0006] 이를 고려하여 본 발명은 목적은 신원 정보의 인증 방법, 장치 및 서버를 제공함으로써, 개인 신원 정보를 효과적으로 보호하고 신원 인증의 안전성, 신뢰성 및 편의성을 향상시키며 사용자 체험도를 강화시키는 데에 있다.

[0007] 상기 목적을 달성하기 위해, 본 발명의 실시예는 하기와 같은 기술적 해결책을 채택한다.

[0008] 제1 양상에 있어서, 본 발명의 실시예는 신원 정보의 인증 방법을 제공한다. 상기 방법은 서버에 의해 실행된다. 서버는 각각 타깃 인증 디바이스 및 사용자 단말과 통신 연결된다. 상기 방법은 타깃 인증 디바이스가 전송하는 인증할 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 수신하는 단계-인증할 사용자의 제1 신원 정보는 인증할 사용자의 현재 생물 특징을 포함하고, 현재 생물 특징은 현재 얼굴 특징을 포함하고, 타깃 인증 디바이스의 식별 정보는 타깃 인증 디바이스의 계정 정보와 타깃 인증 디바이스의 위치 정보를 포함함-; 저장된 합법 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 기반으로, 인증할 사용자의 제1 신원 정보에 대해 합법성 인증을 수행하는 단계; 및 인증 결과를 타깃 인증 디바이스에 전송하는 단계를 포함한다.

[0009] 제1 양상과 함께 본 발명의 실시예는 제1 양상의 가능한 제1 실시방식을 제공한다. 여기에서 타깃 인증 디바이스가 전송한 인증할 사용자의 제1 신원 정보를 수신하는 단계 전에, 상기 방법은, 사용자 단말이 전송하는 사용자 단말의 위치 정보를 수신하는 단계; 및 사용자 단말의 위치 정보에 대해 동적 래스터화 처리를 수행하여, 사

용자 단말의 위치 정보가 위치한 래스터를 확정하는 단계를 더 포함한다.

[0010] 제1 양상의 가능한 제1 실시방식과 함께 본 발명의 실시예는 제1 양상의 가능한 제2 실시방식을 제공한다. 여기에서 저장된 합법 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 기반으로, 인증할 사용자의 제1 신원 정보에 대해 합법성 인증을 수행하는 단계는, 타깃 인증 디바이스의 위치 정보에 대해 동적 래스터화 처리를 수행하여, 타깃 인증 디바이스의 위치 정보가 위치한 래스터를 확정하는 단계; 타깃 인증 디바이스의 위치 정보가 위치한 래스터와 타깃 인증 디바이스의 위치 정보가 위치한 래스터로부터 소정의 범위 내에 떨어진 래스터를 타깃 래스터로 사용하는 단계; 저장된 합법 사용자의 제1 신원 정보를 기반으로, 각 사용자 단말의 위치 정보가 타깃 래스터에 위치한 각 사용자가 저장한 생물 특징을 조회하는 단계; 및 인증할 사용자의 현재 생물 특징과 조회한 각 사용자가 저장한 생물 특징을 매칭시켜, 인증할 사용자의 제1 신원 정보에 대한 합법성 인증을 수행하는 단계를 포함한다.

[0011] 제1 양상의 가능한 제2 실시방식과 함께 본 발명 실시예는 제1 양상의 가능한 제3 실시방식을 제공한다. 여기에서 인증할 사용자의 현재 생물 특징과 조회한 각 사용자가 저장한 생물 특징을 매칭시키는 단계는, 현재 생물 특징이 생체의 생물 특징인지 여부를 판단하는 단계; 그러한 경우, 인증할 사용자의 현재 생물 특징과 조회한 각 사용자가 저장한 생물 특징을 일대일 비교하는 단계; 비교하여 획득한 하나의 저장된 생물 특징과 현재 생물 특징의 유사도가 소정의 유사도 임계값보다 큰 경우, 유사도가 소정의 유사도 임계값보다 큰 저장된 생물 특징을 현재 생물 특징으로 확정하는 단계; 비교하여 획득한 복수의 저장된 생물 특징과 현재 생물 특징의 유사도가 소정의 유사도 임계값보다 큰 경우, 유사도가 소정의 유사도 임계값보다 큰 저장된 생물 특징에 대응하는 계정을 현재 사용자 계정으로 확정하는 단계; 비교하여 획득한 복수의 저장된 생물 특징과 현재 생물 특징의 유사도가 소정의 유사도 임계값보다 큰 경우, 각 유사도가 소정의 유사도 임계값보다 큰 저장된 생물 특징에 각각 대응하는 사용자를 복수의 인증할 사용자로 확정하는 단계; 및 복수의 인증할 사용자에 대해 다시 신원 확인을 수행하는 단계를 포함한다. 여기에서 신원 확인은 신분증의 소정의 자릿수의 숫자 및/또는 생물 인식 매칭을 포함한다.

[0012] 제1 양상의 가능한 제3 실시방식과 함께 본 발명 실시예는 제1 양상의 가능한 제4 실시방식을 제공한다. 여기에서 인증할 사용자의 사용자 단말은 사용자 계정을 포함하고, 다시 신원 확인을 수행하는 인증할 사용자의 사용자 계정은 현재 사용자 계정이다. 상기 방법은, 현재 사용자 계정의 사용자 단말에 사용자의 제2 신원 정보를 획득하는 요청을 전송하는 단계-여기에서 사용자 단말에는 사용자의 제2 신원 정보가 있고, 사용자의 제2 신원 정보에는 사용자의 성명, 사용자의 신분증 번호 및 사용자가 저장한 생물 특징이 포함됨-; 현재 사용자 계정의 사용자 단말이 전송한 사용자의 제2 신원 정보를 수신한 경우, 사용자 단말이 상기 요청에 대한 응답을 허용하도록 설정되었는지 여부를 판단하는 단계; 그러한 경우, 제2 신원 정보의 합법성에 대해 검증을 수행하는 단계; 제2 신원 정보가 합법적인 것으로 검증된 경우, 제2 신원 정보를 타깃 인증 디바이스에 전송하고, 신원 정보 인증 로그를 생성하는 단계; 및 신원 정보 인증 로그를 사용자 계정의 사용자 단말에 전송하는 단계를 더 포함한다.

[0013] 제1 양상의 가능한 제4 실시방식과 함께 본 발명 실시예는 제1 양상의 가능한 제5 실시방식을 제공한다. 여기에서 현재 사용자 계정의 사용자 단말에 사용자의 제2 신원 정보를 획득하는 요청을 전송하는 단계 이후, 상기 방법은, 현재 사용자 계정의 사용자 단말을 통해 제2 신원 정보의 합법성에 대해 검증을 수행하는 단계; 및 제2 신원 정보가 합법적인 경우, 현재 사용자 계정의 사용자 단말을 통해 제2 신원 정보를 서버에 전송하는 단계를 더 포함한다.

[0014] 제1 양상의 가능한 제4 실시방식과 함께 본 발명 실시예는 제1 양상의 가능한 제6 실시방식을 제공한다. 여기에서 서버는 또한 신원 인증 시스템과 통신 연결되고, 상기 방법은, 신원 정보의 인증이 2차 신원 인증 요청인 경우, 제2 신원 정보의 합법성을 검증한 후, 제2 신원 정보를 신원 인증 시스템에 전송하는 단계; 신원 인증 시스템을 통해 제2 신원 정보에 대해 신원 검증을 수행하여, 신원 검증 결과를 획득하는 단계; 신원 인증 시스템을 통해 신원 검증 결과를 서버에 전송하는 단계; 신원 검증 결과에 제2 신원 정보가 합법적이라는 정보가 포함되면, 제2 신원 정보를 타깃 인증 디바이스에 전송하고, 신원 정보 인증 로그를 생성하는 단계; 및 신원 정보 인증 로그를 사용자 계정의 사용자 단말에 전송하는 단계를 더 포함한다.

[0015] 제1 양상의 가능한 제4 실시방식과 함께 본 발명 실시예는 제1 양상의 가능한 제7 실시방식을 제공한다. 여기에서 서버는 또한 신원 인증 시스템과 통신 연결된다. 상기 방법은 신원 인증 시스템을 통해 사용자 단말에 대해 제2 신원 정보의 등록을 수행하는 단계를 더 포함한다.

[0016] 제1 양상의 가능한 제7 실시방식과 함께 본 발명 실시예는 제1 양상의 가능한 제8 실시방식을 제공한다. 여기에

서 신원 인증 시스템을 통해 사용자 단말에 대해 제2 신원 정보의 등록을 수행하는 단계는, 사용자 단말이 전송한 제2 신원 정보를 수신하는 단계; 제2 신원 정보를 신원 인증 시스템에 전송하는 단계; 신원 인증 시스템을 통해 제2 신원 정보에 대해 신원 검증을 수행하는 단계; 신원 인증 시스템을 통해 제2 신원 정보의 신원 검증 결과를 서버에 전송하는 단계; 신원 검증 결과에 제2 신원 정보가 합법적이라는 정보가 포함되면, 제2 신원 정보 중의 사용자가 저장한 생물 특징과 사용자 계정을 연관 짓는 단계; 제2 신원 정보가 합법적이라는 신원 검증 결과를 사용자 단말에 전송하는 단계; 및 사용자 단말이 제2 신원 정보가 합법적이라는 신원 검증 결과를 수신한 후, 제2 신원 정보를 암호화 처리하고 암호화 처리된 제2 신원 정보를 사용자 단말에 저장하는 단계를 포함한다.

[0017] 제2 양상에 있어서, 본 발명의 실시예는 신원 정보의 인증 장치를 더 제공한다. 상기 장치는 서버에 의해 실행된다. 서버는 각각 타깃 인증 디바이스 및 사용자 단말과 통신 연결된다. 상기 장치는, 타깃 인증 디바이스가 전송하는 인증할 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 수신하도록 구성되는 수신 모듈-여기에서 인증할 사용자의 제1 신원 정보는 인증할 사용자의 현재 생물 특징을 포함하고, 현재 생물 특징은 현재 얼굴 특징을 포함하고, 타깃 인증 디바이스의 식별 정보는 타깃 인증 디바이스의 계정 정보와 타깃 인증 디바이스의 위치 정보를 포함함-; 저장된 합법 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 기반으로, 인증할 사용자의 제1 신원 정보에 대해 합법성 인증을 수행하도록 구성되는 인증 모듈; 및 인증 결과를 타깃 인증 디바이스에 전송하도록 구성되는 전송 모듈을 포함한다.

[0018] 제2 양상과 함께 본 발명의 실시예는 제2 양상의 가능한 제1 실시방식을 제공한다. 여기에서 수신 모듈은 사용자 단말이 전송하는 사용자 단말의 위치 정보를 수신하고, 사용자 단말의 위치 정보에 대해 동적 래스터화 처리를 수행하여, 사용자 단말의 위치 정보가 위치한 래스터를 확정하는 데 사용된다.

[0019] 제3 양상에 있어서, 본 발명 실시예는 서버를 더 제공하며, 여기에는 프로세서와 메모리가 포함된다. 메모리에는 프로그램이 저장되고, 프로그램이 프로세서에 의해 실행될 때 제1 양상 내지 제1 양상의 가능한 제8 실시방식 중 어느 하나의 방법이 실행된다.

[0020] 제4 양상에 있어서, 본 발명 실시예는 칩을 제공한다. 칩에는 프로그램이 저장된다. 프로그램은 프로세서에 의해 실행될 때 전술한 제1 양상 내지 제1 양상의 가능한 제8 실시방식 중 어느 하나에 따른 방법의 단계를 실행한다.

[0021] 본 발명의 실시예는 신원 정보의 인증 방법, 장치 및 서버를 제공한다. 이는 타깃 인증 디바이스가 전송하는 인증할 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 수신한다. 또한 저장된 합법 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 기반으로, 인증할 사용자의 신원 정보에 대해 합법성 인증을 수행한다. 인증 결과는 타깃 인증 디바이스에 전송한다. 인증할 사용자의 신원 정보는 인증할 사용자의 현재 생물 특징을 포함한다. 또한 현재 생물 특징은 현재 얼굴 특징을 포함한다. 타깃 인증 디바이스의 식별 정보는 타깃 인증 디바이스의 계정 정보와 타깃 인증 디바이스의 위치 정보를 포함한다. 서버가 타깃 인증 디바이스에서 전송하는 인증할 사용자의 신원 정보에 대해 인증을 수행할 때, 신원 정보 중의 현재 생물 특징에 대해 수행하는 인증을 포함한다. 또한 타깃 인증 디바이스의 식별 정보가 현재 생물 특징 인증에 미치는 영향을 고려하여, 개인 신원 정보를 효과적으로 보호하고 신원 인증의 안전성, 신뢰성 및 편의성을 향상시키며 사용자 체험도를 강화시킬 수 있다.

[0022] 본 발명의 다른 특징 및 장점은 이하의 명세서에서 설명하며, 일부는 명세서에 의해 명확해지거나 본 발명의 실시에 의해 이해될 것이다. 본 발명의 목적과 기타 장점은 명세서, 청구 범위 및 첨부 도면에 특별히 명시된 구조에 의해 구현 및 획득된다.

[0023] 본 발명의 전술한 목적, 특징 및 장점에 대한 더욱 명확한 이해를 돕기 위해, 이하에서는 비교적 바람직한 실시예를 첨부 도면을 참고하여 상세하게 설명한다.

도면의 간단한 설명

[0024] 이하에서는 본 발명의 구체적인 실시방식 또는 종래 기술의 기술적 해결책을 보다 명확하게 설명하기 위해, 구체적인 실시방식 또는 종래 기술의 설명에 사용할 필요가 있는 첨부 도면을 간략하게 소개한다. 이하의 설명에서 첨부 도면은 본 발명의 일부 실시방식이며, 본 발명이 속한 기술분야의 당업자는 창의적인 노력 없이 이러한 첨부 도면으로부터 다른 도면을 얻을 수 있다.

도 1은 본 발명 실시예에 따른 신원 정보의 인증 방법의 흐름도이다.

도 2는 본 발명 실시예에 따른 다른 신원 정보의 인증 방법의 흐름도이다.

도 3은 본 발명 실시예에 따른 신원 정보의 인증 장치의 구조 블록도이다.

도 4는 본 발명 실시예에 따른 서버의 구조 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 본 발명 실시예의 목적, 기술적 해결책 및 장점에 대한 더욱 명확한 이해를 돕기 위해, 이하에서는 첨부 도면을 참고하여 본 발명의 기술적 해결책을 명확하고 완전하게 설명한다. 설명된 실시예는 본 발명의 전부가 아닌 일부 실시예에 불과하다. 본 발명의 실시예를 기반으로, 본 발명이 속한 기술분야의 당업자가 창의적 노동 없이 획득한 모든 기타 실시예는 모두 본 발명의 보호 범위에 속한다.

[0026] 현재 종래의 생물 특징 인식 기술은 얼굴 이미지와 같은 생물 특징을 수집할 때 촬영 각도, 촬영 거리, 빛 조사 방향, 빛 조사 각도, 광선 명암, 광선 컬러 등 조건의 영향을 받아 얼굴 비교 결과에 비교적 큰 편차가 발생한다. 또한 형제, 자매, 쌍둥이 또는 혈연 관계가 없으나 두 사람이 매우 닮은 경우가 있으므로, 생물 특징 인식 기술의 신뢰성은 개선될 필요가 있다. 시민의 개인 신원 정보는 개인의 사생활에 속하며 법으로 보호된다. 어떠한 개인, 단체, 기업도 시민의 개인 신원 정보를 저장할 수 없다. 개인 신원 정보의 불법 저장은 시민의 프라이버시를 침해하고 심지어 개인 정보 유출을 유발하며 각종 사회 문제를 일으킬 수 있다. 따라서 신원 인증의 안전성은 강화되어야 한다. 이를 기반으로 본 발명의 실시예에서 제공하는 신원 정보의 인증 방법, 장치 및 서버는 개인 신원 정보를 효과적으로 효과적으로 보호하고, 신원 인증의 안전성, 신뢰성 및 간편성을 향상시키며, 사용자 체험도를 강화할 수 있다.

[0027] 본 실시예에 대한 이해를 돕기 위해, 먼저 본 발명 실시예에서 개시한 신원 정보의 인증 방법에 대해 상세히 소개한다.

[0028] 도 1은 신원 정보의 인증 방법의 흐름도이다. 상기 방법은 컴퓨터 등과 같은 서버에 의해 실행된다. 서버는 각각 타깃 인증 디바이스 및 사용자 단말과 통신 연결된다. 상기 방법은 하기 단계를 포함한다.

[0029] 단계 S102: 타깃 인증 디바이스가 전송하는 인증할 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 수신한다. 여기에서 인증할 사용자의 제1 신원 정보는 인증할 사용자의 현재 생물 특징을 포함한다. 현재 생물 특징은 현재 얼굴 특징을 포함한다. 타깃 인증 디바이스의 식별 정보는 타깃 인증 디바이스의 계정 정보와 타깃 인증 디바이스의 위치 정보를 포함한다.

[0030] 타깃 인증 디바이스는 사용자가 업무를 처리하는 셀프 처리 단말(전자 정부 셀프 처리 단말, 전자 은행 셀프 처리 단말, 전자 세무 셀프 처리 단말, 호텔 투숙 셀프 처리 단말, ATM(Automatic Teller Machine) 기기, 웨이팅 기기, 번호 발급기, 셀프 주문서 출력기, 셀프 인보이스 발급기, 셀프 티켓 인출기, 셀프 결산기 등), 공유 디바이스, 스마트 로봇, 스마트 자동차, 무인기, 신원 인증기, 회원 및 귀빈 인식 디바이스, 스마트 접근 제한, 스마트 영상 대화 디바이스, 스마트 게이트 등 신원 인증 디바이스일 수 있다.

[0031] 사용자 단말은 휴대폰 외에 노트북, 태블릿 컴퓨터, 스마트 시계, 스마트 팔찌, 스마트 안경, 스마트 이어폰 및 스마트 버튼식 장치 등과 같은 개인 모바일 디바이스일 수도 있다.

[0032] 생물 특징은 얼굴 생물 특징, 홍채 생물 특징, 공막 생물 특징, 눈가 주름 생물 특징, 손바닥 정맥 생물 특징, 손금 생물 특징, 손가락 정맥 생물 특징, 귀 모양 생물 특징, 성문 생물 특징 중 하나 이상일 수 있다.

[0033] 생물 특징이 얼굴 특징인 경우, 인증할 사용자의 현재 생물 특징은 얼굴 생물 특징이다. 여기에는 생체 얼굴 생물 특징 또는 얼굴 표정 정보가 결합된 생체 얼굴 생물 특징이 포함된다.

[0034] 생물 특징이 얼굴 특징인 경우, 사용자가 저장한 현재 생물 특징은 얼굴 생물 특징이다. 여기에는 얼굴 생물 특징, 얼굴 표정 정보가 결합된 얼굴 생물 특징, 생체 얼굴 생물 특징 또는 얼굴 표정 정보가 결합된 생체 얼굴 생물 특징이 포함된다.

[0035] 수동 설치, BDS(BeiDou Navigation Satellite System), GPS(Global Positioning System), LBS(Location Based Service), AGPS(Assisted Global Positioning System), GSM(Global System for Mobile Communications), IP(Internet Protocol) 어드레스 포지셔닝, WIFI(Wireless Fidelity) 등 하나 이상의 포지셔닝 기술을 통해 위치 포지셔닝을 수행하여, 타깃 인증 디바이스의 위치 정보를 획득할 수 있다.

[0036] 사용자가 고속철도역에서 고속철도역의 셀프 처리 단말로 티켓을 수령할 때, 사용자가 셀프 처리 단말을 사용해

티켓 수령 업무를 처리한다면, 이때 사용자는 인증할 사용자이다. 인증할 사용자는 인증을 통해서만 다음 업무 처리를 수행할 수 있다. 인증할 사용자는 타깃 인증 디바이스의 인터페이스에서 제공하는 프롬프트 정보에 따라 작업을 수행할 수 있다. 생물 특징을 수집하는 옵션을 선택하면, 타깃 인증 디바이스는 현재 얼굴 특징과 같은 사용자의 현재 생물 특징을 수집할 수 있다. 여기에는 현재 생체 얼굴 특징 및/또는 얼굴 표정 정보가 결합된 생체 얼굴 특징이 포함된다. 타깃 인증 디바이스가 수집한 전술한 정보는 인증할 사용자의 제1 신원 정보로 사용된다. 인증할 사용자의 제1 신원 정보는 타깃 인증 디바이스를 통해 서버에 전송된다.

[0037] 단계 S104: 저장된 합법 사용자의 신원 정보와 타깃 인증 디바이스의 식별 정보를 기반으로, 인증할 사용자의 제1 신원 정보에 대해 합법성 인증을 수행한다.

[0038] 서버에는 합법 사용자의 신원 정보가 저장되며, 여기에는 저장된 생물 특징이 포함된다. 합법 사용자는 사용자 단말에 입력한 사용자 정보가 공안부 인증을 통과한 사용자를 포함한다. 이처럼 인증을 통과한 사용자는 사용자 단말에 입력된 생물 특징과 사용자 단말의 식별 정보를 사용자 단말에 저장하고 사용자 단말에 의해 서버로 전송되고 서버에 저장된다. 서버는 타깃 인증 디바이스가 전송한 타깃 인증 디바이스의 위치 정보를 더 획득할 수 있다. 또한 타깃 인증 디바이스의 위치 정보에 대해 동적 래스터화 처리를 수행하여 위치 정보가 위치한 래스터를 확정할 수 있다. 타깃 인증 디바이스의 위치 정보가 위치한 래스터에 따라, 서버에 저장된 합법 사용자의 신원 정보에 대응하는 사용자가 있는 위치가 소정의 래스터 범위에 부합하는 사용자를 확정한다. 서버는 인증할 사용자 정보를 소정의 래스터 범위에 부합하는 사용자의 정보와 일대일 비교하여, 인증할 사용자의 신원 정보의 합법성을 확정한다.

[0039] BDS, GPS, LBS, AGPS, GSM, IP, WIFI 및 자이로스코프 포지셔닝 등 하나 이상의 포지셔닝 기술을 통해 위치 포지셔닝을 수행하여, 사용자가 있는 위치를 획득할 수 있다.

[0040] 단계 S106: 인증 결과를 타깃 인증 디바이스에 전송한다.

[0041] 서버는 인증할 사용자의 신원 정보의 합법성을 확정한 후, 인증 결과를 타깃 인증 디바이스에 전송한다. 인증 결과에 인증할 사용자의 신원 정보가 합법적이라는 정보가 포함될 경우, 인증할 사용자는 인증이 통과된다. 또한 타깃 인증 디바이스는 인증할 사용자가 다음 업무 처리 작업을 수행하도록 허용한다. 인증할 사용자가 인증을 통과하지 못하면, 타깃 인증 디바이스는 인증할 사용자가 후속 작업을 수행하도록 허용하지 않는다.

[0042] 사용자가 고속철도역에서 셀프 처리 단말을 통해 티켓을 수령하는 경우, 이때 고속철도의 셀프 처리 단말이 서버로부터의 인증 결과를 수신한다. 인증 결과에 인증할 사용자의 성명, 신분증 번호 등 합법적인 정보가 포함된 경우, 인증할 사용자는 인증이 통과되며, 셀프 처리 단말은 해당 사용자가 다음 티켓 수령 업무 작업을 수행하도록 허용한다. 이때 업무 처리 단말이 해당 사용자의 합법적인 신원 정보를 획득하며, 기계로 실체 신분증을 판독하는 것과 동일한 효과를 구현하고, "실명(實名), 실인(實人), 실증(實證)"의 인증 결과를 수행한다. 인증할 사용자가 인증을 통과하지 못한 경우, 셀프 처리 단말은 해당 사용자가 후속적인 티켓 수령 업무 작업을 수행하도록 허용하지 않는다.

[0043] 본 발명 실시예에서 제공하는 전술한 신원 정보의 인증 방법은, 타깃 인증 디바이스가 전송하는 인증할 사용자의 제1 신원 정보를 수신한다. 또한 저장된 합법 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 기반으로, 인증할 사용자의 제1 신원 정보에 대해 합법성 인증을 수행하며, 인증 결과를 타깃 인증 디바이스에 전송한다. 인증할 사용자의 제1 신원 정보는 인증할 사용자의 현재 생물 특징을 포함한다. 또한 현재 생물 특징은 현재 얼굴 특징을 포함한다. 타깃 인증 디바이스의 식별 정보는 타깃 인증 디바이스의 계정 정보와 타깃 인증 디바이스의 위치 정보를 포함한다. 서버가 타깃 인증 디바이스에서 전송하는 인증할 사용자의 신원 정보에 대해 인증을 수행할 때, 신원 정보 중의 현재 생물 특징에 대해 진행하는 인증을 포함한다. 또한 타깃 인증 디바이스의 식별 정보가 현재 생물 특징 인증에 미치는 영향을 고려하여, 개인 신원 정보를 효과적으로 보호하고 신원 인증의 안전성, 신뢰성 및 편의성을 향상시키며 사용자 체험도를 강화시킬 수 있다.

[0044] 이해를 돕기 위해 이하에서는 본 실시예에서 제공하는 다른 신원 정보의 인증 방법을 제공한다. 도 2는 신원 정보의 인증 방법의 흐름도이다. 상기 방법은 하기 단계를 포함한다.

[0045] 단계 S202: 사용자 단말이 전송하는 사용자 단말의 위치 정보를 수신한다.

[0046] 단계 S204: 사용자 단말의 위치 정보에 대해 동적 래스터화 처리를 수행하여, 사용자 단말의 위치 정보가 위치한 래스터를 확정한다.

[0047] 동적 래스터 관리 기술을 기반으로, 수신한 사용자 단말의 위치 정보가 위치한 래스터를 확정할 수 있다.

[0048] 단계 S206: 타깃 인증 디바이스가 전송하는 인증할 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 수신한다. 여기에서 인증할 사용자의 제1 신원 정보는 인증할 사용자의 현재 생물 특징을 포함한다. 현재 생물 특징은 현재 얼굴 특징을 포함한다. 타깃 인증 디바이스의 식별 정보는 타깃 인증 디바이스의 계정 정보와 타깃 인증 디바이스의 위치 정보를 포함한다.

[0049] 타깃 인증 디바이스는 카메라를 포함한다. 타깃 인증 디바이스의 카메라를 통해 인증할 사용자의 현재 생물 특징을 수집한다.

[0050] 타깃 인증 디바이스에 생체 생물 특징 판단 방법이 미리 저장된 경우, 해당 생체 생물 특징 판단 방법을 통해 인증할 사용자의 현재 생물 특징이 생체인지 여부를 판단한다. 생체가 아닌 것으로 판단되면, 타깃 인증 디바이스는 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 서버에 전송하지 않는다.

[0051] 단계 S208: 타깃 인증 디바이스의 위치 정보에 대해 동적 래스터화 처리를 수행하여, 타깃 인증 디바이스의 위치 정보가 위치한 래스터를 확정한다.

[0052] 동적 래스터 관리 기술을 기반으로, 서버는 타깃 인증 디바이스의 위치 정보에 대해 동적 래스터화 처리를 수행하여, 타깃 인증 디바이스의 위치 정보가 위치한 래스터를 확정한다.

[0053] 단계 S210: 타깃 인증 디바이스의 위치 정보가 위치한 래스터와 타깃 인증 디바이스의 위치 정보가 위치한 래스터로부터 소정 범위 내에 떨어진 래스터를 타깃 래스터로 사용한다.

[0054] 소정 범위는 서버에 미리 저장된 것일 수 있으며, 서버는 미리 저장된 소정 범위에 따라 타깃 래스터를 확정한다.

[0055] 단계 S212: 저장된 합법 사용자의 제1 신원 정보를 기반으로, 각 사용자 단말의 위치 정보가 타깃 래스터에 위치한 각 사용자가 저장한 생물 특징을 조회한다.

[0056] 서버는 타깃 래스터에 위치한 사용자 단말을 검색한다. 검색된 사용자 단말에 따라 타깃 래스터 중 각 사용자 단말에 대응하는 각 사용자가 저장한 생물 특징을 조회한다.

[0057] 단계 S214: 현재 생물 특징이 생체의 생물 특징인지 여부를 판단한다. 그러한 경우 단계 S216을 실행하며, 그러하지 않은 경우 종료한다.

[0058] 미리 저장된 생체의 생물 특징을 판단하는 방법에 따라 현재 생물 특징에 대한 판단을 수행할 수 있다.

[0059] 단계 S216: 인증할 사용자의 현재 생물 특징과 조회한 각 사용자가 저장한 생물 특징을 일대일 비교한다.

[0060] 단계 S218: 비교하여 획득한 하나의 저장된 생물 특징과 현재 생물 특징의 유사도가 소정의 유사도 임계값보다 큰 경우, 유사도가 소정의 유사도 임계값보다 큰 저장된 생물 특징을 현재 생물 특징으로 확정한다.

[0061] 타깃 래스터 중의 사용자가 저장한 생물 특징 중에서 단 하나와 현재 생물 특징의 유사도가 소정의 유사도 임계값보다 큰 경우, 이는 타깃 래스터의 사용자가 저장한 생물 특징 중에 있고 하나의 생물 특징만 현재 생물 특징과 매칭될 수 있음을 의미한다. 또한 유사도가 소정의 유사도 임계값보다 큰 해당 생물 특징을 현재 생물 특징으로 확정한다.

[0062] 단계 S220: 비교하여 획득한 복수의 저장된 생물 특징과 현재 생물 특징의 유사도가 소정의 유사도 임계값보다 큰 경우, 각 유사도가 소정의 유사도 임계값보다 큰 저장된 생물 특징에 각각 대응하는 사용자를 복수의 인증할 사용자로 확정한다.

[0063] 단계 S222: 복수의 인증할 사용자에 대해 다시 신원 인증을 수행한다. 여기에서 신원 확인은 신분증의 소정의 자릿수의 숫자 및/또는 생물 인식 매칭을 포함한다.

[0064] 서버가 타깃 인증 디바이스에 다시 신원을 확인하는 알림을 전송하는 것일 수 있다. 타깃 인증 디바이스는 서버가 전송하는 알림에 따라, 인증할 사용자가 다시 신원 확인을 수행하도록 프롬프트한다. 예를 들어 인증할 사용자가 신분증의 소정의 자릿수의 숫자 및/또는 휴대폰 번호를 입력하거나, 홍채, 공막, 손가락 정맥, 손바닥 정맥, 손금, 눈가 주름, 귀 모양 및 성문 등 생물 인식을 수행하여 확인하도록 프롬프트한다. 또한 신원 재확인 유사도가 소정의 유사도 임계값보다 큰 생물 특징에 대응하는 계정을 현재 사용자 계정으로 확정한다.

[0065] 일 실시방식에 있어서, 서버는 현재 사용자 계정의 사용자 단말에 사용자의 제2 신원 정보를 획득하는 요청을 전송한다. 여기에서 사용자 단말에는 사용자의 제2 신원 정보가 있다. 사용자의 제2 신원 정보는 사용자의

성명, 사용자의 신분증 번호 및 사용자가 저장한 생물 특징을 포함한다. 서버가 현재 사용자 계정의 사용자 단말이 전송한 사용자의 제2 신원 정보를 수신한 경우, 사용자 단말이 상기 요청에 대한 응답을 허용하도록 설정되었는지 여부를 판단하고, 제2 신원 정보의 합법성을 검증한다. 사용자 단말이 요청에 응답하도록 허용하고 제2 신원 정보가 합법적인 경우, 서버는 제2 신원 정보를 타깃 인증 디바이스에 전송하고 서버를 통해 신원 인증 로그를 생성한다. 서버는 신원 정보 인증 로그를 사용자 계정의 사용자 단말에 전송한다.

[0066] 구체적으로, 서버는 사용자 계정의 사용자 단말에 사용자의 제2 신원 정보를 획득하는 요청을 전송한 후, 현재 사용자 계정의 사용자 단말을 통해 제2 신원 정보의 합법성을 검증한다. 제2 신원 정보가 합법적인 경우, 현재 사용자 계정의 사용자 단말을 통해 제2 신원 정보를 서버에 전송한다.

[0067] 일 실시방식에 있어서, 서버는 또한 신원 인증 시스템과 통신 연결된다. 상기 방법은 신원 인증 시스템을 통해 사용자 단말에 대해 제2 신원 정보의 등록을 수행하고, 서버는 사용자 단말이 전송하는 제2 신원 정보를 수신하며, 제2 신원 정보를 신원 인증 시스템에 전송하는 단계; 신원 인증 시스템을 통해 제2 신원 정보에 대한 신원 검증을 수행하고, 제2 신원 정보의 신원 검증 결과를 서버에 전송하는 단계; 신원 검증 결과에 제2 신원 정보가 합법적이라는 정보가 포함되면, 서버가 제2 신원 정보 중의 사용자 생물 특징을 사용자 계정과 연관 짓고, 제2 신원 정보가 합법인 신원 검증 결과를 사용자 단말에 전송하는 단계; 사용자 단말이 제2 신원 정보가 합법적이라는 신원 검증 결과를 수신한 후, 제2 신원 정보를 암호화 처리하고 암호화 처리된 제2 신원 정보를 사용자 단말에 저장하는 단계를 더 포함한다. 전술한 암호화 처리는 소정의 암호화 방식일 수 있으며, 소정의 암호화 방식에 따라 제2 신원 정보에 대해 암호화 처리를 수행한다.

[0068] 단계 S224: 인증 결과를 타깃 인증 디바이스에 전송한다.

[0069] 인증 결과에 인증할 사용자가 인증을 통과한 정보가 포함된 경우, 타깃 인증 디바이스는 인증할 사용자가 다음 업무 처리 작업을 수행하도록 허용한다. 인증할 사용자가 인증을 통과하지 못한 경우, 타깃 인증 디바이스는 인증할 사용자가 후속 작업을 수행하도록 허용하지 않는다.

[0070] 일 실시방식에 있어서, 사용자가 타깃 인증 디바이스를 이용하여 신원 인증을 수행하기 전에, 사용자 단말에 대응하는 APP을 다운로드 및 설치하고 열어야 한다. APP 등록에서 해당 사용자의 고유 ID, 즉 전술한 사용자 단말의 식별 정보를 획득한다. 신분증 정보 입력 페이지를 선택하고 성명, 신분증 번호 등(구체적으로 공안부의 인터페이스 요구)을 입력한다. 개인 사진 이미지 정보를 입력하며, 해당 정보는 정적 이미지, 현장 촬영 이미지, 현장 촬영 생체 생물 특징일 수 있다. 구체적인 공안부 신원 인증 인터페이스 규범에 따라, 사용자 성명, 신분증 번호, 개인 사진 이미지 정보 등을 신원 인증 인터페이스에 전송하여 신원 인증을 수행한다. 인증이 통과하면, 전술한 개인 사진 이미지 정보와 사용자 고유 ID를 연관 지어 서버 데이터베이스에 저장한다. 인증이 통과된 메시지를 사용자 APP에 전송하며, APP은 사용자 고유 ID 및 사용자의 성명, 신분증 번호, 개인 사진 이미지 등 정보를 암호화 처리한다. 또한 암호화 처리된 암호화 정보를 사용자 단말의 저장 유닛에 저장한다. 저장 유닛은 파일, 데이터베이스, 전용 칩 등일 수 있다. 암호화 정보에 사용자 단말의 하드웨어 ID 정보를 추가하여 변조를 방지한다.

[0071] 또한 신원 인증 인터페이스가 채택하는 것이 네트워크 신분증 CTID에서 제공하는 신원 인증 인터페이스인 경우, 해당 사용자 고유의 CTID 일련번호를 다운로드하고 사용자 단말에 저장할 수 있다. 본 디바이스에서 채택하는 것이 전자 신분증 eID인 경우, eID의 하드웨어 정보를 바인딩하여 사용자 단말에 저장할 수 있다. 사용자는 APP의 권한 부여 옵션 중 "권한 부여" 또는 "권한 미부여"를 선택하여, 해당 사용자의 신원 정보가 판독 작업을 허용하는지 여부를 확정할 수 있다. 전술한 과정에서 서버는 사용자의 얼굴 정보와 사용자의 고유 ID, 즉 전술한 서버에 저장된 생물 특징과 사용자 단말의 식별 정보만 저장하며, 사용자의 성명, 신분증 번호 등 개인 신원 정보는 저장하지 않는다.

[0072] 서버는 인증할 사용자의 사용자 계정, 즉 전술한 사용자 단말의 식별 정보를 확정하고, 사용자 계정을 사용자 단말의 APP으로 전송하며, 사용자의 신원 정보를 획득하도록 요청한다. 사용자 단말의 APP은 해당 요청을 수신한 후, 먼저 사용자가 신원 정보를 판독하는 권한을 부여 받았는지 여부를 판단한다. 그 다음 사용자가 완전한 신원 정보인지 여부를 판단한 후, 사용자 단말에 저장된 신원 정보가 합법적인지 여부를 판단한다. 여기에는 해당 정보가 변조된 것인지 여부의 판단, 사용자의 고유 ID가 일치하는지 여부의 판단, 및 사용자 단말의 하드웨어 ID 정보와 일치하는지 여부의 판단이 포함된다. 사용자가 신원 정보를 판독하는 권한을 이미 부여 받았고 사용자 단말의 신원 정보가 합법적인 경우, 해당 APP은 사용자 단말의 신원 정보를 서버로 전송한다. 전술한 사용자 단말이 전자 신분증 eID를 채택하는 경우, eID와 바인딩된 하드웨어 정보가 일치하는지 여부를 판단한다.

[0073] 서버는 APP이 전송한 사용자 단말의 신원 정보를 수신한 후, 먼저 사용자의 고유 ID가 일치하는지 여부를 판단한 다음, 개인 사진 이미지 정보가 일치하는지 여부를 판단한다. 일반적인 업무(예를 들어 주거 커뮤니티에 진입하는 신원 인증, 대기 번호 수령 등)의 경우, 서버는 사용자의 신원 정보를 타깃 인증 디바이스에 곧바로 전송하여, 이번 회차 신원 인증 및 신원 정보 획득 작업을 완료할 수 있다. 또한 신원 인증 기록을 생성하는 동시에 생성된 신원 인증 기록을 사용자 단말의 APP에 전송할 수 있다. 보안 레벨이 비교적 높은 업무(예를 들어 입출국의 신원 인증, ATM 기기의 은행카드 없는 현금 인출 등)의 경우, 서버는 2차 신원 인증을 수행해야 한다. 해당 사용자의 성명, 신분증 번호 및 셀프 처리 단말기에서 촬영한 현장 사진, 즉 전술한 현재 생물 특징(구체적인 내용은 신원 인증 인터페이스 규범에 따라 결정)을 신원 인증 인터페이스에 전송하여 신원 인증을 수행한다. 2차 신원 인증이 통과되면, 다시 사용자의 신원 정보를 타깃 인증 디바이스에 전송하여, 이번 회차 신원 인증 및 신원 정보 획득 작업을 완료한다. 또한 신원 인증 기록을 생성하는 동시에 생성된 신원 인증 기록을 사용자 단말의 APP에 전송한다. 여기에서 네트워크 신분증 CTID이 제공하는 신원 인증 인터페이스를 채택하였고, 사용자 정보에 해당 사용자 고유의 CTID 일련번호가 포함된 경우, 2차 신원 인증을 수행할 때, 해당 사용자의 CTID 일련번호와 셀프 처리 단말기에서 촬영한 현장 사진, 즉 전술한 현재 생물 특징(구체적인 내용은 신원 인증 인터페이스 규범에 따라 결정)을 대응하는 신원 인증 인터페이스로 전송하고, 2차 신원 인증이 통과했는지 여부를 판단한다.

[0074] 상기 내용을 종합하면, 본 발명의 실시예에서 제공하는 전술한 신원 정보의 인증 방법에 있어서, 인증할 사용자의 신원 정보에는 인증할 사용자의 현재 생물 특징이 포함된다. 또한 현재 생물 특징에는 현재 얼굴 특징이 포함된다. 타깃 인증 디바이스의 식별 정보에는 타깃 인증 디바이스의 계정 정보와 타깃 인증 디바이스의 위치 정보가 포함된다. 서버는 타깃 인증 디바이스에서 전송한 인증할 사용자의 신원 정보에 대한 인증을 수행할 때, 타깃 인증 디바이스의 위치 정보가 위치한 래스터에 따라, 인증할 사용자의 신원 정보 중의 현재 생물 특징에 대해 인증을 수행한다. 따라서 타깃 인증 디바이스의 식별 정보가 현재 생물 특징 인증에 미치는 영향을 고려하여, 래스터화 기술을 통해 생물 특징 비교 수량을 효과적으로 줄이고 비교 속도를 향상시켰다. 또한 하드웨어 디바이스의 투입을 줄이고 생물 특징 비교의 정확성 및 신원 인증의 안전성을 효과적으로 향상시켰다. 개인 정보의 안전성과 합법성을 고려하여, 사용자 디바이스를 통해 각각의 개인 정보를 저장하고 신원 정보의 합법성 검증을 통해 변조를 방지하여 개인 신원 정보를 효과적으로 보호한다. 또한 공안부 신원 인증 시스템의 권위성을 통해 신원 인증의 신뢰성을 구현한다. 이를 기반으로 사용자는 실체 신분증을 휴대하지 않고도 기계가 실체 신분증을 판독하는 것과 동일한 효과를 구현한다. 또한 "실명, 실인, 실증"의 신원 검증을 완료하여 외출의 편의성을 향상시키고 신원 인증 간편성을 구현한다. 실체 신분증, 휴대폰 등 실물을 휴대할 필요가 없고 신분증 번호, 휴대폰 번호를 입력하는 작업 없이 곧바로 생물 특징을 통해 기계가 신분증을 판독하는 효과를 구현하여 사용자 체험도를 효과적으로 강화시킨다.

[0075] 전술한 신원 정보의 인증 방법에 대응하여, 본 발명 실시예는 신원 정보의 인증 장치를 제공한다. 도 3은 신원 정보의 인증 장치의 구조 블록도이다. 상기 장치는 서버에 의해 실행된다. 서버는 각각 타깃 인증 디바이스 및 사용자 단말과 통신 연결된다. 상기 장치는 하기 모듈을 포함한다.

[0076] 수신 모듈(302)은 타깃 인증 디바이스가 전송하는 인증할 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 수신하도록 구성된다. 여기에서 인증할 사용자의 제1 신원 정보는 인증할 사용자의 현재 생물 특징을 포함한다. 현재 생물 특징은 현재 얼굴 특징을 포함한다. 타깃 인증 디바이스의 식별 정보는 타깃 인증 디바이스의 계정 정보와 타깃 인증 디바이스의 위치 정보를 포함한다.

[0077] 인증 모듈(304)은 저장된 합법 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 기반으로, 인증할 사용자의 제1 신원 정보에 대해 합법성 인증을 수행하도록 구성된다.

[0078] 전송 모듈(306)은 인증 결과를 타깃 인증 디바이스에 전송하도록 구성된다.

[0079] 본 발명 실시예에서 제공하는 전술한 신원 정보의 인증 장치에 있어서, 인증할 사용자의 신원 정보는 인증할 사용자의 현재 생물 특징을 포함한다. 현재 생물 특징에는 현재 얼굴 특징이 포함된다. 타깃 인증 디바이스의 식별 정보에는 타깃 인증 디바이스의 계정 정보와 타깃 인증 디바이스의 위치 정보가 포함된다. 서버는 타깃 인증 디바이스에서 전송한 인증할 사용자의 신원 정보에 대한 인증을 수행할 때, 신원 정보 중의 현재 생물 특징에 대해 인증을 수행한다. 따라서 타깃 인증 디바이스의 식별 정보가 현재 생물 특징 인증에 미치는 영향을 고려하여, 개인 신원 정보를 효과적으로 보호하고 신원 인증의 안전성, 신뢰성 및 편의성을 향상시키며 사용자 체험도를 강화시킬 수 있다.

[0080] 상기 수신 모듈(302)은 사용자 단말이 전송하는 사용자 단말의 위치 정보를 수신하고, 사용자 단말의 위치 정보

에 대해 동적 래스터화 처리를 수행하여, 사용자 단말의 위치 정보가 위치한 래스터를 확정하도록 더 구성된다.

[0081] 본 실시예에서 제공하는 장치는 그 구현 원리 및 나타나는 기술적 효과가 전술한 실시예와 동일하다. 간단한 설명을 위해 장치 실시예에서 언급되지 않은 부분은 전술한 방법 실시예에서 상응하는 내용을 참조한다.

[0082] 본 발명 실시예는 서버를 제공한다. 도 4는 서버의 구조 개략도이다. 상기 서버는 프로세서(40), 메모리(41), 버스(42) 및 통신 인터페이스(43)를 포함한다. 상기 프로세서(40), 통신 인터페이스(43) 및 메모리(41)는 버스(42)에 의해 연결된다. 프로세서(40)는 메모리(41)에 저장되는 실행 가능 모듈, 예를 들어 컴퓨터 프로그램을 실행하는 데 사용된다.

[0083] 여기에서 메모리(41)는 고속 랜덤 액세스 메모리(RAM, Random Access Memory)를 포함할 수 있다. 또한 비휘발성 메모리(non-volatile memory), 예를 들어 적어도 하나의 디스크 메모리를 더 포함할 수도 있다. 적어도 하나의 통신 인터페이스(43)(유선 또는 무선일 수 있음)가 상기 시스템 네트워크 요소와 적어도 하나의 다른 네트워크 요소 간의 통신 연결을 구현함으로써, 인터넷, 광역 네트워크, 로컬 네트워크, 도시 지역 통신 네트워크 등을 사용할 수 있다.

[0084] 버스(42)는 ISA 버스, PCI 버스 또는 EISA 버스 등일 수 있다. 상기 버스는 어드레스 버스, 데이터 버스, 컨트롤 버스 등으로 나눌 수 있다. 설명의 편의를 위해 도 4에서는 양방향 화살표를 하나만 사용하여 표시하였다. 그러나 이는 하나의 버스 또는 한 유형의 버스만 있음을 의미하지는 않는다.

[0085] 여기에서 메모리(41)는 프로그램을 저장하도록 구성된다. 상기 프로세서(40)는 실행 명령을 수신한 후 상기 프로그램을 실행한다. 전술한 본 발명의 실시예 중 어느 하나의 실시예에 개시된 플로우 프로세스 정의의 장치에 의해 실행되는 방법은 프로세서(40)에 적용되거나 프로세서(40)에 의해 구현될 수 있다.

[0086] 프로세서(40)는 신호 처리 능력을 갖는 집적회로 칩일 수 있다. 구현 과정에서 전술한 방법의 각 단계는 프로세서(40) 중 하드웨어의 집적 논리 회로 또는 소프트웨어 형태의 명령에 의해 완료될 수 있다. 전술한 프로세서(40)는 중앙 처리 장치(Central Processing Unit, CPU) 및 네트워크 프로세서(Network Processor, NP) 등이 포함된 범용 프로세서일 수 있다. 또한 디지털 신호 프로세서(Digital Signal Processor, DSP), 주문형 집적회로(Application Specific Integrated Circuit, ASIC), 필드 프로그래밍 가능 게이트 어레이(Field-Programmable Gate Array, FPGA) 또는 기타 프로그래밍 가능 논리 소자, 이산 게이트 또는 트랜지스터 논리 소자, 이산 하드웨어 구성 요소일 수도 있다. 본 발명 실시예에 개시된 방법, 단계 및 논리 블록도는 구현하거나 실행할 수 있다. 범용 프로세서는 마이크로 프로세서일 수 있으며, 해당 프로세서는 임의의 일반적인 프로세서 등일 수도 있다. 본 발명 실시예에 개시된 방법을 결합한 단계는 하드웨어 디코딩 프로세서에 의해 실행 및 완료되도록 직접 구현될 수 있다. 또는 디코딩 프로세서의 하드웨어 및 소프트웨어 모듈의 조합에 의해 실행 및 완료되도록 구현될 수도 있다. 소프트웨어 모듈은 랜덤 액세스 메모리, 플래시 메모리, 읽기 전용 메모리, 프로그램 가능 읽기 전용 메모리 또는 전기적 소거 및 프로그램 가능 메모리, 레지스터 등 당업계에서 성숙한 저장 매체에 위치할 수 있다. 상기 저장 매체는 메모리(41)에 위치한다. 프로세서(40)는 메모리(41) 내의 정보를 읽고, 그 하드웨어와 결합하여 전술한 방법의 단계를 완료한다.

[0087] 본 발명의 실시예는 칩을 더 제공한다. 칩에는 프로그램이 저장된다. 프로그램이 프로세서에 의해 실행될 때 전술한 실시예 중 어느 하나의 방법의 단계가 실행된다.

[0088] 본 발명이 속한 기술 분야의 당업자는 설명상 편의와 간결함을 위해, 상기에서 설명된 시스템의 구체적인 작업 과정이 전술한 방법 실시예에서의 대응하는 과정을 참조할 수 있음을 명확하게 이해할 수 있다. 따라서 여기에서 반복하여 설명하지 않는다.

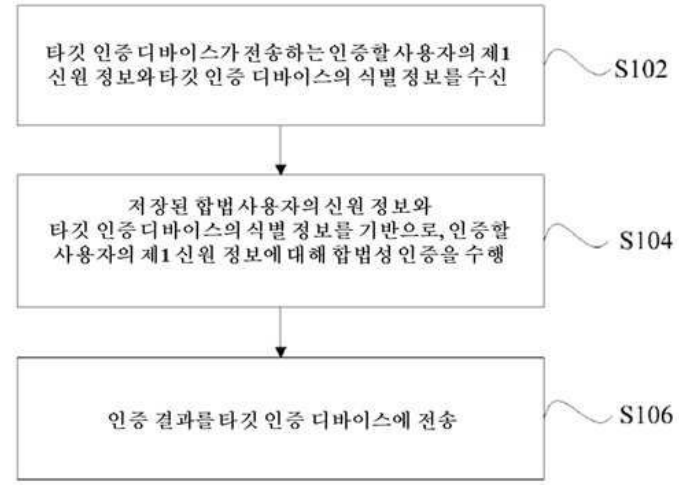
[0089] 본 발명 실시예에서 제공하는 신원 정보의 인증 방법, 장치 및 서버의 프로그램 제품은 프로그램 코드가 저장된 칩을 포함한다. 상기 프로그램 코드에 포함된 명령은 전술한 방법 실시예 중의 방법을 실행하는 데 사용될 수 있다. 구체적인 구현은 방법 실시예를 참고할 수 있으므로 여기에서 더이상 설명하지 않는다.

[0090] 상기 기능이 소프트웨어 기능 유닛의 형태로 구현되어 독립적인 제품으로 판매되거나 사용되는 경우, 하나의 칩에 저장될 수 있다. 이러한 이해를 바탕으로 본 발명의 기술적 해결책은 본질적으로 또는 종래 기술에 기여하는 부분 또는 상기 기술적 해결책의 일부가 소프트웨어 제품의 형태로 구현될 수 있다. 상기 소프트웨어 제품은 하나의 칩에 저장되며, 여기에는 한 대의 컴퓨터 디바이스(개인용 컴퓨터, 서버 또는 네트워크 디바이스 등일 수 있음)가 본 발명 각 실시예에 따른 상기 방법의 모든 또는 일부 단계를 실행하는 데 사용되는 여러 명령이 포함된다.

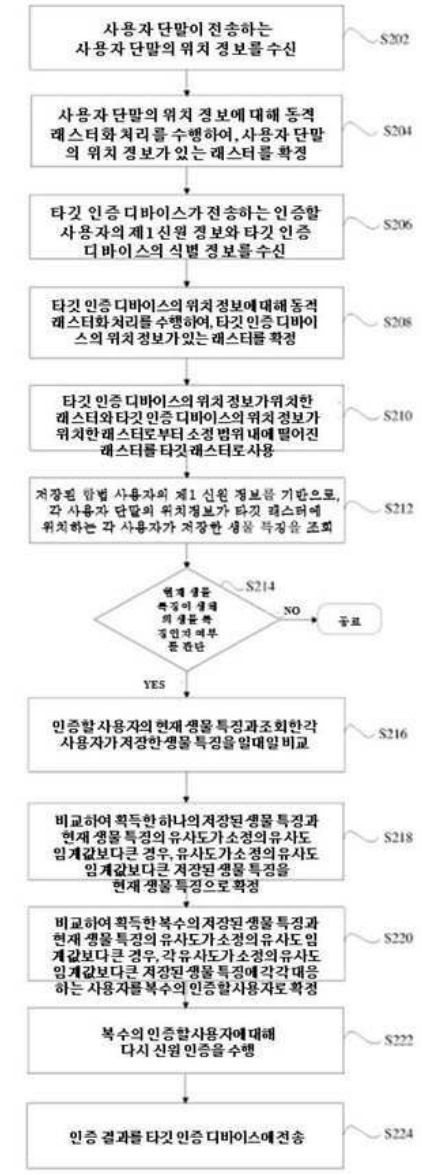
[0091] 마지막으로, 상기 실시예는 본 발명의 구체적인 실시방식일 뿐이며, 본 발명의 기술적 해결책을 설명하기 위한 것으로 이를 제한하지 않는다는 점에 유의해야 한다. 본 발명의 보호 범위는 이에 제한되지 않으며, 전술한 실시예를 참조하여 본 발명을 상세하게 설명하였을 뿐이다. 본 발명이 속한 기술분야의 당업자는 본 발명에 개시된 기술적 범위 내에서 당업계에서 익숙한 당업자라면 전술한 실시예에 기재된 기술적 해결책을 수정하거나 변경하는 것을 용이하게 생각할 수 있으며, 그 중 일부 기술적 특징을 동등한 수준으로 치환할 수도 있다. 이러한 수정, 변경 또는 치환은 상응하는 기술적 해결책의 본질이 본 발명 실시예에 따른 기술적 해결책의 정신과 범위를 벗어나게 만들지 않으므로 모두 본 발명의 보호 범위 내에 속하는 것으로 이해해야 한다. 따라서 본 발명의 보호 범위는 상기 청구 범위의 보호 범위를 기준으로 한다.

도면

도면1



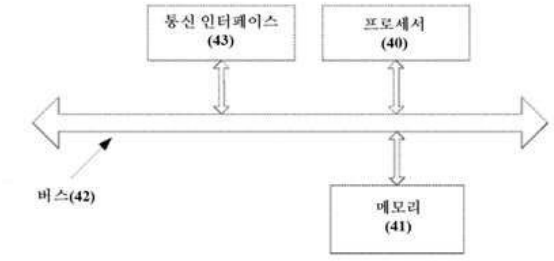
도면2


사용자 단말이 전송하는 사용자 단말의 위치 정보를 수신
S202
사용자 단말의 위치 정보에 대해 동적 래스터화 처리를 수행하여, 사용자 단말의 위치 정보가 있는 래스터를 확정
S204
타깃 인증 디바이스가 전송하는 인증할 사용자의 제1 신원 정보와 타깃 인증 디바이스의 식별 정보를 수신
S206
타깃 인증 디바이스의 위치 정보에 대해 동적 래스터화 처리를 수행하여, 타깃 인증 디바이스의 위치 정보가 있는 래스터를 확정
S208
타깃 인증 디바이스의 위치 정보가 위치한 래스터와 타깃 인증 디바이스의 위치 정보가 위치한 래스터로부터 소정 범위 내에 떨어진 래스터를 타깃 래스터로 사용
S210
저장된 합법 사용자의 제1 신원 정보를 기반으로, 각 사용자 단말의 위치 정보가 타깃 래스터에 위치하는 각 사용자가 저장한 생물 특징을 조회
S212
현재 생물 특징의 생물 특징과 일치하는 생물 특징인지 여부를 판단
S214
NO
종료
YES
인증할 사용자의 현재 생물 특징과 조회한 각 사용자가 저장한 생물 특징을 일대일 비교
S216
비교하여 획득한 하나의 저장된 생물 특징과 현재 생물 특징의 유사도가 소정의 유사도 임계값보다 큰 경우, 유사도가 소정의 유사도 임계값보다 큰 저장된 생물 특징을 현재 생물 특징으로 확정
S218
비교하여 획득한 복수의 저장된 생물 특징과 현재 생물 특징의 유사도가 소정의 유사도 임계값보다 큰 경우, 각 유사도가 소정의 유사도 임계값보다 큰 저장된 생물 특징에 각각 대응하는 사용자를 복수의 인증할 사용자로 확정
S220
복수의 인증할 사용자에 대해 다시 신원 인증을 수행
S222
인증 결과를 타깃 인증 디바이스에 전송
S224

도면3


수신 모듈(302)
인증 모듈(304)
전송 모듈(306)

도면4



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 13

【변경전】

칩에 있어서,

상기 칩에 프로그램이 저장되고, 상기 프로그램은 프로세서에 의해 실행될 때 제1항 내지 제9항 중 어느 한 항에 따른 방법의 단계를 실행하는 것을 특징으로 하는 칩.

【변경후】

칩에 있어서,

상기 칩에 프로그램이 저장되고, 상기 프로그램은 프로세서에 의해 실행될 때 제1항, 또는 제3항 내지 제9항 중 어느 한 항에 따른 방법의 단계를 실행하는 것을 특징으로 하는 칩.

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 12

【변경전】

서버에 있어서,

프로세서 및 메모리를 포함하고,

상기 메모리에 컴퓨터 프로그램이 저장되고, 상기 컴퓨터 프로그램이 상기 프로세서에 의해 실행될 때 제1항 내지 제9항 중 어느 한 항에 따른 방법을 실행하는 것을 특징으로 하는 서버.

【변경후】

서버에 있어서,

프로세서 및 메모리를 포함하고,

상기 메모리에 컴퓨터 프로그램이 저장되고, 상기 컴퓨터 프로그램이 상기 프로세서에 의해 실행될 때 제1항, 또는 제3항 내지 제9항 중 어느 한 항에 따른 방법을 실행하는 것을 특징으로 하는 서버.