

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl.

G06K 19/07 (2006.01)

G06K 17/00 (2006.01)

G06K 9/00 (2006.01)

(11) 공개번호 10-2006-0079059

(43) 공개일자 2006년07월05일

(21) 출원번호 10-2005-0046681

(22) 출원일자 2005년06월01일

(30) 우선권주장 2004101046583 2004년12월31일 중국(CN)

(71) 출원인 삼성전자주식회사
경기도 수원시 영통구 매탄동 416
중국과학원 자동화연구소
중국 베이징 이스트로드 중관춘 95번지

(72) 발명자 기석철
경기 용인시 죽전1동 현대홈타운3차2단지아파트 506-703
왕양생
중국 북경시 중관춘 동로 95번지

(74) 대리인 리앤목특허법인
이해영

심사청구 : 없음

(54) 사용자 식별을 위한 생체정보를 저장하는 카드, 그를이용한 사용자 식별 방법 및 장치.

요약

본 발명은 생체 정보가 저장된 카드를 이용하여 사용자를 식별하는 방법 및 장치에 관한 것이다. 그 방법은 카드의 유효 여부를 판단하는 단계; 카드가 유효한 카드인 경우, 사용자로부터 얼굴, 지문 및 홍채 화상을 획득하는 단계; 획득된 얼굴, 지문 및 홍채 화상을 카드에 저장된 사용자의 얼굴, 지문 및 홍채 화상의 특징 데이터와 비교하는 단계; 및 비교한 결과, 얼굴, 지문 및 홍채 각각에 대한 획득 화상과 카드에 저장된 특징 데이터 사이의 유사도들이 모두 소정의 허용 범위들에 속하는 경우 사용자가 일치하는 것으로 판단하는 단계를 포함하는 것을 특징으로 한다.

본 발명에 의하면, 공항에서의 여권 본인 확인 등 사용자의 진위 여부를 확인하고자 하는 경우, 카드에 저장된 사용자의 얼굴, 지문 및 홍채의 생체정보를 이용하여 사용자를 식별할 수 있도록 함으로써, 수작업을 통한 사용자 식별에 소모되는 시간을 감소시킬 수 있으며, 사용자 식별 결과의 정확성 및 신뢰성을 높일 수 있다.

대표도

도 2

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 사용자 식별 장치의 전체적인 구성을 나타내는 블록도이다.

도 2는 본 발명에 따른 생체정보를 가지는 카드를 이용한 사용자 식별 방법을 나타내는 흐름도이다.

도 3은 도 2의 카드의 유효성을 확인하는 단계에 대한 실시예를 나타내는 흐름도이다.

도 4는 본 발명에 따른 생체정보를 가지는 카드를 이용한 또 다른 사용자 식별 방법을 나타내는 흐름도이다.

도 5는 본 발명에 따른 생체정보를 가지는 카드를 등록하는 방법을 나타내는 흐름도이다.

도 6은 생체정보를 가지는 카드를 이용한 사용자 식별 장치에 대한 실시예를 나타내는 도면이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 사용자의 생체정보를 이용하여 사용자를 식별하는 방법 및 장치에 관한 것으로서, 특히 카드에 저장된 사용자의 얼굴, 지문 및 홍채의 생체정보를 이용하여 사용자를 식별 있도록 하는 사용자 식별 방법 및 장치에 관한 것이다.

일반적으로 보안등을 위해 제한된 사용자에게만 접근을 허용하거나, 특정 작업 수행 시 본인 확인을 위해 사용자를 식별하기 위한 방법들이 사용된다.

특히, 최근에는 항공 사고를 미연에 방지하고자 탑승객의 신원 확인 및 본인 확인을 정확하게 하기 위한 시스템들이 도입되고 있다. 그러나 수작업에 의한 사용자 확인으로 인해 식별 작업에 소모되는 시간이 증가되고, 여권의 위조 등을 본인 불일치를 수작업에 의해서는 정확하게 판단할 수 없어 사용자 식별의 신뢰성이 낮은 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는, 공항 등에서 사용자를 식별함에 있어 상기와 같은 문제점들을 해결하기 위해, 카드에 저장된 사용자의 얼굴, 지문 및 홍채의 생체정보를 이용하여 사용자를 식별할 수 있도록 사용자 식별 방법 및 장치를 제공하는 것이다.

발명의 구성 및 작용

상술한 기술적 과제를 해결하기 위한 본 발명에 의한 사용자 생체정보를 저장하는 카드의 제조 방법은, 사용자의 얼굴, 지문, 홍채의 화상들을 입력받는 단계; 상기 입력된 얼굴, 지문, 홍채의 화상이 소정의 식별 조건에 부합되는지 확인하는 단계; 상기 확인 결과, 상기 식별 조건에 부합되지 않는 경우 상기 식별 조건에 부합될 때까지 상기 화상 입력 단계 및 식별 조건 확인 단계를 반복하고, 상기 식별 조건에 부합되는 경우 상기 입력된 화상들로부터 사용자의 얼굴, 지문, 홍채 화상 각각의 특징 데이터를 추출하는 단계; 상기 추출된 특징 데이터들을 중앙 서버로 전송하는 단계; 및 상기 중앙 서버로부터 암호화된 상기 특징 데이터들을 수신하여 상기 카드에 저장시키는 단계를 포함하는 것을 특징으로 한다.

바람직하게는, 상기 중앙 서버로 전송하는 단계는 상기 추출된 특징 데이터들을 공개 암호(public key)를 이용해 암호화하여 상기 중앙 서버로 전송한다.

상기 중앙 서버는 상기 등록 장치의 개인 암호(secret key)를 이용하여 상기 전송된 특징 데이터의 암호화를 해제하여 저장하고, 상기 암호화가 해제된 특징 데이터를 상기 등록 장치의 개인 암호를 이용해 암호화하여 상기 등록 장치로 재전송 하는 것이 바람직하다.

바람직하게는, 상기 특징 데이터들을 카드에 저장시키는 단계는 상기 등록 장치의 등록 정보 헤드 데이터를 생성하는 단계; 및 상기 특징 데이터들에 상기 생성된 헤드 데이터 및 데이터 교정 코드를 삽입하여 상기 카드에 저장시키는 단계를 포함한다.

상기 카드는 RFID 칩(Radio Frequency Identification chip)을 구비하는 것이 바람직하다.

상술한 기술적 과제를 해결하기 위한 본 발명에 의한 사용자 식별 방법은 상기 카드의 유효 여부를 판단하는 단계; 상기 카드가 유효한 카드인 경우, 사용자로부터 얼굴, 지문 및 홍채 화상을 획득하는 단계; 상기 획득된 얼굴, 지문 및 홍채 화상을 상기 카드에 저장된 상기 사용자의 얼굴, 지문 및 홍채 화상의 특징 데이터와 비교하는 단계; 및 상기 비교한 결과, 얼굴, 지문 및 홍채 각각에 대한 획득 화상과 카드에 저장된 특징 데이터 사이의 유사도들이 모두 소정의 허용 범위들에 속하는 경우 사용자가 일치하는 것으로 판단하는 단계를 포함하는 것을 특징으로 한다

바람직하게는, 상기 카드는 RFID 칩(Radio Frequency Identification chip)을 구비한다.

상기 카드의 유효 여부를 확인하는 단계는 상기 RFID 칩에 전파 식별 접근 개인 암호(RFID access secret key)를 이용해 접근을 시도하여 상기 접근에 오류가 있는 경우, 상기 카드가 유효하지 않은 것으로 판단하는 것이 바람직하다.

바람직하게는, 상기 카드의 유효 여부를 확인하는 단계는 상기 카드를 등록한 등록 장치에 대한 정보를 가지는 등록 정보 헤드를 상기 카드로부터 추출하여 중앙 서버로 전송하는 단계; 상기 중앙 서버가 상기 등록 정보 헤드를 이용하여 검출한 상기 등록 장치의 공개 암호를 상기 중앙 서버로부터 수신하는 단계; 및 상기 수신된 등록 장치의 공개 암호를 이용하여 상기 카드에 저장된 특징 데이터들의 암호 해제를 시도하여, 상기 암호 해제에 오류가 발생하는 경우 상기 카드가 유효하지 않은 것으로 판단하는 단계를 포함한다.

상술한 기술적 과제를 해결하기 위한 본 발명에 의한 또 다른 사용자 식별 방법은, 화상과 상기 카드에 저장된 얼굴 특징 데이터 사이의 유사도가 제1소정 범위에 속하는 지 확인하는 단계; 상기 판단결과, 제1소정 범위에 속하지 않는 경우 사용자가 일치하지 않는 것으로 판단하고, 제1소정 범위에 속하는 경우 사용자로부터 획득된 지문 화상과 상기 카드에 저장된 지문 특징 데이터 사이의 유사도가 제2소정 범위에 속하는 지 확인하는 단계; 및 상기 판단결과, 제2소정 범위에 속하는 경우 사용자가 일치하는 것으로 판단하고, 제2소정 범위에 속하지 않는 경우 사용자로부터 획득된 홍채 화상과 상기 카드에 저장된 홍채 특징 데이터 사이의 유사도가 제3소정 범위에 속하는 지 확인하여, 제3소정범위에 속하는 경우 사용자가 일치하는 것으로 판단하는 단계를 포함하는 것을 특징으로 한다.

상술한 기술적 과제를 해결하기 위한 본 발명에 의한 사용자 식별 장치는, 사용자로부터 사용자의 얼굴, 지문 및 홍채 화상을 획득하는 화상획득부; 상기 카드로부터 사용자의 얼굴, 지문 및 홍채 화상의 특징 데이터를 읽어들이는 데이터독취부; 얼굴, 지문 및 홍채 각각에 대해, 상기 획득된 화상과 상기 읽어진 특징 데이터 사이의 유사도를 계산하는 유사도계산부; 및 상기 계산된 유사도들이 모두 소정의 범위들에 포함되는지 여부를 확인하여, 포함되는 경우 사용자가 일치하는 것으로 판단하는 식별부를 포함하는 것을 특징으로 한다.

바람직하게는, 상기 데이터독취부는 상기 카드와 이격되어, 상기 카드에 구비된 RFID 칩에 저장된 사용자의 얼굴, 지문 및 홍채 화상의 특징 데이터를 읽어들이다.

상기 데이터독취부는 상기 카드로부터 특징 데이터를 읽어들이 수 없는 경우, 상기 카드가 유효하지 않은 것으로 판단하는 것이 바람직하다.

바람직하게는, 상기 데이터독취부는 중앙 서버로부터 수신한 상기 카드를 등록한 장치의 공개 암호를 이용해 상기 카드에 저장된 특징 데이터들의 암호를 해제할 수 없는 경우, 상기 카드가 유효하지 않은 것으로 판단한다.

상술한 기술적 과제를 해결하기 위한 본 발명에 의한 생체정보를 저장하는 카드는 RFID 칩(Radio Frequency Identification chip)을 구비하며, 사용자의 얼굴, 지문 및 홍채 화상에 대한 특징 데이터 및 상기 카드를 등록한 등록 장치에 대한 정보를 가지는 등록 정보 헤드가 저장되어 있는 것을 특징으로 한다.

상기 본 발명에 따른 사용자 식별 방법은 바람직하게는 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체로 구현할 수 있다.

이하, 첨부된 도면을 참조하면서 본 발명에 따른 생체정보를 저장하는 카드 및 상기 카드를 이용한 사용자 식별 방법 및 장치에 대해 상세히 설명한다.

도 1은 본 발명에 따른 사용자 식별 장치의 전체적인 구성을 블록도로 도시한 것으로, 도시된 사용자 식별 장치는 화상획득부(100), 데이터독취부(110), 유사도계산부(120), 식별부(130), 카드확인부(140) 및 경고부(150)를 포함하여 이루어진다. 도 1에 도시된 사용자 식별 장치의 동작을 도 2에 도시된 본 발명에 따른 사용자 식별 방법을 나타내는 흐름도와 결부시켜 설명하기로 한다.

상기 카드확인부(140)는 사용자의 식별을 위해 입력된 카드가 유효한 카드인지 여부를 확인한다(200단계). 상기 카드에 저장된 사용자의 생체정보는 인체 고유의 선천적인 생리 특징 및 사용자의 습관적인 행위 특징을 포함하는 정보이며, 구체적으로는 지문, 손금, 홍채, 얼굴, 목소리, 필적 등이 될 수 있다. 본 발명에서 상기 생체 특징은 사용자의 얼굴, 지문 및 홍채 특징인 것이 바람직하다. 또한, 상기 카드는 RFID(Radio Frequency IDentification) 칩을 구비하여, 상기 카드확인부(140) 또는 데이터독취부(110)가 상기 카드에 접촉하지 않은 상태에서도 상기 카드에 저장된 데이터를 읽어들이 수 있도록 하는 것이 바람직하다.

상기 RFID 시스템은 각종 물품에 소형 칩을 부착해 사물의 정보와 주변 환경정보를 무선주파수로 전송·처리하는 비접촉식 인식시스템으로, 판독·해독기능이 있는 판독기와 고유 정보를 내장한 RF 태그(RF ID tag), 운용 소프트웨어, 네트워크 등으로 구성된 전파식별 시스템은 사물에 부착된 얇은 평면 형태의 태그를 식별함으로써 정보를 처리한다.

상기 200단계에서 상기 카드확인부(140)가 카드의 유효여부를 판단하는 방법에 대해서는, 다음의 도 3에 도시된 실시예를 참조하여 자세히 설명하기로 한다.

상기 카드확인부(140)가 상기 카드가 유효하지 않은 것으로 판단한 경우, 상기 경고부(150)는 유효하지 않은 카드임을 경고하고 관리자에게 통보한다(205단계).

상기 카드가 유효한 경우, 상기 데이터독취부(110)는 상기 카드로부터 저장된 사용자의 얼굴, 지문 및 홍채의 특징 데이터를 읽어들이(210단계). 상기 화상획득부(100)는 사용자의 얼굴 화상을 촬영하여, 사용자의 현재 얼굴 화상 데이터를 획득한다(220단계). 상기 유사도계산부(120)는 상기 카드로부터 읽어들이 사용자 얼굴 특징 데이터와 상기 촬영된 사용자의 얼굴 화상 데이터의 유사도를 계산한다(220단계).

상기 식별부(130)는 상기 계산된 사용자의 얼굴에 대한 유사도가 미리 설정된 유사도 값(a) 이상인지 여부를 확인하여(225단계), 상기 계산된 얼굴 유사도가 미리 설정된 값(a) 미만인 경우에는 상기 경고부(150)가 카드의 사용자가 일치하지 않음을 경고하도록 하고(230단계), 상기 계산된 얼굴 유사도가 미리 설정된 값(a) 이상인 경우에는 다음의 지문 식별 단계를 진행한다.

상기 화상획득부(100)는 사용자의 지문 화상을 촬영하여, 사용자의 현재 지문 화상 데이터를 획득한다(235단계). 상기 유사도계산부(120)는 상기 카드로부터 읽어들이 사용자 지문 특징 데이터와 상기 촬영된 사용자의 지문 화상 데이터의 유사도를 계산한다(240단계).

상기 식별부(130)는 상기 계산된 사용자의 지문에 대한 유사도가 미리 설정된 유사도 값(b) 이상인지 여부를 확인하여(245단계), 상기 계산된 지문 유사도가 미리 설정된 값(b) 미만인 경우에는 상기 경고부(150)가 카드의 사용자가 일치하지 않음을 경고하도록 하고(230단계), 상기 계산된 지문 유사도가 미리 설정된 값(b) 이상인 경우에는 다음의 홍채 식별 단계를 진행한다.

상기 화상획득부(100)는 사용자의 홍채 화상을 촬영하여, 사용자의 현재 홍채 화상 데이터를 획득한다(250단계). 상기 유사도계산부(120)는 상기 카드로부터 읽어들이 사용자 홍채 특징 데이터와 상기 촬영된 사용자의 홍채 화상 데이터의 유사도를 계산한다(255단계).

상기 식별부(130)는 상기 계산된 사용자의 홍채에 대한 유사도가 미리 설정된 유사도 값(c) 이상인지 여부를 확인하여(260단계), 상기 계산된 홍채 유사도가 미리 설정된 값(c) 미만인 경우에는 상기 경고부(150)가 카드의 사용자가 일치하지 않음을 경고하도록 하고(230단계), 상기 계산된 홍채 유사도가 미리 설정된 값(c) 이상인 경우에는 사용자가 일치하는 것으로 최종 판단한다.

상기 화상획득부(100)는 상기 사용자의 얼굴 화상을 촬영하는 얼굴화상획득부, 지문 화상을 촬영하는 지문화상획득부 및 홍채 화상을 촬영하는 홍채화상획득부를 포함하는 것이 바람직하다.

도 3은 도 2의 카드의 유효성을 확인하는 단계에 대한 실시예를 흐름도로 도시한 것이다. 상기 카드확인부(140)는 RFID 칩을 구비하는 카드가 접근 유효 거리 내에 위치하게 되면, 미리 설정된 RFID 접근 개인 암호(RFID access secret key)를 이용하여 상기 RFID 칩에 접근을 시도한다(300단계). 상기 카드확인부(140)는 상기 접근 시도 결과 상기 RFID 칩에 접근 성공하였는지 확인하여(310단계), 상기 접근에 실패하거나 상기 RFID 칩에 저장된 교정 파라미터(parameter)에 오류가 발생했을 경우 상기 카드가 위조카드 아니면 불법조작이 발생한 유효하지 않은 카드로 판단한다(320단계).

상기 접근에 성공한 경우, 상기 카드확인부(140)는 상기 카드에 저장된 데이터 중 상기 카드를 등록한 등록 장치(미도시)에 대한 정보를 가지는 등록 정보 헤드 데이터(head data)를 읽어들이고(330단계), 상기 읽어들이는 등록 정보 헤드 데이터를 중앙 서버(미도시)로 전송한다(340단계). 상기 340단계에서, 상기 카드확인부(140)는 상기 등록 정보 헤드 데이터를 상기 사용자 식별 장치의 공개 암호(public key)를 이용해 암호화한 후 상기 중앙 서버(미도시)로 전송하는 것이 바람직하다.

상기 등록 정보 헤드 데이터를 수신한 중앙 서버(미도시)는 상기 등록 정보 헤드 데이터로부터 상기 카드를 등록한 해당 등록 장치(미도시)의 공개 암호를 검출하여 상기 사용자 식별 장치로 전송한다. 상기 카드확인부(140)가 상기 등록 정보 헤드 데이터를 암호화하여 전송한 경우, 상기 중앙 서버(미도시)는 상기 사용자 식별 장치의 공개 암호를 이용하여 상기 등록 정보 헤드 데이터의 암호화를 해제하고 상기 카드 등록 장치의 공개 암호를 검출한 후 다시 상기 사용자 식별 장치의 공개 암호를 이용해 암호화하여 반송하는 것이 바람직하다.

상기 카드확인부(140)는 상기 중앙 서버(미도시)로부터 상기 카드를 등록한 등록 장치의 공개 암호를 수신하여(350단계), 상기 등록 장치의 공개 암호를 이용해 상기 카드에 저장된 사용자 생체정보에 대한 특징 데이터들의 암호화 해제를 시도한다(360단계). 상기 카드확인부(140)는 상기 중앙 서버(미도시)가 상기 등록 장치의 공개 암호를 상기 식별 장치의 공개 암호를 이용해 암호화한 후 전송한 경우, 상기 중앙 서버(미도시)로부터 수신된 데이터를 상기 식별 장치의 공개 암호를 이용해 암호화 해제한 후 상기 360단계를 수행하는 것이 바람직하다.

상기 카드확인부(140)가 상기 특징 데이터의 암호화 해제에 성공한 경우 상기 카드확인부(140)는 상기 카드가 유효한 것으로 판단하고(380단계), 상기 암호화 해제에 실패한 경우 상기 카드가 유효하지 않은 것으로 판단한다(320단계).

상기 카드의 유효성을 확인하는 단계는, 상기과 같이 사용자 식별 장치에 별도로 카드확인부(140)를 구비하지 아니하고, 상기 카드로부터 사용자 생체 정보의 특징 데이터들을 읽어들이는 데이터독취부(110)에 의해 수행되는 것이 바람직하다.

도 4는 본 발명에 따른 생체정보를 가지는 카드를 이용한 또 다른 사용자 식별 방법을 흐름도로 도시한 것이다. 상기 유사도계산부(120)는 상기 카드로부터 읽어들이는 사용자의 얼굴 특징 데이터와 상기 화상획득부(100)가 촬영한 사용자의 얼굴 화상 데이터의 유사도를 계산한다(400단계).

상기 식별부(130)는 상기 계산된 사용자의 얼굴에 대한 유사도가 미리 설정된 유사도 값(a) 이상인지 여부를 확인하여(410단계), 상기 계산된 얼굴 유사도가 미리 설정된 값(a) 미만인 경우에는 상기 카드의 사용자가 일치하지 않는 것으로 판단한다(460단계).

상기 계산된 얼굴 유사도가 미리 설정된 값(a) 이상인 경우, 상기 유사도계산부(120)는 상기 카드로부터 읽어들이는 사용자의 지문 특징 데이터와 상기 화상획득부(100)가 촬영한 사용자의 지문 화상 데이터의 유사도를 계산한다(420단계). 상기 식별부(130)는 상기 계산된 사용자의 지문에 대한 유사도가 미리 설정된 유사도 값(b) 이상인지 여부를 확인한다(430단계).

상기 지문 유사도 확인 후, 사용자의 홍채를 이용한 사용자 식별을 더 수행할 것인지 여부를 확인하여(440, 450단계), 홍채를 이용한 식별을 진행하지 않고자 하는 경우, 상기 계산된 지문 유사도가 미리 설정된 값(b) 미만인 경우에는 상기 카드의 사용자가 일치하지 않는 것으로 판단하며(460단계), 상기 계산된 지문 유사도가 미리 설정된 값(b) 이상인 경우에는 상기 카드의 사용자가 일치하는 것으로 판단한다(470단계).

상기 사용자의 얼굴 및 지문을 이용한 사용자 식별 후 사용자의 홍채를 이용한 식별을 더 진행하고자 하는 경우, 상기 유사도계산부(120)는 상기 카드로부터 읽어들이는 사용자의 홍채 특징 데이터와 상기 화상획득부(100)가 촬영한 사용자의 홍채

화상 데이터의 유사도를 계산한다(480단계). 상기 식별부(130)는 상기 계산된 사용자의 홍채에 대한 유사도가 미리 설정된 유사도 값(c) 이상인지 여부를 확인한다(490단계). 상기 계산된 홍채 유사도가 미리 설정된 값(c) 미만인 경우에는 상기 카드의 사용자가 일치하지 않는 것으로 판단하고(460단계), 미리 설정된 값(c) 이상인 경우에는 상기 카드의 사용자가 일치하는 것으로 판단한다(470단계).

사용자의 생체 정보 중 홍채에 비해 얼굴과 지문은 사용자로부터 화상을 분리하여 획득하는데 있어 사용자에게 거부감이 적으며 획득이 용이하므로, 상기 도 4에 도시된 바와 같이 사용자의 얼굴 및 지문을 통한 사용자 식별을 우선 진행한 후 식별 결과에 정확성이 의심되는 경우 사용자의 홍채를 이용한 식별을 진행하는 것이 바람직하다.

도 5는 본 발명에 따른 카드 등록 장치에서 생체정보를 가지는 카드를 등록하는 방법을 흐름도로 도시한 것이다. 상기 등록 장치는 구비된 카메라(미도시)를 이용해 사용자의 얼굴 화상을 촬영하여 사용자의 얼굴 화상 데이터를 획득하고(500단계), 상기 획득된 얼굴 화상이 미리 설정된 식별 조건을 만족하는 지 여부를 확인한다(510단계). 상기 미리 설정된 식별 조건은 상기 촬영된 화상에서 사용자의 얼굴 위치가 미리 설정된 위치 범위 내에 존재하는 지, 촬영된 사용자의 얼굴 표정이 적당한 지 여부를 확인하는 것이 바람직하다. 상기 촬영된 얼굴 화상이 상기 식별 조건을 만족하는 경우에는 상기 촬영된 화상으로부터 사용자 얼굴의 특징 데이터를 추출하고(520단계), 상기 식별 조건을 만족하지 못하는 경우에는 식별 조건을 만족할 때까지 상기 500단계 및 510단계를 반복한다.

상기 등록 장치는 구비된 카메라(미도시)를 이용해 사용자의 지문 화상을 촬영하여 사용자의 지문 화상 데이터를 획득하고(530단계), 상기 획득된 지문 화상이 미리 설정된 식별 조건을 만족하는 지 여부를 확인한다(540단계). 상기 촬영된 지문 화상이 상기 식별 조건을 만족하는 경우에는 상기 촬영된 화상으로부터 사용자 지문의 특징 데이터를 추출하고(550단계), 상기 식별 조건을 만족하지 못하는 경우에는 식별 조건을 만족할 때까지 상기 530단계 및 540단계를 반복한다.

상기 등록 장치는 구비된 카메라(미도시)를 이용해 사용자의 홍채 화상을 촬영하여 사용자의 홍채 화상 데이터를 획득하고(560단계), 상기 획득된 홍채 화상이 미리 설정된 식별 조건을 만족하는 지 여부를 확인한다(570단계). 상기 미리 설정된 식별 조건은 상기 촬영된 화상에서 사용자의 홍채 위치가 미리 설정된 위치 범위 내에 존재하는 지, 촬영된 사용자의 홍채 표정이 적당한 지 여부를 확인하는 것이 바람직하다. 상기 촬영된 홍채 화상이 상기 식별 조건을 만족하는 경우에는 상기 촬영된 화상으로부터 사용자 홍채의 특징 데이터를 추출하고(580단계), 상기 식별 조건을 만족하지 못하는 경우에는 식별 조건을 만족할 때까지 상기 560단계 및 570단계를 반복한다.

상기 카드 등록 장치는 상기 추출된 사용자의 얼굴, 지문 및 홍채의 특징 데이터를 상기 등록 장치의 공개 암호를 이용하여 암호화 한 후, 중앙 서버(미도시)로 전송한다(590단계). 상기 중앙 서버(미도시)는 상기 수신한 사용자의 얼굴, 지문 및 홍채의 특징 데이터를 상기 등록 장치의 공개 암호를 이용해 암호화 해제한 후 상기 등록 장치의 공개 암호와 함께 저장한다.

상기 중앙 서버(미도시)는 상기 사용자의 얼굴, 지문 및 홍채의 특징 데이터를 상기 등록 장치의 개인 암호(secret key)를 이용해 암호화 한 후 상기 등록 장치로 전송하고, 상기 등록 장치는 상기 전송된 사용자의 얼굴, 지문 및 홍채의 특징 데이터를 상기 등록 장치에 대한 정보를 가지는 등록 정보 헤드 데이터 및 데이터 교정 파라미터와 함께 상기 카드에 저장시킨다(595단계).

상기 카드는 대용량 RFID 칩을 구비하여, 상기 특징 데이터, 등록 정보 헤드 데이터 및 데이터 교정 파라미터는 상기 카드의 RFID 칩에 저장되는 것이 바람직하다, 또한, 상기 RFID 시스템 및 데이터의 읽기/쓰기를 위한 개인 암호(secret key)는 미리 설정되어, 상기 카드가 여러 개의 식별 장치에서 사용자 식별에 이용될 수 있도록 하는 것이 바람직하다.

도 6은 생체정보를 가지는 카드를 이용한 사용자 식별 장치에 대한 실시예를 도시한 것으로, 사용자의 얼굴 화상을 촬영하는 얼굴화상획득부(600), 사용자의 지문 화상을 촬영하는 지문화상획득부(610), 사용자의 홍채 화상을 촬영하는 홍채화상획득부(620) 및 사용자의 카드가 유효하지 않거나 사용자가 불일치함을 경고하는 경고부(630)가 도시되어 있다.

본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다.

이상 본 발명의 바람직한 실시예에 대해 상세히 기술하였지만, 본 발명이 속하는 기술분야에 있어서 통상의 지식을 가진 사람이라면, 첨부된 청구범위에 정의된 본 발명의 정신 및 범위에 벗어나지 않으면서 본 발명을 여러 가지로 변형 또는 변경하여 실시할 수 있음을 알 수 있을 것이다. 따라서, 본 발명의 앞으로의 실시예들의 변경은 본 발명의 기술을 벗어날 수 없을 것이다.

발명의 효과

상술한 바와 같이 본 발명에 따른 사용자 식별 방법 및 장치에 의하면, 공항에서의 여권 본인 확인 등 사용자의 진위 여부를 확인하고자 하는 경우, 카드에 저장된 사용자의 얼굴, 지문 및 홍채의 생체정보를 이용하여 사용자를 식별할 수 있도록 함으로써, 수작업을 통한 사용자 식별에 소모되는 시간을 감소시킬 수 있으며, 사용자 식별 결과의 정확성 및 신뢰성을 높일 수 있다.

(57) 청구의 범위

청구항 1.

등록 장치를 이용하여 사용자 식별 정보를 가지는 카드를 제조하는 방법에 있어서,

사용자의 얼굴, 지문, 홍채의 화상들을 입력받는 단계;

상기 입력된 얼굴, 지문, 홍채의 화상이 소정의 식별 조건에 부합되는지 확인하는 단계;

상기 확인 결과, 상기 식별 조건에 부합되지 않는 경우 상기 식별 조건에 부합될 때까지 상기 화상 입력 단계 및 식별 조건 확인 단계를 반복하고, 상기 식별 조건에 부합되는 경우 상기 입력된 화상들로부터 사용자의 얼굴, 지문, 홍채 화상 각각의 특징 데이터를 추출하는 단계;

상기 추출된 특징 데이터들을 중앙 서버로 전송하는 단계; 및

상기 중앙 서버로부터 암호화된 상기 특징 데이터들을 수신하여 상기 카드에 저장시키는 단계를 포함하는 것을 특징으로 하는 사용자 식별 카드 제조 방법.

청구항 2.

제1항에 있어서, 상기 중앙 서버로 전송하는 단계는

상기 추출된 특징 데이터들을 공개 암호(public key)를 이용해 암호화하여 상기 중앙 서버로 전송하는 것을 특징으로 하는 사용자 식별 카드 제조 방법.

청구항 3.

제1항에 있어서, 상기 중앙 서버는

상기 등록 장치의 개인 암호(secret key)를 이용하여 상기 전송된 특징 데이터의 암호화를 해제하여 저장하고, 상기 암호화가 해제된 특징 데이터를 상기 등록 장치의 개인 암호를 이용해 암호화하여 상기 등록 장치로 재전송 하는 것을 특징으로 하는 사용자 식별 카드 제조 방법.

청구항 4.

제1항에 있어서, 상기 특징 데이터들을 카드에 저장시키는 단계는

상기 등록 장치의 등록 정보 헤드 데이터를 생성하는 단계; 및

상기 특징 데이터들에 상기 생성된 헤드 데이터 및 데이터 교정 코드를 삽입하여 상기 카드에 저장시키는 단계를 포함하는 것을 특징으로 하는 사용자 식별 카드 제조 방법.

청구항 5.

제1항에 있어서, 상기 카드는

RFID 칩(Radio Frequency IDentification chip)을 구비하는 것을 특징으로 하는 사용자 식별 카드 제조 방법.

청구항 6.

사용자 식별 정보를 가지는 카드를 이용한 사용자 식별 방법에 있어서,

상기 카드의 유효 여부를 판단하는 단계;

상기 카드가 유효한 카드인 경우, 사용자로부터 얼굴, 지문 및 홍채 화상을 획득하는 단계;

상기 획득된 얼굴, 지문 및 홍채 화상을 상기 카드에 저장된 상기 사용자의 얼굴, 지문 및 홍채 화상의 특징 데이터와 비교하는 단계; 및

상기 비교한 결과, 얼굴, 지문 및 홍채 각각에 대한 획득 화상과 카드에 저장된 특징 데이터 사이의 유사도들이 모두 소정의 허용 범위에 속하는 경우 사용자가 일치하는 것으로 판단하는 단계를 포함하는 것을 특징으로 하는 사용자 식별 방법.

청구항 7.

제6항에 있어서, 상기 카드는

RFID 칩(Radio Frequency IDentification chip)을 구비하는 것을 특징으로 하는 사용자 식별 방법.

청구항 8.

제7항에 있어서, 상기 카드의 유효 여부를 확인하는 단계는

상기 RFID 칩에 전파 식별 접근 개인 암호(RFID access secret key)를 이용해 접근을 시도하여 상기 접근에 오류가 있는 경우, 상기 카드가 유효하지 않은 것으로 판단하는 것을 특징으로 하는 사용자 식별 방법.

청구항 9.

제7항에 있어서, 상기 카드의 유효 여부를 확인하는 단계는

상기 카드를 등록한 등록 장치에 대한 정보를 가지는 등록 정보 헤드를 상기 카드로부터 추출하여 중앙 서버로 전송하는 단계;

상기 중앙 서버가 상기 등록 정보 헤드를 이용하여 검출한 상기 등록 장치의 공개 암호를 상기 중앙 서버로부터 수신하는 단계; 및

상기 수신된 등록 장치의 공개 암호를 이용하여 상기 카드에 저장된 특징 데이터들의 암호 해제를 시도하여, 상기 암호 해제에 오류가 발생하는 경우 상기 카드가 유효하지 않은 것으로 판단하는 단계를 포함하는 것을 특징으로 하는 사용자 식별 방법.

청구항 10.

사용자 식별 정보를 가지는 카드를 이용한 사용자 식별 방법에 있어서,

화상과 상기 카드에 저장된 얼굴 특징 데이터 사이의 유사도가 제1소정 범위에 속하는 지 확인하는 단계;

상기 판단결과, 제1소정 범위에 속하지 않는 경우 사용자가 일치하지 않는 것으로 판단하고, 제1소정 범위에 속하는 경우 사용자로부터 획득된 지문 화상과 상기 카드에 저장된 지문 특징 데이터 사이의 유사도가 제2소정 범위에 속하는 지 확인하는 단계; 및

상기 판단결과, 제2소정 범위에 속하는 경우 사용자가 일치하는 것으로 판단하고, 제2소정 범위에 속하지 않는 경우 사용자로부터 획득된 홍채 화상과 상기 카드에 저장된 홍채 특징 데이터 사이의 유사도가 제3소정 범위에 속하는 지 확인하여, 제3소정범위에 속하는 경우 사용자가 일치하는 것으로 판단하는 단계를 포함하는 것을 특징으로 하는 사용자 식별 방법.

청구항 11.

카드에 저장된 사용자 식별 정보를 이용하여 사용자를 식별하는 장치에 있어서,

사용자로부터 사용자의 얼굴, 지문 및 홍채 화상을 획득하는 화상획득부;

상기 카드로부터 사용자의 얼굴, 지문 및 홍채 화상의 특징 데이터를 읽어들이는 데이터독취부;

얼굴, 지문 및 홍채 각각에 대해, 상기 획득된 화상과 상기 읽어진 특징 데이터 사이의 유사도를 계산하는 유사도계산부; 및

상기 계산된 유사도들이 모두 소정의 범위들에 포함되는지 여부를 확인하여, 포함되는 경우 사용자가 일치하는 것으로 판단하는 식별부를 포함하는 것을 특징으로 하는 사용자 식별 장치.

청구항 12.

제11항에 있어서, 상기 데이터독취부는

상기 카드와 이격되어, 상기 카드에 구비된 RFID 칩에 저장된 사용자의 얼굴, 지문 및 홍채 화상의 특징 데이터를 읽어들이는 것을 특징으로 하는 사용자 식별 장치.

청구항 13.

제11항에 있어서, 상기 데이터독취부는

상기 카드로부터 특징 데이터를 읽어들이 수 없는 경우, 상기 카드가 유효하지 않은 것으로 판단하는 것을 특징으로 하는 사용자 식별 장치.

청구항 14.

제11항에 있어서, 상기 데이터독취부는

중앙 서버로부터 수신한 상기 카드를 등록한 장치의 공개 암호를 이용해 상기 카드에 저장된 특징 데이터들의 암호를 해제할 수 없는 경우, 상기 카드가 유효하지 않은 것으로 판단하는 것을 특징으로 하는 사용자 식별 장치.

청구항 15.

사용자 식별 정보를 가지는 카드에 있어서,

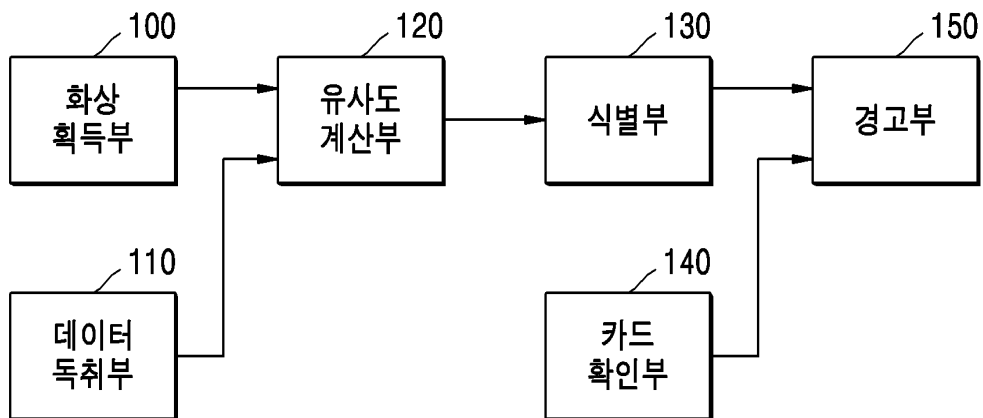
RFID 칩(Radio Frequency IDentification chip)을 구비하며, 사용자의 얼굴, 지문 및 홍채 화상에 대한 특징 데이터 및 상기 카드를 등록한 등록 장치에 대한 정보를 가지는 등록 정보 헤드가 저장되어 있는 것을 특징으로 하는 사용자 식별 카드.

청구항 16.

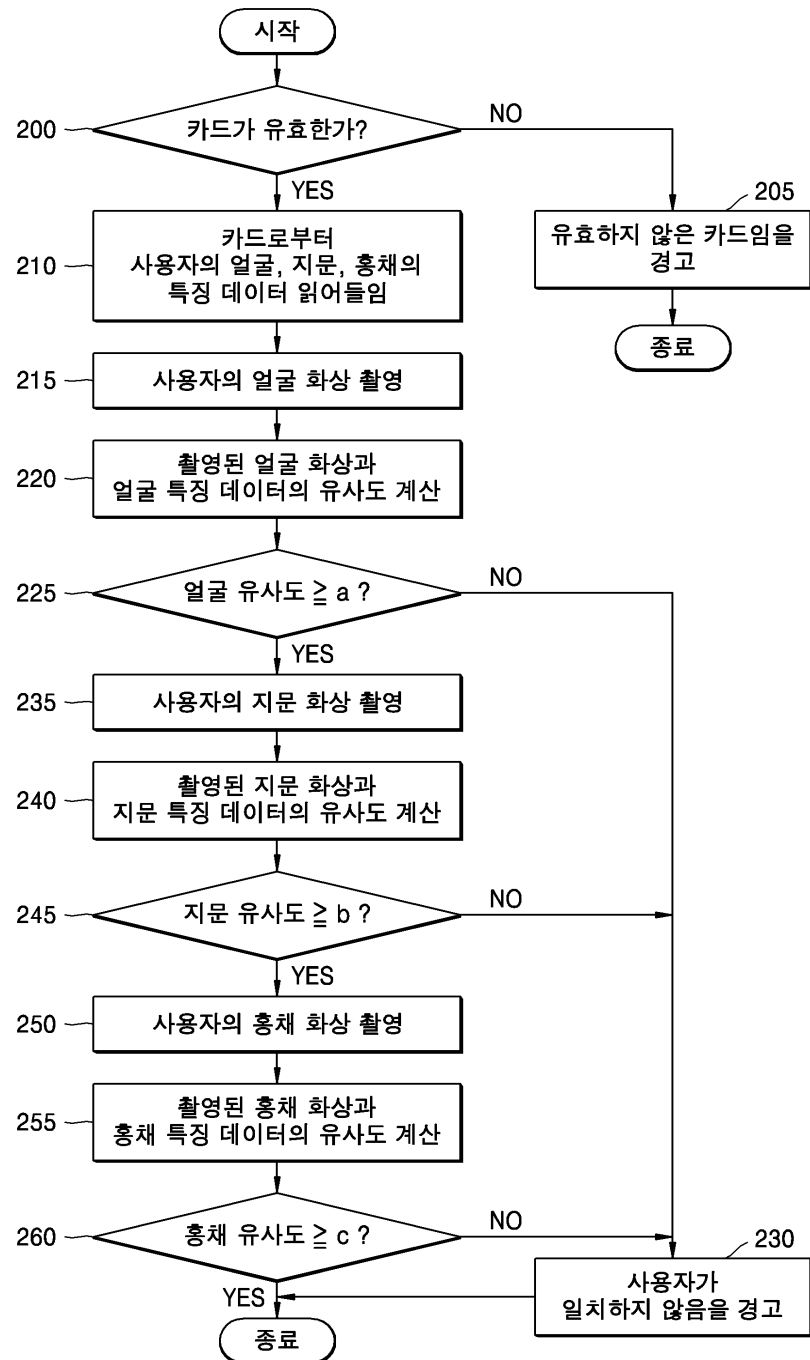
제1항 내지 제10항 중 어느 한 항에 기재된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

도면

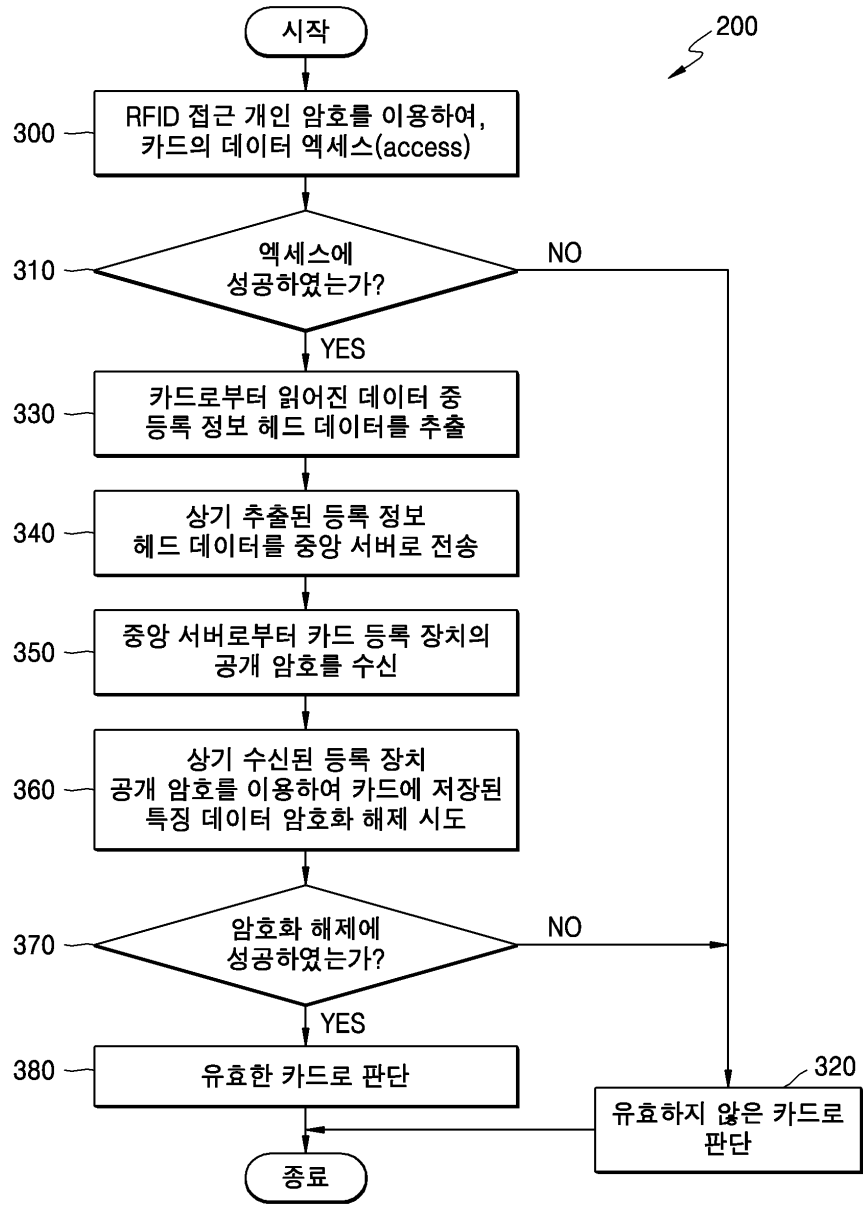
도면1



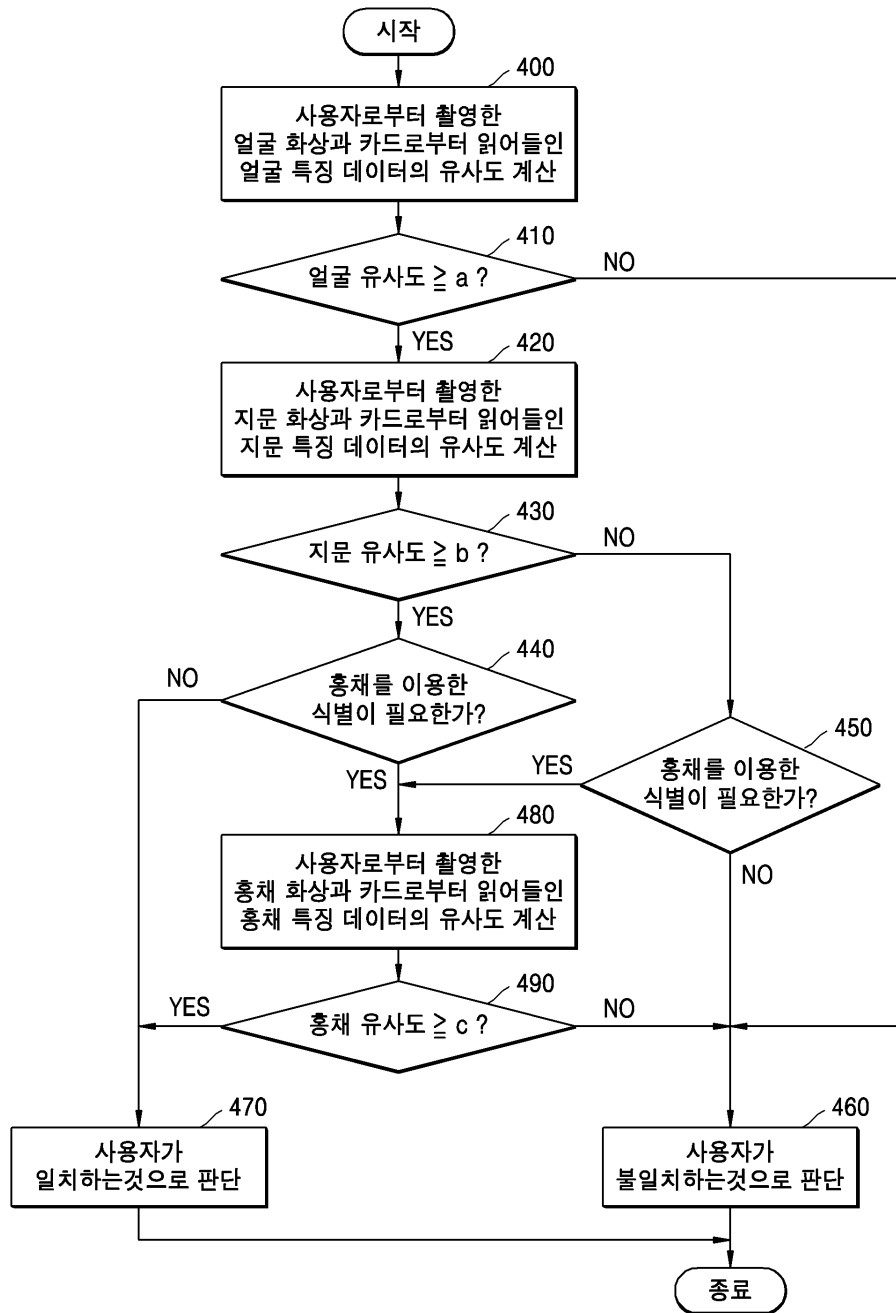
도면2



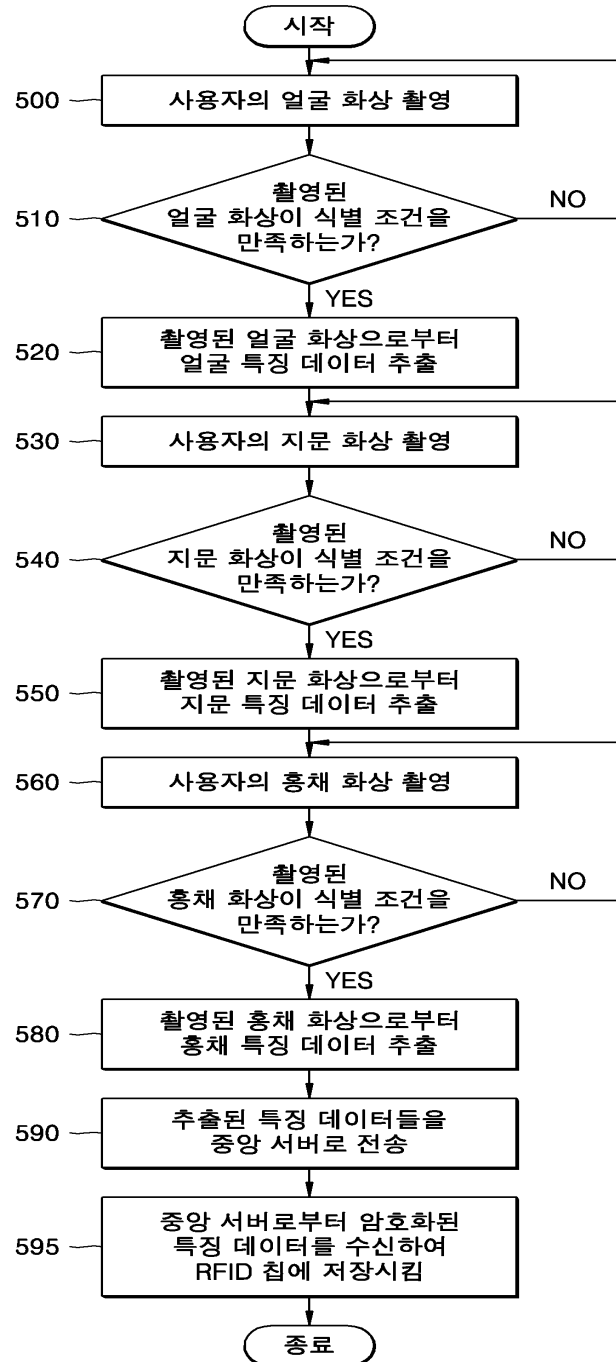
도면3



도면4



도면5



도면6

