(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
G06K 9/00

(11) 공개번호 특2000-0070252
(43) 공개일자 2000년11월25일

(21) 출원번호 10-1999-7006480
(22) 출원일자 1999년07월16일
번역문제출일자 1999년07월16일
(86) 국제출원번호 PCT/GB1998/00154 (87) 국제공개번호 WO 1998/32093
(86) 국제출원출원일자 1998년01월19일 (87) 국제공개일자 1998년07월23일
(81) 지정국 AP ARIPO특허 : 레소토 말라위 수단 스와질랜드 우간다 케냐 가나 감비아 짐바브웨

EA 유라시아특허 : 아르메니아 아제르바이잔 벨라루스 키르기즈 카자흐스탄 몰도바 러시아 타지키스탄 투르크메니스탄

EP 유럽특허 : 오스트리아 벨기에 스위스 리히텐슈타인 독일 덴마크 스페인 프랑스 영국 그리스 아일랜드 이탈리아 룩셈부르크 모나코 네덜란드 포르투칼 스웨덴 핀랜드

OA OAPI특허 : 부르키나파소 베넹 중앙아프리카 콩고 코트디브와르 카메룬 가봉 기네 말리 모리타니 니제르 세네갈 차드 토고

국내특허 : 알바니아 아르메니아 오스트리아 오스트레일리아 아제르바이잔 보스니아-헤르체고비나 바베이도스 불가리아 브라질 벨라루스 캐나다 스위스 중국 쿠바 체코 독일 덴마크 에스토니아 스페인 핀랜드 영국 그루지야 헝가리 이스라엘 아이슬란드 일본 케냐 키르기즈 북한 대한민국 카자흐스탄 세인트루시아 스리랑카 라이베리아 레소토 리투아니아 룩셈부르크 라트비아 몰도바 마다가스카르 마케도니아 몽고 말라위 멕시코 노르웨이 뉴질랜드 슬로베니아 슬로바키아 타지키스탄 투르크메니스탄 터어키 트리니다드토바고 우크라이나 우간다 미국 우즈베키스탄 베트남 가나 감비아 기네비쏘 인도네시아 유고슬라비아 폴란드 포르투칼 루마니아 러시아 수단 스웨덴 싱가포르 시에라리온 짐바브웨

(30) 우선권주장 973003288 1997년01월17일 EP(EP)
(71) 출원인 브리티쉬 텔리커뮤니케이션즈 파블릭 리미티드 캄퍼니 내쉬 로저 윌리엄

영국 런던(우편번호 이시1에이 7에이제이) 뉴게이트 스트리트 81

(72) 발명자 실크리스토퍼헨리

영국서포크(우편번호:아이피142피에프)스토우마켓힌틀샘클로즈16

맥카트니데이비드존

영국서포크(우편번호:아이피42티에이치)입스위치사우스클로즈5

기포드모리스메릭

영국입스위치(우편번호:아이피52지알)케스그레이브디킨슨테라스1

(74) 대리인 김명신, 김원오

*심사청구 : 없음*

**(54) 보안 장치 및 방법**

*요약*

본 발명은 보안 검사를 제공하는데 사용하는 장치 및 방법에 관한 것으로서, 보안 검사를 통과하도록 허가된 사람인지를 판단하기 위해 홍채 인식을 사용하는 방법에 있어서, 보안 검사를 통과하려는 사람은 먼저 허가된 사람에 대한 홍채 코드의 데이터베이스에 저장된 홍채 코드와 캡처되고 디지털화된 홍채 코드를 비교하여 식별되고, 다음에, 허가된 사람에 대한 홍채 코드는 그 사람에 대하여 이전에 기록된 모든 홍채 코드와 비교되고, 정확하게 일치하면, 정확하게 일치할 확률이 상당히 낮기 때문에 식별된 홍채 코드는 부정한 것으로 간주되며, 그 결과, 다른 식별 정보가 요청되거나 그 사람의 자원 또는 시스템에 대한 액세스가 부정되는 것을 특징으로 한다.

*대표도*

*도4*

*색인어*

보안 검사, 디지털 서명, 홍채

*명세서*

본 발명은 보안 검사를 제공하는데 사용하는 장치 및 방법에 관한 것이다. 특히, 본 발명은 한 응용에서 다른 것으로 예측할 수 없게 변화하는 데이터 시퀀스에 의존하는 인식 방법을 사용하는 장치와 관련된 특정 유틸리티를 갖는다.

종래의 보안 검사는 무엇보다도 건물 출입, 보안 컴퓨터 시스템의 사용을 제어하거나 허가된 사람이 자신의 은행 계좌에서 돈을 인출하는 것을 허가한다. 통상, 사용자는 영숫자 암호를 입력해야 한다(이것은 예를 들어 허가된 사람의 은행 계좌와 관련된 개인식별번호일 수 있다). 이 암호가 허가된 사용자와 관련된 저장 암호와 일치하면, 사용자는 보안 검사를 통과한다. 허가되지 않은 사람이 암호를 알고 있을 경우에 문제가 발생한다 - 이 사람은 보안 검사를 용이하게 통과할 수 있다.

최근, 영숫자 암호보다는 디지털 서명을 사용하는 것이 제안되고 있다. 많은 형태의 디지털 서명은 사람의 생리학적 특성(생체측정이라 알려짐)을 나타낸다. 디지털 서명의 근간을 이루는 생리학적 특성은 다른 사람에 의해 제공될 수 없다 - 따라서 생체측정 기반 디지털 서명은 종래의 암호보다 큰 보안성을 제공한다. 제안되고 있는 생체측정은 지문, 음성 표본, 망막 스캔 및 홍채 패턴을 포함한다. 사람의 사인을 디지털화한 것과 같은 다른 형태의 디지털 서명이 또한 고려되고 있다.

영숫자 암호와는 반대로, 2번의 시도로 예를 들어 생체측정 또는 사인으로부터 동일한 디지털 서명을 정확히 얻을 확률은 대체로 낮고, 이러한 일정하지 않은 디지털 서명을 기초로 하는 인식은 기준 디지털 서명에 충분히 비슷한 디지털 서명을 얻는 것에 의존한다. 예를 들어 홍채 인식과 관련하여 측정된 홍채 코드 사이의 차이는 통상 카메라 설정의 차이, 조도 변화 또는 눈꺼풀을 약간 감거나 렌즈상의 파편 또는 먼지 때문에 발생한다. 사인의 경우에, 디지털 서명의 차이는 데이터 캡처의 차이 및 사인 자체의 변화 때문에 발생한다.

유럽특허출원 0 392 159는 사용자의 사인이 허가된 사람이라고 주장하는 사용자에 의해 제공된 기준 사인과 비교되는 사인 확인 방법을 개시한다. 기준 사인은 가입 절차 동안 제공된다. 사용자에 의해 제공된 순간 사인과 허가된 사람이라고 주장하는 사용자에 의해 제공된 기준 사인 사이에 상당한 차이가 있으면, 그 사용자는 사기꾼으로 간주된다. 2개의 사인이 매우 비슷하면, 그 사인은 위조된 것으로 간주된다. 기준 사인과 사용자의 사인 사이의 차이가 예측된 정도인 경우에만 그 사용자를 허가된 사람으로 확인한다.

많은 보안 검사에 있어서 공통된 문제는 허가된 사람이 가입할 때 제공될 수 있는 보안 레벨이 이후에 사용자가 보안 검사를 통과하기 위해 시도할 수 있는 여러 위치에서 일치하지 않을 수도 있다는 것이다. 예를 들어 원격 사용자가 공유 자원에 접근할 수 있도록 하는 시스템에서, 보안 검사가 의존하는 암호 또는 디지털 서명은 검사되기 전에 통신링크를 통해 전송되어야 한다 - 이러한 경우는 예를 들어 은행이 제공한 현금자동지급기와 관련하여 발생할 수 있다. 게다가, 몇몇 경우에 사인 또는 생체측정을 디지털화하는 장치는 허가되지 않은 접근을 용이하게 하도록 변경되기 쉽다. 예를 들어, 허가되지 않은 사용자가 이후에 장치를 사용하는 허가된 사람의 암호 또는 디지털 서명을 습득하기 위해 판매 장치 지점내의 디지털 메모리에 접속할 수 있다.

상기 문제를 방지하는 한 가지 방법은 각각의 암호 또는 디지털 서명을 전송하기 전에 시간 표시하는 것이다. 그러나, 시간 표시를 제공하는 것은 시스템의 분산 노드가 동시성을 가져야 한다 - 이것은 구현하기 어렵고, 비용도 많이 소요된다.

본 발명의 제 1 태양에 따르면,

보안 검사를 통과하려 하는 사람이 제공한 순간 디지털 서명과 저장 디지털 서명을 비교하는 단계,

상기 사인들이 충분히 유사하다고 나타내는 상기 비교에 응답하여 상기 보안 검사를 통과하려 하는 사람을 상기 저장 디지털 서명을 제공한 사람으로서 식별하는 단계,

상기 순간 디지털 서명과, 보안 검사를 통과하기 위한 이전의 시도에서 제공된 하나 이상의 이전의 디지털 서명을 비교하는 단계 및

상기 순간 서명을 하나 이상의 이전의 서명과 부당하게 유사한 것으로 나타내는 상기 비교에 응답하여 상기 식별을 무효화하는 단계를 포함하는 것을 특징으로 하는 일정하지 않은 디지털 서명에 기초하여 보안 검사를 통과하려는 사람이 허가된 사람인지를 판단하는 방법이 제공된다.

일정하지 않은 디지털 서명이 이전에 제공된 서명과 필요 이상으로 엄밀하게 일치하지 않는지를 검사하도록 장치를 구성함으로써 도청자가 시스템에 대한 허가되지 않은 접근을 달성할 수 있는 위험이 감소된다.

몇몇 실시예에서, 상기 순간 서명이 이전의 서명과 동일한 경우에만 식별이 무효화된다. 이 경우, 이전의 디지털 서명을 정확히 복사하는 도청자는 보안 검사를 통해 통과가 거부될 것이고, 반면에 잘못하여 허가된 사람이 거부되는 경우는 감소한다.

다른 실시예에서, 상기 순간 디지털 서명이 하나 이상의 이전의 서명과 정확히 일치하는 경우에 식별은 또한 무효화된다. 이것은 예를 들어 지문을 제공하기 위한 손가락 모형, 홍채 패턴을 제공하기 위한 눈 사진 또는 사인의 복사를 사용하여 보안 검사를 위반하려는 허가되지 않은 사용자를 방해하는 이점을 갖는다.

바람직한 실시예에서 순간 디지털 서명을 기준 서명과 비교하는 것은 순간 및 기준 서명 사이의 제 1 유

사성 정도를 계산하는 것을 포함한다. 제 1 유사성 정도가 소정의 제 1 임계를 초과하는 경우에 사용자는 허가된 사람으로 식별된다. 순간 디지털 서명과 하나 이상의 이전의 디지털 서명을 비교하는 것은 순간 및 이전의 서명 사이의 하나 이상의 제 2 유사성 정도를 계산하는 것을 포함한다. 그리고, 제 2 유사성 정도가 제 1 임계 및 보다 높은 소정의 제 2 임계를 초과하는 경우에 사용자의 식별은 무효화되고, 상기 제 1 및 제 2 임계 중 하나 또는 모두는 조정 가능하다. 이것은 허가된 사람들의 디지털 서명에 내재하는 편차내의 허가된 사람들의 차이가 보상될 수 있다는 이점을 제공한다. 부가적으로, 위치 또는 시간 때문에 발생하는 허가된 사람의 디지털 서명 사이의 차이도 이러한 방식으로 보상될 수 있다.

본 발명의 제 2 태양에 따르면,

사용자에 의해 제공된 디지털 서명을 수신하는 입력수단,

하나 이상의 기준 디지털 서명과, 기준 서명을 제공한 허가된 사용자들을 식별하는 각각의 관련 정보 항목들을 저장하는 제 1 저장수단,

식별된 허가된 사용자에 의한 이전의 인식 시도에서 얻어진 이전의 디지털 서명을 저장하는 제 2 저장수단,

상기 제 1 저장수단에 액세스하고, 수신된 디지털 서명을 하나 이상의 기준 디지털 서명과 비교하며, 상기 수신된 디지털 서명과 기준 디지털 서명의 유사성 정도가 소정의 제 1 유사성 임계를 초과하는 경우에, 사용자를 수신된 디지털 서명의 최초 사용자로서 식별하는 제 1 프로세싱 수단 및

상기 제 2 저장수단에 액세스하고, 수신된 디지털 서명을 식별된 허가된 사람에 의한 이전의 인식 시도와 관련된 이전의 서명과 비교하며, 상기 수신된 디지털 서명과 이전의 디지털 서명의 제 2 유사성 정도가 소정의 제 2 임계를 초과하는 경우에 상기 식별을 무효화하는 제 2 프로세싱 수단을 포함하는 것을 특징으로 하는 보안 검사를 제공하는데 사용하는 장치가 제공된다.

이전의 인식 시도에서 제시된 디지털 서명 사이의 유사성을 부가적으로 고려함으로써, 상기 장치는 종래의 보안 검사 장치에 의해 제공된 것보다 훨씬 높은 보안성을 제공한다.

이제 첨부한 도면을 참조하여 예를 통해 본 발명의 실시예에 대해 기술한다.

도 1은 예시적인 개인 식별 클라이언트/서버 시스템을 설명하는 도면,

도 2는 도 1의 시스템의 서버 프로세싱 플랫폼을 보다 상세히 설명하는 도면,

도 3은 사용자 인식에 필요한 데이터의 구성을 설명하는 도면,

도 4는 사용자 인식을 실시하는데 필요한 단계들을 설명하는 흐름도 및

도 5는 허가된 사람에 대한 홍채 코드 인식의 특성을 보여주는 그래프이다.

도 1에 의하면, 홍채 코드 발생기(100)는 사용자의 눈(110) 이미지를 캡처하도록 구성된다. 이 홍채 코드 발생기는 본 출원인이 동시에 출원한 특허출원 PCT/GB97/01524, PCT/GB97/01525 및 PCT/GB97/01526에 기재된 것과 같은 휴대형 장치이고, 이들 문헌의 내용은 본 명세서에 참조상 포함되어 있다. 발생기(100)는 미국 특허 제5,291,560호에 개시된 기술에 따라 캡처된 이미지를 256바이트 홍채 코드로 인코드하고, 이 문헌의 내용은 또한 본 명세서에 참조상 포함되어 있다. 다음에, 발생기(100)는 홍채 코드를 수신하고, 이후에 이 홍채 코드를 통신채널을 통해 인식 서버(160)로 전송하도록 구성된 클라이언트 컴퓨터 시스템(120)으로 홍채 코드를 전송한다. 미래의 실시예에서 발생기(100)와 클라이언트 컴퓨터 시스템(120)은 단일한 전용 하드웨어 장치로 구현될 것이라고 생각된다.

통신채널은 컴퓨터(120)를 보안 전용 데이터 네트워크와 같은 통신네트워크(140)에 연결하는 모뎀(130)을 포함한다. 네트워크(140)는 제 2 모뎀(150)을 통해 서버(160)로 홍채 코드를 전송한다. 서버(160)는 외부 저장장치(270), 예를 들어 하드디스크에 연결되고, 아래에 보다 상세히 기술되는 바와 같이, 수신된 홍채 코드에 기초하여 인식 처리를 실시한다.

서버(160)는 다른 설비 또는 서비스에 접속하려고 시도하는 허가된 사람을 식별하고 확인한다. 다른 설비(도시하지 않음)는 긍정 응답 후에만 인식 서버(160)를 통해 액세스 가능한 보안 통신 네트워크일 수 있다.

도 2는 인식 서버(160)의 프로세싱 플랫폼(200)의 주요 구성요소를 나타낸다. 서버 플랫폼(200)은 Unix(TM) 운영체계를 사용하고, Oracle(TM) 데이터베이스 관리 시스템을 지원하는 Sun(TM) SPARCstation 20/51과 같은 종래의 컴퓨팅 플랫폼이다. 플랫폼(200)은 어드레스 및 데이터 버스(220)를 통해 주메모리(230)와 입력/출력(I/O) 컨트롤러(240)에 연결된 중앙처리장치(210)의 표준 기능들을 포함한다. 모뎀(150)은 직렬 접속(250)을 통해 I/O 컨트롤러(240)에 연결되고, 하드디스크 드라이브(170)는 병렬 회선(260)을 통해 I/O 드라이버(240)에 연결된다.

디스크 드라이브(170)는 2개의 Oracle 데이터 저장 영역을 포함한다. 제 1 데이터 저장 영역(273)은 복수의 허가된 사람에 대한 기준 홍채 코드 정보를 포함하고, 제 2 데이터 저장 영역(276)은 각각의 허가된 사람에 대한 이력 홍채 코드 정보를 포함한다.

제 1 및 제 2 데이터 저장 영역은 도 3에 보다 상세히 도시되어 있다. 제 1 데이터 영역(273)은 단일 데이터베이스 테이블(300)에 기준 홍채 코드 1 내지 n을 포함하고, 여기서 각각의 홍채 코드는 허가된 사람 1 내지 n과 연관된다. 기준 홍채 코드는 적당한 허가된 사람 등록 절차에 의해 얻어진 것이다. 이 절차는 서로 다른 많은 형태를 가질 수 있지만, 통상 허가된 사람이 일련의 홍채 코드를 발생하고, 단일한 기준 홍채 코드를 선택할 수 있는 등록 센터를 방문해야 한다.

제 2 데이터 영역(276)은 n개의 분리된 데이터베이스 테이블(3101 내지 301n)로 분리되고, 허가된 사람에 대하여 각각 하나의 테이블이 인덱스된다. 도시된 바와 같이, 테이블(3101)은 허가된 사람 1에 대한 홍채 코드 A 내지 D와 유사성 임계 레벨에 대한 값을 포함한다. 홍채 코드 A 내지 D는 허가된 사람 1에 의

한 이전의 인식 시도 때에 서버(160)에 의해 수신되었던 이력 홍채 코드들이다. 아래에 기술되는 바와 같이 허가된 사람 1에 대한 테이블의 크기는 허가된 사람 1이 인식될 때마다 하나의 홍채 코드씩 증가한다. 그러나 실제로는 데이터 저장 용량이 무제한이기 때문에, 저장된 홍채 코드의 수는 예를 들어 100으로 제한될 수 있다.

이제 도 4의 흐름도를 참조하여 홍채 인식 절차에 대해 기술한다. 이 절차 자체는 Oracle SQL 및 C++로 작성된 루틴과 적당한 소프트웨어 처리를 포함한다.

도 4에 따르면, 단계(400)에서 인식 서버(160)는 클라이언트(120)로부터 홍채 코드를 수신한다. 이 홍채 코드는 주메모리(230)의 제 1 임시 메모리 기억영역(TEMP1)에 저장된다. 다음에, 단계(405)에서, 제 1 데이터 저장 영역(273)의 데이터 테이블이 주메모리(230)로 판독된다. 데이터 테이블의 크기가 주메모리보다 크면, 파일 서버(160)는 통상적인 방법에서 요구되는 바와 같이 적당한 크기의 테이블 부분들을 주메모리로 판독하도록 구성된다. 단계(410, 415 및 420)에서, 서버(160)는 주메모리(230)에 액세스하고, 각각의 기준 홍채 코드를 판독하여 일치가 발견될 때까지 임시 메모리 위치(TEMP1)에 저장된 수신된 홍채 코드와 비교한다. 비교는 비트를 기준으로 행해지며(여기서는 256비트임), 각각의 기준 홍채 코드에 대해 일치하는 비트들의 수가 도출된다. 이 실시예에서, 식별을 구성하는 일치는 비트의 30% 이상이 다를 때에도 얻어진다.

약 30%의 임계값은 많은 시험을 거쳐 발견적으로 결정되며, 그 결과는 1993년 11월, 패턴 분석 및 기계 지능(PAMI)에 대한 IEEE 보고서, Vol. 15에 게재된 Daugman J G의 '통계 독립성 검사에 의한 고신뢰성 시각 인식'에 보다 상세히 기술되어 있다. 물론, 값 또는 비교 방법은 사용된 홍채 이미지 캡처 장치(100)의 형태 또는 다른 형태로의 변형 및 이미지 캡처 환경과 같은 다른 요인, 홍채 코드 발생 알고리즘 및 시스템에 요구되는 보안성 정도에 따라 변화할 수 있다. 예를 들어 보다 낮은 보안성의 시스템은 보다 짧고 세밀하지 않은 홍채 코드를 사용한다.

단계(420)에서, 일치가 발견되지 않으면, 홍채 코드는 식별되지 않은 것으로 간주되고, 단계(425)에서, 적당한 신호가 클라이언트(120)로 리턴된다.

수신된 홍채 코드에 대해 일치가 발견되었다고 가정하면, 단계(430)에서 서버(160)는 각각의 기준 홍채 코드와 관련된 허가된 사람의 식별번호를 제 2 임시 메모리 위치(TEMP2)로 판독한다. 일치하는 기준 홍채 코드가 허가된 사람 1과 관련되어 있다고 가정하면, 단계(435)에서 서버(160)는 제 2 데이터 저장 영역(276)에 액세스하고, 허가된 사람 1에 의한 이력 홍채 코드를 포함하는 테이블(3101)을 주메모리(230)로 판독한다. 또한, 허가된 사람 1에 대한 각각의 유사성 정도의 임계값이 제 3 임시 메모리 위치(TEMP3)로 판독된다.

단계(440)에서, 각각의 이력 홍채 코드가 주메모리로부터 판독되고, 수신된 홍채 코드와 비교된다. 각각의 홍채 코드 비교에 대해, 단계(445)에서, 정확한 일치가 발견되면, 수신된 홍채 코드는 부정한 것으로 간주되고, 단계(450)에서 적당한 메시지가 서버(160)에 의해 클라이언트(120)와 처리 단말로 리턴된다.

정확한 일치가 부정한 홍채 코드를 의미한다는 판단의 기준은 2개의 홍채 코드가 심지어 동일한 허가된 사람에게서 나왔을 지라도 일치한다고 생각할 수 없다는 사실로부터 나온다. 따라서, 정확한 일치는 허가된 사용자에 의한 이전의 인식 시도 동안 최초로 서버(160)로 전송되었을 때 일치된 이력 홍채 코드가 허가되지 않은 사용자에 의해 도청되어 복사되었을지도 모른다는 것을 의미한다(허가되지 않은 사용자는 이후 예를 들어 보안 시스템에 액세스하기 위해 허가된 사람으로 가장하려는 시도로 서버에 이 홍채 코드를 전송한다). 도청된 데이터를 사용하여 허가된 사람으로 가장하려는 이러한 형태의 시도는 때로는 재연 공격으로 알려져 있다.

정확한 일치가 존재하지 않으면, (100보다 적은) 일치하는 비트들의 백분율값이 도출되고, 단계(455)에서 제 4 임시 메모리 위치(TEMP4)에 저장된다. 다음에, 단계(460)에서, 제 4 임시 메모리 위치(TEMP4)에 저장된 유사성 정도가 제 3 임시 메모리 위치(TEMP3)에 저장된 임계 유사성 정도보다 크면, 수신된 홍채 코드는 부정한 것으로 간주되고, 단계(450)에서, 적당한 메시지가 서버(160)에 의해 클라이언트(120)와 처리 단말로 리턴된다.

수신된 홍채 코드가 모든 이력 홍채 코드에 대해 인식 판단 기준-정확히 동일하지 않고 너무 유사하지 않은-을 만족하면, 단계(465)에서, 허가된 사람이 성공적으로 식별되고 인증되었다는 것을 나타내는 신호가 서버(160)에 의해 클라이언트(120)로 리턴된다. 최종적으로, 단계(470)에서, 제 1 임시 메모리 위치(TEMP1)에 저장되는 수신된 홍채 코드는 허가된 사람 1에 대한 데이터베이스 테이블(3101)에 이력 홍채 코드로서 기록된다.

홍채 코드가 소정의 임계 유사성 정도보다 큰 이력 홍채 코드에 대한 유사성을 갖으면 홍채 코드를 부정한 것으로 판단하는 기준은 정확한 일치만큼 불가능하지는 않지만 매우 유사한 일치가 불가능하다는 사실로부터 나온다. 임계값은 다시 아래에 기술되는 바와 같이 시험에 기초하여 발견적으로 결정된다. 이 값은 다시 사용된 이미지 캡처 장치(100)의 형태 또는 다른 형태로의 변형, 이미지 캡처 환경과 같은 다른 요인, 사용된 홍채 코드 발생 알고리즘 및 시스템에 요구되는 보안성 정도에 따라 변화한다.

인식 시험은 1996년 10월에 실행되었고, 여기서 시험팀의 훈련된 구성원들은 동일한 태도를 취하고, 인식을 위해 기본적인 인식 시스템을 기동하였다. 도 5는 사용자의 눈이 조정되었을 때 기동된 546개의 인식에 대한 인식 해밍(Hamming) 거리를 보여준다. 이들 인식에 대한 평균 해밍 거리는 0.042의 표준 편차로 0.090이었다(즉, 비트들의 9%가 불일치하였음). 이들 결과들은 사용자에 대한 인식 해밍 거리의 분포가 존재하고, 유사한 결과가 상용 홍채 인식 시스템에서도 예측된다는 것을 보여준다.

도 5의 그래프를 형성하기 위해 사용된 결과를 생각하면, 특정 임계값에 대하여 한 사람에 대한 그릇된 인식을 얻을 확률이 다음과 같이 도출된다.

| 임계(%) | 546개의 시도 중 예측된 실패의 수 |
|---|---|
| 2 | 3 |
| 3 | 9 |
| 4 | 30 |
| 5 | 83 |

예를 들어, 임계가 3%로 고정되면, 결과는 허가된 사람에 의한 546개의 인식 시도 중 9개가 무효로 되는 것을 나타낸다.

실제, 서버(160)는 홍채 코드가 이력 홍채 코드와 동일한 비트를 90% 이상 갖으면 절차를 중단하는 대신에 클라이언트(120)에 식별 및 인증할 사용자로부터 다른 홍채 코드를 얻어 리턴하도록 요청한다. 다음에 클라이언트는 사용자 눈에 대한 다른 이미지를 캡처하기 전에 사용자의 눈에 대한 조도 또는 홍채 코드 발생기내의 광학 초점 길이를 변경하도록 홍채 코드 발생기를 제어한다. 이러한 방식으로 변경된 홍채 이미지를 사용하는 2번째 기회를 제공함으로써 허가된 사용자의 보안 네트워크에 대한 액세스가 거부되는 경우의 수가 감소한다.

당업자는 축약형 인증 판단 기준이 상기한 시나리오에도 적용될 수 있다고 평가할 것이다. 예를 들어, 인증은 정확한 일치의 경우에만 무효화될 수 있다(그리고 제 2 홍채 코드가 요청될 수 있다). 또한, 홍채 코드들을 비교하는 보다 복잡한 구현들은 특정한 비트 불일치의 상대적인 가능성(홍채 코드의 모든 비트들이 동일하게 변화하기 쉽지는 않음) 또는 그 홍채에 대한 이전의 식별에 대한 통계적 일관성을 고려할 수 있다.

실제, 보다 복잡한 검색 알고리즘이 제 1 데이터 영역(273)을 스캔하는 제 1 프로세싱 단계에 사용될 수도 있다. 홍채 인식의 경우에, 예를 들어 눈의 상이한 회전을 고려할 때마다 일치하는 기준 홍채 코드가 발견되기 전에 수차례 제 1 데이터 영역을 스캔할 필요가 있다. 상이한 눈 회전은 사용자들이 머리를 상이한 경사각도로 내밀어, 비틀린 눈 회전 때문에 발생된다. 따라서, 제 1 프로세싱 단계를 목적으로 미국 특허 제 5,291,560 호에 기술된 전용 데이터베이스 검색 알고리즘을 사용하는 것이 보다 유리하다.

상기한 미국 특허를 사용하여 발생된 홍채 코드의 특성은 홍채 코드의 모든 비트들이 동일하게 손상되는 것이 쉽지 않다는 것을 나타낸다. 홍채를 인코드하는데 사용된 알고리즘은 여러 레벨의 등급 및/또는 항목들로 홍채 특성들을 고려하고, 각각의 홍채 코드내의 특정 위치의 비트들에 이들 특성들을 반영하는 정보를 할당한다. 따라서, 보다 거시적인 특성들에 대응하는 홍채 코드의 비트들이 부정확하게 설정되는 것에 덜 민감하다고 가정하는 것이 합리적이다. 역으로, 작거나 매우 상세한 홍채 특성들에 대응하는 홍채 코드의 비트들은 부정확하게 설정되는 것에 더 민감하다.

본 발명자들은 부정확하게 설정되는 특정 비트들의 감수성이 클라이언트 하드웨어의 구성, 사용된 정밀 홍채 코드 발생 알고리즘, 조도 변화, 미세한 초점 차이, 홍채를 차단하는 먼지, 눈꺼풀 등 및 사용자의 특성에 크게 의존한다. 이것은 이러한 원인에 따른 여러 가지 형태의 홍채 코드 손상을 예측하는 것이 합리적이기 때문이다. 예를 들어 눈꺼풀을 닫는 것은 홍채의 일정한 큰 부분에 영향을 미치는 반면에, 먼지 또는 티끌들은 보다 국부적이다. 초점 차이는 홍채의 모든 부분에 영향을 미치지만, 홍채 이미지의 보다 높은 공간 주파수 성분에 보다 큰 영향을 미칠 것이다. 클라이언트 하드웨어와 관련된 이미지 장치의 광학 경로상의 먼지는 각 인식에서 홍채 코드의 동일한 부분에 영향을 미치기 쉬운 반면에 잡음(예를 들어 CCD 칩으로부터)은 그 영향이 보다 가변적이다. 다음으로 캡처된 이미지의 홍채 부분을 분리하는데 사용된 국부화 소프트웨어에서의 변화가 홍채 코드 발생에 사용된 경계선의 위치에 영향을 미칠 것이다. 그 결과, 상세한 특성들을 나타내는 비트들이 대체적으로 거시적인 특성들에 대응하는 비트들보다 훨씬 더 영향을 받게 된다.

따라서, 본 발명의 보다 복잡한 구현은 홍채 코드의 각각의 비트 또는 비트들의 조합이 부정확하게 설정되는 가능성을 고려한다. 비트들이 부정확하게 설정되는 가능성을 판단하는데 있어서, 이 판단 처리는 발생된 홍채 코드의 통계적인 특성과, 클라이언트와 허가된 사람의 이력들을 이용할 수 있다는 것은 당업자에게 명백할 것이다.

게다가, 기준 홍채 코드 또는 임의의 임계값은 식별 및/또는 인증 특성의 변화에 따라 시간적으로 변화할 수 있다. 예를 들어, 특별히 허가된 사람이 일반적으로 기준 홍채 코드의 20%내에서 계속적으로 유사한 홍채 코드 판독을 달성하는 것이 명백하다면, 식별 목적의 유사성 임계는 70 내지 75%로 높아질 수 있다. 마찬가지로, 수신된 홍채 코드와 이력 홍채 코드가 유사한 것으로 간주되는 임계는 2%에서 1%로 감소될 수 있다. 이러한 변수 변화는 인식 서버(160)에 의해 주기적 및 자동적으로 실시된다. 역으로, 허가된 사람이 열악한 홍채 코드 판독으로 인해 계속적으로 인식되지 않으면, 홍채 코드 판독이 얼마나 열악한지, 그리고 시스템의 보안성이 얼마나 많이 양보될 수 있는지에 따라 그 허가된 사람에 대한 임계는 낮아질 수 있다.

상기한 실시예가 사용자가 허가된 사람인지에 대한 판단을 실행하도록 프로세서를 제어하기 위해 소프트웨어 프로그램을 사용하는 것에 대해 기술하고 있지만, 적어도 디지털 서명 비교 단계를 실행하는데는 하드웨어 구성을 사용하는 것이 더 빠르다.

또한, 상기 실시예의 제 1 비교 단계는 각각의 기준 디지털 서명을 차례로 비교하는 것을 포함한다. 따라서, 상기한 장치는 어떤 허가된 사용자가 보안 검사를 통과하려고 하는지를 판단할 수 있다. 본 발명은 또한 보안 검사 장치의 목적이 사용자의 식별번호를 확인하는 것인 경우에 유용하다. 예를 들어, 종래의 현금자동지급기의 사용자들은 거래를 하기 전에 데이터 기록 자기스트립을 수반하는 카드를 삽입할 것으로 예측된다. 사실, 이 카드는 식별번호 토큰으로서 기능한다 - 사용자가 입력하는 PIN이 카드를 제시한 허가된 사람과 관련하여 저장된 PIN과 일치하면 사용자에게 금전출납 거래가 허용된다.

종래 장치의 PIN의 사용이 디지털 사명의 사용으로 대체되면, 중앙 서버는 사용자의 서명이 카드를 제시

한 허가된 사람과 관련된 기준 서명에 대응하는지(그러나 너무 유사하지는 않은)를 확인하기만 하면 된다.

상기 실시예는 일정하지 않은 디지털 서명에 내재하는 가변성을 이용한다는 것을 알 수 있을 것이다. 따라서, 다소 역설적으로 말하면, 본 발명의 실시예는 디지털 서명을 캡처하는데 사용된 장치를 개선함으로써 악화될 수 있다. 예를 들어, 홍채 패턴의 이미지를 캡처하는데 사용된 광학장치의 개선은 허가된 사람의 홍채의 캡처된 이미지의 가변성을 감소시킬 수 있다. 다음에, 이것은 서로 다른 경우에 허가된 사람에 의해 제공된 2개의 홍채 코드 사이의 유사한 일치가 발생할 기회를 더욱 크게 한다. 따라서, 부정한 사용자와 허가된 사람 사이의 판별은 보다 어렵게 됨을 알 수 있을 것이다.

이러한 경우에, 상기한 실시예는 보안 검사를 통과하기 위한 허가된 사용자의 시도 중 상당히 변화하는 디지털 서명을 제공하기 위해 홍채 코드에 가변 변수(예를 들어 동공 직경)를 부가함으로써 개선될 수 있다.

## *(57) 청구의 범위*

### 청구항 1

보안 검사를 통과하려 하는 사람이 제공한 순간 디지털 서명과 저장 디지털 서명을 비교하는 단계,

상기 사인들이 충분히 유사하다고 나타내는 상기 비교에 응답하여 상기 보안 검사를 통과하려 하는 사람을 상기 저장 디지털 서명을 제공한 사람으로서 식별하는 단계,

상기 순간 디지털 서명과, 보안 검사를 통과하기 위한 이전의 시도에서 제공된 하나 이상의 이전의 디지털 서명을 비교하는 단계 및

상기 순간 서명을 하나 이상의 이전의 서명과 부당하게 유사한 것으로 나타내는 상기 비교에 응답하여 상기 식별을 무효화하는 단계를 포함하는 것을 특징으로 하는 일정하지 않은 디지털 서명에 기초하여 보안 검사를 통과하려는 사람이 허가된 사람인지를 판단하는 방법

### 청구항 2

제 1 항에 있어서,

상기 순간 서명이 이전의 서명과 동일할 경우에만 상기 식별은 무효화되는 것을 특징으로 방법.

### 청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 일정하지 않은 디지털 서명은 생체측정 정보를 포함하는 것을 특징으로 하는 방법.

### 청구항 4

제 3 항에 있어서,

상기 생체측정 정보는 홍채 코드를 포함하는 것을 특징으로 하는 방법.

### 청구항 5

제 1 항 내지 제 4 항 중 어느 한 항에 있어서,

상기 순간 디지털 서명과 상기 기준 서명을 비교하는 단계는 상기 순간 및 기준 서명 사이의 제 1 유사성 정도를 계산하는 것을 포함하고,

상기 제 1 유사성 정도가 소정의 제 1 임계를 초과하는 경우에 상기 사용자가 허가된 사람으로 식별되고,

상기 순간 디지털 서명과 하나 이상의 이전의 디지털 서명을 비교하는 단계는 상기 순간 및 이전의 서명 사이의 하나 이상의 제 2 유사성 정도를 계산하는 것을 포함하며,

상기 제 2 유사성 정도가 상기 제 1 임계보다 높은 소정의 제 2 임계를 초과하는 경우에 상기 사용자의 식별은 무효화되는 것을 특징으로 하는 방법.

### 청구항 6

제 5 항에 있어서,

상기 제 1 및 제 2 임계 중 하나 또는 모두는 조정 가능한 것을 특징으로 하는 방법.

### 청구항 7

사용자에 의해 제공된 디지털 서명을 수신하는 입력수단,

하나 이상의 기준 디지털 서명과, 기준 서명을 제공한 허가된 사용자들을 식별하는 각각의 관련 정보 항목들을 저장하는 제 1 저장수단,

식별된 허가된 사용자에 의한 이전의 인식 시도에서 얻어진 이전의 디지털 서명을 저장하는 제 2 저장수단,

상기 제 1 저장수단에 액세스하고, 수신된 디지털 서명을 하나 이상의 기준 디지털 서명과 비교하며, 상기 수신된 디지털 서명과 기준 디지털 서명의 유사성 정도가 소정의 제 1 유사성 임계를 초과하는 경우에, 사용자를 수신된 디지털 서명의 최초 사용자로서 식별하는 제 1 프로세싱 수단 및

상기 제 2 저장수단에 액세스하고, 수신된 디지털 서명을 식별된 허가된 사람에 의한 이전의 인식 시도와 관련된 이전의 서명과 비교하며, 상기 수신된 디지털 서명과 이전의 디지털 서명의 제 2 유사성 정도가 소정의 제 2 임계를 초과하는 경우에 상기 식별을 무효화하는 제 2 프로세싱 수단을 포함하는 것을 특징으로 하는 보안 검사를 제공하는데 사용하는 장치.

**청구항 8**

각각의 허가된 사람에 의해 제공된 하나 이상의 기준 서명을 나타내는 데이터,

보안 검사를 통과하는 위한 이전의 하나 이상의 이전의 시도에서 제공된 하나 이상의 이전의 서명들을 나타내는 각각의 기준 서명과 관련된 데이터 및

보안 검사를 통과하려고 시도한 사람에 의해 제공된 순간 디지털 서명과 기준 디지털 서명을 비교하도록 처리 가능한 수신된 서명 비교 코드,

상기 신호들이 충분히 유사하다고 나타내는 상기 비교에 응답하여 상기 사용자를 상기 기준 디지털 서명을 제공한 사람으로 식별하도록 처리 가능한 사용자 식별 코드,

상기 순간 디지털 서명과, 보안 검사를 통과하기 위한 이전의 시도에서 제공된 하나 이상의 이전의 디지털 서명을 비교하도록 처리 가능한 부가적으로 수신된 서명 비교 코드 및

상기 순간 서명이 하나 이상의 이전의 서명과 부당하게 유사하다고 나타내는 상기 비교에 응답하여 상기 식별을 무효화하도록 처리 가능한 식별 무효화 코드를 포함하는 수신된 디지털 서명이 허가된 사용자에 의해 제공된 것인지를 판단하기 위해 처리 가능한 프로세서 판독 가능 코드가 기록된 하나 이상의 저장 매체를 포함하는 보안 검사를 제공하는 장치.

**청구항 9**

보안 검사를 통과하려고 시도한 사람에 의해 제공된 순간 디지털 서명과 기준 디지털 서명을 비교하는 단계,

상기 서명들이 충분히 유사하다고 나타내는 상기 비교에 응답하여 상기 보안 검사를 통과하려고 시도한 사람을 상기 기준 디지털 서명을 제공한 사람으로 식별하는 단계,

상기 순간 디지털 서명과, 보안 검사를 통과하기 위한 이전의 시도에서 제공된 하나 이상의 이전의 디지털 서명들을 비교하는 단계 및

상기 순간 서명을 하나 이상의 이전의 서명들과 부당하게 유사한 것으로 나타내는 상기 비교에 응답하여 상기 식별을 무효화하는 단계를 포함하는 수신된 디지털 서명이 허가된 사람에 의해 제공된 것인지를 판단하는 방법을 실행하기 위해 프로세서에 의해 실행 가능한 명령들로 이루어진 프로그램을 명확하게 구현하는 것을 특징으로 하는 프로세싱 장치에 의해 판독 가능한 프로그램 저장 장치.

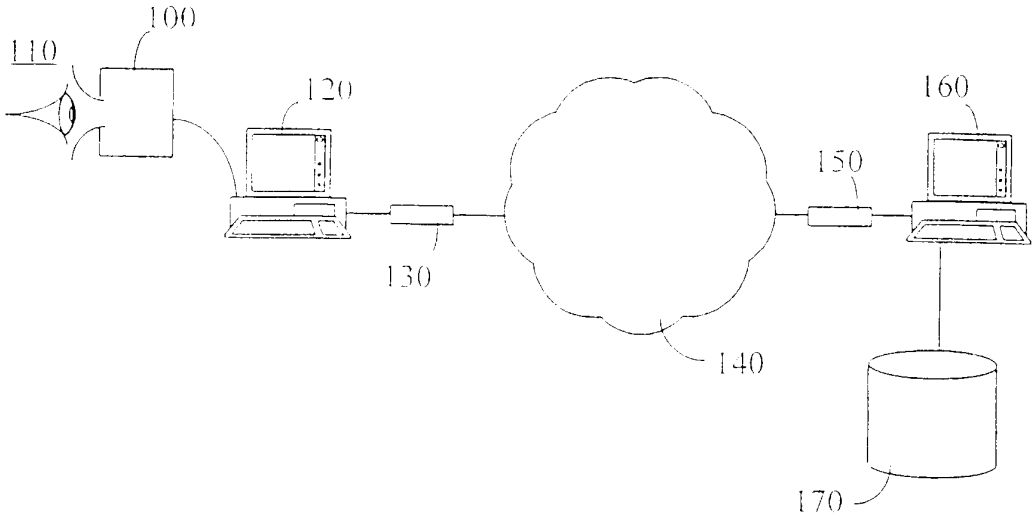
**청구항 10**

가입자로부터의 디지털 서명을 복수의 서로 다른 가입자들에 대한 저장된 디지털 서명들과 비교하여 가입자를 식별하는 단계를 포함하며,

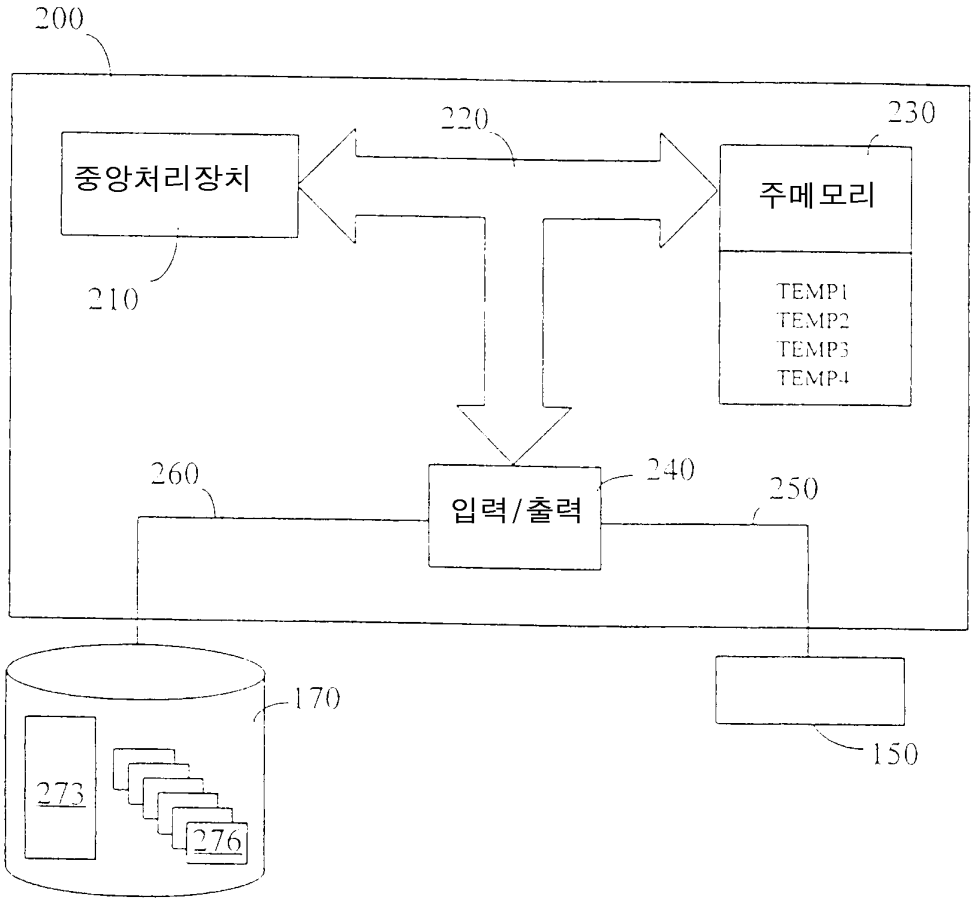
긍정 인정은 소정의 유사성 임계를 초과하는 제공된 디지털 서명과 하나 이상의 저장된 디지털 서명 사이의 도출된 유사성 정도에 의존하고, 제공된 디지털 서명 또는 그로부터 도출된 데이터와 식별된 가입자에 의한 이전의 인식 시도와 관련된 저장된 이력 및/또는 통계 데이터 사이의 비교의 결과에 소정의 판단 기준을 적용하여 식별된 가입자를 인증하고, 긍정 인정은 제공된 디지털 서명과 식별된 가입자에 대한 하나 이상의 이전의 인식 시도로부터 얻어진 하나 이상의 이력 디지털 서명을 비교하고, 제공된 디지털 서명과 임의의 이력 디지털 서명 사이의 유사성이 동일하지 않거나 또는 소정의 제 2 임계를 초과한다고 설정함으로써 실행되는 것을 특징으로 하는 가입자 인식 방법.

*도면*

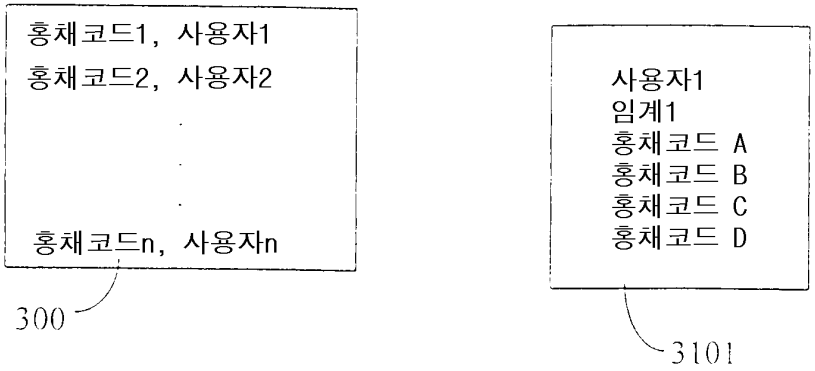
도면1



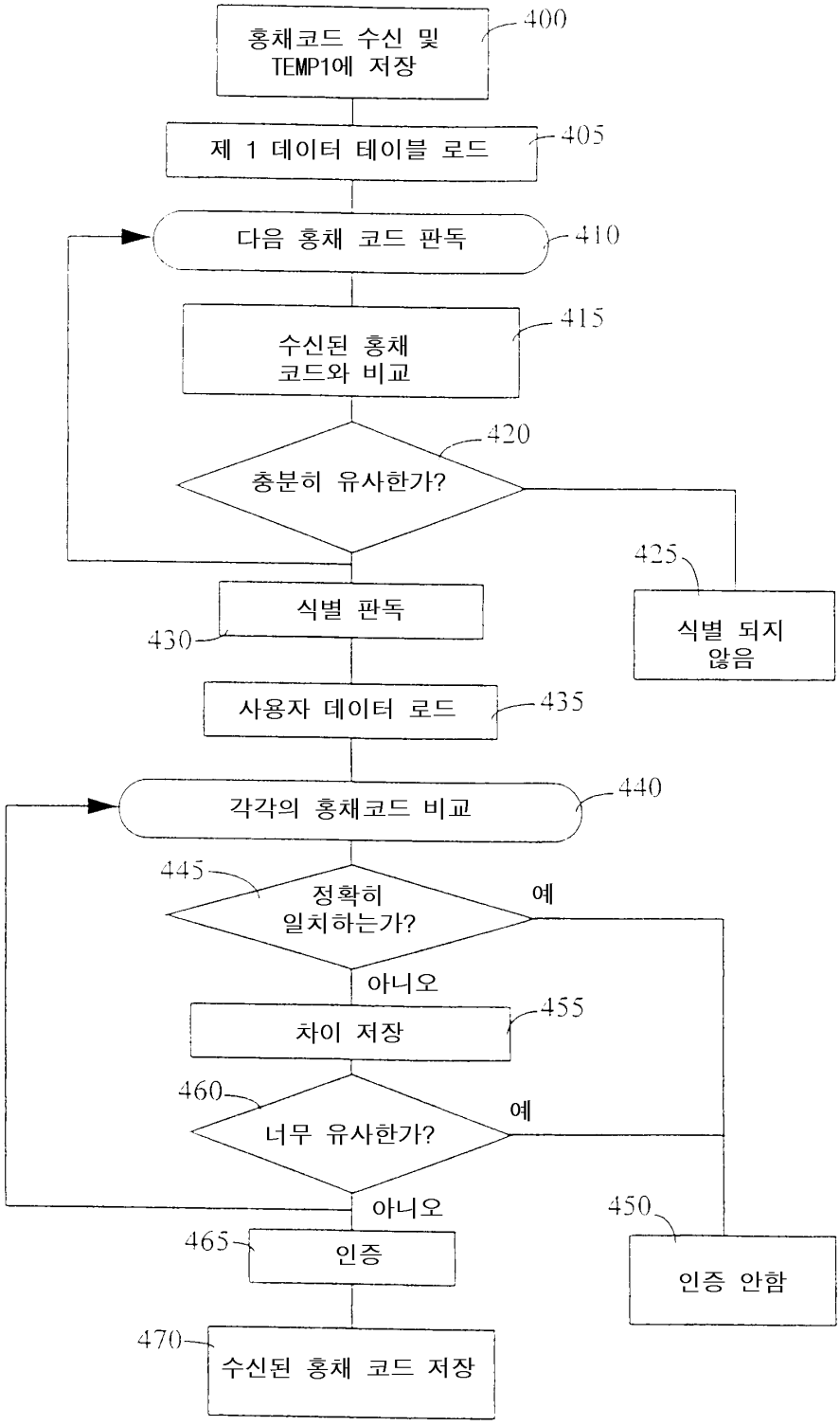
도면2


200
220
230
중앙처리장치
주메모리
210
TEMP1
TEMP2
TEMP3
TEMP4
260
240
250
입력/출력
170
273
276
150

도면3


홍채코드1, 사용자1
홍채코드2, 사용자2
홍채코드n, 사용자n
300
사용자1
임계1
홍채코드 A
홍채코드 B
홍채코드 C
홍채코드 D
3101

도면4


홍채코드 수신 및 TEMP1에 저장
400
제 1 데이터 테이블 로드
405
다음 홍채 코드 판독
410
수신된 홍채 코드와 비교
415
충분히 유사한가?
420
예
425
식별 되지 않음
식별 판독
430
사용자 데이터 로드
435
각각의 홍채코드 비교
440
정확히 일치하는가?
445
예
아니오
차이 저장
455
너무 유사한가?
460
예
아니오
450
인증 안함
인증
465
수신된 홍채 코드 저장
470

도면5