(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년08월12일
(11) 등록번호 10-2289419
(24) 등록일자 2021년08월06일

(51) 국제특허분류(Int. Cl.)
G06F 21/32 (2013.01) *G06F 21/45* (2013.01)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
G06F 21/32 (2013.01)
G06F 21/45 (2013.01)
(21) 출원번호 10-2017-0080752
(22) 출원일자 2017년06월26일
심사청구일자 2020년03월16일
(65) 공개번호 10-2019-0001177
(43) 공개일자 2019년01월04일
(56) 선행기술조사문헌
KR1020150007960 A*
US20050084143 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
허세영
대전광역시 유성구 송림로53번길 10, 107동 203호 (하기동)
앤드류 테오 벵 진
서울시 서대문구 연세로 50, 646호 (신촌동, SK글로벌하우스)
(뒷면에 계속)
(74) 대리인
팬코리아특허법인

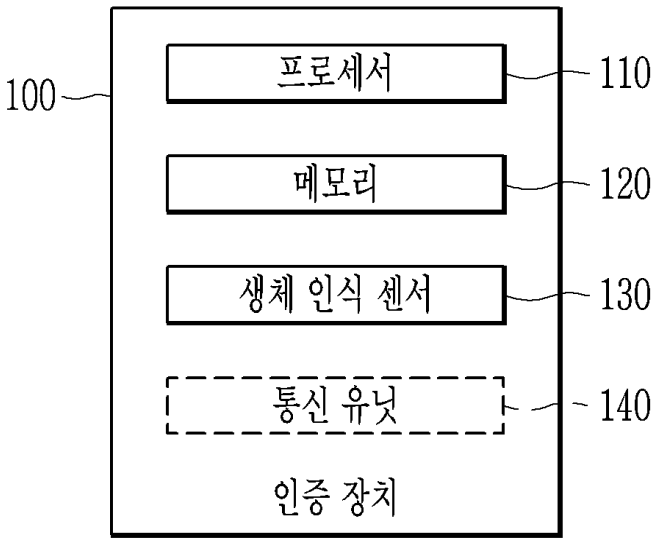
전체 청구항 수 : 총 16 항 심사관 : 문남두

(54) 발명의 명칭 **바이오메트릭을 이용한 사용자의 인증 방법 및 장치**

(57) 요 약

생체 인식 센서를 이용하여 획득된 사용자의 제1 생체 정보로부터 제1 특징 벡터를 생성하고, 제1 특징 벡터와 복수의 의사 난수 행렬을 각각 곱하는 단계, 제1특징 벡터 및 복수의 의사 난수 행렬 간의 행렬곱의 결과 벡터의 원소 중, 최대 값을 갖는 원소의 인덱스를 바탕으로 질의 템플릿을 생성하는 단계, 그리고 저장된 기준 템플릿 및 질의 템플릿을 비교하여 사용자의 인증을 수행하는 단계를 통해 사용자를 인증하는 방법 및 장치가 제공된다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0894 (2013.01)
H04L 9/3231 (2013.01)

(72) 발명자
황정연
대전광역시 유성구 지족로 362, 302동 1001호 (지족동, 반석마을아파트3단지)
김석현
대전광역시 유성구 노은로 416, 508동 801호 (하기동, 송림마을5단지아파트)
김수형
대전광역시 유성구 은구비남로 34, 815동 601호 (노은동, 열매마을8단지)
김승현
대전시 유성구 엑스포로 448, 302동 1003호 (전민동, 엑스포아파트)
김영삼
대전광역시 유성구 죽동로 72, 502동 1301호 (죽동, 천년나무아파트)
노종혁
대전광역시 유성구 반석서로 98, 606동 2103호 (반석동, 반석마을6단지아파트)
조상래
대전광역시 유성구 은구비남로 13, 811호 (지족동, SK허브)
조영섭
대전광역시 유성구 배울2로 78, 604동 1702호 (관평동, 운암네오미아)
조진만
대전시 서구 청사서로 11, 101동 304호 (월평동, 무지개아파트)
진승헌
대전광역시 서구 청사서로 65,109동 1005호 (월평동, 한아름아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호	B0717-16-0114
부처명	미래창조과학부
과제관리(전문)기관명	정보통신기술진흥센터(IITP)
연구사업명	정보통신 방송연구개발사업
연구과제명	비대면 본인확인을 위한 바이오 공개키 기반구조 기술 개발
기 여 율	1/1
과제수행기관명	한국전자통신연구원
연구기간	2017.01.01~2017.12.31

명 세 서

청구범위

청구항 1

사용자의 생체 정보를 이용하여 상기 사용자를 인증하는 방법으로서,

사용자의 제1 생체 정보로부터 획득된 제1 특징 벡터와 복수의 의사 난수 행렬을 각각 곱하는 단계,

상기 제1특징 벡터 및 상기 복수의 의사 난수 행렬 간의 행렬곱의 결과 벡터의 원소 중, 최대 값을 갖는 원소의 인덱스를 바탕으로 질의 템플릿을 생성하는 단계, 그리고

저장된 기준 템플릿 및 상기 질의 템플릿을 비교하여 상기 인증을 수행하는 단계

를 포함하고,

상기 인증을 수행하는 단계는,

비밀키를 상기 기준 템플릿과 결합하는 단계, 그리고

상기 질의 템플릿을 이용하여 상기 비밀키를 복구하는 단계

를 포함하고,

상기 비밀키를 상기 기준 템플릿과 결합하는 단계는,

상기 기준 템플릿의 기준 엔트리를 복수의 볼트(vault)에 할당하는 단계, 그리고

상기 기준 엔트리가 상기 복수의 볼트 내에서 할당된 위치를 나타내는 위치 인덱스를, 상기 비밀키에 기반하여 결정된 다항식의 미지수 x에 입력하여, 상기 기준 엔트리의 상기 위치 인덱스에 대응하는 출력 엔트리를 결정하는 단계

를 포함하는, 인증 방법.

청구항 2

제1항에서,

상기 제1 생체 정보 보다 이전에 생성된, 사용자의 제2 생체 정보로부터 획득된 제2 특징 벡터와 복수의 의사 난수 행렬을 각각 곱하는 단계, 그리고

상기 제2 특징 벡터 및 상기 복수의 의사 난수 행렬 간의 행렬곱의 결과 벡터의 원소 중, 최대 값을 갖는 원소의 인덱스를 바탕으로 기준 템플릿을 생성하고, 상기 기준 템플릿을 저장하는 단계

를 더 포함하는 인증 방법.

청구항 3

제1항에서,

상기 인증을 수행하는 단계는,

상기 질의 템플릿과 상기 기준 템플릿의 차이가 0인 원소가 미리 설정된 개수 이상이면, 상기 질의 템플릿의 사용자를 상기 기준 템플릿의 사용자와 동일하다고 판정하는 단계

를 포함하는, 인증 방법.

청구항 4

제2항에서,

상기 기준 템플릿 및 상기 질의 템플릿은, 상기 결과 벡터의 원소 중 최대 값을 갖는 원소의 인덱스를 원소로서

포함하는, 인증 방법.

청구항 5

삭제

청구항 6

삭제

청구항 7

제1항에서,

상기 비밀키를 상기 기준 템플릿과 결합하는 단계는,

복수의 채프 엔트리를 상기 복수의 볼트에서 상기 기준 엔트리가 할당되지 않은 셀에 할당하는 단계,

상기 채프 엔트리가 상기 복수의 볼트 내에서 할당된 위치를 나타내는 위치 인덱스를, 상기 다항식의 미지수 x에 입력하여, 상기 채프 엔트리의 상기 위치 인덱스에 대응하는 채프 출력 엔트리를 결정하는 단계, 그리고

상기 기준 엔트리와 상기 출력 엔트리의 세트 및 상기 채프 엔트리와 상기 채프 출력 엔트리의 세트를 헬퍼 데이터로서 함께 저장하는 단계

를 더 포함하는, 인증 방법.

청구항 8

제7항에서,

상기 질의 템플릿을 이용하여 상기 비밀키를 복구하는 단계는,

상기 복수의 볼트에 할당된 엔트리 중, 상기 질의 템플릿의 질의 엔트리와 동일한 엔트리의 동일 인덱스를 탐색하는 단계,

상기 질의 엔트리와 동일한 엔트리가 존재하면, 상기 헬퍼 데이터로부터 상기 동일 인덱스에 대응하는 출력 엔트리를 결정하는 단계, 그리고

상기 동일 인덱스 및 상기 출력 엔트리의 순서쌍을 바탕으로 상기 다항식을 결정하는 단계

를 포함하는, 인증 방법.

청구항 9

제8항에서,

상기 질의 템플릿을 이용하여 상기 비밀키를 복구하는 단계는,

상기 동일 인덱스 및 상기 출력 엔트리의 순서쌍을 바탕으로 결정된 다항식의 계수를 입력으로 하는 해시 함수의 결과에 기반하여 상기 계수를 상기 비밀키로 결정하는 단계

를 더 포함하는, 인증 방법.

청구항 10

제7항에서,

상기 복수의 볼트는 각각 적어도 하나의 미니 볼트를 포함하고, 상기 적어도 하나의 미니 볼트는 상기 기준 엔트리가 할당된 하나의 셀 및 상기 복수의 채프 엔트리가 할당된 복수의 셀을 포함하는, 인증 방법.

청구항 11

사용자의 생체 정보를 이용하여 상기 사용자를 인증하는 장치로서,

프로세서, 메모리, 그리고 생체 인식 센서

를 포함하고,

상기 프로세서는 상기 메모리에 저장된 프로그램을 실행하여,

상기 생체 인식 센서를 이용하여 획득된 사용자의 제1 생체 정보로부터 제1 특징 벡터를 생성하고, 상기 제1 특징 벡터와 복수의 의사 난수 행렬을 각각 곱하는 단계,

상기 제1특징 벡터 및 상기 복수의 의사 난수 행렬 간의 행렬곱의 결과 벡터의 원소 중, 최대 값을 갖는 원소의 인덱스를 바탕으로 질의 템플릿을 생성하는 단계, 그리고

저장된 기준 템플릿 및 상기 질의 템플릿을 비교하여 상기 인증을 수행하는 단계

를 수행하고,

상기 프로세서는 상기 인증을 수행하는 단계를 수행할 때,

비밀키를 상기 기준 템플릿과 결합하는 단계, 그리고

상기 질의 템플릿을 이용하여 상기 비밀키를 복구하는 단계

를 수행하고,

상기 프로세서는 상기 비밀키를 상기 기준 템플릿과 결합하는 단계를 수행할 때,

상기 기준 템플릿의 기준 엔트리를 복수의 볼트(vault)에 할당하는 단계, 그리고

상기 기준 엔트리가 상기 복수의 볼트 내에서 할당된 위치를 나타내는 위치 인덱스를, 상기 비밀키에 기반하여 결정된 다항식의 미지수 x에 입력하여, 상기 기준 엔트리의 상기 위치 인덱스에 대응하는 출력 엔트리를 결정하는 단계

를 수행하는, 인증 장치.

청구항 12

제11항에서,

상기 프로세서는 상기 프로그램을 실행하여,

상기 생체 인식 센서를 이용하여 상기 제1 생체 정보 보다 이전에 획득된, 사용자의 제2 생체 정보로부터 제2 특징 벡터를 생성하고, 상기 제2 특징 벡터와 복수의 의사 난수 행렬을 각각 곱하는 단계, 그리고

상기 제2 특징 벡터 및 상기 복수의 의사 난수 행렬 간의 행렬곱의 결과 벡터의 원소 중, 최대 값을 갖는 원소의 인덱스를 바탕으로 기준 템플릿을 생성하고, 상기 기준 템플릿을 저장하는 단계

를 더 수행하는, 인증 장치.

청구항 13

제11항에서,

상기 프로세서는 상기 인증을 수행하는 단계를 수행할 때,

상기 질의 템플릿과 상기 기준 템플릿의 차이가 0인 원소가 미리 설정된 개수 이상이면, 상기 질의 템플릿의 사용자를 상기 기준 템플릿의 사용자와 동일하다고 판정하는 단계

를 수행하는, 인증 장치.

청구항 14

제12항에서,

상기 기준 템플릿 및 상기 질의 템플릿은, 상기 결과 벡터의 원소 중 최대 값을 갖는 원소의 인덱스를 원소로서 포함하는, 인증 장치.

청구항 15

삭제

청구항 16

삭제

청구항 17

제11항에서,

상기 프로세서는 상기 비밀키를 상기 기준 템플릿과 결합하는 단계를 수행할 때,

복수의 채프 엔트리를 상기 복수의 볼트에서 상기 기준 엔트리가 할당되지 않은 셀에 할당하는 단계,

상기 채프 엔트리가 상기 복수의 볼트 내에서 할당된 위치를 나타내는 위치 인덱스를, 상기 다항식의 미지수 x에 입력하여, 상기 채프 엔트리의 상기 위치 인덱스에 대응하는 채프 출력 엔트리를 결정하는 단계, 그리고

상기 기준 엔트리와 상기 출력 엔트리의 세트 및 상기 채프 엔트리와 상기 채프 출력 엔트리의 세트를 헬퍼 데이터로서 함께 저장하는 단계

를 더 수행하는, 인증 장치.

청구항 18

제17항에서,

상기 프로세서는 상기 질의 템플릿을 이용하여 상기 비밀키를 복구하는 단계를 수행할 때,

상기 복수의 볼트에 할당된 엔트리 중, 상기 질의 템플릿의 질의 엔트리와 동일한 엔트리의 동일 인덱스를 탐색하는 단계,

상기 질의 엔트리와 동일한 엔트리가 존재하면, 상기 헬퍼 데이터로부터 상기 동일 인덱스에 대응하는 출력 엔트리를 결정하는 단계, 그리고

상기 동일 인덱스 및 상기 출력 엔트리의 순서쌍을 바탕으로 상기 다항식을 결정하는 단계

를 수행하는, 인증 장치.

청구항 19

제18항에서,

상기 프로세서는 상기 질의 템플릿을 이용하여 상기 비밀키를 복구하는 단계를 수행할 때,

상기 동일 인덱스 및 상기 출력 엔트리의 순서쌍을 바탕으로 결정된 다항식의 계수를 입력으로 하는 해시 함수의 결과에 기반하여 상기 계수를 상기 비밀키로 결정하는 단계

를 더 수행하는, 인증 장치.

청구항 20

제17항에서,

상기 복수의 볼트는 각각 적어도 하나의 미니 볼트를 포함하고, 상기 적어도 하나의 미니 볼트는 상기 기준 엔트리가 할당된 하나의 셀 및 상기 복수의 채프 엔트리가 할당된 복수의 셀을 포함하는, 인증 장치.

발명의 설명

기 술 분 야

[0001] 본 기재는 바이오메트릭을 이용하여 사용자를 인증하는 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 개인의 신원 확인(identification) 또는 인증(authentication)은 컴퓨터 시스템의 관리자가 어떤 형

태의 거래가 허용되기 전에 물어야 하는 주요한 질문이다. 현재 이용되고 있는 사용자 신원 확인 및 메모리-의존 암호-기반 인증 시스템은 일반적으로 저렴하고, 쉽게 구현되고, 많은 시스템에 의해 지원될 수 있다. 하지만, 그런 선행 시스템은 특정 단점을 가지고 있으며, 이러한 단점들은 업계 종사자들 사이에서 널리 인식되고 있다. 그 중에서도, 암호는 쉽게 복사되어 배포될 수 있다. 종종 사용자 신원 확인 및 암호 시스템에서, 사용자는 암호를 잊어버려서 사용자 및 시스템 관리자에게 많은 불편을 발생시킨다.

[0003] 인증되지 않은 접속으로부터 정보 및 재산을 보호하기 위한 장치 및 방법이 있다. 예를 들어, 스마트 카드 시스템, 마그네틱 키, 마그네틱 스트립 카드 등이 있다. 하지만, 이러한 시스템도 넓은 범위의 응용에 제한적이라는 약점을 갖는다.

[0004] 바이오메트릭(biometric)은, 인간 해부학, 행동 측정, 및 특성의 분야에서, 흥미로운 잠재력을 제공한다. 바이오메트릭 인증의 주된 장점은, 개인의 내재된 측면에 기반하여 개인을 인식할 수 있고, 사람이 인증 장소에 물리적으로 존재할 것만을 요구한다는 것이다. 이러한 특징은 초기 인증 방법, 예를 들어, 아주 쉽게 손상될 수 있는 암호 및 토큰 기반의 인증 방법의 문제점을 극복할 수 있다. 바이오메트릭 기술 분야에는, 키 스트로크 바이오메트릭, 지문 바이오메트릭, 망막 스캔 바이오메트릭, 손바닥 인쇄 바이오메트릭, 및 얼굴 바이오메트릭 등 여러 옵션이 있다.

[0005] 정보 및 데이터의 암호화 및 복호화 분야에서, 통신 매체를 통한 정보 전송을 보장하기 위해서 다양한 방법들이 제안 및 구현되어 왔다. 일반적으로 특수 목적 소프트웨어 프로그램의 응용 프로그램이, 기초를 이루는 내용을 숨기고, 액세스를 제한하고, 역공학을 금지하고, 출처 및 기타 보안 또는 비밀 메시지 활동을 인증하기 위해서 사용된다. 암호 시스템은 의도된 수신자를 제외하고, 난해한 비밀 또는 다른 유형의 메시지 및 정보메시지의 전송을 허용한다.

[0006] 오늘날 애플리케이션에는, 두 가지 일반적인 유형의 암호화 알고리즘, 대칭형 알고리즘 및 비대칭형 알고리즘이 존재한다. 대칭형 알고리즘에서, 암호키(encryption key)는 복호키(decryption key)로부터 계산될 수 있고, 그 반대의 경우도 가능하다. 일반적으로 대칭형 암호화를 위한 암호키는 복호키와 동일하다. 비대칭형 암호화에서, 암호화 및 복호화에 사용되는 키는 그러한 방법과 달라서, 적어도 하나의 키가 다른 키로부터 결정되는 것은 계산상으로 불가능하다. 키는, 공개 키(암호화) 및 개인키(복호화)의 쌍으로 존재하고, 데이터 무결성의 보존 및 비밀성을 위해서, 복호키는 비밀로 유지되고, 반면 공개키는 임의의 이해 관계자에 대해 가용하게 될 수 있다. 공개키를 사용하여 암호화된 메시지는 대응하는 개인키를 사용해서만 복호될 수 있다. 전통적으로 키는 암호, 토큰, 또는 이들의 조합에 의해 생성된다. 최근, 키 생성 및 그에 따른 암호화 애플리케이션을 위해서 바이오메트릭을 사용하기 위한 몇 가지 시도가 있다.

발명의 내용

해결하려는 과제

[0007] 한 실시예는, 바이오메트릭 특징 벡터와 난수 행렬의 행렬곱 결과를 바탕으로 생성된 템플릿 간의 비교를 통해 사용자를 인증하는 방법을 제공한다.

[0008] 다른 실시예는, 바이오메트릭 특징 벡터와 난수 행렬의 행렬곱 결과를 바탕으로 생성된 템플릿 간의 비교를 통해 사용자를 인증하는 장치를 제공한다.

과제의 해결 수단

[0009] 한 실시예에 따르면, 사용자의 생체 정보를 이용하여 상기 사용자를 인증하는 방법이 제공된다. 상기 인증 방법은, 사용자의 제1 생체 정보로부터 획득된 제1 특징 벡터와 복수의 의사 난수 행렬을 각각 곱하는 단계, 제1특징 벡터 및 복수의 의사 난수 행렬 간의 행렬곱의 결과 벡터의 원소 중, 최대 값을 갖는 원소의 인덱스를 바탕으로 질의 템플릿을 생성하는 단계, 그리고 저장된 기준 템플릿 및 질의 템플릿을 비교하여 인증을 수행하는 단계를 포함한다.

[0010] 상기 인증 방법은, 제1 생체 정보 보다 이전에 생성된, 사용자의 제2 생체 정보로부터 획득된 제2 특징 벡터와 복수의 의사 난수 행렬을 각각 곱하는 단계, 그리고 제2 특징 벡터 및 복수의 의사 난수 행렬 간의 행렬곱의 결과 벡터의 원소 중, 최대 값을 갖는 원소의 인덱스를 바탕으로 기준 템플릿을 생성하고, 기준 템플릿을 저장하는 단계를 더 포함할 수 있다.

[0011] 상기 인증 방법에서 인증을 수행하는 단계는, 질의 템플릿과 기준 템플릿의 차이가 0인 원소가 미리 설정된 개

수 이상이면, 질의 템플릿의 사용자를 기준 템플릿의 사용자와 동일하다고 판정하는 단계를 포함할 수 있다.

[0012] 상기 인증 방법에서 기준 템플릿 및 질의 템플릿은, 결과 벡터의 원소 중 최대 값을 갖는 원소의 인덱스를 원소로서 포함할 수 있다.

[0013] 상기 인증 방법에서 인증을 수행하는 단계는, 비밀키를 기준 템플릿과 결합하는 단계, 그리고 질의 템플릿을 이용하여 비밀키를 복구하는 단계를 포함할 수 있다.

[0014] 상기 인증 방법에서 비밀키를 기준 템플릿과 결합하는 단계는, 기준 템플릿의 기준 엔트리를 복수의 볼트(vault)에 할당하는 단계, 그리고 기준 엔트리가 복수의 볼트 내에서 할당된 위치를 나타내는 위치 인덱스를, 비밀키에 기반하여 결정된 다항식의 미지수 x에 입력하여, 기준 엔트리의 위치 인덱스에 대응하는 출력 엔트리를 결정하는 단계를 포함할 수 있다.

[0015] 상기 인증 방법에서 비밀키를 기준 템플릿과 결합하는 단계는, 복수의 채프 엔트리를 복수의 볼트에서 기준 엔트리가 할당되지 않은 셀에 할당하는 단계, 채프 엔트리가 복수의 볼트 내에서 할당된 위치를 나타내는 위치 인덱스를, 다항식의 미지수 x에 입력하여, 채프 엔트리의 위치 인덱스에 대응하는 채프 출력 엔트리를 결정하는 단계, 그리고 기준 엔트리와 출력 엔트리의 세트 및 채프 엔트리와 채프 출력 엔트리의 세트를 헬퍼 데이터로서 함께 저장하는 단계를 더 포함할 수 있다.

[0016] 상기 인증 방법에서 질의 템플릿을 이용하여 비밀키를 복구하는 단계는, 복수의 볼트에 할당된 엔트리 중, 질의 템플릿의 질의 엔트리와 동일한 엔트리의 동일 인덱스를 탐색하는 단계, 질의 엔트리와 동일한 엔트리가 존재하면, 헬퍼 데이터로부터 동일 인덱스에 대응하는 출력 엔트리를 결정하는 단계, 그리고 동일 인덱스 및 출력 엔트리의 순서쌍을 바탕으로 다항식을 결정하는 단계를 포함할 수 있다.

[0017] 상기 인증 방법에서 질의 템플릿을 이용하여 비밀키를 복구하는 단계는, 동일 인덱스 및 출력 엔트리의 순서쌍을 바탕으로 결정된 다항식의 계수를 입력으로 하는 해시 함수의 결과에 기반하여 계수를 비밀키로 결정하는 단계를 더 포함할 수 있다.

[0018] 상기 인증 방법에서 복수의 볼트는 각각 적어도 하나의 미니 볼트를 포함하고, 적어도 하나의 미니 볼트는 기준 엔트리가 할당된 하나의 셀 및 복수의 채프 엔트리가 할당된 복수의 셀을 포함할 수 있다.

[0019] 다른 실시예에 따르면, 사용자의 생체 정보를 이용하여 사용자를 인증하는 장치가 제공된다. 상기 인증 장치는, 프로세서, 메모리, 그리고 생체 인식 센서를 포함하고, 프로세서는 메모리에 저장된 프로그램을 실행하여, 생체 인식 센서를 이용하여 획득된 사용자의 제1 생체 정보로부터 제1 특징 벡터를 생성하고, 제1 특징 벡터와 복수의 의사 난수 행렬을 각각 곱하는 단계, 제1특징 벡터 및 복수의 의사 난수 행렬 간의 행렬곱의 결과 벡터의 원소 중, 최대 값을 갖는 원소의 인덱스를 바탕으로 질의 템플릿을 생성하는 단계, 그리고 저장된 기준 템플릿 및 질의 템플릿을 비교하여 인증을 수행하는 단계를 수행한다.

[0020] 상기 인증 장치에서 프로세서는 프로그램을 실행하여, 생체 인식 센서를 이용하여 제1 생체 정보 보다 이전에 획득된, 사용자의 제2 생체 정보로부터 제2 특징 벡터를 생성하고, 제2 특징 벡터와 복수의 의사 난수 행렬을 각각 곱하는 단계, 그리고 제2 특징 벡터 및 복수의 의사 난수 행렬 간의 행렬곱의 결과 벡터의 원소 중, 최대 값을 갖는 원소의 인덱스를 바탕으로 기준 템플릿을 생성하고, 기준 템플릿을 저장하는 단계를 더 수행할 수 있다.

[0021] 상기 인증 장치에서 프로세서는 인증을 수행하는 단계를 수행할 때, 질의 템플릿과 기준 템플릿의 차이가 0인 원소가 미리 설정된 개수 이상이면, 질의 템플릿의 사용자를 기준 템플릿의 사용자와 동일하다고 판정하는 단계를 수행할 수 있다.

[0022] 상기 인증 장치에서 기준 템플릿 및 질의 템플릿은, 결과 벡터의 원소 중 최대 값을 갖는 원소의 인덱스를 원소로서 포함할 수 있다.

[0023] 상기 인증 장치에서 프로세서는 인증을 수행하는 단계를 수행할 때, 비밀키를 기준 템플릿과 결합하는 단계, 그리고 질의 템플릿을 이용하여 비밀키를 복구하는 단계를 수행할 수 있다.

[0024] 상기 인증 장치에서 프로세서는 비밀키를 기준 템플릿과 결합하는 단계를 수행할 때, 기준 템플릿의 기준 엔트리를 복수의 볼트(vault)에 할당하는 단계, 그리고 기준 엔트리가 복수의 볼트 내에서 할당된 위치를 나타내는 위치 인덱스를, 비밀키에 기반하여 결정된 다항식의 미지수 x에 입력하여, 기준 엔트리의 위치 인덱스에 대응하는 출력 엔트리를 결정하는 단계를 수행할 수 있다.

[0025] 상기 인증 장치에서 프로세서는 비밀키를 기준 템플릿과 결합하는 단계를 수행할 때, 복수의 채프 엔트리를 복수의 볼트에서 기준 엔트리가 할당되지 않은 셀에 할당하는 단계, 채프 엔트리가 복수의 볼트 내에서 할당된 위치를 나타내는 위치 인덱스를, 다항식의 미지수 x에 입력하여, 채프 엔트리의 위치 인덱스에 대응하는 채프 출력 엔트리를 결정하는 단계, 그리고 기준 엔트리와 출력 엔트리의 세트 및 채프 엔트리와 채프 출력 엔트리의 세트를 헬퍼 데이터로서 함께 저장하는 단계를 더 수행할 수 있다.

[0026] 상기 인증 장치에서 프로세서는 질의 템플릿을 이용하여 비밀키를 복구하는 단계를 수행할 때, 복수의 볼트에 할당된 엔트리 중, 질의 템플릿의 질의 엔트리와 동일한 엔트리의 동일 인덱스를 탐색하는 단계, 질의 엔트리와 동일한 엔트리가 존재하면, 헬퍼 데이터로부터 동일 인덱스에 대응하는 출력 엔트리를 결정하는 단계, 그리고 동일 인덱스 및 출력 엔트리의 순서쌍을 바탕으로 다항식을 결정하는 단계를 수행할 수 있다.

[0027] 상기 인증 장치에서 프로세서는 질의 템플릿을 이용하여 비밀키를 복구하는 단계를 수행할 때, 동일 인덱스 및 출력 엔트리의 순서쌍을 바탕으로 결정된 다항식의 계수를 입력으로 하는 해시 함수의 결과에 기반하여 계수를 비밀키로 결정하는 단계를 더 수행할 수 있다.

[0028] 상기 인증 장치에서 복수의 볼트는 각각 적어도 하나의 미니 볼트를 포함하고, 적어도 하나의 미니 볼트는 기준 엔트리가 할당된 하나의 셀 및 복수의 채프 엔트리가 할당된 복수의 셀을 포함할 수 있다.

발명의 효과

[0029] 바이오메트릭 특징 벡터와 난수 행렬의 행렬곱에서 최대값을 갖는 원소의 인덱스를 이용하여 인증을 위한 바이오메트릭 템플릿을 생성함으로써, 바이오메트릭의 미약하고 미묘한 변화에도 성공적으로 사용자를 인증해낼 수 있다. 또한, 바이오메트릭 템플릿과 비밀키의 결합을 통해 암호 시스템의 개인키, 공개키 등의 보안에도 바이오메트릭의 특징이 활용될 수 있다.

도면의 간단한 설명

[0030] 도 1은 한 실시예에 따른 인증 장치를 나타낸 블록도이다.

도 2는 한 실시예에 따른 바이오메트릭 템플릿을 이용한 인증 방법을 나타낸 개념도이다.

도 3은 한 실시예에 따른 바이오메트릭 템플릿을 이용한 인증 방법의 흐름도이다.

도 4는 다른 실시예에 따른 바이오메트릭 템플릿을 이용한 인증 방법을 나타낸 개념도이다.

도 5는 다른 실시예에 따른 바이오메트릭 템플릿을 이용한 인증 방법의 흐름도이다.

도 6은 다른 실시예에 따른 인증 장치를 나타낸 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0031] 아래에서는 첨부한 도면을 참고로 하여 본 기재의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 기재는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 기재를 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0032] 도 1은 한 실시예에 따른 인증 장치를 나타낸 블록도이다.

[0033] 도 1을 참조하면, 한 실시예에 따른 인증 장치(100)는, 프로세서(110), 메모리(120), 그리고 바이오메트릭 센서(130)를 포함한다. 한 실시예에 따른 인증 장치(100)는 저장 장치 또는 디스플레이(미도시)를 더 포함할 수 있고, 이때 저장 장치는 메모리(120)에 포함될 수 있다. 또는 한 실시예에 따른 인증 장치(100)는 유선/무선 네트워크에 접속하기 위한 통신 유닛(140)을 더 포함할 수 있다.

[0034] 프로세서(110)는 본 기재의 실시예에서 제안한 기능, 과정, 또는 방법을 구현할 수 있다. 메모리(120)는 프로세서(110)와 연결되어 프로세서(110)를 구동하기 위한 다양한 정보 또는 프로세서(110)에 의해 실행되는 적어도 하나의 프로그램을 저장할 수 있다. 또한 메모리(120)는 바이오메트릭 센서(130)를 통해 입력된 바이오메트릭 정보를 저장할 수 있다. 프로세서(110)는 메모리(120)에 저장된 바이오메트릭 정보를 사용하여 바이오메트릭 템플릿을 생성할 수 있다.

[0035] 메모리(120)는 프로세서의 내부 또는 외부에 위치할 수 있고, 메모리(120)는 이미 알려진 다양한 수단을 통해 프로세서와 연결될 수 있다. 메모리(120)는 다양한 형태의 휘발성 또는 비휘발성 저장 매체이다. 메모리(120)는 하드 디스크, RAM, ROM, 플래시 메모리 등을 포함할 수 있다.

[0036] 또한, 한 실시예에 따른 인증 장치(100)는 키패드, 키보드, 마우스, 또는 포인팅 장치와 같은 입력 장치를 포함할 수 있다. 인증 장치(100)에 포함되는 디스플레이는 터치스크린으로 구현될 수 있고, 이때 디스플레이는 가상 키패드를 포함할 수 있다. 일반적으로, 한 실시예에 따른 인증 장치(100)는 단일 독립형 PC, 또는 다수의 PC에 구현되거나, 또는 단말, 이동 장치 등과 연결된 서버에 구현될 수 있다.

[0037] 도 2는 한 실시예에 따른 바이오메트릭 템플릿을 이용한 인증 방법을 나타낸 개념도이고, 도 3은 한 실시예에 따른 바이오메트릭 템플릿을 이용한 인증 방법의 흐름도이다.

[0038] 한 실시예에 따른 바이오메트릭 템플릿에는 임의의 길이를 갖는 생체 특징이 사용될 수 있다. 또는, 홍채, 지문, 또는 안면의 바이오메트릭 결과가 바이오메트릭 템플릿으로서 사용될 수 있고, 각 바이오메트릭 결과의 조합이 사용될 수도 있다. 고차원의 바이오메트릭 로-데이터(raw data)는 특징 변환(feature transformation)에 따라서 고정 길이의 특징 벡터로 변환된다. 본 기재에서 특징 벡터는 X 또는 Y로 표현된다. 이 표현은 기준(reference) 바이오메트릭 X 또는 질의(query) 바이오메트릭 Y로 사용될 수 있다. 기준 바이오메트릭 X는 각종 인증을 수행하기 위한 기준으로서 등록되는 기준 템플릿 T를 생성하기 위한 바이오메트릭이고, 질의 바이오메트릭 Y는 각종 인증의 시점에 생성된, 기준 템플릿 T와의 비교를 통해 각종 인증을 수행하기 위한 바이오메트릭이다.

[0039] 한 실시예에 따르면, 먼저 토큰화된 의사 난수(pseudo random number, PRN) 행렬 w 및 기준 바이오메트릭 X(또는 질의 바이오메트릭 Y)의 연산을 바탕으로 바이오메트릭 템플릿 T가 생성된다. 이때, PRN 행렬 w의 원소는 가우시안 분포 N(0, 1)에 따라서 분포되어 있을 수 있다. 도 2를 참조하면, PRN 행렬 w 및 기준 바이오메트릭 X(또는 질의 바이오메트릭 Y)에 대해서 행렬곱 연산이 수행되고, 이후 행렬곱 연산의 결과로부터 기준 바이오메트릭 템플릿 T(또는 질의 바이오메트릭 템플릿 T')이 생성된다.

[0040] 한 실시예에 따르면, PRN 행렬 w는 USB 토큰 또는 스마트 카드 등과 같은 임의의 PRN 생성 수단에 의해 생성될 수 있다. 또는 특정 응용 프로그램에서, w는 USB 토큰 또는 스마트 카드의 마이크로 프로세서에 저장된 시드(seed)에 기반하여 임의의 PRN 생성 수단에 의해 계산된다. 이때 시드는 등록하는 동안의 다른 사용자들 사이에서는 동일할 수 있지만, 사용자 및 응용 프로그램마다 다를 수 있다. 다른 실시예에 따르면, 애드혹(ad-hoc) 방식에 따르는 ANSI X9.17 생성기, 또는 FIPS 186 생성기와 같은 PRN 생성 장치와, CSPBG(cryptographically secure pseudo random generator)-RSA 의사 랜덤비트 생성기, 미컬리-쉬노르(Micali-Schnorr) 의사 랜덤비트 생성기, 또는 블럼-블럼-셔브(Blum-Blum-Shub) 의사 랜덤비트 생성기와 같은 고도로 보안된 방식 등 이미 알려진 의사 난수/랜덤비트 생성 장치 또는 알고리즘이 사용될 수 있다. 그리고, 바이오메트릭 템플릿 T를 생성하기 위한 처리 단계는, 최종 템플릿이 저장되기 전에, 컴퓨터 시스템에 대한 액세스를 허용하기 전에 비교에 사용되기 위해서 반복적으로 수행된다. PRN은 등록 동안 기록된 사용자들에 대해서는 동일하고, 다른 사용자 및 다른 애플리케이션 사이에서는 다를 수 있다.

[0041] 한 실시예에 따르면 기준 바이오메트릭 X는 수학식 1과 같이 정의될 수 있다.

수학식 1

[0042] $$X \in \mathbb{R}^d$$

[0043] 수학식 1에서, d는 특징 벡터의 차원을 나타낸다. 그리고, PRN 생성 장치에 의해 생성되는 PRN 행렬 w^i는 아래 수학식 2과 같다.

수학식 2

[0044] $$\{w^i \in \mathbb{R}^d | i = 1 \ldots, m\}$$

[0045] 도 2를 참조하면, 특징 벡터 X는 5×1 벡터이고, w^i는 5×5 행렬이다. 특징 벡터 X 및 PRN 행렬 w에 대해 행렬 곱 연산이 수행(S310)되면, 하나의 PRN 행렬 w^i 마다 t_i가 도출된다. t_i는 아래 수학식 3과 같이 표현될 수 있다.

수학식 3

[0046] $$t_i = \text{argmax}\langle w^i, X\rangle \text{ where } i = 1 \ldots, m$$

[0047] 하나의 t_i는 바이오메트릭 템플릿 T를 구성하는 하나의 원소이다. 한 실시예에 따르면, 특징 벡터 X 및 PRN 행렬 w에 대한 행렬 곱 연산의 결과에서, 최대 값을 갖는 원소의 인덱스가 바이오메트릭 템플릿 T의 원소 t_1로 결정된다(S320).

[0048] 도 2를 참조하면, 특징 벡터 X 및 PRN 행렬 w_1의 행렬곱 연산의 결과는 {-1.44, 1.56, 0.45, 0.60, -1.17}이고, 최대값인 1.56의 인덱스 2가 바이오메트릭 템플릿 T의 첫 번째 원소인 t_1로 결정된다. 이때, t_1로서 2가 선택될 때 크기 3인 윈도우가 적용되었다. 한 실시예에 따르면 특징 벡터 X의 길이가 상대적으로 길 때, 행렬 곱 연산 결과로부터 t_i를 신속하게 결정하기 위해서 윈도우가 사용될 수 있고, 이때 윈도우의 크기는 특징 벡터 X의 길이에 따라서 결정될 수 있다. 바이오메트릭 템플릿 T의 마지막 원소인 t_m이 2인 것은, 행렬 곱 연산 결과의 최대값은 0.60이지만, 크기 3인 윈도우 내의 최대값은 인덱스 2의 -1.08이기 때문이다.

[0049] 이후, 특징 벡터 X와 m개의 PRN 행렬의 행렬 곱 연산을 바탕으로 바이오메트릭 템플릿 T가 생성되고(S330), 수학식 4는 생성된 바이오메트릭 템플릿 T를 나타낸다.

수학식 4

[0050] $$T = [t_i \in [1, q] | i = 1, \ldots, m]$$

[0051] 이후, 바이오메트릭 템플릿 T는 등록 과정 동안 중앙의 데이터베이스 또는 외부 토큰 등에 저장될 수 있다(S340).

[0052] 한편, 질의 바이오메트릭 템플릿 T'도 바이오메트릭 템플릿 T와 동일한 방식으로 생성된다(S350). 즉, 인증의 시점에 사용자의 바이오메트릭으로부터 생성된 특징 벡터 X'와 PRN 행렬 w에 대해서 행렬 곱 연산이 수행되고, 행렬 곱 연산의 수행 결과에서 최대값을 갖는 원소의 인덱스가 질의 바이오메트릭 템플릿 T'의 원소로서 결정될 수 있다.

[0053] 이후, 인증 과정에서, 질의 바이오메트릭 템플릿 T'는 기준 바이오메트릭 템플릿 T와 비교된다(S360). 이때, 질의 바이오메트릭 템플릿 T' 및 기준 바이오메트릭 템플릿 T의 비교는, 둘 간의 원소 간 차이를 카운트하는 방식이 사용될 수 있다. 예를 들어, 템플릿 T' 및 템플릿 T의 원소 간 차이가 0인 원소가 미리 설정된 개수 이상이 되면, 질의 바이오메트릭 템플릿 T'의 사용자가 기준 바이오메트릭 템플릿 T의 사용자와 동일하다고 판정될 수 있다.

[0054] 위에서 설명한 바와 같이, 한 실시예에 따르면, 바이오메트릭 특징 벡터와 난수 행렬의 행렬곱에서 최대값을 갖는 원소의 인덱스를 이용하여 인증을 위한 바이오메트릭 템플릿을 생성함으로써, 바이오메트릭의 미약하고 미묘한 변화에도 성공적으로 사용자를 인증해낼 수 있다.

[0055] 소위 '도난 당한 토큰 시나리오'에서, 도둑이 피해자 A의 의사 난수를 훔쳐서 A로 가장하여 인증을 시도할 수 있다. 이 상황(도난 당한 토큰 시나리오)이 발생하면, 한 실시예에 따른 생체 인식 시스템이 적용되지 않은 시스템의 성능이 상당히 현저하게 저하될 수 있다. 하지만, 한 실시예에 따른 인증 장치에 의해 생성된 바이오메트릭 템플릿을 사용하면, 도난 당한 토큰 시나리오에서도 사용자 인증 성능은 크게 영향을 받지 않는다

[0056] 한 실시예에 따르면, 입력된 바이오메트릭 데이터는, 토큰 또는 중앙 데이터베이스에 저장된 난수를 사용하여

바이오메트릭 템플릿으로 변환된다. 이후, 미리 저장된 바이오메트릭 템플릿과 인증시 생성된 바이오메트릭 템플릿 간의 비교를 통해 두 템플릿의 매치의 근접성이 판단되고, 매치의 근접성의 판단 결과에 따라서 사용자의 인증 결과가 출력될 수 있다. 또는 다른 실시예에 따르면, 템플릿은 등록 중에 오프라인(offline) 토큰에 저장될 수 있고, 오프라인 토큰에 저장된 템플릿이 사용자 인증을 위한 기준으로 사용될 수 있다. 템플릿을 저장한 토큰이 분실되거나 도난 당하더라도, 템플릿은 도 2에서 설명된 방법을 통해 교체될 수 있다.

[0057] 표 1은 한 실시예에 따른 바이오메트릭 템플릿을 이용한 인증 시스템의 성능을 평가한 표를 나타낸다.

표 1

[0058]

방법	FGC2002			FVC2004		
	DB1	DB2	DB3	DB1	DB2	DB3
본 발명이 적용되지 않은 EER 성능						
	0.20%	0.19%	2.30%	4.70%	3.13%	2.80%
본 발명이 적용된 EER 성능						
도난 당한 토큰 케이스	0.22%	0.47%	3.07%	4.74%	4.1%	3.99%
원본 토큰 케이스	0.16%	0.45%	2.51%	1.15%	2.36%	2.70%

[0060] 한 실시예에 따른 인증 시스템의 성능을 평가하기 위해서 2개의 지문 데이터베이스(FVC2002 및 FVC2004)가 사용되었다. FVC2002와 FVC2004 모두 4개의 지문 데이터베이스를 제공했고, 이중 DB1, DB2, 및 DB3는 다양한 센서, 저비용, 고품질, 광학, 및 용량성 센서에 의해 수집된 데이터를 포함하고, DB4는 합성된 생성 이미지를 포함한다. FVC2002 및 FVC 2004의 각 데이터 세트는, 100개의 다른 손가락 마다 8개의 지문을 포함하여 총 800개의 지문 데이터를 포함한다. 그리고 성능 평가를 위해서 FAR 테스트 및 FRR 테스트가 수행되었다. FAR 테스트 및 FRR 테스트는 아래 수학식 5와 같다.

수학식 5

[0061]

$$\text{FAR} = \frac{\text{접속된 도둑의 요청의 개수}}{\text{도둑의 요청의 총 개수}}$$

$$\text{FRR} = \frac{\text{거절된 진짜 요청의 개수}}{\text{진짜 요청의 총 개수}}$$

[0062] 그리고 EER은 FAR 및 FRR의 평균이다.

수학식 6

[0063]

$$\text{EER} = \frac{\text{FAR} + \text{FRR}}{2}$$

[0064] 도 4는 다른 실시예에 따른 바이오메트릭 템플릿을 이용한 인증 방법을 나타낸 개념도이고, 도 5는 다른 실시예에 따른 바이오메트릭 템플릿을 이용한 인증 방법의 흐름도이다.

[0065] 다른 실시예에 따르면, 바이오메트릭 템플릿 T는, 암호 및 암호화 애플리케이션과 관련된 사용을 위해서 비밀키(secret key)과 결합되고, 인증 시점의 바이오메트릭 템플릿 T'는 비밀키를 복구하기 위해 사용될 수 있다. 한 실시예에 따른 비밀키는, 대칭 암호 시스템의 개인키, 비대칭 암호 시스템의 공개키, 디지털 서명의 메시지 해시, 트랜잭션 일회용 패드 등을 포함할 수 있다. 다른 실시예는 샤미르(Shamir)의 비밀 공유 방식에 기초할 수 있다. 샤미르의 비밀 공유 방식은 비밀 결합(secret binding) 및 비밀 복구(secret retrieval)의 두 스테이지를 포함한다. 비밀 결합 스테이지에서, 비밀키는 차수 k의 유한 필드 다항식 P(x)의 계수에 인코딩되고, 바이오메트릭 템플릿과 결합된다. 원본 비밀 공유(genuine shares)는 바이오메트릭 세트 내의 원소인 x로서 정의되는, 포인트 (x, P(x))로 표현되며, 일괄하여 원소의 개수가 t인 원본 집합(genuine set) G로 알려진다. 이후, 함수

P(x) 위에 놓여 있지 않은 채프 포인트(chaff point)의 집합 C((a, b)∈C)가 무작위로 생성된다. G와 C의 합집합(union set)은 볼트(vault) V를 형성한다. 비밀 복구 스테이지에서 비밀키는, 질의 바이오메트릭 세트를 제시하여 t개의 진짜 포인트 중 가능한 k+1을 식별한 이후에, 다항식 재구성(polynomial reconstruction)을 통해 계수를 알아냄으로써 복원될 수 있다.

[0066] 먼저, 비밀 결합 스테이지를 설명한다.

[0067] 바이오메트릭 특징 벡터 X로부터 생성되는 바이오메트릭 템플릿 T_X이 등록되고, 등록된 바이오메트릭 템플릿 T_X의 엔트리 t_{Xi}는 아래 수학식 7과 같이 표현될 수 있다.

수학식 7

[0068] $$[t_{Xi} \in [1, q] | \ i = 1, \ldots, m]$$

[0069] 그리고 t_{Xi}는 아래 수학식 8을 통해 t'_{Xi}로 변환될 수 있다.

수학식 8

[0070] $$t'_{Xi} = (t_{Xi} + r_i) \bmod N \text{ where } r_i \in [1, N]$$

[0071] 수학식 8에서 r_i는 무작위로 선택된 정수(random integer)이다. 그리고 N>>q이면 아래 수학식 9가 도출될 수 있다.

수학식 9

[0072] $$T'_X = [t'_{Xi} \in [0, N-1] | \ i = 1, \ldots, m]$$

[0073] 위 수학식 7 내지 9의 과정에 따라서, 각 엔트리의 범위가 q에서 매우 큰 수인 N으로 확장되고, T'_X내의 엔트리의 충돌 확률이 효과적으로 감소될 수 있다. 이렇게 함으로써, 범위 [0,N-1] 내의 더 많은 채프 엔트리가 비밀 결합 단계 동안 추가되어, 비밀 복구 단계에서의 채프와 원본 간의 충돌을 최소화할 수 있다. 한 실시예에 따르면 비밀 결합 스테이지는 다음 두 단계를 포함한다.

[0074] 단계 1: 기준 바이오메트릭 템플릿 T'_x의 기준 엔트리 t'_{Xi}가 m개의 슬롯에 포함된 셀에 무작위로 할당된다(S510). 이때 각 슬롯은 v개의 셀을 포함하고, 기본 미니 볼트(primary mini vault)라고 한다. 각 기본 미니 볼트는 볼트 내에 위치한다. 기본 미니 볼트 v_i는 수학식 10과 같이 표현된다.

수학식 10

[0075] $$\{\mathbf{v}_i \ | i = 1, \ldots, m\}$$

[0076] 도 4에서, 엔트리 T'_{1X}인 (5, 6, 1)이 각각 첫 번째 볼트 내의 기본 미니 볼트의 두 번째 셀, 두 번째 볼트 내의 기본 미니 볼트의 첫 번째 셀, 및 세 번째 볼트 내의 기본 미니 볼트의 네 번째 셀에 할당된다.

[0077] 다음 엔트리 t'_{Xi}가 할당되지 않은 슬롯 내의 v-1개의 셀에 채프 엔트리가 할당된다(S515). 이때, 수학식 11은 채프 엔트리를 나타낸다.

수학식 11

[0078] $$\{c_{j(i)} \in [0, N-1] | j = 1, \ldots, v-1, i = 1, \ldots, m\}$$

[0079] 그리고 b개의 추가 미니 볼트(added mini vault) $\mathbf{v}_{ib}$에, 동일한 바이오메트릭 특징 벡터로부터 생성된 다른 템플릿 T'_X의 엔트리가 할당되고(S520), 추가 미니 볼트에도 채프 엔트리가 할당된다(S525). 이는 다른 토큰화된 PRN 세트를 사용하여 수행될 수 있다. 각각의 추가 미니 볼트 $\mathbf{v}_{ib}$에 대해서, 엔트리 t'_{Xi}의 배치는 기본 미니 볼트에 따른다. 즉, 모든 엔트리 t'_X의 위치는 모든 미니 볼트에서 동일하다. 각 엔트리 t'_{Xi} 및 채프 엔트리 cj(i)가 모든 미니 볼트 $\mathbf{v}_{ib}$에서 무작위로 균일하게(randomly and uniformly) 배치되어 있음을 보장하기 위해 셔플(shuffle) 되기 때문에, 볼트 또는 미니 볼트 내에서 채프 엔트리와 엔트리 t'_{Xi}가 구별되기 어렵다.

[0080] 도 4를 참조하면, 엔트리 T'_{2X}인 (2, 3, 5)는 각각 첫 번째 볼트 내의 추가 미리 볼트의 두 번째 셀, 두 번째 볼트 내의 추가 미니 볼트의 첫 번째 셀, 및 세 번째 볼트 내의 추가 미니 볼트의 네 번째 셀에 할당된다. 즉, 각 추가 미니 볼트 내에서 엔트리 T'_{2X}가 할당된 셀의 번호는 기본 미니 볼트와 동일하다.

[0081] 단계 2: v개의 슬롯을 포함하는 미니 볼트의 집합의 위치 인덱스를 **E**라 하고, 아래 수학식 12와 같이 정의한다.

수학식 12

[0082] $$\mathbf{E} = \{1, \ldots, mv\}$$

[0083] 즉, 위치 인덱스는 엔트리 t'_{Xi}가 볼트 내에서 할당된 위치를 나타낼 수 있다. 도 4를 참조하면, 하나의 엔트리에 대해, 볼트의 개수 m은 3이고, 각 볼트에 포함된 미니 폴트가 포함하는 셀의 개수 v는 4이므로, 위치 인덱스 **E**는 1 내지 12 중 하나이다. 엔트리 t'_{Xi} 및 채프 엔트리의 셔플링 프로세스에서, 엔트리 t'_{Xi}의 위치는 **A**(**A**⊂**E**)로 결정된다. 도 4에서 엔트리 t'_{Xi}의 위치 **A**는 (2, 5, 12)이다. 이때, t'_{Xi}의 위치 인덱스가 차수 k의 유한 필드 다항식 *P*의 미지수 x로서 다항식 *P*에 입력되고(S530), 기준 엔트리에 대응하는 출력 엔트리 y가 결정된다. 여기서 다항식 *P*의 계수가 다항식 *P*에 인코딩된 비밀키이다. 도 4를 참조하면, 2차 다항식 P에 인코딩된 비밀키, 즉, 2차 다항식의 각 항의 계수는 (53, 155, 255)이다. 따라서, t'_{Xi}의 위치 인덱스인 $idxt'_{Xi}$($idxt'_{Xi}$∈**A**)는 P에 내재되고(embeded), 아래 수학식 13이 성립한다.

수학식 13

[0084] $$[y_i = P(idxt'_{Xi}) \bmod (Q) \in \mathbb{Z}_Q | i = 1, \ldots, m]$$

[0085] 수학식 13에서 Q는 상대적으로 큰 소수(prime number)이고, 한 실시예에서 Q는 89989이다. 기준 엔트리 t'_{Xi} 및 그에 대응하는 임베디드된 엔트리 y_i의 쌍은 원본 세트 $\mathbf{G}_b$로 결정되고(S535), 아래 수학식 14와 같다.

수학식 14

[0086] $$\mathbf{G}_b = [(idxt'_{Xi}, y_i) | i = 1, \ldots, m]$$

[0087] 이때, 단계 1에서 복수의 미니 볼트가 도입되었지만, 모든 미니 폴트에 대한 t'_{Xi}의 위치는 동일하므로, 하나의 $\mathbf{G}_b$만이 존재한다. 즉, 도 4에서 다항식 *P*(y=53x^2+155x+255)에 따른 $\mathbf{G}_b$는 [(2,777) (5,2355) (12,9747)]이다. 동일한 절차가 채프 엔트리 $c_{j(i)}$에 대해서도 수행되고, 채프 엔트리에는 $y_{j(i)}$가 대응하며, 채프 엔트리 쌍 $\mathbf{c}_b$는 아

래 수학식 15와 같다(S540).

수학식 15

[0088] $$\mathbf{C}_b = \{(c_{j(i)}, y_{j(i)}) | \, y_{j(i)} \neq y_i, i = 1, \ldots, m, j = 1, \ldots, v-1\}$$

[0089] 한편, 보안 관련하여 대응하는 채프가 반복되지 않음을 보장하기 위해서 $Q(Q > m(v-1))$ 값이 제한된다. 원본과, 원본에 대응하는 채프의 합집합 $\mathbf{V}_b(\mathbf{V}_b=\mathbf{G}_b \cup \mathbf{C}_b)$이 헬퍼 데이터(Helper Data, HD)로서 저장된다(S545). 마지막으로 P는 SHA-1과 같은 표준 메시지 해시 함수를 통해 해시되고, P의 해시 결과 SHA(p)는 비밀 결합 스테이지에서 HD와 함께 저장된다.

[0090] 다음은 비밀 복구 스테이지를 설명한다.

[0091] 비밀 복구 스테이지에서 비밀키가 복구되기 위해서는, 질의 바이오메트릭 템플릿에 따른 엔트리 t'_{yi}에 대응하는 엔트리 쌍이 결정되어야 하고 결정된 엔트리 쌍으로부터 다항식 P가 다항식 P'로서 재구성 되어야 한다.

[0092] 먼저, b(b≥1)번째 질의 바이오메트릭 템플릿 T'_{bY_i}을 아래 수학식 16과 같이 정의한다.

수학식 16

[0093] $$T'_{bY_i} \in [1, q]^m$$

[0094] 그리고 비밀 결합 스테이지와 동일한 확장 연산(expansion operation)을 수학식 17과 같이 수행하여, 수학식 18을 산출한다.

수학식 17

[0095] $$t'_{bY_i} = (t_{bY_i} + r_i)$$

수학식 18

[0096] $$[t'_{bY_i} \in [0, N-1] | i = 1, \ldots, m\,] \subset \boldsymbol{T}'_{bY}$$

[0097] 단계 1: 각 미니 볼트 $\mathbf{v}_{bi}$에서 질의 템플릿 T'_y의 질의 엔트리 t'_{yi}와 t'_{xi}를 매칭할 때, t'_{xi}와 동일한 t'_{yi}의 인덱스를 탐색한다(S550). $\mathbf{v}_{bi}$내에 매치가 존재하면, HD를 통해서 결정된 출력 엔트리가 포함된 순서쌍을 포함하는 집합 B가 결정된다(S555). 도 4를 참조하면, 템플릿 T'_{1y}의 엔트리 중 첫 번째 엔트리 t'_{1y1}가 t'_{1X1}와 동일하고, 템플릿 T'_{2y}의 엔트리 중 첫 번째 엔트리 t'_{2y1}가 t'_{2x1}와 동일하므로, 인덱스 2에 대응하는 y_1(777)이 HD를 통해 결정될 수 있다. 또한, 템플릿 T'_{2y}의 엔트리 중 세 번째 엔트리 t'_{2y3}가 t'_{2x3}와 동일하므로, 인덱스 12에 대응하는 y_3(9747)이 HD를 통해 결정될 수 있다. 엔트리의 순서쌍을 포함하는 B는 아래 수학식 19과 같이 표현될 수 있다.

수학식 19

[0098] $$\mathbf{B} = [(x(t'_{bXi} = t'_{bYi}), y(t'_{bXi} = t'_{bYi})) | i = 1, \ldots, m]$$

[0099] 수학식 19에서 x 및 y는 각각 아래 수학식 20과 같다.

수학식 20

$$x \in \mathbf{E}$$

[0100] $$y \in \mathbb{Z}_Q$$

[0101] 도 4를 참조하면, T'_{1y}인 (5, 2 ,3) 및 T'_{2y}과 동일한 엔트리를 포함하는 셀의 인덱스 2 및 12가 결정된다.두 번째 볼트에는 두 개의 질의 엔트리 T'_{1y} 및 T'_{2y}에 불구하고 동일한 엔트리를 포함하는 셀이 존재하지 않는다. 따라서, 두 개의 질의 엔트리에 대응하는 B는 $\{(2,y_1),(12,y_3)\}$이고, 2개의 순서쌍을 갖는 B로부터 2차 다항식 P'가 특정될 수 없으므로, 두 개의 질의 엔트리 T'_{1y} 및 T'_{2y}를 이용한 인증은 실패하게 된다. 즉, 두 개의 질의 엔트리 T'_{1y} 및 T'_{2y}는 엔트리 T'_{1x} 및 T'_{2x}와 동일한 사용자로부터 생성된 것으로 판정될 수 없다.

[0102] 단계 2: B에 대해서, k차 다항식 P'가 B에 포함된 k+1개의 순서쌍으로부터 결정될 수 있다(S560). 이후, $SHA(P)=SHA(P')$이면 비밀키가 복구된다(S565). 즉, 두 개의 질의 엔트리 T'_{1y} 및 T'_{2y}로부터 세 개의 순서쌍을 포함하는 B가 결정되면($B=\{(2,y_1),(5,y_2),(12,y_3)\}$), B로부터 다항식 P'가 특정될 수 있고, $SHA(P)$와 동일한 결과를 갖는 $SHA(P')$를 얻을 수 있다. 이때, 다항식 P'의 계수가 비밀키이다.

[0103] 만약, 두 번째 볼트의 미니 볼트의 6번 셀, 7번 셀, 또는 8번 셀에 2 또는 6이 있다면, 채프 엔트리에 대응하는 채프 출력 엔트리가 결정될 수 있다. 즉, 질의 엔트리가 볼트 내의 셀에 할당된 숫자와 모두 동일하면, $B=\{(2,y_1),(6,y_2),(12,y_3)\}$, 또는 $B=\{(2,y_1),(7,y_2),(12,y_3)\}$, 또는 $B=\{(2,y_1),(8,y_2),(12,y_3)\}$가 결정될 수 있다. 이 경우 3개의 순서쌍을 갖는 B로부터 2차 다항식 P'가 재구성될 수는 있지만, $SHA(P)=SHA(P')$이 성립할 수 없으므로, 역시 비밀키가 복구될 수 없다.

[0104] 위에서 설명한 바와 같이 바이오메트릭 템플릿과 비밀키의 결합을 통해 암호 시스템의 개인키, 공개키 등의 보안에도 한 실시예에 따른 바이오메트릭 템플릿의 장점이 활용될 수 있다.

[0105] 한 실시예에 따른 인증 장치는 다양한 애플리케이션에 적용될 수 있다. 예를 들어, 컴퓨터화된 접속 제어 시설, 컴퓨터 시스템에 대한 접속, 암호화 응용 프로그램 등과 함께 사용될 수 있다. 이때, 한 실시예에 따른 인증 장치가 생체 인식 센서와 같은 입력 장치를 포함하는 경우, 사용자는 한 실시예에 따른 인증 장치가 다른 전형적인 컴퓨터 장치에 통합되어서, 자신의 생체 특성이 측정 또는 분석되고 있다는 것을 의식적으로 알지 못할 수 있다.

[0106] 도 6은 다른 실시예에 따른 인증 장치를 나타낸 블록도이다.

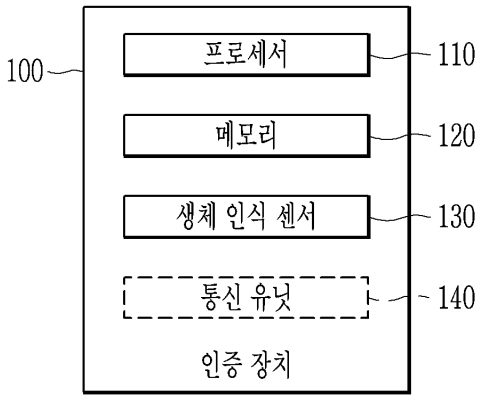
[0107] 한 실시예에 따른 인증 장치는, 컴퓨터 시스템, 예를 들어 컴퓨터 판독 가능 매체로 구현될 수 있다. 도 6을 참조하면, 컴퓨터 시스템(600)은, 버스(620)를 통해 통신하는 프로세서(610), 메모리(630), 사용자 인터페이스 입력 장치(660), 사용자 인터페이스 출력 장치(670), 및 저장 장치(680) 중 적어도 하나를 포함할 수 있다. 컴퓨터 시스템(600)은 또한 네트워크에 결합된 네트워크 인터페이스(690)를 포함할 수 있다. 프로세서(610)는 중앙처리 장치(central processing unit, CPU)이거나, 또는 메모리(630) 또는 저장 장치(680)에 저장된 명령을 실행하는 반도체 장치일 수 있다. 메모리(630) 및 저장 장치(680)는 다양한 형태의 휘발성 또는 비휘발성 저장 매체를 포함할 수 있다. 예를 들어, 메모리는 ROM(read only memory)(631) 및 RAM(random access memory)를 포함할 수 있다.

[0108] 따라서, 본 발명의 실시예는 컴퓨터에 구현된 방법으로서 구현되거나, 컴퓨터 실행 가능 명령이 저장된 비일시적 컴퓨터 판독 가능 매체로서 구현될 수 있다. 한 실시예에서, 프로세서에 의해 실행될 때, 컴퓨터 판독 가능 명령은 본 기재의 적어도 하나의 양상에 따른 방법을 수행할 수 있다.

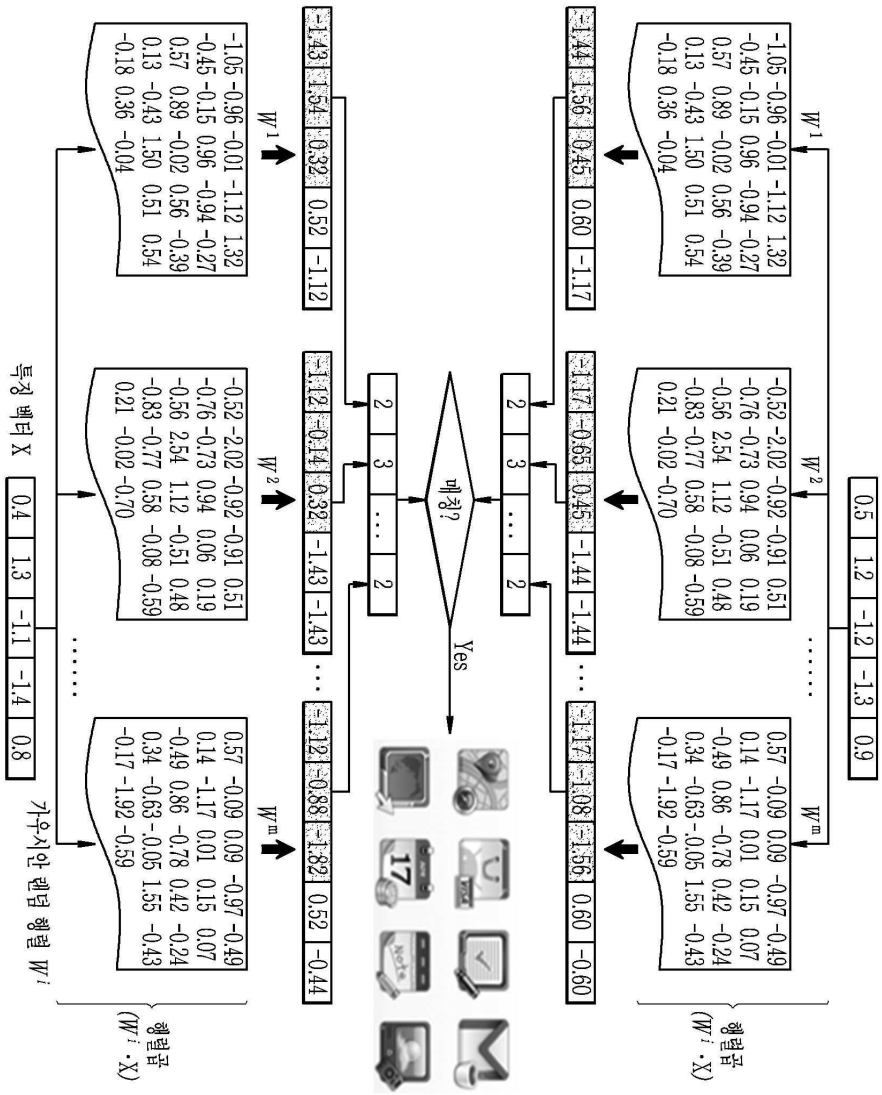
[0109] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면

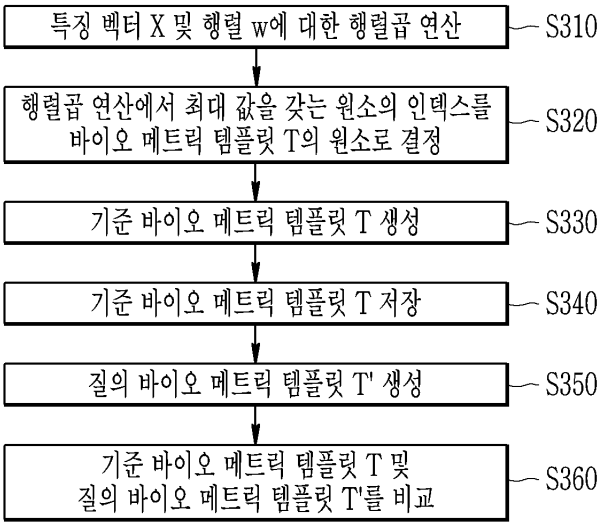
도면1


100
프로세서
110
메모리
120
생체 인식 센서
130
통신 유닛
140
인증 장치

도면2

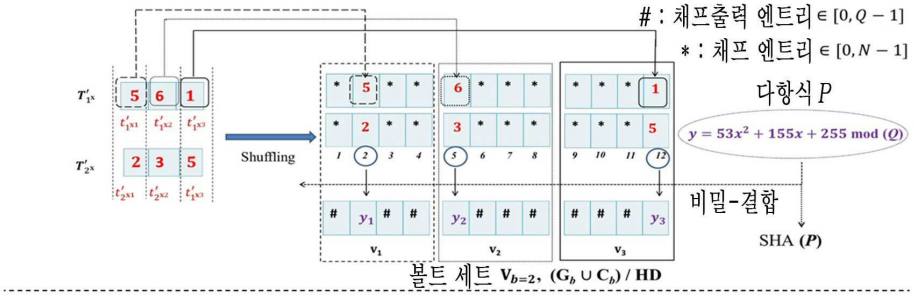

특징 벡터 X
0.4 1.3 -1.1 -1.4 0.8
가우시안 랜덤 행렬 W^i
W^1
W^2
W^m
행렬곱 $(W^i \cdot X)$
메칭?
Yes
No
0.5 1.2 -1.2 -1.3 0.9
2 3 ... 2

도면3

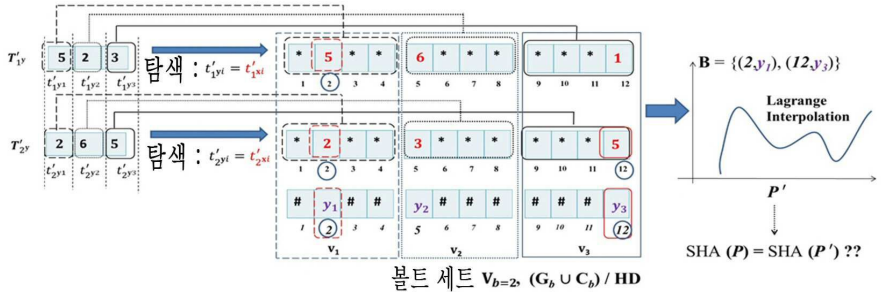


도면4

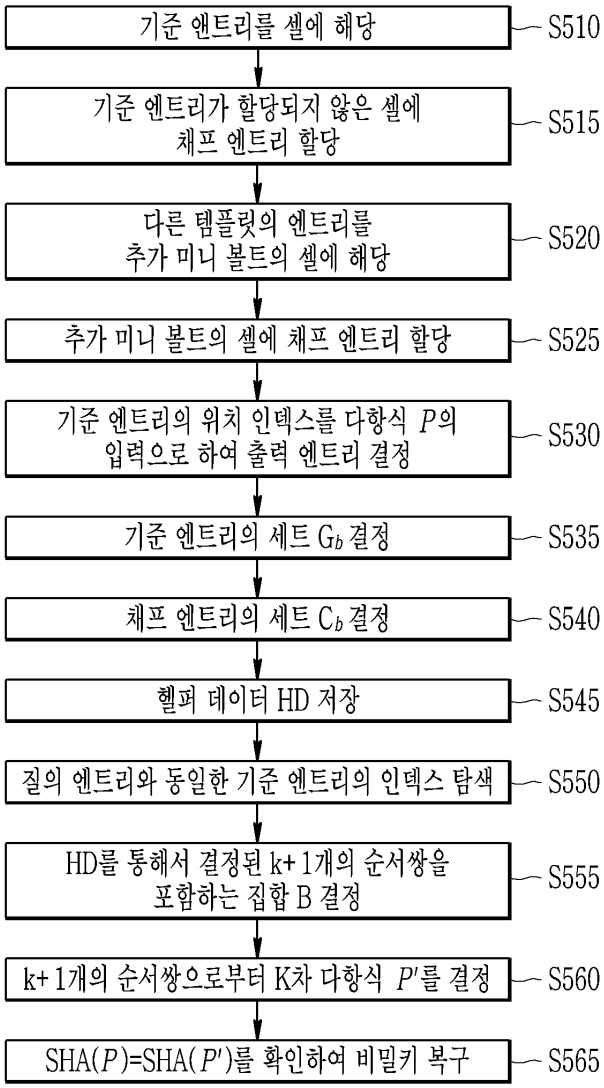
<비밀 결합 스테이지>



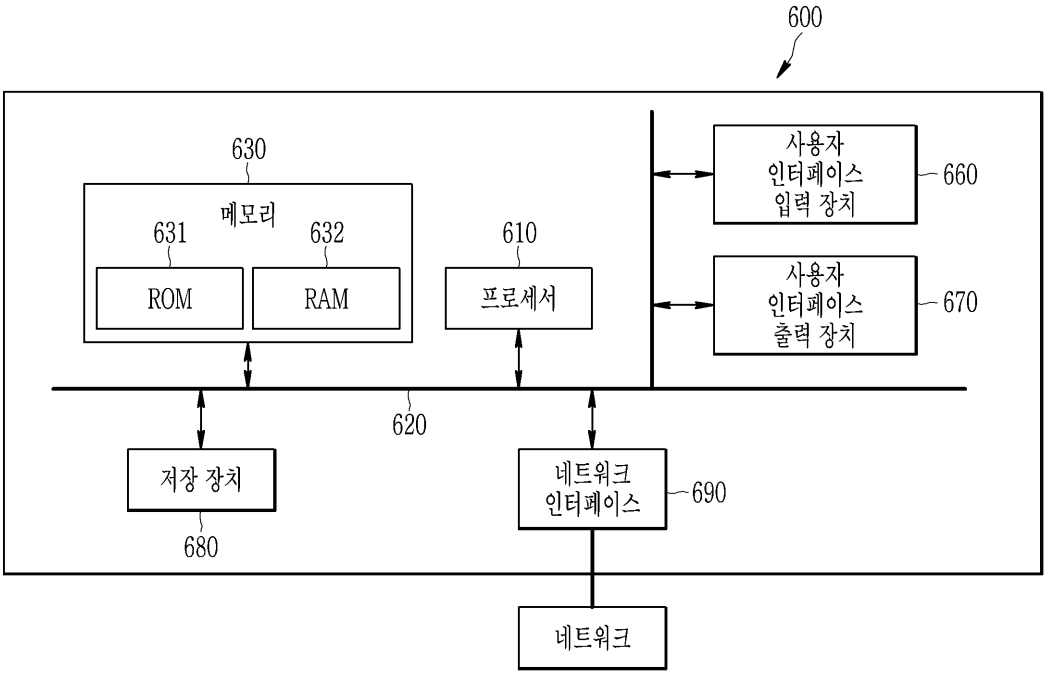
<비밀 결합 스테이지>



도면5


기준 앤트리를 셀에 해당
S510
기준 엔트리가 할당되지 않은 셀에 채프 엔트리 할당
S515
다른 템플릿의 엔트리를 추가 미니 볼트의 셀에 해당
S520
추가 미니 볼트의 셀에 채프 엔트리 할당
S525
기준 엔트리의 위치 인덱스를 다항식 P의 입력으로 하여 출력 엔트리 결정
S530
기준 엔트리의 세트 G_b 결정
S535
채프 엔트리의 세트 C_b 결정
S540
헬퍼 데이터 HD 저장
S545
질의 엔트리와 동일한 기준 엔트리의 인덱스 탐색
S550
HD를 통해서 결정된 k+1개의 순서쌍을 포함하는 집합 B 결정
S555
k+1개의 순서쌍으로부터 K차 다항식 P′를 결정
S560
SHA(P)=SHA(P′)를 확인하여 비밀키 복구
S565

도면6


600
630
메모리
631
ROM
632
RAM
610
프로세서
620
사용자
인터페이스
입력 장치
660
사용자
인터페이스
출력 장치
670
저장 장치
680
네트워크
인터페이스
690
네트워크