



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년04월05일
(11) 등록번호 10-1845192
(24) 등록일자 2018년03월28일

(51) 국제특허분류(Int. Cl.)
G06K 9/00 (2006.01) G06K 17/00 (2006.01)
(52) CPC특허분류
G06K 9/00087 (2013.01)
G06K 9/00067 (2013.01)
(21) 출원번호 10-2017-0023681
(22) 출원일자 2017년02월22일
심사청구일자 2017년02월22일
(56) 선행기술조사문헌
KR1020070078036 A*
JP2003178307 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대현
서울특별시 서초구 서초중앙로 200, 17동 901호(서초동, 삼풍아파트)
(74) 대리인
양성보

전체 청구항 수 : 총 6 항

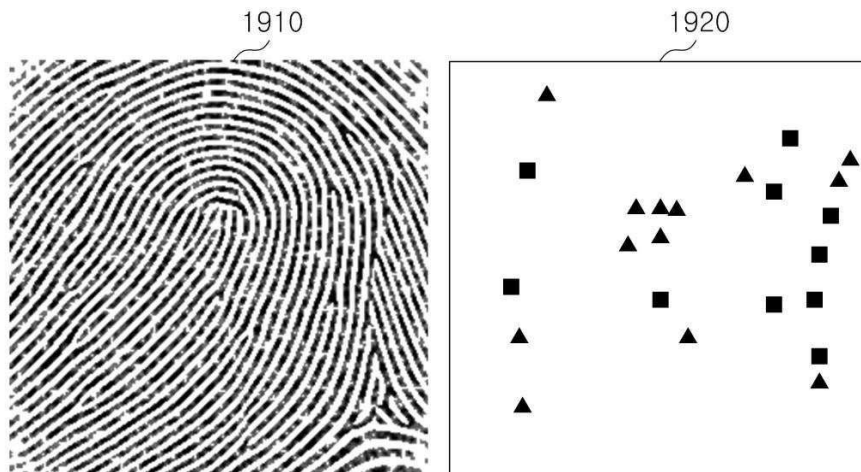
심사관 : 노용완

(54) 발명의 명칭 내적 연산 적용을 위한 지문 정보 변경 방법 및 시스템

(57) 요약

내적 연산 적용을 위한 지문 정보 변경 방법 및 시스템이 개시된다. 지문 정보 변경 방법은, 지문에 대한 특징점(minutiae points)의 타입별로 기설정된 서로 다른 표식을 관리하는 단계, 사용자의 지문 이미지로부터 특징점, 특징점의 타입 및 상기 특징점의 지오메트리 정보를 추출하는 단계 및 상기 추출된 특징점들에 대해, 특징점의 타입에 대응하는 표식을 특징점의 지오메트리 정보에 대응하는 위치에 포함하는 변환 이미지를 생성하는 단계를 포함할 수 있다.

대표도 - 도19



(52) CPC특허분류
G06K 2017/0093 (2013.01)

명세서

청구범위

청구항 1

지문 정보 변경 방법에 있어서,

지문에 대한 특징점(minutiae points)의 타입별로 기설정된 서로 다른 표식을 관리하는 단계;

TTP(Trust Third Party)의 비밀키 및 상기 TTP의 공개키를 생성하고, 상기 TTP의 공개키를 사용자 및 검증자에게 전달하는 단계;

상기 사용자의 지문 이미지로부터 특징점, 특징점의 타입 및 상기 특징점의 지오메트리 정보를 추출하는 단계;

상기 추출된 특징점들에 대해, 특징점의 타입에 대응하는 표식을 특징점의 지오메트리 정보에 대응하는 위치에 포함하는 변환 이미지를 생성하는 단계;

상기 생성된 변환 이미지로부터 상기 사용자의 바이오매트릭스 정보를 추출하는 단계;

상기 추출된 바이오매트릭스 정보를 이용한 학습을 통해 투영 행렬을 생성하는 단계; 및

상기 투영 행렬과 상기 바이오매트릭스 정보간의 내적에 기반하여 상기 사용자의 특징 정보를 추출하는 단계;

상기 투영 행렬 및 상기 TTP의 비밀키를 이용하여 검증자용 비밀키 및 검증자용 공개키를 생성하는 단계; 및

상기 검증자용 비밀키를 상기 검증자의 단말로 네트워크를 통해 전송하고, 상기 검증자용 공개키를 상기 사용자의 단말로 네트워크를 통해 전송하는 단계

를 포함하고,

상기 TTP의 공개키와 상기 검증자용 공개키 및 상기 사용자의 제1 바이오매트릭스 정보를 이용하여 상기 사용자의 단말에서 생성된 인증 정보가 네트워크를 통해 상기 검증자의 단말로 전송되고,

상기 검증자의 단말에서 상기 TTP의 공개키와 상기 검증자용 비밀키 및 상기 사용자의 단말로부터 전송된 인증 정보를 이용하여 상기 제1 바이오매트릭스 정보와 상기 투영 행렬간의 내적이 상기 제1 바이오매트릭스 정보에 대한 특징 정보로서 계산되는 것을 특징으로 하는 지문 정보 변경 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 지문에 대한 특징점의 타입은 끝점(ending point) 및 분기점(bifurcation)을 적어도 포함하고,

상기 기설정된 서로 다른 표식은 상기 끝점을 위한 제1 표식과 상기 분기점을 위한 제2 표식을 적어도 포함하는 것을 특징으로 하는 지문 정보 변경 방법.

청구항 4

제1항에 있어서,

상기 변환 이미지는 상기 특징점에 대해 배치된 표식만을 포함하는 것을 특징으로 하는 지문 정보 변경 방법.

청구항 5

제1항, 제3항 또는 제4항 중 어느 한 항의 방법을 컴퓨터에 실행시키기 위한 프로그램이 기록되어 있는 것을 특징으로 하는 컴퓨터에서 판독 가능한 기록매체.

청구항 6

지문 정보 변경 방법을 실행하기 위해 컴퓨터 장치로 구현되는 지문 정보 변경 시스템에 있어서,
 컴퓨터에서 판독 가능한 명령을 저장하는 메모리; 및
 상기 메모리에 저장된 명령을 실행하도록 구현되는 적어도 하나의 프로세서
 를 포함하고,
 상기 적어도 하나의 프로세서는,
 지문에 대한 특징점(minutiae points)의 타입별로 기설정된 서로 다른 표식을 관리하고,
 TTP(Trust Third Party)의 비밀키 및 상기 TTP의 공개키를 생성하고, 상기 TTP의 공개키를 사용자 및 검증자에
 게 전달하고,
 상기 사용자의 지문 이미지로부터 특징점, 특징점의 타입 및 상기 특징점의 지오메트리 정보를 추출하고,
 상기 추출된 특징점들에 대해, 특징점의 타입에 대응하는 표식을 특징점의 지오메트리 정보에 대응하는 위치에
 포함하는 변환 이미지를 생성하고,
 상기 생성된 변환 이미지로부터 상기 사용자의 바이오매트릭스 정보를 추출하고,
 상기 추출된 바이오매트릭스 정보를 이용한 학습을 통해 투영 행렬을 생성하고,
 상기 투영 행렬과 상기 바이오매트릭스 정보간의 내적에 기반하여 상기 사용자의 특징 정보를 추출하고,
 상기 투영 행렬 및 상기 TTP의 비밀키를 이용하여 검증자용 비밀키 및 검증자용 공개키를 생성하고,
 상기 검증자용 비밀키를 상기 검증자의 단말로 네트워크를 통해 전송하고, 상기 검증자용 공개키를 상기 사용자
 의 단말로 네트워크를 통해 전송하며,
 상기 TTP의 공개키와 상기 검증자용 공개키 및 상기 사용자의 제1 바이오매트릭스 정보를 이용하여 상기 사용자
 의 단말에서 생성된 인증 정보가 네트워크를 통해 상기 검증자의 단말로 전송되고,
 상기 검증자의 단말에서 상기 TTP의 공개키와 상기 검증자용 비밀키 및 상기 사용자의 단말로부터 전송된 인증
 정보를 이용하여 상기 제1 바이오매트릭스 정보와 상기 투영 행렬간의 내적이 상기 제1 바이오매트릭스 정보에
 대한 특징 정보로서 계산되는 것
 을 특징으로 하는 지문 정보 변경 시스템.

청구항 7

삭제

청구항 8

제6항에 있어서,
 상기 변환 이미지는 특징점에 대해 배치된 표식만을 포함하는 것을 특징으로 하는 지문 정보 변경 시스템.

발명의 설명

기술 분야

[0001] 아래의 설명은 내적 연산 적용을 위한 지문 정보 변경 방법 및 시스템, 그리고 컴퓨터와 결합되어 지문 정보 변경 방법을 컴퓨터에 실행시키기 위해 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램에 관한 것이다.

배경 기술

[0002] 바이오매트릭스는 생체 인식 기술에 관한 것으로, 망막, 지문, 음성, 얼굴 등 개인의 신체적 특성이나 혹은 개인의 행동적 특성을 추출하여 신원을 확인하거나 범죄자를 가려내는 등 개개인을 비교 또는 확인하는 기술이다. 예를 들어, 한국공개특허 제10-2004-0090473호는 정전 용량 검출 장치 및 그 구동 방법, 지문센서 및 바이오매

트릭스 인증 장치에 관한 것으로, 바이오메트릭스 정보로서 지문 정보를 이용하여 본인 인증을 행하는 기술에 대해 개시하고 있다.

- [0003] 이러한 바이오메트릭스의 정확도가 높아짐에 따라, 바이오메트릭스의 사용 범위가 점차 확장되고 있으나, 이러한 바이오메트릭스 정보로부터는 키를 추출할 수 없다는 한계가 있다. 바이오메트릭스 정보는 사용자의 지문이나 얼굴 등을 인식할 때마다 추출되는 정보가 매번 조금씩 달라진다. 예를 들어, 사용자의 얼굴을 촬영할 때의 조명의 밝기나 촬영 각도 등에 따라, 또는 지문을 인식하는 순간의 사용자 손가락의 압력 등에 따라 조금씩 다른 정보가 추출된다. 반면, 암호화나 전자 서명에 사용되는 키는 항상 정확한 값을 가져야 한다. 따라서, 바이오메트릭스는 입력된 정보와 기 저장된 정보간의 비교를 통한 개인의 인증 또는 비교의 분야로만 사용될 수 있을 뿐, 인증, 암호화 및/또는 전자 서명을 위한 키 생성을 위해 사용할 수 없다는 문제점이 있다.

발명의 내용

해결하려는 과제

- [0004] 바이오메트릭스 정보로부터 인증, 암호화 및/또는 전자 서명 등에 활용 가능한 키를 추출할 수 있는 키 생성 방법 및 시스템을 제공한다.
- [0005] 바이오메트릭스 정보를 이용하여 전자 서명을 처리할 수 있는 인증 방법 및 시스템을 제공한다.
- [0006] 지문과 같은 바이오메트릭스 정보에 대해서도 내적 전달을 위한 투영 행렬 기반의 인증 방법을 적용할 수 있도록 지문의 특징점을 이용하여 지문 정보를 이미지화할 수 있는 지문 정보 변경 방법 및 시스템을 제공한다.

과제의 해결 수단

- [0007] 지문 정보 변경 방법에 있어서, 지문에 대한 특징점(minutiae points)의 타입별로 기설정된 서로 다른 표식을 관리하는 단계; 사용자의 지문 이미지로부터 특징점, 특징점의 타입 및 상기 특징점의 지오메트리 정보를 추출하는 단계; 및 상기 추출된 특징점들에 대해, 특징점의 타입에 대응하는 표식을 특징점의 지오메트리 정보에 대응하는 위치에 포함하는 변환 이미지를 생성하는 단계를 포함하는 것을 특징으로 하는 지문 정보 변경 방법을 제공한다.
- [0008] 일측에 따르면, 상기 지문 정보 변경 방법은 상기 생성된 변환 이미지로부터 상기 사용자의 바이오메트릭스 정보를 추출하는 단계; 상기 추출된 바이오메트릭스 정보를 이용한 학습을 통해 투영 행렬을 생성하는 단계; 및 상기 투영 행렬과 상기 바이오메트릭스 정보간의 내적에 기반하여 상기 사용자의 특징 정보를 추출하는 단계를 더 포함하는 것을 특징으로 할 수 있다.
- [0009] 다른 측면에 따르면, 상기 지문에 대한 특징점의 타입은 끝점(ending point) 및 분기점(bifurcation)을 적어도 포함하고, 상기 기설정된 서로 다른 표식은 상기 끝점을 위한 제1 표식과 상기 분기점을 위한 제2 표식을 적어도 포함하는 것을 특징으로 할 수 있다.
- [0010] 또 다른 측면에 따르면, 상기 변환 이미지는 상기 특징점에 대해 배치된 표식만을 포함하는 것을 특징으로 할 수 있다.
- [0011] 상기 지문 정보 변경 방법을 컴퓨터에 실행시키기 위한 프로그램이 기록되어 있는 것을 특징으로 하는 컴퓨터에서 판독 가능한 기록매체를 제공한다.
- [0012] 컴퓨터와 결합되어 상술한 지문 정보 변경 방법을 컴퓨터에 실행시키기 위해 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램을 제공한다.
- [0013] 지문 정보 변경 방법을 실행하기 위해 컴퓨터 장치로 구현되는 지문 정보 변경 시스템에 있어서, 컴퓨터에서 판독 가능한 명령을 저장하는 메모리; 및 상기 메모리에 저장된 명령을 실행하도록 구현되는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 지문에 대한 특징점(minutiae points)의 타입별로 기설정된 서로 다른 표식을 관리하고, 사용자의 지문 이미지로부터 특징점, 특징점의 타입 및 상기 특징점의 지오메트리 정보를 추출하고, 상기 추출된 특징점들에 대해, 특징점의 타입에 대응하는 표식을 특징점의 지오메트리 정보에 대응하는 위치에 포함하는 변환 이미지를 생성하는 것을 특징으로 하는 지문 정보 변경 시스템을 제공한다.

발명의 효과

- [0014] 바이오메트릭스 정보로부터 인증, 암호화 및/또는 전자 서명 등에 활용 가능한 키를 추출할 수 있다. 또한, 바

이오매트릭스 정보를 이용하여 전자 서명을 처리할 수 있다. 또한, 지문과 같은 바이오매트릭스 정보에 대해서도 내적 전달을 위한 투영 행렬 기반의 인증 방법을 적용할 수 있도록 지문의 특징점을 이용하여 지문 정보를 이미지화할 수 있다.

도면의 간단한 설명

[0015]

도 1은 본 발명의 일실시예에 있어서, 바이오매트릭스 정보를 이용하여 기계 학습을 위한 분류기를 학습시키는 예를 도시한 도면이다.

도 2는 본 발명의 일실시예에 있어서, 학습된 분류기들의 출력 예를 도시한 도면이다.

도 3은 본 발명의 일실시예에 있어서, 키 생성 과정의 예를 도시한 도면이다.

도 4는 본 발명의 일실시예에 있어서, 데이터를 암호화하는 컴퓨터 장치의 예를 도시한 도면이다.

도 5는 본 발명의 일실시예에 있어서, 키 생성 시스템의 내부 구성을 설명하기 위한 블록도이다.

도 6은 본 발명의 일실시예에 있어서, 키 생성 시스템의 프로세서가 포함할 수 있는 구성요소의 예를 도시한 블록도이다.

도 7은 본 발명의 일실시예에 따른 키 생성 시스템이 수행할 수 있는 키 생성 방법의 예를 도시한 흐름도이다.

도 8은 본 발명의 일실시예에 따른 키 생성 시스템이 수행할 수 있는 키 생성 방법의 다른 예를 도시한 흐름도이다.

도 9는 본 발명의 일실시예에 있어서, 키 생성 시스템의 프로세서가 포함할 수 있는 구성요소의 다른 예를 도시한 블록도이다.

도 10은 본 발명의 일실시예에 따른 키 생성 시스템이 수행할 수 있는 키 생성 방법의 또 다른 예를 도시한 흐름도이다.

도 11은 종래기술에 있어서, 얼굴 인증 시스템을 설명하기 위한 도면이다.

도 12 및 도 13은 본 발명의 일실시예에 있어서, 내적의 전달 과정의 예를 설명하기 위한 도면들이다.

도 14는 본 발명의 일실시예에 있어서, 인증 시스템의 내부 구성을 설명하기 위한 블록도이다.

도 15는 본 발명의 일실시예에 있어서, 신뢰할 수 있는 제3자를 위한 컴퓨터 장치의 프로세서가 포함할 수 있는 구성요소의 예를 도시한 블록도이다.

도 16은 본 발명의 일실시예에 따른 신뢰할 수 있는 제3자를 위한 컴퓨터 장치가 수행할 수 있는 인증 방법의 예를 도시한 흐름도이다.

도 17은 본 발명의 일실시예에 있어서, 사용자의 단말이 수행할 수 있는 인증 방법의 예를 도시한 흐름도이다.

도 18은 본 발명의 일실시예에 있어서, 검증자의 단말이 수행할 수 있는 인증 방법의 예를 도시한 흐름도이다.

도 19는 본 발명의 일실시예에 있어서, 지문의 특징점(minutiae points) 표현하는 이미지의 예를 도시한 도면이다.

도 20은 본 발명의 일실시예에 있어서, 지문의 특징점(minutiae points) 표현하는 이미지의 다른 예를 도시한 도면이다.

도 21은 본 발명의 일실시예에 있어서, 지문 정보 변경 시스템의 프로세서가 포함할 수 있는 구성요소의 예를 도시한 블록도이다.

도 22는 본 발명의 일실시예에 따른 지문 정보 변경 시스템이 수행할 수 있는 지문 정보 변경 방법의 예를 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0016]

이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0017]

본 발명에 따른 실시예들은 바이오매트릭스 정보를 이용하여 키를 추출하는 키 생성 방법 및 시스템에 관한 것으로, 키 생성 시스템은 물리적인 컴퓨터 장치로 구현될 수 있으며, 키 생성 방법은 이러한 키 생성 시스템에

의해 수행될 수 있다. 예를 들어, 컴퓨터 장치에는 본 발명의 일실시예에 따른 컴퓨터 프로그램이 설치 및 구동될 수 있고, 컴퓨터 장치는 컴퓨터 프로그램이 저장된 컴퓨터 판독 가능 기록매체로부터 컴퓨터 프로그램의 코드에 따른 명령을 읽어 들여 처리함으로써 키 생성 방법을 수행할 수 있다.

[0019] 도 1은 본 발명의 일실시예에 있어서, 바이오매트릭스 정보를 이용하여 기계 학습을 위한 분류기를 학습시키는 예를 도시한 도면이다. 도 1은 N 명의 사용자들(110) 각각의 바이오매트릭스 정보가 N 개의 분류기들(120)로 입력되는 예를 나타내고 있다. 이때, N 개의 분류기들(120) 각각은 N 명의 사용자들(110)을 위한 N 비트 벡터를 출력할 수 있으며, 동일한 사용자의 바이오매트릭스 정보에 대해 서로 다른 비트가 '1'로 설정되도록 학습될 수 있다. 예를 들어, 사용자 1의 바이오매트릭스 정보에 대해, 분류기 1은 첫 번째 비트가, 분류기 2는 세 번째 비트가, 분류기 3은 N 번째 비트가 각각 '1'로 설정되고, 나머지 비트들은 '0'으로 설정되도록 N 개의 분류기들(120) 각각이 학습될 수 있다. 이때, 특정 사용자에게 어느 분류기가 어느 비트를 '1'로 설정하는가에 대한 정보는 외부로 알려지지 않도록 N 개의 분류기들(120)이 블랙박스 처리될 수 있으며, 이러한 N 개의 분류기들(120) 각각이 특정 사용자에게 어느 비트를 '1'로 설정하는가에 대한 정보를 이용하여 키를 추출하는데 이용할 수 있다. 분류기를 학습하는 구체적인 기술에 대해서는 기존의 잘 알려진 기계학습 기술들(일례로, 딥러닝(deep learning))을 통해 당업자가 용이하게 이해할 수 있을 것이다. 또한, N은 2 이상의 자연수일 수 있으나, 실시예에 따라 N이 2의 m(m은 자연수) 승이 되도록 설정될 수도 있다.

[0020] 도 2는 본 발명의 일실시예에 있어서, 학습된 분류기들의 출력 예를 도시한 도면이다. 도 2는 발명의 이해를 돕기 위해 N이 4로 설정되어, 4 개의 분류기들(210)이 네 명의 사용자들의 바이오매트릭스 정보들을 통해 학습된 경우의 예를 설명한다. 이때, 네 명의 사용자들 중 사용자 1의 바이오매트릭스 정보(220)가 4 개의 분류기들(210)로 각각 입력됨에 따라, 4 개의 분류기들(210)이 학습된 바와 같이 각각 서로 다른 비트를 '1'로 설정한 4 비트 벡터들을 출력한 예를 나타내고 있다. 다시 말해, 사용자 1의 바이오매트릭스 정보(220)에 대해 분류기 1은 첫 번째 비트를, 분류기 2는 네 번째 비트를, 분류기 3은 두 번째 비트를, 분류기 4는 세 번째 비트를 각각 '1'로 설정하도록 학습되었음을 알 수 있다. 이미 설명한 바와 같이, 어느 분류기가 어느 사용자에게 어느 비트를 '1'로 설정하는가에 대해서는 키 생성 시스템의 외부로 알려지지 않도록 처리될 수 있다.

[0021] 이와 같이, 본 발명의 실시예들에서는 학습된 N 개의 분류기들(120)이 N 명의 사용자들(110) 중 특정 사용자의 바이오매트릭스 정보가 입력됨에 따라 각각 서로 다른 비트가 '1'로 설정된 N 개의 N 비트 벡터들을 출력할 수 있다.

[0022] 도 3은 본 발명의 일실시예에 있어서, 키 생성 과정의 예를 도시한 도면이다. 키 생성 시스템(300)은 입력된 사용자 a의 바이오매트릭스 정보(310)를 학습된 N개의 분류기들(320)에 입력시킴에 따라, N 개의 분류기들(320) 각각으로부터 N 비트 벡터를 얻을 수 있다. 이때, N 개의 분류기들(320)에서 출력된 N 개의 N 비트 벡터들은 $\{C_1, C_2, C_3, \dots, C_N\}$ 으로 표현될 수 있다. 여기서 C_i 는 $1 \leq i \leq N$ 일 때, i 번째 N 비트 벡터로서 i 번째 분류기에서 출력된 N 개의 비트들을 포함할 수 있다.

[0023] 또한, 각각의 N 비트 벡터들은 인코딩 과정을 거칠 수 있다. 도 3은 N 개의 N 비트 벡터들 $\{C_1, C_2, C_3, \dots, C_N\}$ 이 키 생성 시스템(300)이 포함하는 인코딩 모듈(330)을 거쳐 인코딩된 N 개의 N 비트 벡터들 $\{ENCo(C_1), ENCo(C_2), ENCo(C_3), \dots, ENCo(C_N)\}$ 와 같이 표현됨을 나타내고 있다. 이때, N 비트 벡터들의 인코딩은 다양한 방법으로 이루어질 수 있다. 예를 들어, N 비트 벡터에서 '1'로 설정된 비트의 위치를 바이너리 수로 표현함으로써, N 비트 벡터의 인코딩이 이루어질 수 있다. N이 16이고, 세 번째 비트가 '1'로 설정된 N 비트 벡터는 인코딩을 거쳐 '0011'과 같은 이진수로 표현될 수 있다. N이 16이고 네 번째 비트가 '1'로 설정된 N 비트 벡터는 인코딩을 거쳐 '0100'과 같은 이진수로 표현될 수 있다. 다른 예로, 인코딩은 해쉬함수를 이용하여 이루어질 수도 있다. 보다 구체적인 예로 N 비트 벡터를 파라미터로 갖는 해쉬함수의 출력 중 하위 log N 비트가 인코딩 출력으로 이용될 수 있다. 이러한 인코딩 방식은 상술한 예시로 한정되지 않으며, 상술한 N 비트 벡터들을 특정 값으로 변환하기 위한 다양한 방법들 중 하나가 이용될 수 있다.

[0024] 한편, 이미 설명한 바와 같이 바이오매트릭스에서는 새로운 바이오매트릭스 정보에 대한 N 개의 분류기들(120)의 출력값이 부정확할 가능성이 존재한다. 따라서, 본 발명의 실시예에서 키 생성 시스템(300)은 N 개의 N 비트 벡터들 $\{C_1, C_2, C_3, \dots, C_N\}$ 에 대한 ECC(Error Correcting Code)를 N개 생성하거나 또는 인코딩 과정을 거친 N 개의 N 비트 벡터들인 $\{ENCo(C_1), ENCo(C_2), ENCo(C_3), \dots, ENCo(C_N)\}$ 에 대한 N개의 ECC를 생성하여 관리하고, 추후 새로운 바이오매트릭스 정보에 대한 N 개의 분류기들(120)의 출력값을 보정하여 이용할 수 있다. 도 3에서는 ECC 생성 모듈(340)을 이용하여 인코딩된 N 개의 N 비트 벡터들에 대한 N 개의 ECC를 생성하는 실시예를

설명하고 있다.

- [0025] 이때, 키 생성 모듈(350)은 인코딩 과정을 거친 N 개의 N 비트 벡터들인 $\{ENCo(C_1), ENCo(C_2), ENCo(C_3), \dots, ENCo(C_N)\}$ 의 해쉬값을 계산함으로써 키를 생성될 수 있다. 다시 말해, 본 실시예에서 키 'key'는 해쉬함수를 $H()$ 라 할 때, $H(\{ENCo(C_1), ENCo(C_2), ENCo(C_3), \dots, ENCo(C_N)\})$ 와 같이 표현될 수 있다.
- [0026] 도 4는 본 발명의 일실시예에 있어서, 데이터를 암호화하는 컴퓨터 장치의 예를 도시한 도면이다. 도 4의 컴퓨터 장치(400)에는 키 생성 시스템(300)이 구현될 수 있으며, 키 생성 시스템(300)이 생성한 키 'key'(410)를 이용하여 데이터 'data'(420)를 암호화할 수 있다. 암호화된 데이터는 $ENC_{key}[data](430)$ 와 같이 표현될 수 있다.
- [0027] 이후, 키 'key'(410)는 컴퓨터 장치(400)나 키 생성 시스템(300)에 저장되지 않으며, 도 3을 통해 설명한 학습된 N 개의 분류기들(320)과 N 개의 ECC이 키 생성 시스템(300)에 의해 관리될 수 있으며, 도 4에서 암호화된 데이터 $ENC_{key}[data](430)$ 가 컴퓨터 장치(400)에 저장 및 관리될 수 있다.
- [0028] 이때, 사용자 a의 새로운 바이오매트릭스 정보가 입력되면, 키 생성 시스템(300)은 도 3과 유사한 방법을 통해 키 'key'(410)를 생성할 수 있다. 이때, 키 생성 시스템(300)은 사용자 a의 새로운 바이오매트릭스 정보를 학습된 N 개의 분류기들(320)에 입력하여 얻어지는 N 개의 N 비트 벡터들을 인코딩한 후에 인코딩된 N 개의 N 비트 벡터들을 키 생성 시스템(300)이 저장하고 있는 N 개의 ECC를 통해 보정함으로써 $\{ENCo(C_1), ENCo(C_2), ENCo(C_3), \dots, ENCo(C_N)\}$ 를 얻을 수 있다. 또한, 키 생성 시스템(300)은 얻어진 $\{ENCo(C_1), ENCo(C_2), ENCo(C_3), \dots, ENCo(C_N)\}$ 를 위에서 설명한 해쉬함수 $H()$ 의 파라미터로 입력함으로써 해쉬값으로서 키 'key'(410)를 생성할 수 있다.
- [0029] 컴퓨터 장치(400)는 키 생성 시스템(300)이 제공하는 키 'key'(410)를 이용하여 암호화된 데이터 $ENC_{key}[data](430)$ 를 복호화함으로써 데이터 'data'(420)를 복원할 수 있게 된다.
- [0030] 상술한 도 4에서는 키 생성 시스템(300)이 생성하는 키 'key'(410)를 데이터의 암호화 및 복호화에 활용하는 실시예를 설명하였으나, 본 발명의 실시예들을 통해 퍼지한(fuzzy)한 바이오매트릭스 정보를 이용하여 정확한 키를 추출하는 것이 가능해졌기 때문에 생성되는 키를 암호화 및 복호화를 위한 키뿐만 아니라, 인증 키나 전자서명을 위한 키로 활용하는 것 역시 가능하다.
- [0031] 도 5는 본 발명의 일실시예에 있어서, 키 생성 시스템의 내부 구성을 설명하기 위한 블록도이다. 본 발명의 실시예들에 따른 키 생성 시스템(500)은 적어도 하나의 물리적인 컴퓨터 장치를 통해 구현될 수 있으며, 도 5에 도시된 바와 같이 메모리(510), 프로세서(520), 통신 모듈(530) 그리고 입출력 인터페이스(540)를 포함할 수 있다. 메모리(510)는 컴퓨터에서 판독 가능한 기록매체로서, RAM(random access memory), ROM(read only memory) 및 디스크 드라이브와 같은 비소멸성 대용량 기록장치(permanent mass storage device)를 포함할 수 있다. 여기서 ROM과 비소멸성 대용량 기록장치는 메모리(510)와 분리되어 별도의 영구 저장 장치로서 포함될 수도 있다. 또한, 메모리(510)에는 운영체제와 적어도 하나의 프로그램 코드(일례로 본 발명의 실시예들에 따른 키 생성 방법을 수행하도록 키 생성 시스템(500)이 포함하는 기록매체에 저장되어 키 생성 시스템(500)을 제어하기 위한 컴퓨터 프로그램)가 저장될 수 있다. 이러한 소프트웨어 구성요소들은 메모리(510)와는 별도의 컴퓨터에서 판독 가능한 기록매체로부터 로딩될 수 있다. 이러한 별도의 컴퓨터에서 판독 가능한 기록매체는 플로피 드라이브, 디스크, 테이프, DVD/CD-ROM 드라이브, 메모리 카드 등의 컴퓨터에서 판독 가능한 기록매체를 포함할 수 있다. 다른 실시예에서 소프트웨어 구성요소들은 컴퓨터에서 판독 가능한 기록매체가 아닌 통신 모듈(530)을 통해 메모리(510)에 로딩될 수도 있다.
- [0032] 프로세서(520)는 기본적인 산술, 로직 및 입출력 연산을 수행함으로써, 컴퓨터 프로그램의 명령을 처리하도록 구성될 수 있다. 명령은 메모리(510) 또는 통신 모듈(530)에 의해 프로세서(520)로 제공될 수 있다. 예를 들어 프로세서(520)는 메모리(510)에 로딩된 프로그램 코드에 따라 수신되는 명령을 실행하도록 구성될 수 있다. 보다 구체적인 예로, 프로세서(520)는 메모리(510)에 로딩된 컴퓨터 프로그램의 코드에 따른 명령을 순차적으로 실행하여 본 발명의 실시예에 따른 키 생성 방법을 수행할 수 있다.
- [0033] 통신 모듈(530)은 실제 컴퓨터 네트워크를 통해 다른 물리적인 기기들과 서로 통신하기 위한 기능을 제공할 수 있다. 일례로, 키 생성 시스템(500)의 프로세서(520)가 처리하기 위한 얼굴 이미지와 패스워드는 컴퓨터 네트워크상의 다른 물리적인 기기로부터, 컴퓨터 네트워크와 통신 모듈(530)을 통해 키 생성 시스템(500)으로 수신되어 메모리(510)나 프로세서(520)로 전달될 수 있다. 역으로, 키 생성 시스템(500)이 수신된 얼굴 이미지와

패스워드에 대한 연산의 처리 결과가 통신 모듈(530)과 컴퓨터 네트워크를 통해 다른 물리적인 기기로 전송될 수도 있다.

[0034] 입출력 인터페이스(540)는 입출력 장치(550)와의 인터페이스를 위한 수단일 수 있다. 예를 들어, 입출력 장치(550)에서 입력 장치는 키보드 또는 마우스 등의 장치를, 그리고 출력 장치는 디스플레이나 스피커와 같은 장치를 포함할 수 있다. 도 5에서 입출력 장치(550)는 키 생성 시스템(500)과 별도의 장치로 표현되었으나, 실시예에 따라 입출력 장치(550)가 키 생성 시스템(500)에 포함되도록 구현될 수도 있다.

[0035] 또한, 다른 실시예들에서 키 생성 시스템(500)은 도 5의 구성요소들보다 더 많은 구성요소들을 포함할 수도 있다. 그러나, 대부분의 종래기술적 구성요소들을 명확하게 도시할 필요성은 없다. 예를 들어, 키 생성 시스템(500)은 각종 물리적인 버튼이나 터치패널, 또는 광출력 장치 등의 다양한 구성요소들을 더 포함하도록 구현될 수 있음을 알 수 있다.

[0036] 도 6은 본 발명의 일실시예에 있어서, 키 생성 시스템의 프로세서가 포함할 수 있는 구성요소의 예를 도시한 블록도이고, 도 7은 본 발명의 일실시예에 따른 키 생성 시스템이 수행할 수 있는 키 생성 방법의 예를 도시한 흐름도이다. 도 6은 앞서 설명한 키 생성 시스템(500)의 프로세서(520)가 포함할 수 있는 구성요소들로서 분류기 학습부(610), N 비트 벡터 계산부(620), 인코딩부(730), ECC 처리부(640) 및 키 생성부(650)를 나타내고 있다. 이러한 프로세서(520) 및 프로세서(520)의 구성요소들은 도 7의 키 생성 방법이 포함하는 단계들(710 내지 750)을 수행할 수 있다. 이때, 프로세서(520) 및 프로세서(520)의 구성요소들은 메모리(510)가 포함하는 운영체제의 코드 및/또는 적어도 하나의 컴퓨터 프로그램의 코드에 따른 명령(instruction)을 실행하도록 구현될 수 있다. 여기서, 프로세서(520)의 구성요소들은 키 생성 시스템(500)에 저장된 컴퓨터 프로그램의 코드가 제공하는 제어 명령에 따라 프로세서(520)에 의해 수행되는 프로세서(520)의 서로 다른 기능들(different functions)의 표현들일 수 있다. 이때, 프로세서(520)는 키 생성 시스템(500)의 제어와 관련된 명령이 로딩된 메모리(510)로부터 필요한 제어 명령을 읽어드릴 수 있으며, 읽어 들인 제어 명령에 따라 이후 설명될 단계들(710 내지 750)을 수행하도록 키 생성 시스템(500)을 제어할 수 있다.

[0037] 단계(710)에서 분류기 학습부(610)는 N (N 은 2 이상의 자연수) 명의 사용자들의 바이오매트릭스 정보를 이용하여 N 개의 분류기들이 동일한 사용자의 바이오매트릭스 정보에 대해 서로 다른 하나의 비트가 '1'로 설정된 N 개의 N 비트 벡터들을 출력하도록 N 개의 분류기들을 학습할 수 있다. 다시 말해, N 명의 사용자들 중 제1 사용자의 제1 바이오매트릭스 정보를 입력하는 경우, N 개의 분류기들은 각각 N 비트 벡터를 출력할 수 있으며, 이때 N 개의 N 비트 벡터는 동일한 위치의 비트가 '1'로 설정되지 않을 수 있다. 이를 위해, 서로 다른 하나의 비트가 '1'로 설정된 N 개의 N 비트 벡터들은 N 비트에서 '1'로 설정된 서로 다른 하나의 비트를 제외한 나머지 비트들이 '0'으로 설정될 수 있다.

[0038] 단계(720)에서 N 비트 벡터 계산부(620)는 N 명의 사용자들 중 제1 사용자의 제1 바이오매트릭스 정보를 학습된 N 개의 분류기들에 입력하여 제1 바이오매트릭스 정보에 대응하는 N 개의 제1 N 비트 벡터들을 계산할 수 있다. 이러한 단계(720)은 제1 사용자를 위한 키를 생성하기 위해 입력되는 제1 바이오매트릭스 정보를 단계(710)에서 학습된 N 개의 분류기들 각각에 입력하고, 학습된 N 개의 분류기들 각각이 제1 바이오매트릭스 정보에 대응하는 제1 N 비트 벡터를 출력하는 과정일 수 있다.

[0039] 단계(730)에서 인코딩부(730)는 계산된 N 개의 제1 N 비트 벡터들 각각을 인코딩할 수 있다. 인코딩은 앞서 설명한 바와 같이 제1 N 비트 벡터에서 '1'로 설정된 비트의 위치를 바이너리 수로 표현한 값을 계산하는 방식이나, 제1 N 비트 벡터를 파라미터로 갖는 해쉬함수의 출력 중 하위 $\log N$ 비트의 값을 계산하는 방식 등 다양한 방법을 통해 이루어질 수 있다.

[0040] 단계(740)에서 ECC 처리부(740)는 계산된 N 개의 제1 N 비트 벡터들 또는 인코딩된 N 개의 제1 N 비트 벡터들 각각에 대한 ECC(Error Correcting Code)를 생성할 수 있다. ECC 처리부(740)가 계산된 N 개의 제1 N 비트 벡터들 각각에 대한 ECC를 생성하는 경우, 단계(740)는 단계(730) 이전에 수행될 수도 있다.

[0041] 단계(750)에서 키 생성부(650)는 인코딩된 N 개의 제1 N 비트 벡터들을 파라미터로 갖는 해쉬함수의 출력값을 제1 키로서 생성할 수 있다. 생성된 키는 이미 설명한 바와 같이, 인증 키, 암호화 키, 전자 서명을 위한 키 등으로 활용될 수 있다.

[0042] 도 8은 본 발명의 일실시예에 따른 키 생성 시스템이 수행할 수 있는 키 생성 방법의 다른 예를 도시한 흐름도이다. 도 8의 단계(810 내지 840)는 도 7의 단계(750) 이후에 수행될 수 있다.

[0043] 단계(810)에서 N 비트 벡터 계산부(620)는 제1 사용자의 제2 바이오매트릭스 정보를 학습된 N 개의 분류기들에

입력하여 제2 바이오매트릭스 정보에 대응하는 N 개의 제2 N 비트 벡터들을 계산할 수 있다. 이러한 단계(810)는 단계(720)과 동일한 과정으로 이루어질 수 있으나, 제1 바이오매트릭스 정보와 제2 바이오매트릭스 정보간의 차이로 인해, 제2 N 비트 벡터들은 제1 N 비트 벡터들과 일부 다를 수도 있다.

[0044] 단계(820)에서 인코딩부(730)는 계산된 N 개의 제2 N 비트 벡터들을 인코딩할 수 있다. 인코딩 방식에 대해서는 이미 자세히 설명한 바 있다.

[0045] 단계(830)에서 ECC 처리부(740)는 인코딩된 N 개의 제2 N 비트 벡터들을 단계(740)에서 생성된 ECC를 이용하여 보정할 수 있다. 이 경우, 보정 및 인코딩된 N 개의 제2 N 비트 벡터들은 단계(750)의 인코딩된 N 개의 제1 N 비트 벡터들과 동일한 값을 갖게 된다. 만약, 단계(740)에서 N 개의 제1 N 비트 벡터들 각각에 대한 ECC를 생성한 경우에는 단계(830)이 단계(820) 보다 먼저 수행되어 N 개의 제2 N 비트 벡터들을 ECC를 이용하여 보정한 후에 보정된 N 개의 제2 N 비트 벡터들을 인코딩부(730)가 인코딩할 수도 있다.

[0046] 단계(840)에서 키 생성부(660)는 보정 및 인코딩된 N 개의 제2 N 비트 벡터들을 파라미터로 갖는 해쉬함수의 출력값을 제2 키로서 생성할 수 있다. 이 경우, 제1 키 및 제2 키는 동일한 값을 가질 수 있다. 이처럼, 바이오매트릭스 정보를 통해서도 동일한 키 값을 추출할 수 있게 되기 때문에 바이오매트릭스 정보를 이용하여 생성된 키를 인증 키나 암호화 키 또는 전자 서명을 위한 키로 활용할 수 있게 된다.

[0047] 도 9는 본 발명의 일실시예에 있어서, 키 생성 시스템의 프로세서가 포함할 수 있는 구성요소의 다른 예를 도시한 블록도이고, 도 10은 본 발명의 일실시예에 따른 키 생성 시스템이 수행할 수 있는 키 생성 방법의 또 다른 예를 도시한 흐름도이다. 도 9에서 프로세서(520)는 도 6에서 설명한 분류기 학습부(610), N 비트 벡터 계산부(620), 인코딩부(730), ECC 처리부(640) 및 키 생성부(650)를 포함할 수 있고, 도 9에 도시된 바와 같이 암호화부(910)를 더 포함할 수 있다. 또한, 도 10의 단계(1010)는 도 7의 단계(750)와 도 8의 단계(810) 사이에 수행될 수 있고, 도 10의 단계(1020)는 도 8의 단계(840) 이후에 수행될 수 있다.

[0048] 단계(1010)에서 암호화부(910)는 제1 키로 데이터를 암호화할 수 있다. 이 경우, 제1 키는 키 생성 시스템에 저장되지 않고, 암호화된 데이터가 저장될 수 있다.

[0049] 단계(1020)에서 암호화부(910)는 제2 키로 암호화된 데이터를 복호화할 수 있다. 제2 키는 제1 키와 동일한 값을 갖기 때문에 암호화된 데이터를 복호화할 수 있게 된다.

[0051] 이하에서는 바이오매트릭스 정보를 이용하여 전자 서명을 처리하기 위한 인증 방법 및 인증 시스템에 대해 설명한다.

[0052] 도 11은 종래기술에 있어서, 얼굴 인증 시스템을 설명하기 위한 도면이다. 얼굴 인증 시스템은 사용자의 얼굴 이미지에 기반한 얼굴 벡터들 ' $x_1, x_2, \dots$ '을 학습(1110)하여 투영 행렬(Projection Matrix) U 를 생성하고, 생성된 투영 행렬 U 를 이용하여 특징 추출(1120)을 통해 특징들(가중 벡터) ' $w_1, w_2, \dots$ '을 생성 및 관리할 수 있다. 또한, 얼굴 인증 시스템은 새롭게 입력되는 얼굴 이미지와 관련하여 얼굴 벡터 x 에 대한 특징 추출(1130)을 통해 특징 W 를 계산할 수 있다. 이때, 특징 W 는 얼굴 벡터 x 와 투영 행렬 U 간의 내적(Inner-Product)을 이용하여 계산될 수 있다. 얼굴 인증 시스템은 계산된 특징 W 와 앞서 생성 및 관리되는 특징들 ' $w_1, w_2, \dots$ '을 비교하여 사용자를 인증할 수 있다.

[0053] 이하의 실시예들에서는 신뢰할 수 있는 제3자(Trust Third Party)가 사용자 A의 바이오매트릭스 정보를 학습하여 특징을 추출하고, 사용자 A는 자신의 바이오매트릭스 정보 X 를 암호화하여 사용자 B에게 전달하여 사용자 B가 사용자 A의 바이오매트릭스 정보 x 와 투영 행렬 U 를 모두 모르는 상태로 바이오매트릭스 정보 x 와 투영 행렬 U 간의 내적을 획득할 수 있는 방식의 인증 방법 및 인증 시스템을 설명한다.

[0054] 도 12 및 도 13은 본 발명의 일실시예에 있어서, 내적의 전달 과정의 예를 도시한 도면이다.

[0055] 도 12는 신뢰할 수 있는 제3자(Trust Third Party, TTA, 1210), 사용자 A(1220) 및 사용자 B(1230)를 나타내고 있다. 이때, 실질적으로 신뢰할 수 있는 제3자(1210), 사용자 A(1220) 및 사용자 B(1230)는 각각 컴퓨터 네트워크를 통해 연결되어 통신하는 컴퓨터 장치들일 수 있으며, 화살표를 통해 나타난 데이터의 이동은 통신 프로토콜을 이용하여 컴퓨터 네트워크를 통해 데이터들이 전송되는 것을 의미할 수 있다.

[0056] 신뢰할 수 있는 제3자(1210)는 적어도 사용자 A(1220)의 바이오매트릭스 정보를 이용하여 학습 및 특징 추출을 처리함에 따라 사용자 A(1220)의 바이오매트릭스 정보에 대한 투영 행렬 U 와 특징들 ' $w_1, w_2, \dots$ '을 저장 및 관리하고 있다고 가정한다. 이때, 신뢰할 수 있는 제3자(1210)는 비밀키 ' msk '와 공개키 ' mpk '를 생성하여 공개

키 ' mpk '를 사용자 A(1220) 및 사용자 B(1230)에게 제공할 수 있다. 이 경우, 사용자 A(1220)는 공개키 ' mpk '와 전자 서명을 위한 벡터 x 를 저장하고 있을 수 있으며, 사용자 B(1230)는 공개키 ' mpk '를 저장하고 있을 수 있다.

[0057] 도 13에 도시된 바와 같이, 신뢰할 수 있는 제3자(1210)가 비밀키 ' msk '와 투영 행렬 u 를 이용한 키 유도(key derivation)를 통해 (pk_u , sk_u)를 생성하여 pk_u 는 사용자 A(1220)에게 sk_u 는 사용자 B(1230)에게 각각 전달할 수 있다. 이때, 사용자 A(1220)는 공개키 ' mpk '와 전자 서명을 위한 벡터 x , 그리고 pk_u 를 함께 암호화하여 암호화된 결과 C 를 생성하고, 생성된 C 를 사용자 B(1230)에게 전달할 수 있다.

[0058] 이때, 사용자 B(1230)는 공개키 ' mpk '와 sk_u , 그리고 사용자 A(1220)로부터 제공받은 C 를 인자로 복호화를 진행하여 사용자 A(1220)의 바이오메트릭스 정보에 따른 벡터 x 와 투영 행렬 u 간의 내적인 $\langle x, u \rangle$ 를 얻을 수 있다. 이러한 내적을 구하기 위한 전체 수학적 과정에 대해서는 이후 더욱 자세히 설명한다.

[0059] 아래 수학적 식 1은 비밀키 ' msk '와 공개키 ' mpk '를 생성하는 예를 설명하고 있다.

수학적 식 1

$$\text{Setup}(1^\lambda, 1^\ell) \rightarrow (mpk, msk)$$

$$\text{GroupGen}(1^\lambda) \rightarrow (\mathbb{G}, p, \langle g \rangle \in \langle h \rangle = \mathbb{G})$$

$$s \leftarrow \mathbb{Z}_p^\ell, t \leftarrow \mathbb{Z}_p^\ell$$

$$mpk = (h_i = g^{s_i} h^{t_i})_{i \in [1..\ell]}, msk = (s, t)$$

[0060]

[0061] 이러한 수학적 식 1은 이미 잘 알려진 FE(Functional Encryption) 스킴(scheme)에서 비밀키와 공개키를 생성하는 기술, 특히 DDH(Decision Diffie-Hellman) 스킴을 통해 내적을 전달하기 위한 기술로부터 당업자가 용이하게 이해할 수 있을 것이다.

[0062] 반면, 본 발명의 실시예에서는 DDH 스킴과는 달리, 아래 수학적 식 2에서와 같이 sk_u 뿐만 아니라, pk_u 를 더 유도한다.

수학적 식 2

$$\text{KeyDer}(msk, u \in \mathbb{Z}_p^\ell) \rightarrow (pk_u, sk_u)$$

$$sk_u = (s_u = \langle u, s \rangle, t_u = \langle u, t \rangle)$$

$$pk_u = \{w_i = h_i^{u_i}, v_i = g^{u_i}\}_{i \in [1..\ell]}$$

[0063]

[0064] 이러한 pk_u 는 신뢰할 수 있는 제3자(1210)가 인정한, 다시 말해 신뢰할 수 있는 제3자(1210)로부터 sk_u 를 수신한 특정 사용자(본 실시예에서는 사용자 B(1230))만이 사용자 A(1220)에 대한 인증을 수행할 수 있도록 제한할 수 있는 효과를 불러온다. 예를 들어, sk_u 는 사용자 B(1230)의 비밀키와 같이, pk_u 는 사용자 B(1230)의 공개키와 같이 활용될 수 있다. 이때, 수학적 식 2에 나타난 바와 같이, 투영 행렬 u 는 사용자 B(1230)의 비밀키로서 제공되는 sk_u 에 은닉되어 사용자 B(1230)가 투영 행렬 u 를 획득할 수 없는 형태로 사용자 B(1230)에게 제공될 수 있다.

[0065] 아래 수학적 식 3은 사용자 A(1220)가 신뢰할 수 있는 제3자(1210)의 공개키 ' mpk ', 사용자 B(1230)의 공개키 pk_u , 그리고 사용자 A(1220)의 바이오메트릭스 정보의 특징 벡터 x 를 이용한 암호화를 통해 앞서 설명한 바와 같이 암호화된 결과 C (인증 정보)를 생성하는 예를 나타내고 있다.

수학식 3

$$\text{Enc}(mpk, pk_u, x \in \mathbb{Z}_p^\ell) \rightarrow C$$

$$r \leftarrow \mathbb{Z}_p, C = g^r, D = h^r, E = \prod_{i=1}^{\ell} w_i^r \cdot v_i^{x_i}$$

$$C = (C, D, E)$$

[0066]

[0067]

이러한 수학식 3 역시 DDH 스킴에 기반하나, E를 생성함에 있어, pk_u 를 통해 전달된 v_i (수학식 2에서와 같이 투영 행렬 u_i 가 반영된)에 벡터 x_i (암호화하려는 벡터 x)를 반영하고, 벡터 x_i 가 반영된 v_i 와 w_i 간의 하다마드 곱(Hadamard products)이 적용된다는 점에서 DDH 스킴과는 차이가 있으며, 이러한 E를 통해 사용자 A(1220)의 바이오매트릭스 정보에 따른 벡터 x 를 은닉하여 사용자 B(1230)에게 전달할 수 있다. 이러한 벡터 x 역시 사용자 B(1230)가 벡터 x 를 직접적으로 획득할 수 없는 형태로 사용자 B(1230)에게 전달될 수 있다.

[0068]

사용자 B(1230)는 인증 정보 C를 전달받은 후 아래 수학식 4와 같이, 복호화를 수행하여 내적 $\langle x, u \rangle$ 를 얻을 수 있다.

수학식 4

$$\text{Dec}(mpk, sk_u, C) \rightarrow \langle x, u \rangle$$

$$\langle x, u \rangle = \text{dlog}_g \left(\frac{E}{C^{s_u} \cdot D^{t_u}} \right)$$

[0069]

[0070]

여기서, E, C^{s_u} , D^{t_u} 는 아래 수학식 5와 같으며, 각각 수학식 4에 대입하여 E를 C^{s_u} 와 D^{t_u} 간의 하다마드 곱으로 나눈 결과는 g의 $\langle x, u \rangle$ 승이 되고, 이 결과에 대한 이산로그(discrete logarithm, dlog)를 통해 내적 $\langle x, u \rangle$ 를 얻을 수 있다.

수학식 5

$$\begin{aligned} E &= \prod_{i=1}^{\ell} w_i^r \cdot v_i^{x_i} = \prod_{i=1}^{\ell} h_i^{ru_i} \cdot g^{u_i x_i} \\ &= \prod_{i=1}^{\ell} g^{s_i ru_i} h^{t_i ru_i} g^{u_i x_i} = \prod_{i=1}^{\ell} g^{s_i ru_i + u_i x_i} h^{t_i ru_i} \\ &= g^{\sum_{i=1}^{\ell} s_i ru_i + u_i x_i} h^{\sum_{i=1}^{\ell} t_i ru_i} \\ &= g^{r \langle s, u \rangle + \langle u, x \rangle} h^{r \langle t, u \rangle} \\ C^{s_y} &= g^{r \langle s, u \rangle} \\ D^{t_y} &= h^{r \langle t, u \rangle} \end{aligned}$$

[0071]

[0072]

이처럼, 사용자 A(1220)의 바이오매트릭스의 벡터 x 와 투영 행렬 u 를 모두 사용자 B(1230)에게 노출되지 않은 상태로 x 와 u 간의 내적 $\langle x, u \rangle$ 를 사용자 B(1230)에게 전달하는 것이 가능해진다. 도 11을 통해 설명한 바와 같이 내적 $\langle x, u \rangle$ 는 벡터 x 에 대한 특징 W 가 되기 때문에 사용자 B(1230)는 특징 W 와 학습 및 특징 추출을 통해

추출된 특징 ' $w_1, w_2, \dots$ ' 간의 비교가 가능해진다.

[0073] 벡터 x 와 투영 행렬 u 를 사용자 B(1230)에게 노출되지 않은 상태로 x 와 u 간의 내적 $\langle x, u \rangle$ 를 사용자 B(1230)에게 전달하는 방법이 상술한 수학적식 1 내지 5로 한정되는 것은 아니다. 예를 들어, 아래 수학적식 6 내지 수학적식 9은 내적 $\langle x, u \rangle$ 의 전달을 위한 다른 실시예를 설명한다.

[0074] 우선, 수학적식 1과 동일한 방법으로 비밀키 ' msk '와 공개키 ' mpk '를 생성할 수 있다. 이때, 수학적식 2 내지 수학적식 5는 아래 수학적식 6 내지 수학적식 9와 같이 변경될 수 있다. 수학적식 6 내지 수학적식 9는 u_i 들이 크기가 작기 때문에 이러한 u_i 들이 노출될 가능성을 줄이기 위해 $(e_1, e_2, \dots, e_\ell)$ 와 τ 를 더 활용하여 sk_u 와 pk_u 를 구한 것으로, 수학적식 7 내지 수학적식 9는 새로운 sk_u 와 pk_u 에 따라 내적 $\langle x, u \rangle$ 을 구하기 위해 변경되었다. 결과적으로 기본적인 개념은 수학적식 2 내지 수학적식 5에서와 유사하다.

수학적식 6

$$\begin{aligned} \text{KeyDer}(msk, \mathbf{u} \in \mathbb{Z}_p^\ell) &\rightarrow (sk_{\mathbf{u}}, pk_{\mathbf{u}}) \\ (e_0, e_1, \dots, e_\ell) &\leftarrow \mathbb{Z}_p^{1+\ell}, \tau \leftarrow \mathbb{Z}_p \\ sk_{\mathbf{u}} &= (s_u = e_0 \cdot \langle \mathbf{u}, \mathbf{s} \rangle, t_u = e_0 \cdot \langle \mathbf{u}, \mathbf{t} \rangle, \tau) \\ pk_{\mathbf{u}} &= \{w_i = h_i^{e_0 u_i}, v_i = h^{\tau e_i} g^{u_i}, z_i = h^{e_i}\}_{i \in [1..\ell]} \end{aligned}$$

[0075]

수학적식 7

$$\begin{aligned} \text{Enc}(mpk, pk_{\mathbf{u}}, \mathbf{x} \in \mathbb{Z}_p^\ell) &\rightarrow C \\ r &\leftarrow \mathbb{Z}_p, C = g^r, D = h^r, \\ E &= \prod_{i=1}^{\ell} w_i^r \cdot v_i^{x_i}, F = \prod_{i=1}^{\ell} z_i^{x_i} \\ C &= (C, D, E, F) \end{aligned}$$

[0076]

수학적식 8

$$\begin{aligned} \text{Dec}(mpk, sk_{\mathbf{u}}, C) &\rightarrow \langle \mathbf{x}, \mathbf{u} \rangle \\ \langle \mathbf{x}, \mathbf{u} \rangle &= \text{dlog}_g \left(\frac{E}{C^{s_u} \cdot D^{t_u} \cdot F^\tau} \right) \end{aligned}$$

[0077]

수학식 9

$$\begin{aligned}
E &= \prod_{i=1}^{\ell} w_i^r \cdot v_i^{x_i} = \prod_{i=1}^{\ell} h_i^{re_0 u_i} \cdot h^{\tau e_i x_i} \cdot g^{u_i x_i} \\
&= \prod_{i=1}^{\ell} g^{s_i re_0 u_i} h^{t_i re_0 u_i} h^{\tau e_i x_i} g^{u_i x_i} = \prod_{i=1}^{\ell} g^{s_i re_0 u_i + u_i x_i} h^{t_i re_0 u_i + \tau e_i x_i} \\
&= g^{\sum_{i=1}^{\ell} s_i re_0 u_i + u_i x_i} h^{\sum_{i=1}^{\ell} t_i re_0 u_i + \tau e_i x_i} \\
&= g^{re_0 \langle \mathbf{s}, \mathbf{u} \rangle + \langle \mathbf{u}, \mathbf{x} \rangle} h^{re_0 \langle \mathbf{t}, \mathbf{u} \rangle + \tau \langle \mathbf{e}, \mathbf{x} \rangle} \\
C^{s_y} &= g^{re_0 \langle \mathbf{s}, \mathbf{u} \rangle} \\
D^{t_y} &= h^{re_0 \langle \mathbf{t}, \mathbf{u} \rangle} \\
F^{\tau} &= h^{\tau \langle \mathbf{e}, \mathbf{x} \rangle}
\end{aligned}$$

[0078]

[0079] 여기서 e 는 $(e_1, e_2, \dots, e_l)$ 일 수 있다.

[0080] 이와 같이, 본 발명의 실시예들에서 x 와 u 간의 내적 $\langle x, u \rangle$ 은 x 와 u 를 각각 다른 파라미터와의 내적이나 다른 파라미터의 근지수(cubic root)로 이용하여 전달하고, 사용자 B(1230)의 공개키 pk_u 로 암호화된 인증 정보 C 를 사용자 B(1230)의 비밀키 sk_u 를 이용하여 복호화하는 과정에서 내적 $\langle x, u \rangle$ 를 계산할 수 있는 방식이면 어떠한 방법이라도 사용될 수 있다.

[0081] 또한, 전달된 내적 $\langle x, u \rangle$ 을 활용하여 메시지 M 에 대한 전자 서명이 이루어질 수 있다. 비밀키 ' msk '와 공개키 ' mpk '는 수학식 1에서와 유사하게 아래 수학식 10과 같이 얻어질 수 있다.

수학식 10

$$\begin{aligned}
&\text{Setup}(1^\lambda, 1^\ell) \rightarrow (mpk, msk) \\
&(mpk, msk) \leftarrow \text{mIP.Setup}(1^\lambda, 1^\ell)
\end{aligned}$$

[0082]

[0083] 이때, 함수 $\text{mIP.Setup}()$ 가 수학식 1의 $\text{Setup}()$ 에 대응될 수 있다.

수학식 11

$$\begin{aligned}
&\text{Enroll}(\mathbf{x}_1, \mathbf{x}_2, \dots) \\
&\mathbf{U} \in \mathbb{N}^{m \times \ell} \leftarrow \text{Bio.Learn}(\mathbf{x}_1, \mathbf{x}_2, \dots) \\
&(\mathbf{w}_1, \mathbf{w}_2, \dots) \leftarrow \text{Bio.FeatExt}(\mathbf{U}, \mathbf{x}_1, \mathbf{x}_2, \dots)
\end{aligned}$$

[0084]

[0085] 함수 $\text{Enroll}()$ 는 입력되는 바이오메트릭스 정보들 ' $x_1, x_2, \dots$ '을 이용한 등록 과정(Enrollment)을 의미할 수 있다. 이때, 함수 $\text{Bio.Learn}()$ 는 ' $x_1, x_2, \dots$ '를 이용한 학습의 과정으로서 투영 행렬 U 가 결과로서 출력될 수 있다. 또한, 함수 $\text{Bio.FeatExt}()$ 는 ' $x_1, x_2, \dots$ '와 투영 행렬 U 를 이용한 특징 추출의 과정으로서 특징들 ' $w_1, w_2, \dots$ '이 결과로서 출력될 수 있다.

[0086] 수학식 12는 키 pk_u 와 sk_u 를 유도하는 과정으로서 함수 $\text{mIP.KeyDer}(msk, u_i)$ 는 수학식 2 또는 수학식 6의 함수

KeyDer()에 대응될 수 있다.

수학식 12

$$\text{KeyDer}(msk, \mathbf{U} = [\mathbf{u}_1, \dots, \mathbf{u}_m]^\top) \rightarrow (\text{pk}_{\mathbf{U}}, \text{sk}_{\mathbf{U}})$$

$$(\text{pk}_{\mathbf{u}_i}, \text{sk}_{\mathbf{u}_i}) \leftarrow \text{mIP.KeyDer}(msk, \mathbf{u}_i)$$

[0087]

사용자 A(1220)는 아래 수학식 13의 예에서와 같이 전자 서명 σ 를 생성할 수 있다.

수학식 13

$$\text{Sign}(mpk, \text{pk}_{\mathbf{U}}, \mathbf{x} \in \mathbb{N}^\ell, M) \rightarrow \sigma$$

$$\mathbf{b} \leftarrow H(M) \in \mathbb{N}^m$$

$$\mathbf{Y} = \mathbf{x} \cdot \mathbf{b}^\top = [\mathbf{y}_1, \dots, \mathbf{y}_m] \in \mathbb{N}^{\ell \times m}$$

$$\mathbf{c}_i = \text{mIP.Enc}(mpk, \text{pk}_{\mathbf{u}_i}, \mathbf{y}_i)$$

$$\sigma = (\mathbf{c}_1, \dots, \mathbf{c}_m)$$

[0089]

수학식 13은 메시지 M 을 파라미터로 이용한 해쉬함수 $H()$ 의 결과인 벡터 $\mathbf{b}$ 의 전치벡터와 사용자 A(1220)의 바이오매트릭스 정보 $\mathbf{x}$ 간의 하다마드 곱을 통해 $\mathbf{Y}$ 를 구할 수 있다. 따라서 $\mathbf{Y}$ 는 메시지 M 의 해쉬값 M 과 바이오매트릭스 정보 $\mathbf{x}$ 의 정보를 모두 포함하게 된다. 이때, 함수 $\text{mIP.Enc}()$ 는 수학식 3 또는 수학식 7의 함수 $\text{Enc}()$ 에 대응할 수 있다. 결과적으로 수학식 13에 따라 전자 서명 σ 는 메시지 M 과 바이오매트릭스 정보 $\mathbf{x}$ 가 곱해진 $\mathbf{Y} (= [\mathbf{y}_1, \dots, \mathbf{y}_m])$ 를 암호화한 형태로 얻어질 수 있다.

[0090]

사용자 B(1230)는 수학식 14의 예에서와 같이 전자 서명 σ 를 이용하여 메시지 M 을 인증할 수 있다.

[0091]

수학식 14

$$\text{Verify}(mpk, \text{sk}_{\mathbf{U}}, \mathbf{w}, \sigma, M) \rightarrow 1/0$$

$$\mathbf{b} \leftarrow H(M) \in \mathbb{N}^m$$

$$\bar{\mathbf{w}}_i = \text{mIP.Dec}(mpk, \text{sk}_{\mathbf{u}_i}, \mathbf{c}_i) / b_i$$

$$1/0 \leftarrow \text{Bio.Match}(\mathbf{w}, \bar{\mathbf{w}}, \theta)$$

[0092]

여기서, 함수 $\text{mIP.Dec}()$ 는 도 4 또는 도 8의 함수 $\text{Dec}()$ 에 대응할 수 있다. $\mathbf{c}_i$ 를 이용하여 함수 $\text{mIP.Dec}()$ 의 출력을 구하면, 내적 $\langle \mathbf{x}_i, \mathbf{u}_i \rangle$ 와 메시지의 해쉬값 b_i 가 곱해진 형태의 결과가 나오게 되고, 이를 메시지의 해쉬값 b_i 로 나누면 내적 $\langle \mathbf{x}_i, \mathbf{u}_i \rangle$ 다시 말해 바이오매트릭스 정보 $\mathbf{x}$ 에 대한 특징 $\mathbf{w}$ (수학식 14의 $\bar{\mathbf{w}}_i$)이 얻어지게 된다. 함수 $\text{Bio.Match}()$ 는 $\mathbf{w}$ 와 $\bar{\mathbf{w}}$ 간의 거리(차이)를 계산하여 거리가 기설정된 θ 값 이내인 경우, '1'을 출력하여 메시지 M 이 변조되지 않았음을 인증할 수 있다. 만약, $\mathbf{w}$ 와 $\bar{\mathbf{w}}$ 간의 거리를 계산하여 거리가 기설정된 θ 값을 벗어나는 경우에는 메시지 M 이 중간에 변조된 것으로 판단할 수 있다.

[0093]

도 14는 본 발명의 일실시예에 있어서, 인증 시스템이 포함하는 컴퓨터 장치의 내부 구성을 설명하기 위한 블록도이다. 도 12 및 도 13을 통해 설명한 바와 같이, 인증 시스템은 신뢰할 수 있는 제3자(1210), 사용자

[0094]

A(1220) 및 사용자 B(1230) 각각에 대응하는 컴퓨터 장치(1400)를 포함할 수 있다. 또한, 컴퓨터 장치(1400)는 도 14에 도시된 바와 같이 메모리(1410), 프로세서(1420), 통신 모듈(1430) 그리고 입출력 인터페이스(1440)를 포함할 수 있다. 이러한 인증 시스템(1400)의 구성요소들은 도 5를 통해 설명한 메모리(510), 프로세서(520), 통신 모듈(530) 그리고 입출력 인터페이스(540)에 대응될 수 있기 때문에 구체적인 설명은 생략한다.

- [0095] 도 15는 본 발명의 일실시예에 있어서, 신뢰할 수 있는 제3자를 위한 컴퓨터 장치의 프로세서가 포함할 수 있는 구성요소의 예를 도시한 블록도이고, 도 16은 본 발명의 일실시예에 따른 신뢰할 수 있는 제3자(Trust Third Party, TTP)를 위한 컴퓨터 장치가 수행할 수 있는 인증 방법의 예를 도시한 흐름도이다. 도 15은 도 14의 컴퓨터 장치(1400)의 프로세서(1420)가 포함할 수 있는 구성요소들로서 키 생성부(1510), 키 전송부(1520) 및 특징 정보 추출부(1530)를 나타내고 있다. 이러한 프로세서(1420) 및 프로세서(1420)의 구성요소들은 도 16의 인증 방법이 포함하는 단계들(1610 내지 1640)을 수행할 수 있다. 이때, 프로세서(1420) 및 프로세서(1420)의 구성요소들은 메모리(1410)가 포함하는 운영체제의 코드 및/또는 적어도 하나의 컴퓨터 프로그램의 코드에 따른 명령(instruction)을 실행하도록 구현될 수 있다. 여기서, 프로세서(1420)의 구성요소들은 컴퓨터 장치(1400)에 저장된 컴퓨터 프로그램의 코드가 제공하는 제어 명령에 따라 프로세서(1420)에 의해 수행되는 프로세서(1420)의 서로 다른 기능들(different functions)의 표현들일 수 있다. 이때, 프로세서(1420)는 컴퓨터 장치(1400)의 제어와 관련된 명령이 로딩된 메모리(1410)로부터 필요한 제어 명령을 읽어드릴 수 있으며, 읽어 들인 제어 명령에 따라 이후 설명될 단계들(1610 내지 1640)을 수행하도록 컴퓨터 장치(1400)을 제어할 수 있다.
- [0096] 단계(1610)에서 키 생성부(1510)는 TTP(Trust Third Party)의 비밀키 및 TTP의 공개키를 생성할 수 있다. TTP의 비밀키와 TTP의 공개키를 생성하는 방법은 수학적 1을 통해 설명한 바 있다.
- [0097] 단계(1620)에서 키 전송부(1520)는 TTP의 공개키를 사용자 및 검증자에게 전달할 수 있다. 도 12에서는 TTA(1210)가 공개키 "*mpk*"를 사용자 A(1220)과 사용자 B(1230)에게 각각 전달하는 실시예를 설명한 바 있다. 이때, 사용자 A(1220)가 본 실시예의 사용자에게 대응될 수 있고, 사용자 B(1230)가 본 실시예의 검증자에게 대응될 수 있다.
- [0098] 단계(1630)에서 특징 정보 추출부(1530)는 사용자의 바이오매트릭스 정보를 이용한 학습을 통해 투영 행렬을 생성하고, 투영 행렬과 바이오매트릭스 정보간의 내적에 기반하여 사용자의 특징 정보를 추출할 수 있다. 특징 정보의 추출은 도 11에서 특징 ' $W_1, W_2, \dots$ '를 추출하는 것에 대응될 수 있다.
- [0099] 단계(1640)에서 키 생성부(1510)는 투영 행렬 및 TTP의 비밀키를 이용하여 검증자용 비밀키 및 검증자용 공개키를 생성할 수 있다. 검증자용 비밀키와 검증자용 공개키를 생성하는 것은 수학적 2 및 수학적 6을 통해 이미 자세히 설명한 바 있다. 일례로 수학적 2에서는 파라미터 s, t 를 포함하는 TTP의 비밀키와 투영 행렬 u 를 이용하여 내적 $\langle u, s \rangle$ 및 내적 $\langle u, t \rangle$ 를 포함하는 검증자용 비밀키를 생성하고, 투영 행렬 u 를 근지수(cubic root)로 이용하여 검증자용 공개키를 생성하는 예를 설명하였다.
- [0100] 단계(1650)에서 키 전송부(1520)는 검증자용 비밀키를 검증자의 단말로 네트워크를 통해 전송하고, 검증자용 공개키를 사용자의 단말로 네트워크를 통해 전송할 수 있다.
- [0101] 이때, 사용자의 단말은 TTP의 공개키와 검증자용 공개키 및 사용자의 제1 바이오매트릭스 정보를 이용하여 사용자의 단말에서 생성된 인증 정보를 네트워크를 통해 검증자의 단말로 전송할 수 있다.
- [0102] 또한, 검증자의 단말은 TTP의 공개키와 검증자용 비밀키 및 사용자의 단말로부터 전송된 인증 정보를 이용하여 제1 바이오매트릭스 정보와 투영 행렬간의 내적이 제1 바이오매트릭스 정보에 대한 특징 정보로서 계산할 수 있다. 예를 들어, 검증자의 단말은 TTP에서 관리하는 사용자의 특징 정보와 상기 계산된 특징 정보를 비교하여 사용자를 검증할 수 있게 된다.
- [0103] 이때, 사용자의 단말에서 제1 바이오매트릭스 정보를 검증자용 공개키로 암호화함으로써 TTP의 인증 시스템인 컴퓨터 장치(1400)으로부터 검증자용 비밀키를 수신한 검증자만이 인증 정보를 복원 가능하도록 제한할 수 있다.
- [0104] 투영 행렬은 기설정된 적어도 하나의 제1 파라미터와의 내적을 통해 검증자용 비밀키에 은닉되어 검증자의 단말로 전달될 수 있고, 제1 바이오매트릭스 정보는 기설정된 적어도 하나의 제2 파라미터의 근지수로서 인증 정보에 은닉되어 검증자의 단말로 전달될 수 있다. 또한, 검증자의 단말이 검증자용 공개키로 암호화된 인증 정보가 검증자용 비밀키로 복호화되는 과정에서 제1 바이오매트릭스 정보와 인증 정보간의 내적을 계산할 수 있다.
- [0105] 또한, 인증 정보는 사용자의 단말에서 검증자의 단말로 전달될 메시지의 해쉬값에 따른 벡터의 전치벡터와 제1

바이오메트릭스 정보간의 제1내적을 검증자의 공개키 및 TTP의 공개키로 암호화하여 생성될 수 있고, 메시지와 함께 검증자의 단말로 전송될 수 있다. 예를 들어 수학적식 13을 통해 사용자 A(1220)가 인증 정보를 생성하여 사용자 B(1230)에게 전달하는 예를 설명한 바 있다. 이 경우, 검증자의 단말은 인증 정보를 검증자의 비밀키와 TTP의 공개키로 복호화한 결과에 메시지의 해쉬값에 따른 벡터를 반영하여 제1 바이오메트릭스 정보와 투영 행렬간의 내적이 계산할 수 있다. 이 경우, 단계(1650)에서 키 전송부(1520)는 사용자의 특징 정보를 검증자용 비밀키와 함께 검증자의 단말로 더 전송할 수 있고, 검증자의 단말에서 계산된 내적을 특징 정보와 비교하여 메시지를 인증할 수 있다.

- [0106] 사용자의 단말과 검증자의 단말 역시 도 14를 통해 설명한 컴퓨터 장치(1400)와 같이 구현될 수 있으며, 사용자의 단말은 도 17의 인증 방법을, 검증자의 단말은 도 18의 인증 방법을 각각 수행할 수 있다.
- [0107] 도 17은 본 발명의 일실시예에 있어서, 사용자의 단말이 수행할 수 있는 인증 방법의 예를 도시한 흐름도이다.
- [0108] 단계(1710)에서 사용자의 단말은 TTP(Trust Third Party)의 공개키를 네트워크를 통해 수신할 수 있다. 예를 들어, 사용자의 단말이 포함하는 프로세서는 네트워크를 통해 TTP의 공개키를 수신하도록 사용자의 단말이 포함하는 통신 모듈을 제어할 수 있다.
- [0109] 단계(1720)에서 사용자의 단말은 TTP로부터 검증자용 공개키를 수신할 수 있다. 이때, 검증자용 공개키는 TTP에서 사용자의 바이오메트릭스 정보들을 이용한 학습을 통해 생성된 투영 행렬과 TTP의 비밀키를 이용하여 생성될 수 있다.
- [0110] 단계(1730)에서 사용자의 단말은 사용자의 제1 바이오메트릭스 정보를 생성할 수 있다. 제1 바이오메트릭스 정보는 사용자가 인증을 받거나 전자 서명을 하기 위해 새롭게 입력한 바이오메트릭스 정보(홍채 정보, 지문 정보, 얼굴 정보 등과 같이 해당 시스템에서 사용하는 종류의 정보)일 수 있다.
- [0111] 단계(1740)에서 사용자의 단말은 TTP의 공개키, 검증자용 공개키 및 제1 바이오메트릭스 정보를 이용하여 인증 정보를 생성할 수 있다. 이러한 인증 정보의 생성은 수학적식 3 및 수학적식 7을 통해 이미 자세히 설명한 바 있다.
- [0112] 단계(1750)에서 사용자의 단말은 생성된 인증 정보를 네트워크를 통해 검증자의 단말로 제공할 수 있다. 이때, 검증자의 단말에서 TTP의 공개키와 검증자 단말이 TTP로부터 수신한 검증자용 비밀키 및 인증 정보를 이용하여 제1 바이오메트릭스 정보와 투영 행렬간의 내적이 제1 바이오메트릭스 정보에 대한 특징 정보로서 계산될 수 있다.
- [0113] 도 18은 본 발명의 일실시예에 있어서, 검증자의 단말이 수행할 수 있는 인증 방법의 예를 도시한 흐름도이다.
- [0114] 단계(1810)에서 검증자의 단말은 TTP(Trust Third Party)의 공개키를 네트워크를 통해 수신할 수 있다. 예를 들어, 검증자의 단말이 포함하는 프로세서는 TTP의 공개키를 수신하도록 검증자의 단말을 제어할 수 있다.
- [0115] 단계(1820)에서 검증자의 단말은 TTP로부터 검증자용 비밀키를 수신할 수 있다. 이때, 검증자용 비밀키는 TTP에서 사용자의 바이오메트릭스 정보들을 이용한 학습을 통해 생성된 투영 행렬과 TTP의 비밀키를 이용하여 생성될 수 있다.
- [0116] 단계(1830)에서 검증자의 단말은 TTP의 공개키, 사용자의 단말이 TTP로부터 수신한 검증자용 공개키 및 사용자의 제1 바이오메트릭스 정보를 이용하여 사용자의 단말에서 생성된 인증 정보를 네트워크를 통해 수신할 수 있다.
- [0117] 단계(1840)에서 검증자의 단말은 TTP의 공개키와 검증자용 비밀키 및 인증 정보를 이용하여 제1 바이오메트릭스 정보와 투영 행렬간의 내적을 제1 바이오메트릭스 정보에 대한 특징 정보로서 계산할 수 있다.
- [0118] 이처럼, 본 실시예들에 따른 내적의 전달을 통해 검증자에게 사용자의 바이오메트릭스 정보와 투영 정보를 노출하지 않고도 사용자를 인증하거나 또는 전자 서명이 가능해질 수 있다.
- [0120] 한편, 도 11을 통해 설명한 바와 같이 얼굴 인증에서는 얼굴 이미지로부터 추출되는 벡터들과 투영 행렬을 이용하여 사용자별 특징을 추출할 수 있다. 그러나 얼굴 인증과 같은 바이오메트릭스 정보는 대부분 행렬 연산과 같은 내적 연산을 이용하기 때문에 상술한 인증 방법 및 인증 시스템에 쉽게 적용하여 내적을 전달하거나 전자 서명을 처리하는데 이용할 수 있다.
- [0121] 반면, 지문(fingerprint)은 끝점(ending point)과 분기점(bifurcation)으로 대표되는 특징점(minutiae point

s)들과 타입, 지오메트리 정보 등을 직접 비교하는 방식으로 비교가 이루어지기 때문에 상술한 인증 방법 및 인증 시스템에 쉽게 적용하기 어렵다. 예를 들어, 얼굴 인증을 위한 학습에 이용되는 얼굴 이미지 샘플들은 해상도가 제한(일례로, 40x40 픽셀)된다. 한편, 지문의 경우에는 이러한 제한된 해상도의 지문 이미지로부터 지문에 따른 특징을 추출하는 경우, 정확한 특징을 추출할 수 없다.

[0122] 따라서 본 실시예에서는 지문 이미지를 그대로 이용하지 않고, 지문의 끝점(ending point)와 분기점(bifurcation)으로 대표되는 특징점(minutiae point)들을 표현하는 새로운 이미지를 생성하고, 생성된 이미지를 이용하여 상술한 인증 방법 및 인증 시스템에 적용하여 내적을 전달하거나 전자 서명을 처리할 수 있다.

[0123] 예를 들어, 끝점에 대응하는 위치에는 삼각형을, 분기점에 대응하는 위치에는 사각형을 포함하는 이미지를 생성하거나, 또는 끝점에 대응하는 위치에는 밸리(valley)의 표현을, 분기점에 대응하는 위치에는 피크(peak)의 표현을 포함하는 이미지를 생성하고, 생성된 이미지를 통해 지문 정보를 바이오매트릭스 정보로서 상술한 인증 방법 및 인증 시스템에 적용할 수 있다.

[0124] 도 19는 본 발명의 일실시예에 있어서, 도 19는 본 발명의 일실시예에 있어서, 지문의 특징점(minutiae points) 표현하는 이미지의 예를 도시한 도면이다. 도 19는 지문 이미지(1910)와 지문 이미지(1910)가 포함하는 끝점 및 분기점 중 일부를 삼각형과 사각형으로 표현한 변환 이미지(1920)를 각각 도시하고 있다. 지문 이미지(1910)는 앞서 설명한 바와 같이, 특징점(minutiae point)들의 타입과 위치에 대한 지오메트리 정보를 포함하고 있으며, 이러한 특징점, 특징점의 타입 그리고 위치에 대한 정보를 비교하는 방식으로 지문간의 비교가 이루어지기 때문에 앞서 설명한 내적을 이용한 인증 방법을 적용하기 어렵다. 이에 본 실시예에서는 지문 이미지(1910)를 변환 이미지(1920)와 같이 특징점의 종류와 위치를 쉽게 파악 가능하도록 변환함으로써, 변환 이미지(1920)를 이용한 내적 방식의 인증 방법을 지문과 같은 바이오매트릭스 정보에도 적용할 수 있게 된다.

[0125] 도 20은 본 발명의 일실시예에 있어서, 지문의 특징점(minutiae points) 표현하는 이미지의 다른 예를 도시한 도면이다. 도 20은 지문 이미지(1910)에서 끝점을 "v"로 표현하고 분기점을 "^" 표현한 변환 이미지(2010)를 도시하고 있다.

[0126] 이처럼, 지문 이미지에 대해, 지문 이미지의 특징점을 특징점의 타입에 따른 기설정된 표식으로 표시한 변환 이미지를 생성함으로써, 변환 이미지를 이용한 내적 방식의 인증 방법을 이용할 수 있게 된다.

[0127] 도 21은 본 발명의 일실시예에 있어서, 지문 정보 변경 시스템의 프로세서가 포함할 수 있는 구성요소의 예를 도시한 블록도이고, 도 22는 본 발명의 일실시예에 따른 지문 정보 변경 시스템이 수행할 수 있는 지문 정보 변경 방법의 예를 도시한 흐름도이다. 도 21에서 지문 정보 변경 시스템은 앞서 설명한 컴퓨터 장치(1400)와 같이 구현될 수 있으며, 컴퓨터 장치(1400)의 프로세서(1420)가 포함할 수 있는 구성요소들로서 표식 관리부(2110), 지문 정보 추출부(2120), 변환 이미지 생성부(2130), 바이오매트릭스 정보 추출부(2140), 투영 행렬 생성부(2150) 및 특징 정보 추출부(2160)를 나타내고 있다. 이러한 프로세서(1420) 및 프로세서(1420)의 구성요소들은 도 22의 지문 정보 변경 방법이 포함하는 단계들(2210 내지 2260)을 수행할 수 있다. 이때, 프로세서(1420) 및 프로세서(1420)의 구성요소들은 메모리(1410)가 포함하는 운영체제의 코드 및/또는 적어도 하나의 컴퓨터 프로그램의 코드에 따른 명령(instruction)을 실행하도록 구현될 수 있다. 여기서, 프로세서(1420)의 구성요소들은 지문 정보 변경 시스템이 구현된 컴퓨터 장치(1400)에 저장된 컴퓨터 프로그램의 코드가 제공하는 제어 명령에 따라 프로세서(1420)에 의해 수행되는 프로세서(1420)의 서로 다른 기능들(different functions)의 표현들일 수 있다. 이때, 프로세서(1420)는 컴퓨터 장치(1400)의 제어와 관련된 명령이 로딩된 메모리(1410)로부터 필요한 제어 명령을 읽어드릴 수 있으며, 읽어 들인 제어 명령에 따라 이후 설명될 단계들(2210 내지 2260)을 수행하도록 컴퓨터 장치(1400)를 제어할 수 있다.

[0128] 단계(2210)에서 표식 관리부(2110)는 지문에 대한 특징점(minutiae points)의 타입별로 기설정된 서로 다른 표식을 관리할 수 있다. 예를 들어, 관리되는 표식은 특징점의 타입별로 타입들 각각을 식별할 수 있는 이미지, 텍스트 또는 이미지와 텍스트의 조합 등의 표식일 수 있다. 이때, 지문에 대한 특징점의 타입은 끝점(ending point) 및 분기점(bifurcation)을 적어도 포함할 수 있고, 이 경우 기설정된 서로 다른 표식은 끝점을 위한 제1 표식과 분기점을 위한 제2 표식을 적어도 포함할 수 있다. 필요에 따라 지문의 특징점에 대해 이미 잘 알려진 중심점(core), 삼각주(delta) 등과 같은 다른 특징점의 타입들이 더 활용될 수도 있으며, 이 경우 또 다른 표식들이 더 활용될 수 있다.

[0129] 단계(2220)에서 정보 추출부(2120)는 사용자의 지문 이미지로부터 특징점, 특징점의 타입 및 특징점의 지오메트리 정보를 추출할 수 있다. 이러한 지문에 대한 정보의 추출은 지문 인식과 관련된 잘 알려진 기술들을 통해

당업자가 용이하게 이해할 수 있을 것이다.

- [0130] 단계(2230)에서 변환 이미지 생성부(2130)는 추출된 특징점들에 대해, 특징점의 타입에 대응하는 표식을 특징점의 지오메트리 정보에 대응하는 위치에 포함하는 변환 이미지를 생성할 수 있다. 이때, 지문 이미지상에 표식을 배치하는 것이 아니라, 표식을 포함하는 별도의 변환 이미지가 생성될 수 있다. 예를 들어, 변환 이미지는 특징점에 대해 배치된 표식만을 포함하도록 생성될 수 있다.
- [0131] 단계(2240)에서 바이오메트릭스 정보 추출부(2140)는 생성된 변환 이미지로부터 사용자의 바이오메트릭스 정보를 추출할 수 있다. 이때 추출된 바이오메트릭스 정보는 변환 이미지를 분석하여 추출되는 특징 벡터들일 수 있다.
- [0132] 단계(2250)에서 투영 행렬 생성부(2150)는 추출된 바이오메트릭스 정보를 이용한 학습을 통해 투영 행렬을 생성할 수 있다. 일례로 도 11에서와 같이 이미지에 따른 벡터들을 이용한 학습을 통해 투영 행렬을 생성하는 예를 이미 설명한 바 있다.
- [0133] 단계(2260)에서 특징 정보 추출부(2160)는 투영 행렬과 바이오메트릭스 정보간의 내적에 기반하여 사용자의 특징 정보를 추출할 수 있다. 이처럼, 본 발명의 실시예들에 따르면, 지문 정보에 대해 특징점과 타입, 그리고 지오메트리 정보를 추출하고, 추출된 정보들을 비교하여 지문 정보를 활용하는 것이 아니라, 이러한 정보를 이용하여 변환 이미지를 생성하고, 변환 이미지의 학습에 따라 바이오메트릭스 정보와 투영 행렬간의 내적을 통해 사용자의 특징 정보를 추출함으로써, 지문 이미지를 통해서도 내적을 이용한 인증 방법 및 시스템의 적용이 가능해질 수 있다.
- [0135] 이처럼 본 발명의 실시예들에 따르면, 바이오메트릭스 정보로부터 인증, 암호화 및/또는 전자 서명 등에 활용 가능한 키를 추출할 수 있다. 또한, 바이오메트릭스 정보를 이용하여 전자 서명을 처리할 수 있다. 또한, 지문과 같은 바이오메트릭스 정보에 대해서도 내적 전달을 위한 투영 행렬 기반의 인증 방법을 적용할 수 있도록 지문의 특징점을 이용하여 지문 정보를 이미지화할 수 있다.
- [0136] 이상에서 설명된 시스템 또는 장치는 하드웨어 구성요소, 소프트웨어 구성요소 또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 어플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.
- [0137] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록매체에 저장될 수 있다.
- [0138] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하

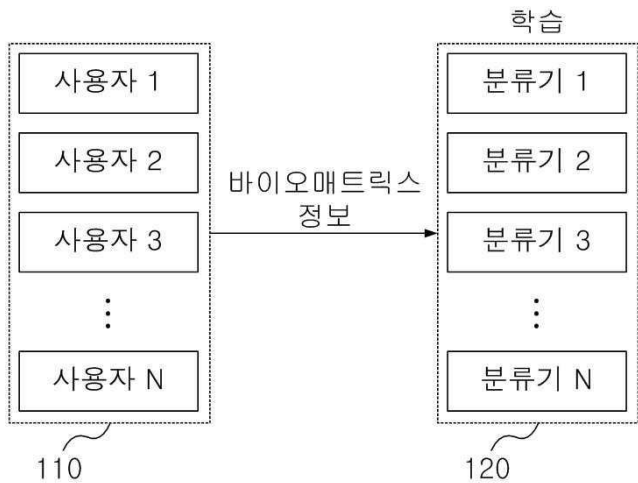
록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0139] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

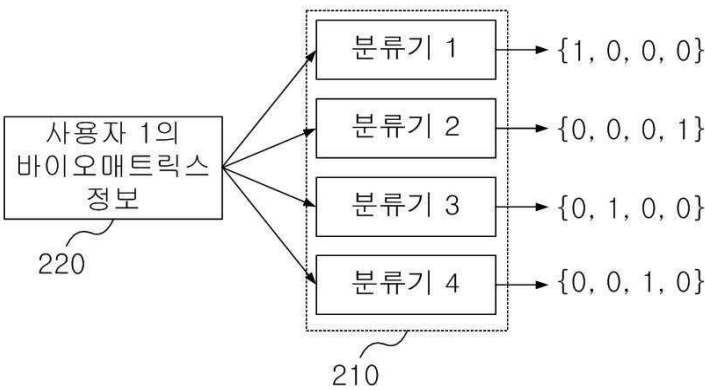
[0140] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

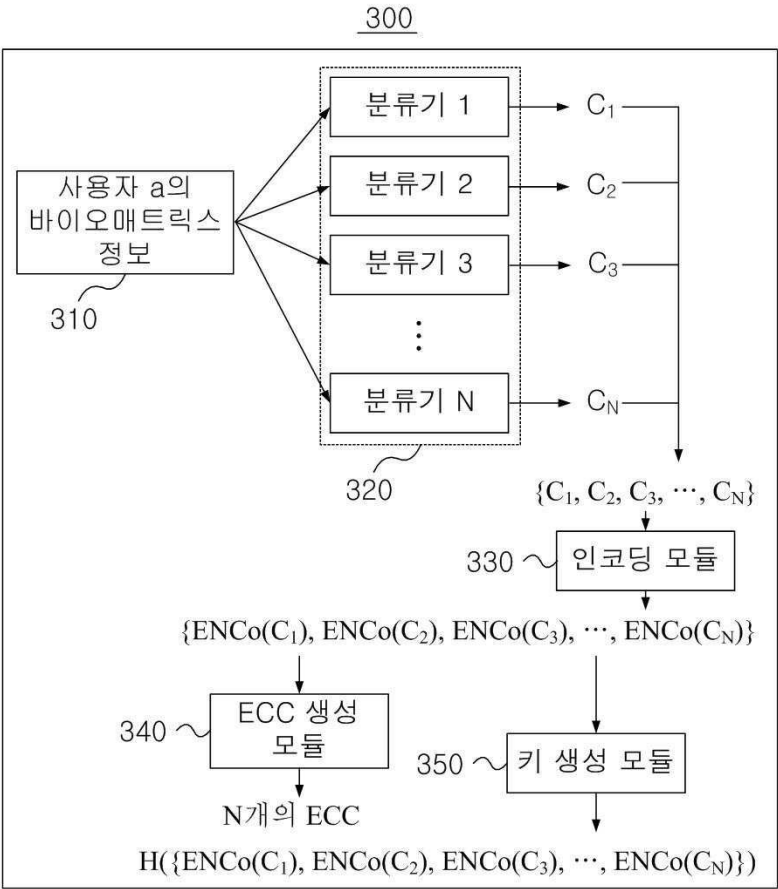
도면1



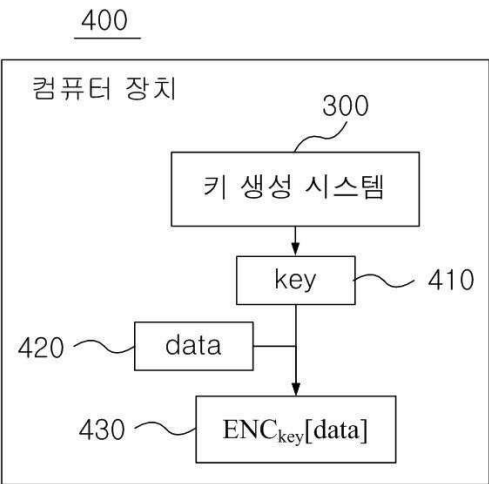
도면2



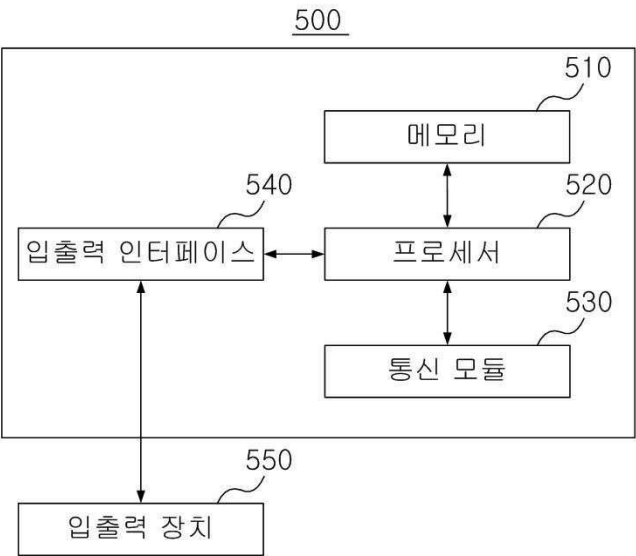
도면3



도면4



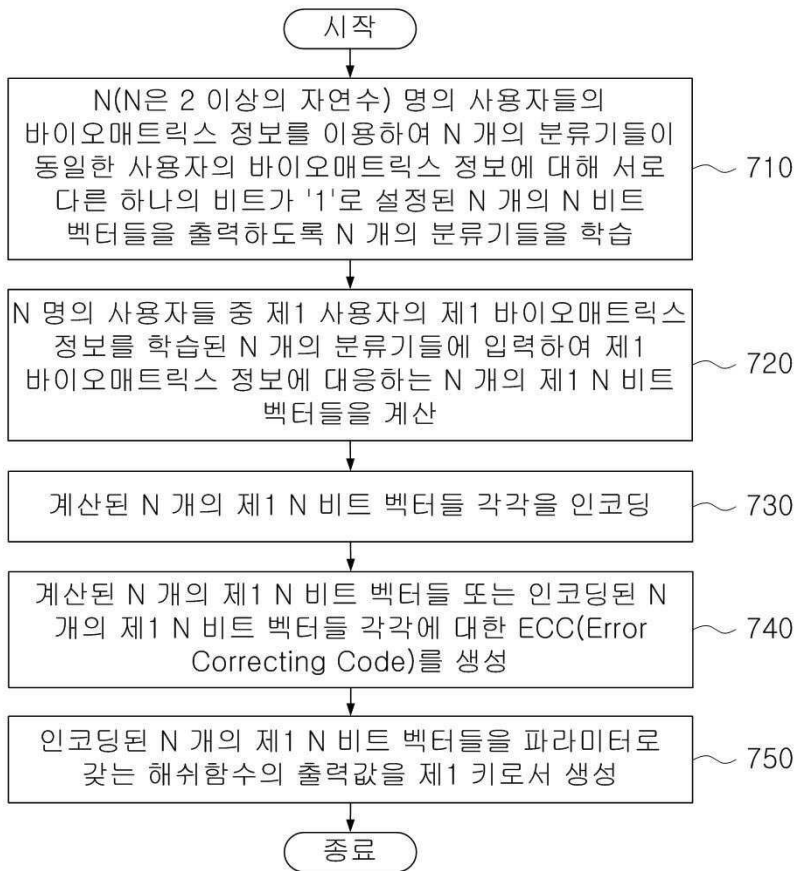
도면5



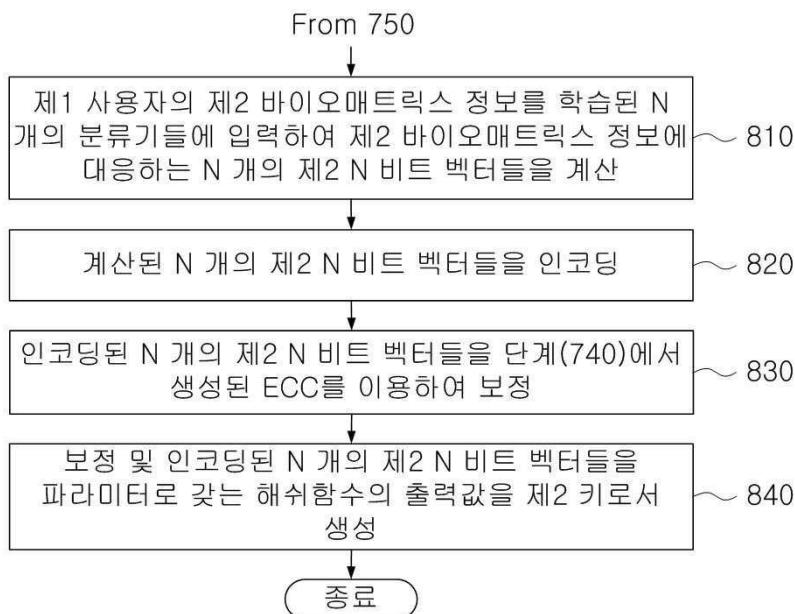
도면6



도면7



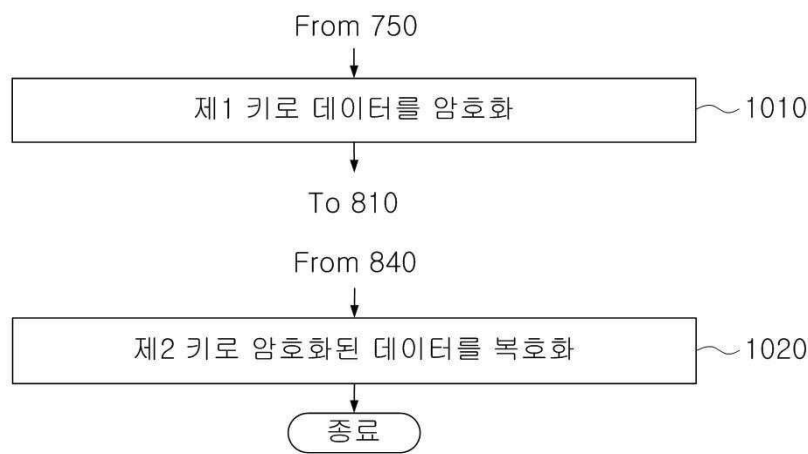
도면8



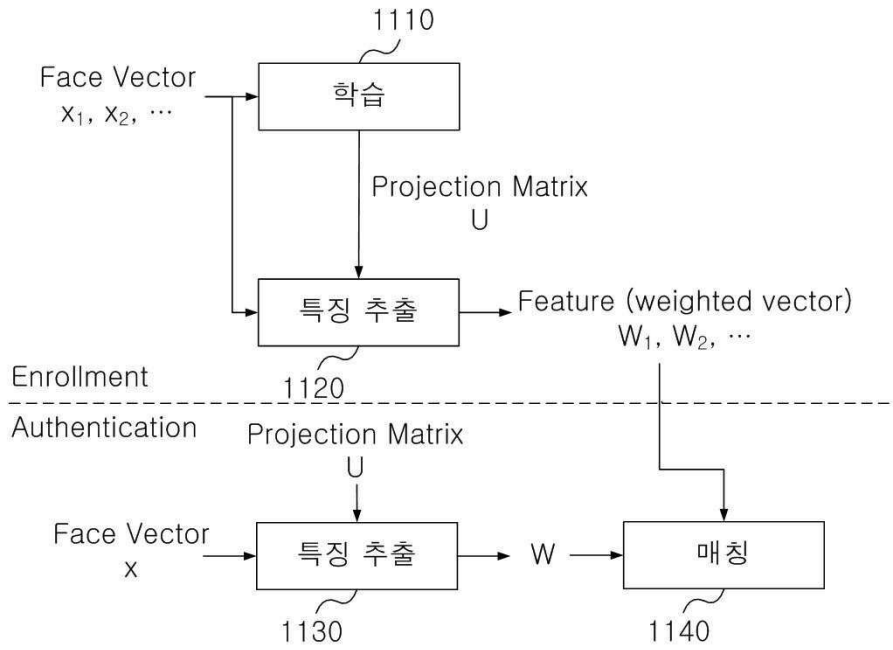
도면9



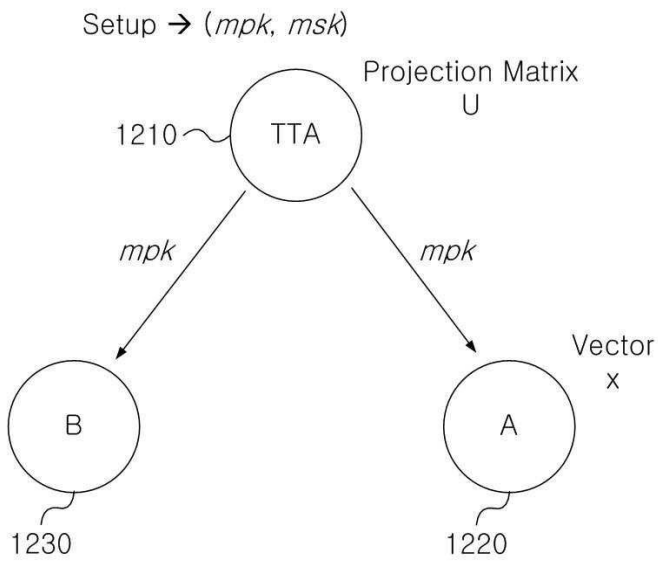
도면10



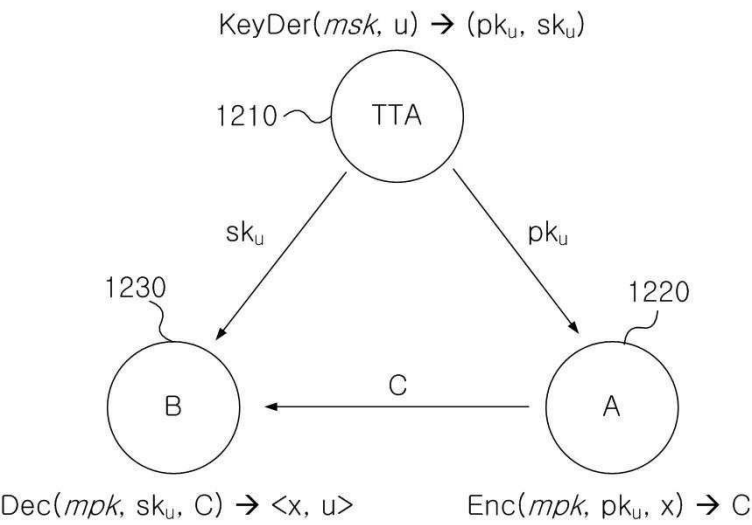
도면11



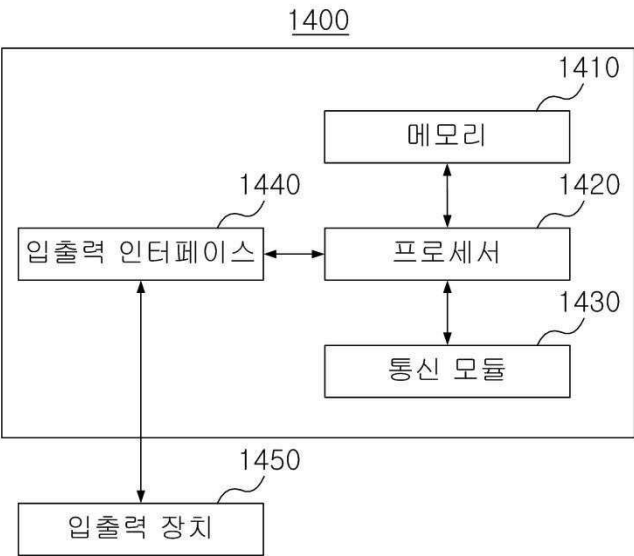
도면12



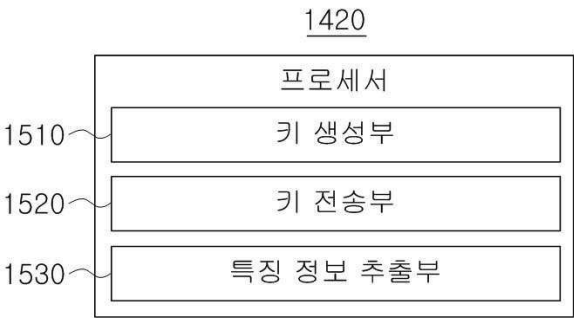
도면13



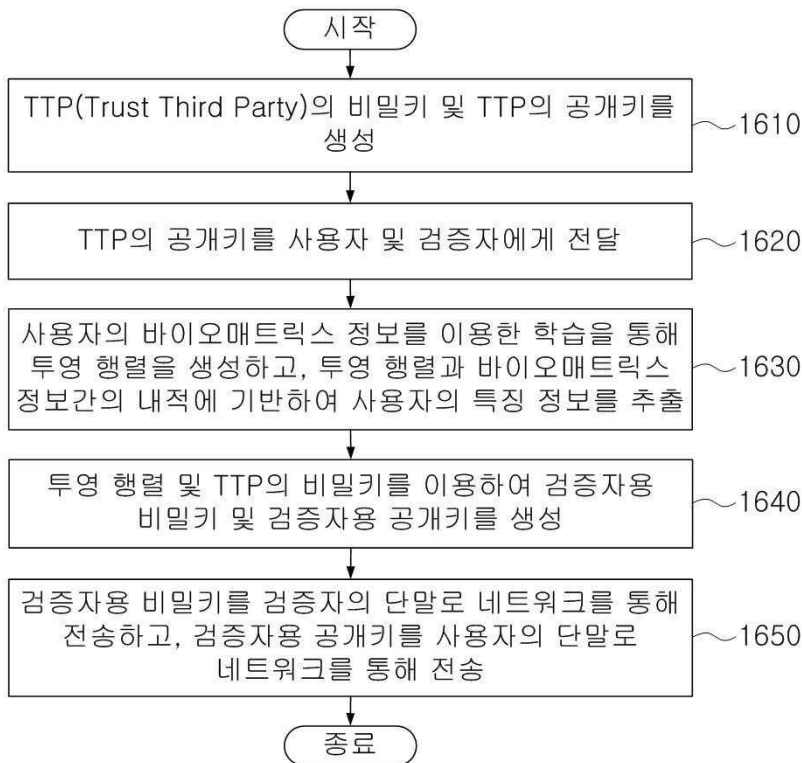
도면14



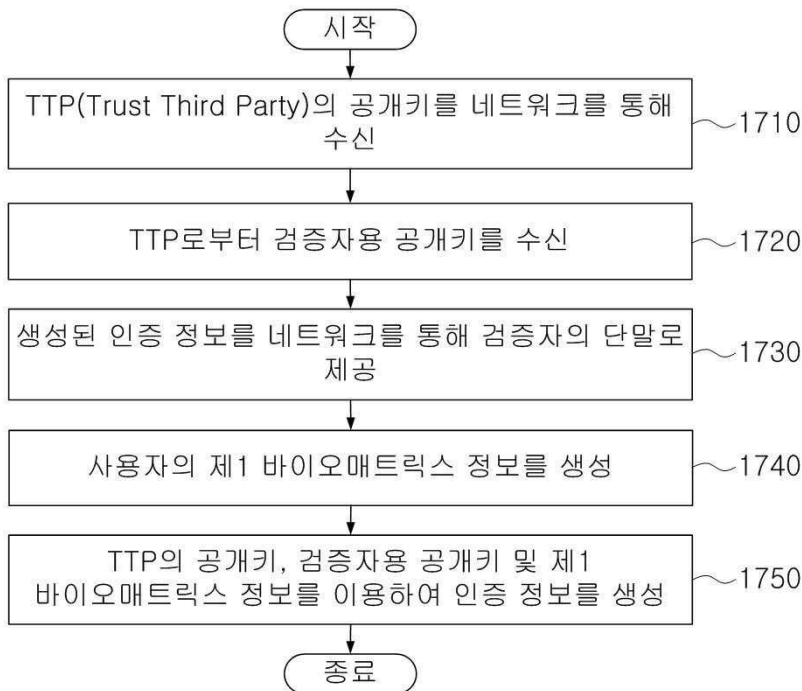
도면15



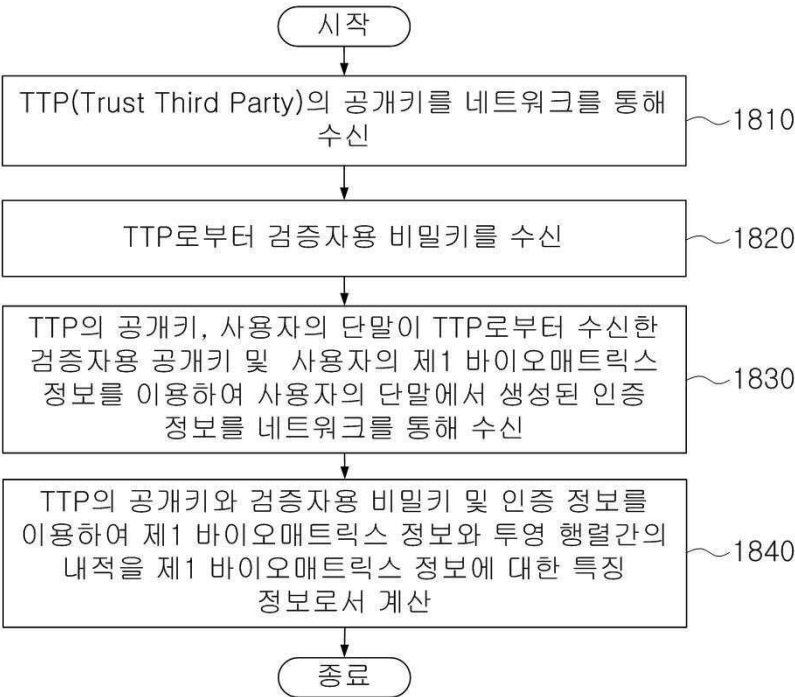
도면16



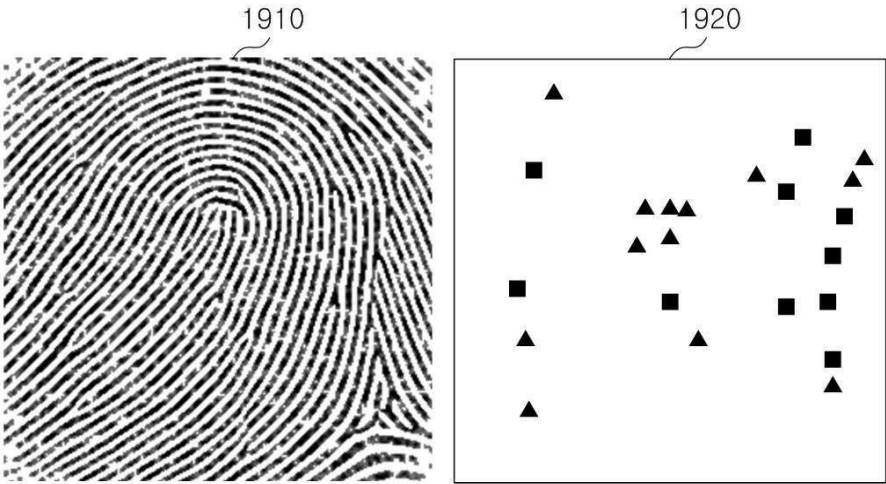
도면17



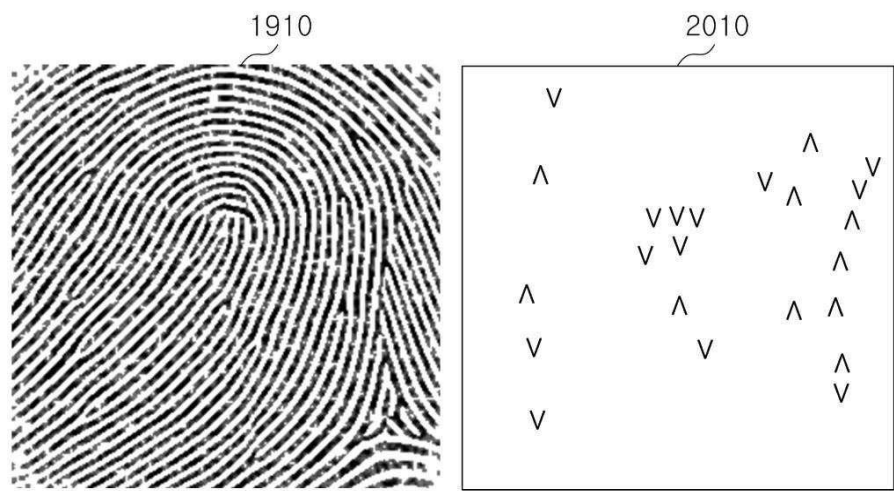
도면18



도면19



도면20



도면21



도면22

