(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0129417
(43) 공개일자 2019년11월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06F 21/31* (2013.01)
H04L 9/06 (2006.01)
(52) CPC특허분류
H04L 9/0866 (2013.01)
G06F 21/31 (2013.01)
(21) 출원번호 10-2018-0054032
(22) 출원일자 2018년05월11일
심사청구일자 2018년05월11일

(71) 출원인
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
양대헌
서울특별시 서초구 서초중앙로 200, 17동 901호(서초동, 삼풍아파트)
(74) 대리인
양성보

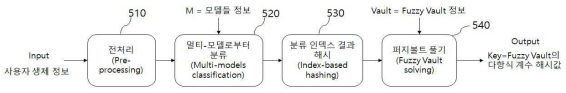
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 **바이오매트릭스와 Fuzzy Vault를 이용하여 암호학적 키를 생성하는 방법 및 시스템**

(57) 요 약

일 실시예에 따른 암호키를 생성하는 방법은, 사용자 인증을 위한 적어도 하나 이상의 인증 정보가 입력됨을 수신하는 단계; 상기 수신된 적어도 하나 이상의 인증 정보를 멀티 모델로부터 분류하는 단계; 상기 멀티 모델로부터 상기 적어도 하나 이상의 인증 정보를 분류한 인덱스 결과를 해시함에 따라 해시 값을 획득하는 단계; 및 상기 획득된 해시 값을 기 생성된 퍼지 볼트 정보에 기반하여 키를 추출하는 단계를 포함할 수 있다.

대 표 도 - 도5



(52) CPC특허분류
H04L 9/0643 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 20160000970022002
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 방송통신산업기술개발사업
연구과제명 [IITP-Ezbaro] 비대면 본인확인을 위한 바이오 공개키 기반 구조 기술 개발(2차년도)
기 여 율 1/1
주관기관 한국전자통신연구원
연구기간 2017.01.01 ~ 2017.12.31

명 세 서

청구범위

청구항 1

암호키를 생성하는 방법에 있어서,

사용자 인증을 위한 적어도 하나 이상의 인증 정보가 입력됨을 수신하는 단계;

상기 수신된 적어도 하나 이상의 인증 정보를 멀티 모델로부터 분류하는 단계;

상기 멀티 모델로부터 상기 적어도 하나 이상의 인증 정보를 분류한 인덱스 결과를 해시함에 따라 해시 값을 획득하는 단계; 및

상기 획득된 해시 값을 기 생성된 퍼지 볼트 정보에 기반하여 키를 추출하는 단계

를 포함하는 암호키 생성 방법.

청구항 2

제1항에 있어서,

사용자의 생체 정보 및 사용자의 입력 정보에 기반하여 사용자 정보를 등록하는 단계

를 더 포함하고,

상기 사용자 정보를 등록하는 단계는,

상기 사용자의 생체 정보를 포함하는 다수의 사용자의 생체 정보를 이용하여 멀티 모델을 생성하고, 상기 멀티 모델로부터 분류 가능한 사용자에 대하여 각각의 인덱스를 부여하고, 상기 부여된 각각의 인덱스와 사용자의 입력 정보를 해시함에 따라 해시 값을 획득하는 단계

를 포함하는 암호키 생성 방법.

청구항 3

제2항에 있어서,

상기 사용자 정보를 등록하는 단계는,

상기 해시 값에 대한 좌표 값을 생성하는 단계

를 포함하고,

상기 좌표 값은, 상기 해시 값을 x값으로 갖는 좌표쌍들을 생성하고, 상기 x 값을 상기 해시 값 이외의 다른 값으로 갖는 노이즈 좌표쌍들을 생성하고, 상기 좌표쌍들과 상기 노이즈 좌표쌍들을 병합하여 퍼지 볼트를 생성하는

암호키 생성 방법.

청구항 4

제1항에 있어서,

상기 사용자 인증을 위한 적어도 하나 이상의 인증 정보가 입력됨을 수신하는 단계는,

상기 사용자 인증을 위한 인증용 생체 정보 및 인증용 입력 정보가 입력됨을 수신하는 단계

를 포함하는 암호키 생성 방법.

청구항 5

제1항에 있어서,

상기 수신된 적어도 하나 이상의 인증 정보를 멀티 모델로부터 분류하는 단계는,

상기 인증 정보로 입력된 인증용 생체 정보를 멀티 모델에 입력함에 따라 분류된 인증용 인덱스를 생성하는 단계

를 포함하고,

상기 멀티 모델로부터 상기 적어도 하나 이상의 인증 정보를 분류한 인덱스 결과를 해시함에 따라 해시 값을 획득하는 단계는,

상기 인증용 인덱스를 사용자의 입력 정보와 해시함에 따라 해시 값을 획득하는 단계

를 포함하는 암호키 생성 방법.

청구항 6

제1항에 있어서,

상기 획득된 해시 값을 기 생성된 퍼지 볼트 정보에 기반하여 키를 추출하는 단계는,

기 생성된 퍼지 볼트로부터 상기 인증용 인덱스를 상기 사용자의 입력 정보와 해시함에 따라 획득된 해시 값에 대응하는 좌표값을 선택하여 사용자 인증을 수행하고, 상기 인증이 완료됨에 따라 키를 복구하는 단계

를 포함하는 암호키 생성 방법.

청구항 7

암호키를 생성하는 시스템에 있어서,

컴퓨터 판독 가능한 명령을 저장하는 메모리; 및

상기 메모리에 저장된 명령을 실행하도록 구현되는 적어도 하나 이상의 프로세서를 포함하고,

상기 적어도 하나 이상의 프로세서는,

사용자 인증을 위한 적어도 하나 이상의 인증 정보가 입력됨을 수신하는 수신부;

상기 수신된 적어도 하나 이상의 인증 정보를 멀티 모델로부터 분류하는 분류부;

상기 멀티 모델로부터 상기 적어도 하나 이상의 인증 정보를 분류한 인덱스 결과를 해시함에 따라 해시 값을 획득하는 획득부; 및

상기 획득된 해시 값을 기 생성된 퍼지 볼트 정보에 기반하여 키를 추출하는 추출부

를 포함하는 암호키 생성 시스템.

발명의 설명

기 술 분 야

[0001] 아래의 설명은 생체정보와 사용자 입력 정보(예를 들면, 비밀번호, PIN)에 기반한 사용자 인증 및 정보 보호에 관한 것이다.

배 경 기 술

[0003] 이미지 분류하기 위하여 이미지 데이터로부터 특징 값들을 추출하는 방법이다. 이미지 특징 추출 방법은 크게 분류기(classifier)를 이용한 방법과, 이미지의 지역적 정보를 이용한 방법으로 나눌 수 있다. 분류기를 이용한 방법에는 PCA(Principal Component Analysis)나 LDA(Linear Discriminant Analysis) 종류의 통계적 분류 방법이 대표적이다. 이러한 방법은 일반적으로 훈련용 데이터를 통하여 분류기를 생성하고, 데이터를 분류기에 projection하여 특징 값들을 추출한다. 최근에는 딥러닝과 같은 다수의 레이어들을 가진 신경망 네트워크를 분류기로 생성하여 특징을 추출하기도 한다. 이미지의 지역적 정보를 이용한 방법으로는 LBP(Local Binary

Pattern), LFI(Local edge/corner Feature Integration)등과 같이, 이미지를 일정 크기로 분할하여 해당 구역의 히스토그램 분포 특성을 통하여 분류하는 방법이 있다.

[0004] 퍼지 볼트(Fuzzy Vault)는 바이오매트릭스 같이 일정하지 않은 데이터를 동일한 문자열(스트링)로 변환하기 위한 방법이다. Vault는 수많은 좌표 쌍들의 데이터를 가지고 있으며, 그 중 일부만이 실제 값이다. Fuzzy Vault 생성 시 k차의 다항식 $f(x) = c_0 + c_1x + c_2x^2 + \ldots + c_mx^m$ 을 생성하고, $(a, f(a)), a \in \mathbb{N}$ 인 정상적인 값들을 생성한다. 그 다음, $(b, y), y \neq f(b)$ 인 다수의 노이즈 좌표 값을 생성한 후, $(a, f(a))$를 포함시킨다. 다항식의 차수에 따라서 사용자가 일정 개수 이상의 실제 값인 $(a, f(a))$을 추출한다면 정상적인 $f(x)$를 복구할 수 있고, 다항식의 계수들을 나란히 붙여 항상 동일한 문자열을 생성할 수 있다. 사용자가 실제 좌표 값을 일정 개수 미만으로 골라냈다면 다항식을 복구할 수 없다.

[0005] Reed-solomon decoding은 이러한 Fuzzy Vault의 오류를 보정하기 위한 방법으로서, 사용자가 선택한 좌표값 중에 일부가 노이즈 좌표여도, 노이즈 좌표 개수가 일정 개수 이하면 정상적인 다항식을 복원할 수 있다.

[0006] 참고자료: KR 10-2018-0000849, KR 10-2011-0065139

발명의 내용

해결하려는 과제

[0008] 바이오매트릭스 데이터를 암호학 알고리즘에 적용할 수 있도록, 아날로그 데이터로부터 동일한 암호학적 키를 생성하기 위한 방법 및 시스템을 제공할 수 있다.

과제의 해결 수단

[0010] 암호키를 생성하는 방법은, 사용자 인증을 위한 적어도 하나 이상의 인증 정보가 입력됨을 수신하는 단계; 상기 수신된 적어도 하나 이상의 인증 정보를 멀티 모델로부터 분류하는 단계; 상기 멀티 모델로부터 상기 적어도 하나 이상의 인증 정보를 분류한 인덱스 결과를 해시함에 따라 해시 값을 획득하는 단계; 및 상기 획득된 해시 값을 기 생성된 퍼지 볼트 정보에 기반하여 키를 추출하는 단계를 포함할 수 있다.

[0011] 상기 암호키 생성 방법은, 사용자의 생체 정보 및 사용자의 입력 정보에 기반하여 사용자 정보를 등록하는 단계를 더 포함하고, 상기 사용자 정보를 등록하는 단계는, 상기 사용자의 생체 정보를 포함하는 다수의 사용자의 생체 정보를 이용하여 멀티 모델을 생성하고, 상기 멀티 모델로부터 분류 가능한 사용자에 대하여 각각의 인덱스를 부여하고, 상기 부여된 각각의 인덱스와 사용자의 입력 정보를 해시함에 따라 해시 값을 획득하는 단계를 포함할 수 있다.

[0012] 상기 사용자 정보를 등록하는 단계는, 상기 해시 값에 대한 좌표 값을 생성하는 단계를 포함하고, 상기 좌표 값은, 상기 해시 값을 x값으로 갖는 좌표쌍들을 생성하고, 상기 x 값을 상기 해시 값 이외의 다른 값으로 갖는 노이즈 좌표쌍들을 생성하고, 상기 좌표쌍들과 상기 노이즈 좌표쌍들을 병합하여 퍼지 볼트를 생성할 수 있다.

[0013] 상기 사용자 인증을 위한 적어도 하나 이상의 인증 정보가 입력됨을 수신하는 단계는, 상기 사용자 인증을 위한 인증용 생체 정보 및 인증용 입력 정보가 입력됨을 수신하는 단계를 포함할 수 있다.

[0014] 상기 수신된 적어도 하나 이상의 인증 정보를 멀티 모델로부터 분류하는 단계는, 상기 인증용 생체 정보를 멀티 모델에 입력함에 따라 분류된 인증용 인덱스를 생성하는 단계를 포함하고, 상기 멀티 모델로부터 상기 적어도 하나 이상의 인증 정보를 분류한 인덱스 결과를 해시함에 따라 해시 값을 획득하는 단계는, 상기 인증용 인덱스를 사용자의 입력 정보와 해시함에 따라 해시 값을 획득하는 단계를 포함할 수 있다.

[0015] 상기 획득된 해시 값을 기 생성된 퍼지 볼트 정보에 기반하여 키를 추출하는 단계는, 기 생성된 퍼지 볼트로부터 상기 인증용 인덱스를 상기 사용자의 입력 정보와 해시함에 따라 획득된 해시 값에 대응하는 좌표값을 선택하여 사용자 인증을 수행하고, 상기 인증이 완료됨에 따라 키를 복구하는 단계를 포함할 수 있다.

[0016] 암호키를 생성하는 시스템은, 컴퓨터 판독 가능한 명령을 저장하는 메모리; 및 상기 메모리에 저장된 명령을 실행하도록 구현되는 적어도 하나 이상의 프로세서를 포함하고, 상기 적어도 하나 이상의 프로세서는, 사용자 인증을 위한 적어도 하나 이상의 인증 정보가 입력됨을 수신하는 수신부; 상기 수신된 적어도 하나 이상의 인증 정보를 멀티 모델로부터 분류하는 분류부; 상기 멀티 모델로부터 상기 적어도 하나 이상의 인증 정보를 분류한 인덱스 결과를 해시함에 따라 해시 값을 획득하는 획득부; 및 상기 획득된 해시 값을 기 생성된 퍼지 볼트 정보에 기반하여 키를 추출하는 추출부를 포함할 수 있다.

발명의 효과

[0018] 일 실시예에 따른 암호키 생성 시스템은 아날로그 데이터인 생체 정보로부터 항상 일정한 암호학적 키를 생성하여 본인 인증에 사용할 수 있다. 생체 정보는 'What you are'에 해당하는 정보로 위조에 난이도가 있다. 1개의 분류기 혹은 검증을 요하는 방법보다 다수의 모델로부터 분류된 결과를 이용하기 때문에 타인 혹은 위조자가 통과하기 더욱 어렵다. 이에 따라 결과물인 암호학적 키를 이용하여 암호화나 공개키에 기반한 시스템에 적용이 가능하다.

[0019] 일 실시예에 따른 암호키 생성 시스템은 금융 거래에서 사용되는 전자 서명 또는 공개키 시스템으로 활용이 가능하다.

[0020] 일 실시예에 따른 암호키 생성 시스템은 다양한 종류의 생체 정보를 사용할 수 있다.

[0021] 일 실시예에 따른 암호키 생성 시스템은 사용자의 입력 정보와 사용자의 생체 정보를 결합함에 따라 종래의 PIN(혹은 패스워드)와 생체 정보 각각이 가지는 약한 보안성을 향상시킬 수 있다.

[0022] 일 실시예에 따른 암호키 생성 시스템은 Feature Extraction + Classification 방법의 적용이 가능하다.

[0023] 일 실시예에 따른 암호키 생성 시스템은 다수의 classifier(Model)을 사용하여 분류 오류를 감소시킬 수 있다.

[0024] 일 실시예에 따른 암호키 생성 시스템은 인덱스와 모델을 변경하여 사용자에게 새로운 키 부여(Key-binding Scheme)하는 것이 가능하다.

[0025] 일 실시예에 따른 암호키 생성 시스템은 키가 노출되어도 새로운 모델과 인덱스 정보를 생성하여 새로운 키를 부여할 수 있다.

도면의 간단한 설명

[0027] 도 1은 일 실시예에 따른 암호키 생성 시스템의 사용자 정보를 등록하는 과정을 설명하기 위한 흐름도이다.

도 2는 일 실시예에 따른 암호키 생성 시스템에서 멀티 모델을 생성하는 방법을 설명하기 위한 도면이다.

도 3은 일 실시예에 따른 암호키 생성 시스템에서 해시 값을 획득하는 방법을 설명하기 위한 도면이다.

도 4는 실시예에 따른 암호키 생성 시스템에서 퍼지 볼트를 생성하는 방법을 설명하기 위한 도면이다.

도 5는 일 실시예에 따른 암호키 생성 시스템의 사용자 인증 과정을 설명하기 위한 흐름도이다.

도 6은 일 실시예에 따른 암호키 생성 시스템에서 사용자의 인증용 생체 정보를 멀티 모델로부터 분류하는 방법을 설명하기 위한 도면이다.

도 7은 일 실시예에 따른 암호키 생성 시스템에서 인덱스 결과를 해시하고 퍼지 볼트를 탐색하는 방법을 설명하기 위한 도면이다.

도 8은 일 실시예에 따른 암호키 생성 시스템의 구성을 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0028] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0030] 아래의 실시예에서는 바이오 매트릭스와 퍼지 볼트를 이용하여 암호학적 키를 생성하는 방법에 대하여 설명하기로 한다. 다시 말해서, 얼굴 정보, 지문 정보 또는 홍채 정보 등과 같은 생체 정보와 사용자의 입력 정보(예를 들면, PIN)를 이용하여 암호학적 키를 생성할 수 있다. 이를 위하여 사용자 정보 등록 과정과 사용자 인증 과정이 수행될 수 있다.

[0031] 도 1은 일 실시예에 따른 암호키 생성 시스템의 사용자 정보를 등록하는 과정을 설명하기 위한 흐름도이다.

[0032] 암호키 생성 시스템은 사용자로부터 사용자의 생체 정보가 입력됨을 수신할 수 있다. 예를 들면, 사용자는 사용자 단말(예를 들면, 스마트 폰)을 통하여 사용자의 생체 정보 n(n은 자연수)개 $X_i = x_{i,}$와 입력 정보 pw_i를 암호키 생성 시스템(서버)로 전송하여 등록 과정을 수행할 수 있다.

[0033] 암호키 생성 시스템은 사용자로부터 입력된 사용자의 생체 정보에 기초하여 전처리 과정(110)을 수행한 뒤, 멀티 모델(120)을 생성할 수 있다. 전처리 과정은 입력된 정보인 사용자의 생체 정보와 모델의 특성에 기반하여 입력된 정보를 가공할 수 있다. 예를 들면, 입력된 정보가 얼굴 이미지일 경우, 명암 보정, 이목구비 크롭(crop)등을 수행할 수 있고, 지문 정보일 경우, 노이즈 제거, Wavelet-Filter 등을 수행할 수 있다. 실시예에서 기재된 사용자의 생체 정보란, 사용자가 고유하게 지니고 있는 정보로서, 예를 들면, 지문 정보, 얼굴 정보, 홍채 정보 등이 해당될 수 있다.

[0034] 암호키 생성 시스템은 사용자로부터 전송받은 생체 정보 X_i로부터 k(k는 자연수)개의 모델 $M_i^k\,(k \in \mathbb{N})$을 생성한다. 도 2를 참고하면, 멀티 모델을 생성하는 방법을 설명하기 위한 도면이다. 사용자의 생체 정보와 타인의 생체 정보를 이용하여 다수의 멀티 모델(M_i^k)을 생성할 수 있다. 이때, 각 모델 생성 시 사용되는 타인의 정보는 사용자의 본인이 아닌 임의의 사용자들의 정보로 구성될 수 있다. 구체적으로, 예를 들면, 한 개의 모델을 생성하기 위하여 적어도 하나 이상의 템플릿이 필요하다. 사용자의 템플릿은 전송받은 생체 정보 X_i로부터 생성할 수 있고, 나머지 템플릿은 암호키 생성 시스템에 저장되어 있는 템플릿을 사용할 수 있다. 동일한 과정으로, 총 k개의 모델 M_i^k을 생성할 수 있다. 이때, 생체 정보의 특성에 따라 다양한 분류 기법들을 모델 생성에 사용할 수 있다. 또한, 모델 생성 기법에 따라 모델들이 포함하는 데이터가 달라질 수 있으며, 모델의 개수와 각 모델에 포함되는 사용자의 수는 조정될 수 있다.

[0035] 암호키 생성 시스템은 생성된 멀티-모델로부터 분류 가능한 사용자에 대하여 각각의 인덱스를 부여하고, 부여된 각각의 인덱스와 사용자의 입력 정보를 해시함에 따라 해시 값을 획득할 수 있다(130). 이때, 사용자의 입력 정보는 사용자의 생체 정보를 입력하는 과정에서 입력 정보가 입력될 수 있고, 또는, 해시를 수행할 때 입력될 수도 있다. 도 3을 참고하면, 해시 값을 획득하는 방법을 설명하기 위한 도면이다. 멀티 모델로부터 분류될 수 있는 모든 사용자들에 대하여 고유한 인덱스들을 부여함에 따라 각 모델 안에서 등록할 사용자에게 부여된 인덱스를 a_i로 정의할 수 있다. 인덱스 a_i와 사용자의 입력 정보(예를 들면, PIN 번호) pw_i를 해시(hash)한 결과값(해시 값)을 h_i로 정의할 수 있다. 다시 말해서, 각 모델 M_i^k에서 특정 템플릿에 대응하는 위치(인덱스)값 a_i와 사용자의 입력 정보 pw_i를 해시 함수 *H*에 입력하여 결과값 h_i을 생성할 수 있다.

[0036] 이때, 모델 생성 시 고유한 결과값 h_i들이 도출될 수 있도록 설계될 수 있다. 사용자의 입력 정보란, 사용자가 전자 기기를 통하여 사용자를 인증하기 위한 패스워드 정보로서, 문자, 숫자, 기호, 위치 정보 등이 조합되어 기 설정된 자리 또는 기 설정된 길이로 구성될 수 있다. 예를 들면, 사용자의 입력 정보는 PIN, 패턴 정보 등이 해당될 수 있다.

[0037] 암호키 생성 시스템은 해시 값에 대한 좌표 값을 생성할 수 있다. 이때, 암호키 생성 시스템은 해시 값을 x 값으로 갖는 좌표쌍들을 생성하고, 해시 값이 아닌 노이즈 좌표쌍들을 생성하고, 좌표쌍들과 노이즈 좌표쌍들을 병합하여 퍼지 볼트를 생성할 수 있다(140). 도 4를 참고하면, 퍼지 볼트를 생성하는 방법을 설명하기 위한 도

면이다. 암호키 생성 시스템은 m차 다항식 $p(x)$를 임의로 생성할 수 있다. h_i를 x값으로 갖는 좌표쌍 $(h_i, p(h_i))$들을 생성할 수 있다. 실시예에서 h_i를 x값으로 갖는 좌표쌍 $(h_i, p(h_i))$을 정답 좌표라고 기재할 수 있다. 또한, x값이 h_i이 아닌 노이즈 좌표쌍 $(x, p(x))$들을 생성할 수 있다. 이때, 노이즈 좌표쌍은 정답 좌표를 감추기 위한 것으로 정답 좌표와 일치하지 않는 좌표쌍으로 생성될 수 있다. 노이즈 좌표쌍은 랜덤으로 생성될 수 있으며, 또는 사용자에 의하여 선택된 좌표쌍이 노이즈 좌표쌍으로 지정될 수도 있다. 암호키 생성 시스템은 정답 좌표(좌표쌍)과 노이즈 좌표쌍을 병합하여 퍼지 볼트를 생성할 수 있다. 사용자의 키는 $p(x)$의 계수들을 합쳐서 해시한 값을 의미할 수 있다. 사용자의 키는 $key = H(c_0, c_1, ..., c_m)$으로 암호키 생성 시스템에 key의 공개키인 pk_{key}를 저장할 수 있다.

[0038] 도 5는 일 실시예에 따른 암호키 생성 시스템의 사용자 인증 과정을 설명하기 위한 흐름도이다.

[0039] 암호키 생성 시스템은 사용자 인증을 위한 인증 정보가 입력됨을 수신할 수 있다. 암호키 생성 시스템은 인증용 생체 정보가 입력됨을 수신할 수 있다. 이때, 인증용 생체 정보가 입력됨과 동시에 인증용 입력 정보가 입력될 수 있고, 또는 인증용 생체 정보가 입력된 후에 추후에 인증용 입력 정보가 입력될 수도 있다. 암호키 생성 시스템은 사용자로부터 입력된 인증용 생체 정보에 대한 전처리 과정을 수행할 수 있다(510). 암호키 생성 시스템은 사용자의 인증용 생체 정보를 멀티 모델로부터 분류할 수 있다(520). 도 6을 참고하면, 사용자의 인증용 생체 정보를 멀티 모델로부터 분류하는 방법을 설명하기 위한 도면이다. 인증용 생체 정보를 멀티 모델 각각에 입력하여 분류된 인증용 인덱스 a'_i를 생성할 수 있다. 일례로, 로컬 환경에서 사용자는 사용자의 모델 M_i^k과 좌표쌍들을 포함하는 볼트 데이터를 저장하고 있을 수 있다. 예를 들면, 사용자가 새로운(인증용) 생체 정보와 새로운(인증용) 입력 정보를 입력할 경우, 새로운 생체 정보로부터 새로운 템플릿을 생성할 수 있다. 이때, 사용자의 모델 M_i^k 내에 존재하는 템플릿들 중 새로운 템플릿과 가장 유사한 템플릿을 탐색할 수 있다. 새로운 템플릿과 가장 유사한 템플릿 간의 거리를 계산한 후, 통계적으로 가장 작은 거리 차이를 갖는 템플릿을 새로운 생체 정보에서 갖는 인증용 인덱스 값을 a'_i로 정의할 수 있다.

[0040] 암호키 생성 시스템은 멀티 모델에 기반하여 인증용 생체 정보를 분류한 인덱스 결과를 해시함에 따라 결과값(해시 값)을 획득할 수 있다(530). 암호키 생성 시스템은 획득된 해시 값을 기 생성된 퍼지 볼트 정보에 기반하여 키를 추출할 수 있다(540). 도 7을 참고하면, 인덱스 결과를 해시하고 퍼지 볼트를 탐색하는 방법을 설명하기 위한 도면이다. 암호키 생성 시스템은 인증용 인덱스 a'_i를 사용자의 입력 정보(예를 들면, PIN 번호)와 해시한 결과값을 h'_i로 정의할 수 있다. 암호키 생성 시스템은 결과값 h'_i을 이용하여 퍼지 볼트 내의 좌표들 중에서 정답으로 추측되는 좌표들을 선별할 수 있다. 암호키 생성 시스템은 퍼지 볼트 내에서 $(h'_k, p'(h'_k))$인 값들을 선택할 수 있다. 다시 말해서, 암호키 생성 시스템은 퍼지 볼트 내에서 h'_i에 대응하는 좌표쌍을 선택할 수 있다. 이때, RS 디코딩(Reed-Solomon Decoding)을 거쳐 다항식 계수를 복구할 수 있다. 또한, 다항식 계수를 복구함에 따라 키를 추출할 수 있다.

[0041] 암호키 생성 시스템은 퍼지 볼트 내에서 정답인 $(h'_k, p'(h'_k))$ 좌표가 일정 개수 이상일 경우, RS 디코딩(Reed-Solomon Decoding)이 오류를 보정하여 키를 생성할 수 있다. 또한, 정답인 좌표가 일정 개수 미달일 경우, 정상적인 다항식의 계수를 획득할 수 없게 된다. 또한, 등록된 사용자의 입력 정보가 아닌 틀린/다른 입력 정보가 입력되었을 경우에도, 다항식의 계수를 획득할 수 없다.

[0042] 도 8은 일 실시예에 따른 암호키 생성 시스템의 구성을 설명하기 위한 블록도이다.

[0043] 암호키 생성 시스템(100)의 프로세서는 수신부(810), 분류부(820), 획득부(830) 및 추출부(840)를 포함할 수 있다. 또한, 암호키 생성 시스템(100)는 사용자의 생체 정보 및 사용자의 입력 정보에 기반하여 사용자 정보를 등록하는 등록부(도시되지 않음)를 더 포함할 수 있다. 이러한 프로세서의 구성요소들은 암호키 생성 시스템에 저장된 프로그램 코드가 제공하는 제어 명령에 따라 프로세서에 의해 수행되는 서로 다른 기능들(different functions)의 표현들일 수 있다. 이때, 프로세서 및 프로세서의 구성요소들은 메모리가 포함하는 운영체제의 코드와 적어도 하나의 프로그램의 코드에 따른 명령(instruction)을 실행하도록 구현될 수 있다.

[0044] 등록부는 사용자의 생체 정보 및 사용자의 입력 정보에 기반하여 사용자 정보를 등록할 수 있다. 등록부는 사용자의 생체 정보를 포함하는 다수의 사용자의 생체 정보를 이용하여 멀티 모델을 생성하고, 생성된 멀티 모델로부터 분류 가능한 사용자에 대하여 각각의 인덱스를 부여하고, 부여된 각각의 인덱스와 사용자의 입력 정보를 해시함에 따라 해시 값을 획득할 수 있다. 등록부는 해시 값에 대한 좌표 값을 생성할 수 있다. 이때, 등록부는 좌표 값은 해시 값을 x 값으로 갖는 좌표쌍들을 생성하고, x값을 해시 값 이외의 다른 값으로 갖는 노이즈 좌표쌍들을 생성하고, 좌표쌍들과 노이즈 좌표쌍들을 병합하여 퍼지 볼트를 생성할 수 있다.

[0045] 수신부(810)는 사용자 인증을 위한 적어도 하나 이상의 인증 정보가 입력됨을 수신할 수 있다. 수신부(810)는 사용자의 인증용 생체 정보 및 인증용 입력 정보가 입력됨을 수신할 수 있다.

[0046] 분류부(820)는 수신된 적어도 하나 이상의 인증 정보를 멀티 모델로부터 분류할 수 있다. 분류부(820)는 인증 정보로 입력된 인증용 생체 정보를 멀티 모델에 입력함에 따라 분류된 인증용 인덱스를 생성할 수 있다.

[0047] 획득부(830)는 멀티 모델로부터 적어도 하나 이상의 인증 정보를 분류한 인덱스 결과를 해시함에 따라 해시 값을 획득할 수 있다. 획득부(830)는 인증용 인덱스를 사용자의 입력 정보와 해시함에 따라 해시 값을 획득할 수 있다.

[0048] 추출부(840)는 획득된 해시 값을 기 생성된 퍼지 볼트 정보에 기반하여 키를 추출할 수 있다. 추출부(840)는 기 생성된 퍼지 볼트로부터 인증용 인덱스를 사용자의 입력 정보와 해시함에 따라 획득된 해시 값에 대응하는 좌표값을 선택하여 사용자 인증을 수행하고, 인증이 완료됨에 따라 키를 복구할 수 있다.

[0049] 이에 따라 최근 금융권에서 바이오 매트릭스를 이용하는 바이오 인증 기능을 확대하는 상황에서, 금융 거래에서 사용되는 전자 서명 또는 공개키 시스템으로 활용이 가능하다.

[0050] 일 실시예에 따른 암호키 생성 시스템은 아날로그 데이터인 생체 정보로부터 항상 일정한 암호학적 키를 생성하여 본인 인증에 사용할 수 있다. 생체 정보는 'What you are'에 해당하는 정보로 위조에 난이도가 있다. 1개의 분류기 혹은 검증을 요하는 방법보다 다수의 모델로부터 분류된 결과를 이용하기 때문에 타인 혹은 위조자가 통과하기 더욱 어렵다. 이에 따라 결과물인 암호학적 키를 이용하여 암호화나 공개키에 기반한 시스템에 적용이 가능하다.

[0051] 일 실시예에 따른 암호키 생성 시스템은 다양한 종류의 생체 정보를 사용할 수 있다.

[0052] 일 실시예에 따른 암호키 생성 시스템은 사용자의 입력 정보와 사용자의 생체 정보를 결합함에 따라 종래의 PIN(혹은 패스워드)와 생체 정보 각각이 가지는 약한 보안성을 향상시킬 수 있다.

[0053] 일 실시예에 따른 암호키 생성 시스템은 Feature Extraction + Classification 방법의 적용이 가능하다.

[0054] 일 실시예에 따른 암호키 생성 시스템은 다수의 classifier(Model)을 사용하여 분류 오류를 감소시킬 수 있다(앙상블 기법).

[0055] 일 실시예에 따른 암호키 생성 시스템은 인덱스와 모델을 변경하여 사용자에게 새로운 키 부여하는 것이 가능(Key-binding Scheme)하다.

[0056] 일 실시예에 따른 암호키 생성 시스템은 키가 노출되어도 새로운 모델과 인덱스 정보를 생성하여 새로운 키를 부여할 수 있다.

[0057] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/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 이상

의 소프트웨어 애플리케이션을 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.

[0058] 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(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

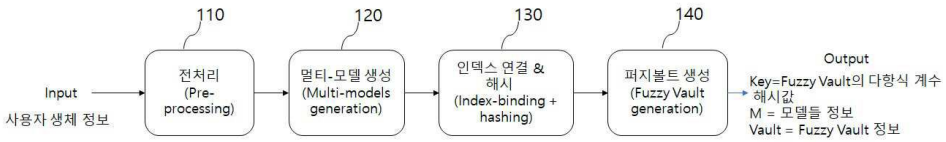
[0059] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(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 수행하도록 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.

[0060] 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.

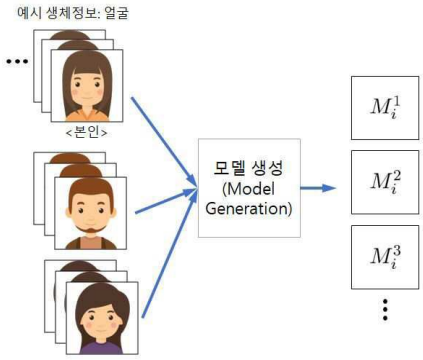
[0061] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

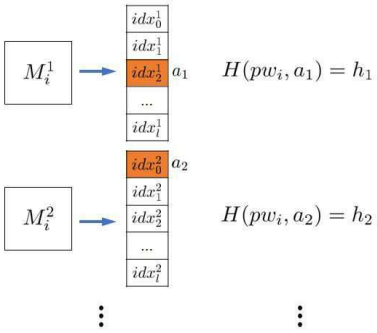
도면1



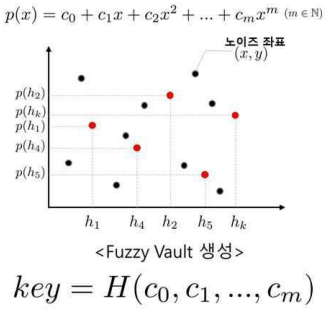
도면2



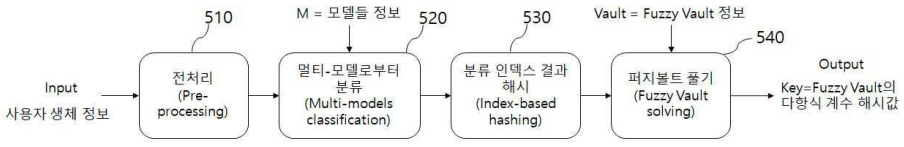
도면3



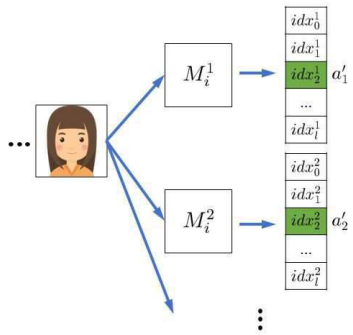
도면4



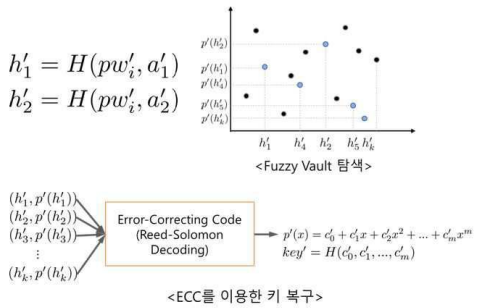
도면5



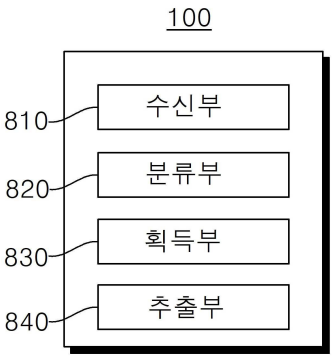
도면6


M_i^1
M_i^2
idx_0^1
idx_1^1
idx_2^1
idx_l^1
a'_1
idx_0^2
idx_1^2
idx_2^2
idx_l^2
a'_2

도면7


$h'_1 = H(pw'_i, a'_1)$
$h'_2 = H(pw'_i, a'_2)$
<Fuzzy Vault 탐색>
Error-Correcting Code (Reed-Solomon Decoding)
$p'(x) = c'_0 + c'_1 x + c'_2 x^2 + ... + c'_m x^m$
$key' = H(c'_0, c'_1, ..., c'_m)$
<ECC를 이용한 키 복구>

도면8


100
수신부
분류부
획득부
추출부
810
820
830
840