



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년08월06일
(11) 등록번호 10-2008101
(24) 등록일자 2019년07월31일

(51) 국제특허분류(Int. Cl.)
G06F 21/32 (2013.01) G06F 21/60 (2013.01)
G06F 21/62 (2013.01) H04L 9/08 (2006.01)
(52) CPC특허분류
G06F 21/32 (2013.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2018-0074964
(22) 출원일자 2018년06월28일
심사청구일자 2018년06월28일
(56) 선행기술조사문헌
JP2010039890 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
이문규
경기도 부천시 계남로 81, 2222동 702호(상동, 진달래마을)
임중혁
경기도 수원시 권선구 서수원로 589, 302동 503호(금곡동, 삼익3차아파트)
(74) 대리인
양성보

전체 청구항 수 : 총 8 항

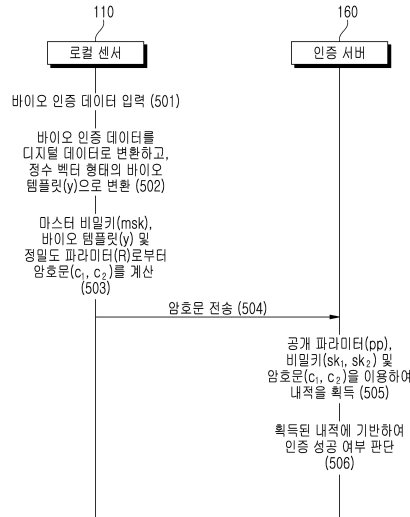
심사관 : 문남두

(54) 발명의 명칭 함수 암호를 이용한 안전한 바이오 인증 방법

(57) 요약

함수 암호를 이용한 안전한 바이오 인증 방법이 개시된다. 일 실시예에 따른 인증 서버에서 수행되는 인증 방법은, 로컬 센서에 입력된 사용자의 바이오 데이터를 등록하는 단계; 및 상기 로컬 센서에 입력된 바이오 인증 데이터를 적어도 하나 이상의 계산 방법을 조합하여 계산함에 따라 사용자의 바이오 인증 데이터를 인증하는 단계를 포함할 수 있다.

대표도 - 도5



(52) CPC특허분류

G06F 21/62 (2013.01)

H04L 9/0819 (2013.01)

H04L 9/0852 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711067718

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보보호핵심원천기술개발(R&D)

연구과제명 차세대 인증 기술 개발

기 여 율 1/1

주관기관 연세대학교 산학협력단

연구기간 2017.04.01 ~ 2019.12.31

명세서

청구범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

인증 서버에서 수행되는 인증 방법에 있어서,

로컬 센서에 입력된 사용자의 바이오 데이터를 함수 암호의 비밀키로 등록하는 단계; 및

상기 로컬 센서에 입력된 바이오 인증 데이터에 기반하여 계산된 암호문을 적어도 하나 이상의 계산 방법을 조합하여 복호화함에 따라 사용자의 바이오 인증 데이터를 인증하는 단계

를 포함하고,

상기 사용자의 바이오 데이터를 등록하는 단계는,

상기 로컬 센서에 입력된 사용자의 바이오 데이터로부터 변환된 바이오 템플릿(x)과 키 분배 서버의 마스터 비밀키를 이용하여 생성된 비밀키(sk_1 , sk_2)를 저장하여 사용자의 바이오 데이터를 등록하는 단계

를 포함하는 인증 방법.

청구항 5

제4항에 있어서,

상기 사용자의 바이오 데이터를 등록하는 단계는,

상기 로컬 센서에서 상기 바이오 데이터가 정수 형태의 바이오 템플릿(x)로 변환되고, 상기 바이오 데이터의 바이오 템플릿이 정밀도 파라미터(Q , S)를 이용하여 양자화된 바이오 템플릿(x'_1 , x'_2)이 계산됨에 따라 상기 키 분배 서버에서 마스터 비밀키(msk)와 상기 양자화된 바이오 템플릿(x'_1 , x'_2)를 이용하여 생성된 비밀키(sk_1 , sk_2)를 저장하는 단계

를 포함하는 인증 방법.

청구항 6

인증 서버에서 수행되는 인증 방법에 있어서,

로컬 센서에 입력된 사용자의 바이오 데이터를 함수 암호의 비밀키로 등록하는 단계; 및

상기 로컬 센서에 입력된 바이오 인증 데이터에 기반하여 계산된 암호문을 적어도 하나 이상의 계산 방법을 조합하여 복호화함에 따라 사용자의 바이오 인증 데이터를 인증하는 단계

를 포함하고,

상기 사용자의 바이오 인증 데이터를 인증하는 단계는,

상기 로컬 센서에 입력된 바이오 인증 데이터에 기반하여 변환된 1)바이오 템플릿(y), 키 분배 서버의 마스터

비밀키(msk) 및 정밀도 파라미터(R) 또는 2)상기 바이오 템플릿(y)과 상기 마스터 비밀키(msk) 중 어느 하나를 이용하여 상기 로컬 센서에서 암호문을 계산하고, 상기 인증 서버가 상기 계산된 암호문을 상기 함수 암호의 비밀키(sk_1 , sk_2)를 이용하여 복호화함에 따라 상기 바이오 데이터에 기반하여 변환된 바이오 템플릿 및 상기 바이오 인증 데이터에 기반하여 변환된 바이오 템플릿의 내적 계산을 수행하는 단계를 포함하는 인증 방법.

청구항 7

제6항에 있어서,

상기 사용자의 바이오 인증 데이터를 인증하는 단계는,

상기 로컬 센서에서 상기 바이오 인증 데이터가 정수 형태의 바이오 템플릿(y)으로 변환되고, 1)상기 마스터 비밀키(msk), 상기 바이오 인증 데이터의 바이오 템플릿(y) 및 정밀도 파라미터(R) 또는 2)상기 마스터 비밀키(msk)와 상기 바이오 인증 데이터의 바이오 템플릿(y) 중 어느 하나를 이용하여 계산된 암호문(c_1 , c_2)을 수신하는 단계

를 포함하는 인증 방법.

청구항 8

제7항에 있어서,

상기 사용자의 바이오 인증 데이터를 인증하는 단계는,

공개 파라미터, 비밀키(sk_1 , sk_2) 및 상기 암호문을 이용하여 어느 하나의 바이오 데이터의 양자화된 바이오 템

플릿(x'_1)과 상기 바이오 인증 데이터의 양자화된 바이오 템플릿(y')의 내적(r_1)을 획득하는 단계

를 포함하는 인증 방법.

청구항 9

제7항에 있어서,

상기 사용자의 바이오 인증 데이터를 인증하는 단계는,

공개 파라미터, 비밀키(sk_1 , sk_2) 및 상기 암호문을 이용하여 다른 하나의 바이오 데이터의 양자화된 바이오 템

플릿(x'_2)과 상기 바이오 인증 데이터의 바이오 템플릿(y)의 내적(r_2)을 획득하는 단계

를 포함하는 인증 방법.

청구항 10

제8항 또는 제9항 중 어느 한 항에 있어서,

상기 사용자의 바이오 인증 데이터를 인증하는 단계는,

상기 획득된 내적을 적어도 하나 이상의 코사인 유사도 계산 방법의 OR 조건, AND 조건 및 가중치 조건 중 어느 하나에 기반하여 인증 성공 여부를 판단하는 단계를 포함하고,

상기 OR 조건은, $QR - T_1 < r_1 \leq QR$ 또는 $S - T_2 < r_2 \leq S + T_3$ 이고,

상기 AND 조건은, $QR - T_1 < r_1 \leq QR$ 그리고 $S - T_2 < r_2 \leq S + T_3$ 이고,

상기 가중치 조건은, $(a \times QR + b \times S) - T_4 < a \times r_1 + b \times r_2 \leq (a \times QR + b \times S) + T_5$ 인

것을 특징으로 하는 인증 방법.

청구항 11

인증 서버에 있어서,

로컬 센서에 입력된 사용자의 바이오 데이터를 함수 암호의 비밀키로 등록하는 등록부; 및

상기 로컬 센서에 입력된 바이오 인증 데이터에 기반하여 계산된 암호문을 적어도 하나 이상의 계산 방법을 조합하여 복호화함에 따라 사용자의 바이오 인증 데이터에 대한 인증을 수행하는 인증부

를 포함하고,

상기 등록부는,

상기 로컬 센서에 입력된 사용자의 바이오 데이터로부터 변환된 바이오 템플릿(x)과 키 분배 서버의 마스터 비밀키를 이용하여 생성된 비밀키(sk_1 , sk_2)를 저장하여 사용자의 바이오 데이터를 등록하는

인증 서버.

발명의 설명

기술 분야

[0001] 아래의 설명은 보안 기술에 관한 것으로, 바이오 데이터의 인증 방법에 관한 것이다.

배경 기술

[0003] 사용자 인증은 특정 시스템(예를 들면, 컴퓨터, 웹 서버, 스마트 폰 등)에 접근을 시도하는 사용자가 접근 권한이 있는지를 확인하여 접근을 허용하는 일련의 절차로서, 패스워드나 개인식별번호를 이용한 지식 기반 인증, 지문이나 홍채, 얼굴 등 신체 정보를 이용한 바이오 인증, 카드나 동글 등 하드웨어를 이용한 소유 기반 인증 등이 이용되고 있다. 이 중 바이오 인증은 그 편의성으로 인해 점차 많은 곳에서 활용되고 있으나, 안전성 측면에서 한 가지 문제점을 가지고 있다. 지식 기반 인증에서 패스워드 유출 시에는 패스워드를 교체하면 되며, 소유 기반 인증에서도 인증용 하드웨어의 도난 또는 분실 시에는 새로운 하드웨어로 대체하면 되지만, 바이오 데이터 유출 시에는 적절한 대응 방안이 없기 때문이다. 따라서, 바이오 인증에서는 지문, 홍채 등 바이오 데이터 원본을 시스템에서 안전하게 관리하는 것이 다른 종류의 인증에 비해 더 중요하다.

[0004] 이러한 문제에 대한 대안으로, 바이오 데이터를 로컬 시스템보다는 좀더 안전하게 관리되는 원격 서버에 저장하는 클라우드 형태의 개선 방안이 널리 고려되고 있다. 다만, 이 경우에는 원격 클라우드 서버가 바이오 데이터를 무단으로 활용할 가능성을 배제할 수 없으므로, 클라우드 서버에 바이오 데이터를 원본(예를 들면, 홍채의 비트맵 이미지)이 아닌 변환된 형태로 저장하도록 하는 것이 바람직하다. 이 경우 클라우드 서버가 데이터를 악용하려고 시도하여도 해당 데이터는 바이오 데이터 원본이 아닌 변환된 형태이므로 유출 시 쓸모가 없게 된다.

[0005] 참고문헌: [1] Jong-Hyuk Im, JinChun Choi, DaeHun Nyang and Mun-Kyu Lee, "Privacy-Preserving Palm Print Authentication Using Homomorphic Encryption," 2nd Intl Conf on Big Data Intelligence and Computing (DataCom) 2016, pp. 878-881, 2016.

[0006] [2] Sam Kim, Kevin Lewi, Avradip Mandal, Hart William Montgomery, Arnab Roy and David J. Wu, "Function-Hiding Inner Product Encryption is Practical", IACR Cryptology ePrint Archive, 2016:440, 2016.

발명의 내용

해결하려는 과제

[0008] 본 발명은 함수 암호(functional encryption) 기술을 이용하여 안전한 바이오 인증을 수행하는 방법을 제공할 수 있다

과제의 해결 수단

- [0010] 인증 서버에서 수행되는 인증 방법은, 로컬 센서에 입력된 사용자의 바이오 데이터를 등록하는 단계; 및 상기 로컬 센서에 입력된 바이오 인증 데이터를 적어도 하나 이상의 계산 방법을 조합하여 계산함에 따라 사용자의 바이오 인증 데이터를 인증하는 단계를 포함할 수 있다.
- [0011] 상기 사용자의 바이오 데이터를 등록하는 단계는, 상기 로컬 센서에 입력된 사용자의 바이오 데이터를 함수 암호의 비밀키로 등록하는 단계를 포함할 수 있다.
- [0012] 상기 사용자의 바이오 인증 데이터를 인증하는 단계는, 상기 로컬 센서에 입력된 바이오 인증 데이터에 기반하여 계산된 암호문을 적어도 하나 이상의 계산 방법을 조합하여 복호화함에 따라 사용자의 바이오 인증 데이터를 인증하는 단계를 포함할 수 있다.
- [0013] 상기 사용자의 바이오 데이터를 등록하는 단계는, 상기 로컬 센서에 입력된 사용자의 바이오 데이터로부터 변환된 바이오 템플릿(x)과 키 분배 서버의 마스터 비밀키를 이용하여 생성된 비밀키(sk_1, sk_2)를 저장하여 사용자의 바이오 데이터를 등록하는 단계를 포함할 수 있다.
- [0014] 상기 사용자의 바이오 데이터를 등록하는 단계는, 상기 로컬 센서에서 상기 바이오 데이터가 정수 형태의 바이오 템플릿(x)로 변환되고, 상기 바이오 데이터의 바이오 템플릿이 정밀도 파라미터(Q, S)를 이용하여 양자화된 바이오 템플릿(x'_1, x'_2)이 계산됨에 따라 상기 키 분배 서버에서 마스터 비밀키(msk)와 상기 양자화된 바이오 템플릿(x'_1, x'_2)를 이용하여 생성된 비밀키(sk_1, sk_2)를 저장하는 단계를 포함할 수 있다.
- [0015] 상기 사용자의 바이오 인증 데이터를 인증하는 단계는, 상기 로컬 센서에 입력된 바이오 인증 데이터에 기반하여 변환된 1)바이오 템플릿(y), 상기 마스터 비밀키(msk) 및 정밀도 파라미터(R) 또는 2)상기 바이오 템플릿(y)과 상기 마스터 비밀키(msk) 중 어느 하나를 이용하여 상기 로컬 센서에서 계산된 암호문을 이용하여 상기 바이오 데이터에 기반하여 변환된 바이오 템플릿 및 상기 바이오 인증 데이터에 기반하여 변환된 바이오 템플릿의 내적 계산을 수행하는 단계를 포함할 수 있다.
- [0016] 상기 사용자의 바이오 인증 데이터를 인증하는 단계는, 상기 로컬 센서에서 상기 바이오 인증 데이터가 정수 형태의 바이오 템플릿(y)으로 변환되고, 1)상기 마스터 비밀키(msk), 상기 바이오 인증 데이터의 바이오 템플릿(y) 및 정밀도 파라미터(R) 또는 2)상기 마스터 비밀키(msk)와 상기 바이오 인증 데이터의 바이오 템플릿(y) 중 어느 하나를 이용하여 계산된 암호문(c_1, c_2)을 수신하는 단계를 포함할 수 있다.
- [0017] 상기 사용자의 바이오 인증 데이터를 인증하는 단계는, 공개 파라미터, 상기 비밀키 및 상기 암호문을 이용하여 어느 하나의 바이오 데이터의 양자화된 바이오 템플릿(x'_1)과 상기 바이오 인증 데이터의 양자화된 바이오 템플릿(y')의 내적(r_1)을 획득하는 단계를 포함할 수 있다.
- [0018] 상기 사용자의 바이오 인증 데이터를 인증하는 단계는, 공개 파라미터, 상기 비밀키 및 상기 암호문을 이용하여 다른 하나의 바이오 데이터의 양자화된 바이오 템플릿(x'_2)과 상기 바이오 인증 데이터의 바이오 템플릿(y)의 내적(r_2)을 획득하는 단계를 포함할 수 있다.
- [0019] 상기 사용자의 바이오 인증 데이터를 인증하는 단계는, 상기 획득된 내적을 적어도 하나 이상의 코사인 유사도 계산 방법의 OR 조건, AND 조건 및 가중치 조건 중 어느 하나에 기반하여 인증 성공 여부를 판단하는 단계를 포함하고, 상기 OR 조건은, $QR - T_1 < r_1 \leq QR$ 또는 $S - T_2 < r_2 \leq S + T_3$ 이고,
- [0020] 상기 AND 조건은, $QR - T_1 < r_1 \leq QR$ 그리고 $S - T_2 < r_2 \leq S + T_3$ 이고, 상기 가중치 조건은, $(a \times QR + b \times S) - T_4 < a \times r_1 + b \times r_2 \leq (a \times QR + b \times S) + T_5$ 일 수 있다.
- [0021] 인증 서버는, 로컬 센서에 입력된 사용자의 바이오 데이터를 등록하는 등록부; 및 상기 로컬 센서에 입력된 바이오 인증 데이터를 적어도 하나 이상의 계산 방법을 조합하여 계산함에 따라 사용자의 바이오 인증 데이터에

대한 인증을 수행하는 인증부를 포함할 수 있다.

발명의 효과

- [0023] 본 발명은 암호문 사이의 연산 결과가 평문으로 도출되는 함수 암호를 이용함으로써 간편하고 빠르게 바이오 인증을 수행할 수 있다.
- [0024] 본 발명은 벡터 내적의 계산이 가능한 변형된 코사인 유사도 계산 방법을 통하여 내적 함수 암호에 기반한 바이오 템플릿 간 거리를 측정할 수 있어 다양한 바이오 인증 분야에 적용할 수 있다.
- [0025] 본 발명은 변형된 코사인 유사도 계산 방법을 조합하여 보다 정확한 바이오 인증을 수행할 수 있다.

도면의 간단한 설명

- [0027] 도 1은 일 실시예에 따른 네트워크 환경의 예를 도시한 도면이다.
- 도 2는 일 실시예에 따른 인증 시스템의 구성을 설명하기 위한 블록도이다.
- 도 3은 일 실시예에 따른 인증 시스템의 인증 방법을 설명하기 위한 흐름도이다.
- 도 4는 일 실시예에 따른 인증 시스템에서 바이오 데이터 등록 방법을 설명하기 위한 도면이다.
- 도 5는 일 실시예에 따른 인증 시스템에서 바이오 데이터의 인증 방법을 설명하기 위한 도면이다.
- 도 6은 일 실시예에 따른 인증 시스템에서 인증 성공 여부를 판단하는 방법을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0028] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.
- [0030] 함수 암호(functional encryption)란 평문(plaintext) m 에 대한 암호문과 함수 f 에 대한 비밀키가 해독기(decryptor)에 주어지면, 해독기가 해당 비밀키를 이용해 암호문으로부터 $f(m)$ 을 계산할 수 있는 암호이다.
- 예를 들어, 함수 $f(x) = ax + b$ (a, b 는 정수)에 대한 함수 암호는 평문 m 의 암호문 $E(m)$ 및 f 에 대한 비밀키 K 가 주어질 때 복호화 연산 $D_K(E(m)) = f(m) = a \times m + b$ 를 만족하는 암호이다. 단, K 를 보유한 측은 암호문에 대해 함수 f 에 대한 결과만을 복호화할 뿐, 다른 복호화는 불가능한 특성이 있다. 실시예에서는 내적 계산을 수행하는 함수 암호를 활용하는데, [2]에 따르면 이는 다음과 같은 기능들로 구성된다.
- [0031] (1) 초기 설정(setup) 작업: 주어진 안전성 요구조건(안전성 파라미터 L)을 만족하는 공개 파라미터(pp), 마스터 비밀키(msk)를 생성한다. 다시 말해서, $(pp, msk) = setup(L)$
- [0032] (2) 키 생성(keygen) 작업: 마스터 비밀키(msk)와 입력 벡터(x)로부터 비밀키(sk)를 생성한다. 즉, $sk = keygen(msk, x)$
- [0033] (3) 암호화(encrypt) 작업: 마스터 비밀키(msk)와 벡터(y)로부터 암호문(c)을 계산한다. 즉, $c = encrypt(msk, y)$
- [0034] (4) 복호화(decrypt) 작업: 공개 파라미터(pp)와 비밀키(sk), 암호문(c)로부터 입력 벡터(x)와 벡터(y)의 내적을 계산한다. 즉, $r = decrypt(pp, sk, c)$ 로 계산된 결과에 대해 $r = x \cdot y$ 가 만족된다.
- [0035] 도 1은 일 실시예에 따른 네트워크 환경의 예를 도시한 도면이다.
- [0036] 도 1의 네트워크 환경은 복수의 전자 기기들(110, 120, 130, 140), 복수의 서버들(150, 160) 및 네트워크(170)를 포함하는 예를 나타내고 있다. 이러한 도 1은 발명의 설명을 위한 일례로 전자 기기의 수나 서버의 수가

도 1과 같이 한정되는 것은 아니다.

[0037] 복수의 전자 기기들(110, 120, 130, 140)은 컴퓨터 장치로 구현되는 고정형 단말이거나 이동형 단말일 수 있다. 복수의 전자 기기들(110, 120, 130, 140)의 예를 들면, 스마트폰(smart phone), 휴대폰, 네비게이션, 컴퓨터, 노트북, 디지털방송용 단말, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 태블릿 PC 등이 있다. 일례로 전자 기기 1(110)은 무선 또는 유선 통신 방식을 이용하여 네트워크(170)를 통해 다른 전자 기기들(120, 130, 140) 및/또는 서버(150, 160)와 통신할 수 있다. 실시예에서는 전자 기기는 얼굴 인식, 지문 인식, 홍채 인식 등 사용자의 바이오 데이터를 인식하기 위한 카메라, 센서 기능이 탑재된 기기일 수 있다.

[0038] 통신 방식은 제한되지 않으며, 네트워크(170)가 포함할 수 있는 통신망(일례로, 이동통신망, 유선 인터넷, 무선 인터넷, 방송망)을 활용하는 통신 방식뿐만 아니라 기기들간의 근거리 무선 통신 역시 포함될 수 있다. 예를 들어, 네트워크(170)는, PAN(personal area network), LAN(local area network), CAN(campus area network), MAN(metropolitan area network), WAN(wide area network), BBN(broadband network), 인터넷 등의 네트워크 중 하나 이상의 임의의 네트워크를 포함할 수 있다. 또한, 네트워크(170)는 버스 네트워크, 스타 네트워크, 링 네트워크, 메쉬 네트워크, 스타-버스 네트워크, 트리 또는 계층적(hierarchical) 네트워크 등을 포함하는 네트워크 토폴로지 중 임의의 하나 이상을 포함할 수 있으나, 이에 제한되지 않는다.

[0039] 서버(150, 160) 각각은 복수의 전자 기기들(110, 120, 130, 140)과 네트워크(170)를 통해 통신하여 명령, 코드, 파일, 콘텐츠, 서비스 등을 제공하는 컴퓨터 장치 또는 복수의 컴퓨터 장치들로 구현될 수 있다.

[0040] 아래의 실시예에서는 전자 기기(110)는 사용자로부터 입력되는 바이오 데이터를 인식하는 로컬 센서, 서버(150)는 키 생성 서버, 서버(160)는 인증 서버를 의미할 수 있다. 이에, 로컬 센서, 키 생성 서버 및 인증 서버간의 바이오 데이터 등록 과정 및 바이오 데이터 인증 과정을 설명하기로 한다.

[0041] 일반적인 바이오 인증에서는 사용자 등록 당시 인식된 바이오 데이터를 벡터 형태의 템플릿 x 으로 변환하여 저장하고, 추후 사용자 인증에서는 같은 방식으로 바이오 데이터를 인식하여 템플릿 y 를 구성한 후 x 와 y 의 유클리드 거리를 측정하는 방식으로 매칭을 수행한다. 이때, 바이오 데이터는 인식 시마다 약간의 오차가 생겨 정확히 동일한 벡터로 만들어지지 않는으나, x 와 y 가 동일한 사용자의 바이오 데이터로부터 생성된 벡터라면 차이가 매우 작을 것이기 때문에 x 와 y 의 유클리드 거리는 매우 작게 된다. 반면, 다른 사람의 바이오 데이터로부터 생성된 템플릿은 유클리드 거리가 크다. 이에 따라, 경계값(threshold) T 를 적절히 정하고, 두 템플릿 벡터의 거리가 T 보다 작으면 동일 사용자로 인식하는 방식이 널리 이용된다.

[0042] 실시예에서는 바이오 인증의 매칭 점수 계산을 위한 새로운 기준으로, 유클리드 거리를 대체할 수 있는 변형된 코사인 유사도(modified cosine similarity)를 제안하기로 한다. 먼저, 두 벡터 x, y 에 대해 $|x|, |y|$ 를 두 벡터의 크기라 하고, 두 벡터 사이의 내각을 θ 라 하면, 내적과 내각 사이에는 $x \cdot y = |x||y|\cos\theta$,

[0043] 다시 말해서, 식 A:

$$\cos\theta = \left(\frac{x}{|x|}\right) \cdot \left(\frac{y}{|y|}\right)$$

[0044]

[0045]의 관계가 성립하므로, x, y 가 동일한 또는 유사한(거의 같은) 벡터라면 $\cos\theta \approx 1$ 이다. 따라서, 유클리드

거리를 측정하는 대신 x 와 y 를 정규화(normalization)한 두 템플릿 벡터 $\frac{x}{|x|}$ 와 $\frac{y}{|y|}$ 간의 내적을 이용하여 코사인 값을 계산함으로써 1에 가까울 경우 인증에 성공하도록 하는 사용자 인증을 수행할 수 있다. 이는 기존에 여러 특성(attribute)을 가지는 데이터들 간의 유사도를 판별하기 위해 많이 이용하는 코사인 유사도에 기반한 방법이다.

[0046] 그러나, 식 A를 이용하여 계산된 $\cos\theta$ 는 두 벡터 x 와 y 사이의 내각 θ 만을 고려하기 때문에, x, y 가 서

로 다른 사용자 템플릿 벡터여서 $|x|$, $|y|$ 가 다르더라도 벡터 간의 내적이 작다면 식 A에 의해 계산된 $\cos\theta$ 는 1에 가까운 가능성이 있어 동일한 사용자로 오인될 가능성이 있다. 이러한 문제를 보완하기 위하여 실시예에서는 변형된 코사인 유사도 계산 방법을 제안한다. 이를 위하여 식 A에서 $|y|$ 를 $|x|$ 로 대체하여,

식 B:

$$r = \left(\frac{x}{|x|^2} \right) \cdot (y)$$

로 인증 점수 r 을 계산할 수 있다.

만약, x , y 두 벡터가 동일한 사용자의 템플릿일 경우, 이 두 벡터 사이의 각 θ 의 크기가 매우 작은 동시에 $|x|$ 도 $|y|$ 와 거의 같을 것이므로, r 은 1에 가까운 값이 될 것이다. 다만, 낮은 확률이긴 하나, x , y 가 동일한 또는 유사한(거의 같은) 벡터가 아니라도 벡터 y 의 x 방향 성분인 $|y|\cos\theta$ 가 우연히 $|x|$ 와 거의 같아 식 B가 1에 가까운 경우가 생길 수 있다.

이에 따라 두 가지의 오류를 모두 방지하기 위해서 식 A와 식 B를 동시에 고려하는 방법을 제안하기로 한다.

(식 A) ≈ 1 및 (식 B) ≈ 1 을 동시에 만족하면 인증에 성공하게 할 수 있다. 다만, 바이오 인증 응용에 따라서는 식 A 또는 식 B 중 한가지만을 고려하거나, 둘 다 고려하되 (식 A) ≈ 1 또는 (식 B) ≈ 1 중 하나만을 만족하면 인증에 성공하도록 구성할 수도 있다. 또한, 이 두 기준에 대해 각각 가중치를 부여하여 가중 평균을 계산하도록 할 수 있다. 즉, 적절한 두 상수 a , b 에 대해 $a \times (\text{식 A}) + b \times (\text{식 B}) \approx 1$ 일 경우 인증에 성공하게 할 수 있다.

식 A에서 정규화된 두 벡터 $\frac{x}{|x|}$ 와 $\frac{y}{|y|}$ 및 식 B에서 정규화된 벡터 $\frac{x}{|x|^2}$ 의 원소는 매우 작은 소수들인 반면, 내적 함수 암호는 정수로 구성된 벡터에 대해서만 동작하므로, 계산의 정밀도를 유지하기 위해서는 양자화(quantization)를 적용할 수 있다. 즉, 식 A 및 식 B가 1인지를 확인하는 대신 큰 정수 Q , R 에 대하여 식 D, 큰 정수 S 에 대해 식 E로 나타낼 수 있음을 확인할 수 있다.

$$\left(\frac{Q}{|x|} x \right) \cdot \left(\frac{R}{|y|} y \right) \approx QR$$

식 D:

$$\left(\frac{S}{|x|^2} x \right) \cdot (y) \approx S$$

식 E:

본 발명에 의하면 사용자는 등록 시 바이오 데이터를 암호화된 상태로 원격 서버에 저장하며, 인증 시에는 로컬 센서가 바이오 데이터를 인식하여 암호화된 상태로 원격 서버로 전송하면, 원격 서버는 암호화 상태의 두 데이터를 비교하며, 유사도가 높을 경우 인증에 성공하게 된다. 기존에 이러한 목표를 달성하고자 하는 여러 시도가 있었으나, 본 발명은 아래와 같은 측면에서 기존 방법들보다 진보된 특성을 가진다.

동형 암호를 이용한 원격 바이오 인증 방법은 역시 암호화 상태의 연산을 수행하는 동형 암호를 이용하고 있으나, 동형 암호는 암호화 연산 결과(바이오 인증의 경우 템플릿 매칭 점수)가 역시 암호문으로 도출되기 때문에 이를 해결하기 위한 복잡한 프로토콜이 필요하다. 그러나, 본 발명은 암호문 사이의 연산 결과가 평문으로 도출되는 함수 암호를 이용함으로써 상기 언급한 문제를 해결할 수 있다.

함수 암호를 이용한 기존의 원격 바이오 인증 방법은, 현재 제안되어 있는 다양한 함수 암호들 중 유일하게 실

용적 성능을 제공하는 내적 함수 암호(암호문 벡터 간의 내적 계산이 가능한 함수 암호)를 이용하였다. 그러나, 내적 계산을 직접 활용할 경우 벡터들 간의 해밍 거리만 계산 가능하며, 바이오 인증에서 일반적으로 많이 쓰이는 유클리드 거리 계산은 불가능하므로, 함수 암호를 이용한 기존의 원격 바이오 인증 방법의 활용 범위는 매우 제약적이다. 본 발명에서는 유클리드 거리와 유사한 특성을 갖는, 즉 유클리드 거리를 대체할 수 있는 변형된 코사인 유사도를 이용하여 바이오 템플릿 간의 거리를 측정한다. 이러한 변형된 코사인 유사도는 벡터 내적만으로 계산이 가능하므로 내적 함수 암호를 이용하여 쉽게 구현 가능한 동시에, 유클리드 거리와 유사한 특성을 가지므로 해밍 거리보다 다양한 바이오 인증 응용에 적용 가능하다.

[0058] 도 2는 일 실시예에 따른 인증 시스템의 구성을 설명하기 위한 블록도이고, 도 3은 일 실시예에 따른 인증 시스템의 인증 방법을 설명하기 위한 흐름도이다.

[0059] 인증 서버(160)의 프로세서(200)는 등록부(210) 및 인증부(220)를 포함할 수 있다. 이러한 프로세서(200)의 구성요소들은 인증 서버에 저장된 프로그램 코드가 제공하는 제어 명령에 따라 프로세서(200)에 의해 수행되는 서로 다른 기능들(different functions)의 표현들일 수 있다. 프로세서(200) 및 프로세서(200)의 구성요소들은 도 3의 바이오 인증 방법이 포함하는 단계들(310 내지 320)을 수행하도록 인증 서버를 제어할 수 있다. 이때, 프로세서(200) 및 프로세서(200)의 구성요소들은 메모리가 포함하는 운영체제의 코드와 적어도 하나의 프로그램의 코드에 따른 명령(instruction)을 실행하도록 구현될 수 있다.

[0060] 프로세서(200)는 인증 방법을 위한 프로그램의 파일에 저장된 프로그램 코드를 메모리에 로딩할 수 있다. 예를 들면, 인증 서버에서 프로그램이 실행되면, 프로세서는 운영체제의 제어에 따라 프로그램의 파일로부터 프로그램 코드를 메모리에 로딩하도록 인증 서버를 제어할 수 있다. 이때, 프로세서(200) 및 프로세서(200)가 포함하는 등록부(210) 및 인증부(220) 각각은 메모리에 로딩된 프로그램 코드 중 대응하는 부분의 명령을 실행하여 이후 단계들(310 내지 320)을 실행하기 위한 프로세서(200)의 서로 다른 기능적 표현들일 수 있다.

[0061] 단계(310)에서 등록부(210)는 로컬 센서에 입력된 사용자의 바이오 데이터를 등록할 수 있다. 등록부(210)는 로컬 센서에 입력된 사용자의 바이오 데이터를 함수 암호의 비밀키로 등록할 수 있다. 등록부(210)는 로컬 센서에 입력된 사용자의 바이오 데이터로부터 변환된 바이오 템플릿(x)과 키 분배 서버의 마스터 비밀키를 이용하여 키 분배 서버에서 생성된 비밀키(sk_1 , sk_2)를 저장하여 사용자의 바이오 데이터를 등록할 수 있다. 등록부(210)는 로컬 센서에서 바이오 데이터가 정수 형태의 바이오 템플릿(x)로 변환되고, 바이오 데이터의 바이오 템플릿이 정밀도 파라미터(Q , S)를 이용하여 양자화된 바이오 템플릿(x'_1 , x'_2)이 계산됨에 따라 키 분배 서버에서 마스터 비밀키(msk)와 양자화된 바이오 템플릿(x'_1 , x'_2)를 이용하여 생성된 비밀키(sk_1 , sk_2)를 저장할 수 있다.

[0062] 단계(320)에서 인증부(220)는 로컬 센서에 입력된 바이오 인증 데이터를 적어도 하나 이상의 계산 방법을 조합하여 계산함에 따라 사용자의 바이오 인증 데이터를 인증할 수 있다. 인증부(220)는 로컬 센서에 입력된 바이오 인증 데이터에 기반하여 계산된 암호문을 적어도 하나 이상의 계산 방법을 조합하여 복호화함에 따라 사용자의 바이오 인증 데이터를 인증할 수 있다. 인증부(220)는 로컬 센서에 입력된 바이오 인증 데이터에 기반하여 변환된 1)바이오 템플릿(y), 마스터 비밀키(msk) 및 정밀도 파라미터(R) 또는 2)상기 바이오 템플릿(y)과 상기 마스터 비밀키(msk) 중 어느 하나를 이용하여 로컬 센서에서 계산된 암호문을 이용하여, 바이오 데이터에 기반하여 변환된 바이오 템플릿 및 바이오 인증 데이터에 기반하여 변환된 바이오 템플릿의 내적 계산을 수행할 수 있다. 인증부(220)는 로컬 센서에서 바이오 인증 데이터가 정수 형태의 바이오 템플릿(y)로 변환되고, 1)마스터 비밀키(msk), 바이오 인증 데이터의 바이오 템플릿(y) 및 정밀도 파라미터(R) 또는 2)상기 마스터 비밀키(msk)와 상기 바이오 인증 데이터의 바이오 템플릿(y) 중 어느 하나를 이용하여 계산된 암호문(c_1 , c_2)을 수신할 수 있다. 인증부(220)는 공개 파라미터, 비밀키 및 암호문을 이용하여 어느 하나의 바이오 데이터의 양자화된 바이오 템플릿(x'_1)과 바이오 인증 데이터의 양자화된 바이오 템플릿(y')의 내적을 획득할 수 있다. 인증부(220)는 획득된 내적을 적어도 하나 이상의 코사인 유사도 계산 방법의 OR 조건, AND 조건 및 가중치 조건 중 어느 하나에 기반하여 인증 성공 여부를 판단할 수 있다.

[0063] 도 4는 일 실시예에 따른 인증 시스템에서 바이오 데이터 등록 방법을 설명하기 위한 도면이다.

[0064] 인증 시스템은 로컬 센서, 인증 서버 및 키 분배 서버로 구성될 수 있다. 도 4에서는, 로컬 센서(110), 인증 서버(160) 및 키 분배 서버(150) 간의 데이터 송수신을 통하여 바이오 데이터를 등록하는 동작을 구체적으로 설명하기로 한다. 이때, 사전에 키 분배 서버(150)는 (pp , msk)= $setup(L)$ 에 의해 공개 파라미터(pp)와 마스터 비밀키(msk)를 생성할 수 있다. 키 분배 서버(150)는 생성된 마스터 비밀키(msk)를 로컬 센서(110)에게 전송함에

따라 로컬 센서(110)에서 마스터 비밀키가 저장될 수 있고, 공개 파라미터(pp)를 인증 서버(160)에게 전송함에 따라 인증 서버(160)에서 공개 파라미터(pp)가 저장될 수 있다. 키 분배 서버(150)는 정밀도 파라미터 Q, R, S 를 결정하여 로컬 센서(110)와 인증 서버(150)에게 정밀도 파라미터를 전송할 수 있다. 인증 서버(160)는 사전에 매칭 수행을 위한 경계값(threshold) T_1, T_2, T_3, T_4, T_5 를 결정할 수 있다.

[0065] 로컬 센서(110)는 사용자로부터 입력되는 바이오 데이터를 수신할 수 있다(401). 일례로, 로컬 센서는 출입 통제 시스템 상의 바이오 센서, 스마트 디바이스 상의 바이오 센서 등이 해당될 수 있다. 또한, 사용자로부터 입력되는 바이오 데이터는 지문, 홍채, 얼굴 인식 등 사용자를 식별할 수 있는 사용자 고유의 데이터를 의미할 수 있다.

[0066] 로컬 센서(110)는 바이오 데이터를 디지털 데이터로 변환할 수 있다(402). 구체적으로, 로컬 센서(110)는 바이오 데이터에 이미지 처리, 정규화 및 양자화(quantization)를 수행하여 디지털 데이터로 변환할 수 있다.

또한, 변환된 디지털 데이터를 직렬화(serialization)하여 정수 벡터 형태의 바이오 템플릿(x)으로 변환할 수

있다. 로컬 센서(110)는 정밀도 파라미터 Q, S 를 이용하여 양자화된 바이오 템플릿($x'_1 = \left(\frac{Q}{|x|}x\right)$ 와 $x'_2 = \left(\frac{S}{|x|^2}x\right)$)을 계산할 수 있다(403).

[0067] 키 분배 서버(150)는 마스터 비밀키(msk)와 정규화된 바이오 템플릿(x'_1, x'_2)을 이용하여 $sk_1 = \text{keygen}(msk, x'_1)$ 과 $sk_2 = \text{keygen}(msk, x'_2)$ 로 비밀키(sk_1, sk_2)를 생성할 수 있다. 키 분배 서버(150)로부터 생성된 비밀키(sk_1, sk_2)가 인증 서버에게 전달됨에 따라 인증 서버(160)에 비밀키(sk_1, sk_2)저장될 수 있다. 이러한 과정 통해 바이오 데이터가 등록될 수 있다.

[0068] 도 5는 일 실시예에 따른 인증 시스템에서 바이오 데이터의 인증 방법을 설명하기 위한 도면이다.

[0069] 인증 시스템은 로컬 센서, 인증 서버 및 키 분배 서버로 구성될 수 있다. 도 5에서는, 로컬 센서(110), 인증 서버(160) 및 키 분배 서버(150) 간의 데이터 송수신을 통하여 바이오 인증 동작을 구체적으로 설명하기로 한다.

[0070] 로컬 센서(110)는 사용자로부터 입력되는 바이오 인증 데이터를 수신할 수 있다(501). 일례로, 로컬 센서는 출입 통제 시스템 상의 바이오 센서, 스마트 디바이스 상의 바이오 센서 등이 해당될 수 있다. 또한, 사용자로부터 입력되는 바이오 인증 데이터는 지문, 홍채, 얼굴 인식 등 사용자를 식별할 수 있는 사용자 고유의 데이터를 의미할 수 있다.

[0071] 로컬 센서(110)는 바이오 인증 데이터를 디지털 데이터로 변환할 수 있다(502). 구체적으로, 로컬 센서(110)는 바이오 인증 데이터에 이미지 처리, 정규화 및 양자화(quantization)를 수행하여 디지털 데이터로 변환할 수 있다. 또한, 변환된 디지털 데이터를 직렬화(serialization)하여 정수 벡터 형태의 바이오 템플릿(y)으로 변환할 수 있다.

[0072] 로컬 센서(110)는 마스터 비밀키(msk), 바이오 템플릿(y) 및 정밀도 파라미터(R)로부터 $c_1 = \text{encrypt}(msk, \frac{R}{|y|}y)$ 와 $c_2 = \text{encrypt}(msk, y)$ 로 암호문(c_1, c_2)를 계산하여 인증 서버(160)로 전송할 수 있다(503, 504).

[0073] 인증 서버(160)는 공개 파라미터(pp), 비밀키(sk_1, sk_2) 및 암호문(c_1, c_2)를 이용하여 복호화함에 따라 내적을 획득할 수 있다(505). 구체적으로, 인증 서버(160)는 $r_1 = \text{decrypt}(pp, sk_1, c_1)$ 로 바이오 데이터에 대

한 양자화된 바이오 템플릿(x'_1)과 바이오 인증 데이터에 대한 양자화된 바이오 템플릿($y' = \left(\frac{R}{|y|}y\right)$)의 내적 $r_1 = x'_1 \cdot y'$ 을 획득할 수 있다. 또한, 인증 서버(160)는 $r_2 = \text{decrypt}(pp, sk_2, c_2)$ 로 바이오 테

이터에 대한 양자화된 바이오 템플릿(x'_2)과 바이오 인증 데이터에 대한 정수 형태의 템플릿(y)의 내적 $r_2 = x'_2 \cdot y$ 을 획득할 수 있다.

[0074] 인증 서버(160)는 획득된 내적에 기반하여 인증 성공 여부를 판단할 수 있다(506). 인증 서버(160)는 다음의 조건 중 어느 하나를 선택하여 인증 성공 여부를 판단할 수 있다. 도 6은, 인증 성공 여부를 판단하는 방법을 설명하기 위한 도면이다. 일례로, 인증 서버(160)에 의하여 OR 조건, AND 조건 및 가중치 조건 중 어느 하나의 조건이 선택될 수 있다(610). 또는 사용자에게 의하여 조건이 선택될 수 있고, 컴퓨터에 의하여 랜덤으로 조건이 선택될 수도 있다. 인증 서버(160)가 OR 조건을 선택함에 따라 $QR - T_1 < r_1 \leq QR$ 또는 $S - T_2 < r_2 \leq S + T_3$ 인지 여부를 판단할 수 있다(621). 인증 서버(160)는 $QR - T_1 < r_1 \leq QR$ 또는 $S - T_2 < r_2 \leq S + T_3$ 일 경우, 인증에 성공한 것으로 판단할 수 있다(640). 또는, 인증 서버(160)가 AND 조건을 선택함에 따라 $QR - T_1 < r_1 \leq QR$ 그리고 $S - T_2 < r_2 \leq S + T_3$ 인지 여부를 포함할 수 있다. 인증 서버(160)가 $QR - T_1 < r_1 \leq QR$ 그리고 $S - T_2 < r_2 \leq S + T_3$ 일 경우, 인증에 성공한 것으로 판단할 수 있다(640). 또는, 인증 서버(160)가 가중치 조건을 선택함에 따라 $(a \times QR + b \times S) - T_4 < a \times r_1 + b \times r_2 \leq (a \times QR + b \times S) + T_5$ 인지 여부를 판단할 수 있다. 인증 서버(160)가 $(a \times QR + b \times S) - T_4 < a \times r_1 + b \times r_2 \leq (a \times QR + b \times S) + T_5$ 일 경우, 인증에 성공한 것으로 판단할 수 있다(640). 또한, 인증 서버(160)가 각각의 선택된 조건에 대하여 만족하지 못하는 경우, 인증에 실패한 것으로 판단할 수 있다(641).

[0075] 일 실시예에 따른 암호 시스템에서 제공하는 내적 함수 암호 기반의 바이오 인증 방법은 안전성 측면에서 다음과 같은 장점을 지닌다.

[0076] 로컬 센서가 공격당하는 경우, 마스터 비밀키(msk)가 유출되는데, 이 키 자체는 바이오 데이터에 대한 어떠한 정보도 담고 있지 않다. 그러나, 키 유출 이후에 진행되는 바이오 인증 세션에 대해서는 암호문 c_1 과 c_2 로부터 양자화된 바이오 템플릿 y' 및 바이오 템플릿 y 을 복구할 수 있으므로, 키가 유출된 즉시 마스터 키를 갱신하는 것이 바람직하다.

[0077] 인증 서버는 마스터 비밀키(msk)를 알지 못하므로, 인증 서버 또는 인증 서버를 공격한 공격자는 사용자의 바이오 데이터를 복원할 수 없다.

[0078] 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 이상의 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.

[0079] 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.

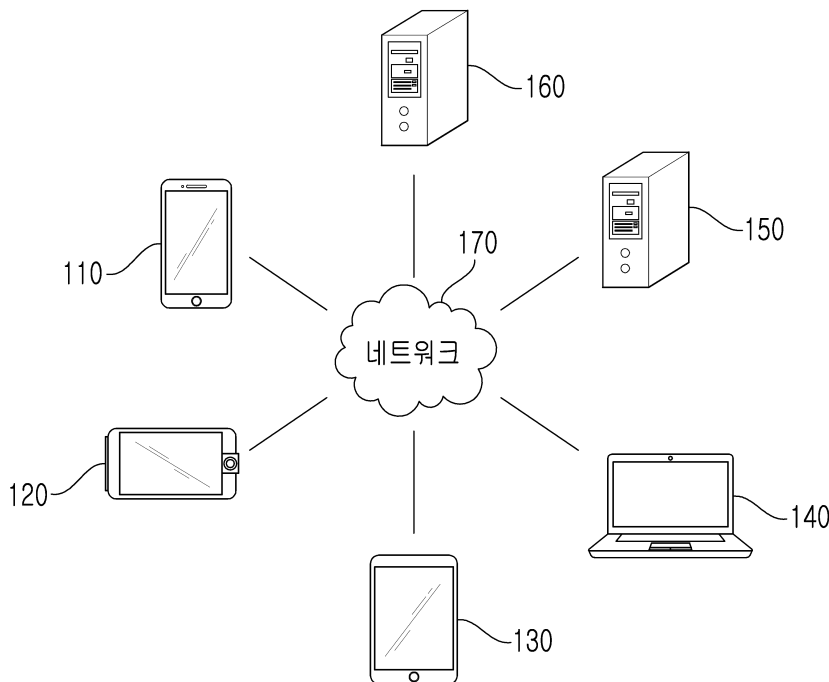
[0080] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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.

[0081] 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.

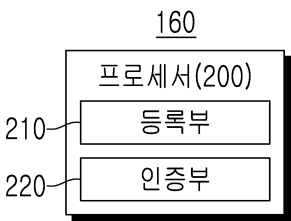
[0082] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

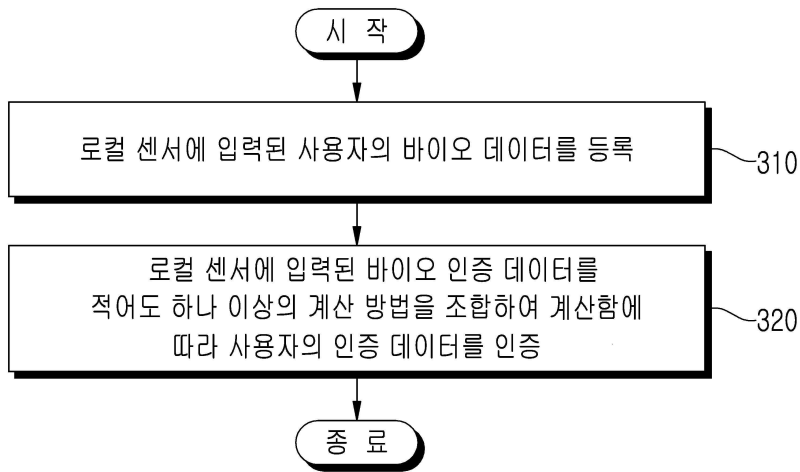
도면1



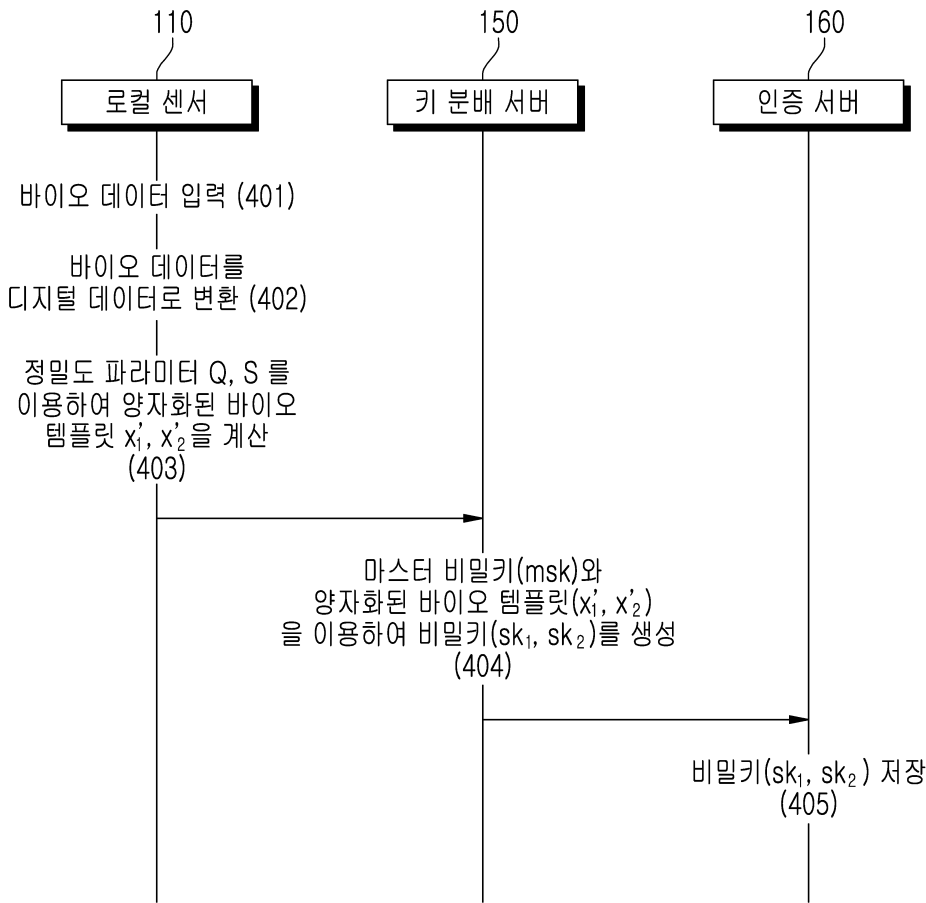
도면2



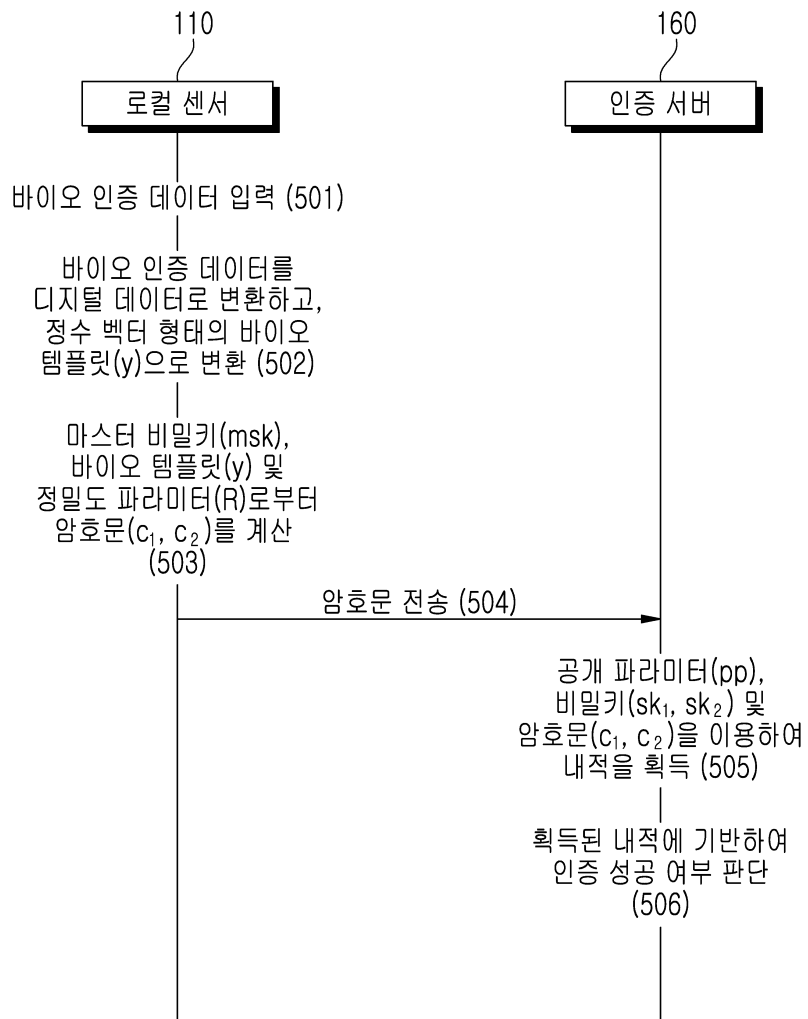
도면3



도면4



도면5



도면6

