(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년09월30일
(11) 등록번호 10-1659226
(24) 등록일자 2016년09월13일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/00* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/0866 (2013.01)
H04L 9/008 (2013.01)
(21) 출원번호 10-2015-0073534
(22) 출원일자 2015년05월27일
심사청구일자 2015년05월27일
(56) 선행기술조사문헌
JP2011211593 A
김세환 외 1인, "클라우드 컴퓨팅 환경에서의 개인정보보호를 위한 완전 동형 암호 적용 방안 고찰", 정보보호학회 논문지 24(5) (2014.10. 공개)

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
이문규
경기도 부천시 원미구 계남로 81, 2222동 702호(상동, 진달래마을)
(74) 대리인
양성보

전체 청구항 수 : 총 5 항 심사관 : 문형섭

(54) 발명의 명칭 **완전 동형 암호를 이용한 원격 바이오 인증 방법 및 시스템**

(57) 요 약

완전 동형 암호를 이용한 원격 바이오 인증 방법 및 시스템이 개시된다. 원격 바이오 인증 방법은, 사용자 단말에서, 등록하고자 하는 아이디와 생체 정보를 포함하는 제1 이미지를 입력 받는 단계; 상기 사용자 단말에서, 상기 제1 이미지로부터 특징점을 추출하여 상기 특징점으로 구성된 제1 템플릿을 생성하는 단계; 상기 사용자 단말에서, 동형 암호(homomorphic encryption)를 이용하여 상기 제1 템플릿을 암호화 한 제1 암호문을 생성하는 단계; 및 상기 사용자 단말에서, 상기 제1 암호문을 상기 아이디와 함께 클라우드 서버로 전송하여 상기 클라우드 서버 상에 등록하는 단계를 포함한다.

대 표 도 - 도4



(52) CPC특허분류
H04L 9/3231 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2014R1A1A2058514
부처명 교육부
연구관리전문기관 한국연구재단
연구사업명 기본연구지원사업
연구과제명 스마트 디바이스를 위한 안전한 바이오인식 서비스 기술 연구
기 여 율 1/1
주관기관 인하대학교 산학협력단
연구기간 2014.11.01 ~ 2017.04.30

명 세 서

청구범위

청구항 1

사용자 단말에서, 등록하고자 하는 아이디와 생체 정보를 포함하는 제1 이미지를 입력 받는 단계;

상기 사용자 단말에서, 상기 제1 이미지로부터 특징점을 추출하여 상기 특징점으로 구성된 제1 템플릿을 생성하는 단계;

상기 사용자 단말에서, 동형 암호(homomorphic encryption)를 이용하여 상기 제1 템플릿을 암호화한 제1 암호문을 생성하는 단계; 및

상기 사용자 단말에서, 상기 제1 암호문을 상기 아이디와 함께 클라우드 서버로 전송하여 상기 클라우드 서버상에 등록하는 단계

를 포함하고,

상기 클라우드 서버는,

상기 암호화한 제1 암호문을 대상으로, 암호화된 특정 수의 암호문을 동형 뺄셈하여 상기 제1 템플릿과 관련하여 확장된 암호화 좌표 값 순서쌍을 생성하고,

상기 확장된 암호화 좌표 값 순서쌍에 기초하여 제2 암호문과의 비교 연산을 수행하고,

상기 제2 암호문은,

상기 사용자 단말에서 인증 요청 시 입력된 생체정보를 포함하는 제2 이미지로부터 추출된 특징점으로 구성된 제2 템플릿을 암호화하여 생성된 암호문인 것

을 특징으로 하는 원격 바이오 인증 방법.

청구항 2

제1항에 있어서,

상기 사용자 단말에서, 아이디 등록 요청에 따라 동형 암호화 키(homomorphic encryption key)를 생성하여 상기 사용자 단말 상에 저장하는 단계

를 더 포함하는 원격 바이오 인증 방법.

청구항 3

제1항에 있어서,

상기 사용자 단말에서, 상기 아이디에 대한 인증 요청으로서 상기 아이디와 함께 생체 정보를 포함하는 제2 이미지가 입력되면 상기 제2 이미지로부터 특징점을 추출하여 상기 특징점으로 구성된 제2 템플릿을 생성하는 단계;

상기 사용자 단말에서, 동형 암호를 이용하여 상기 제2 템플릿을 암호화 한 제2 암호문을 생성하는 단계;

상기 사용자 단말에서, 상기 아이디와 상기 제2 암호문을 상기 클라우드 서버로 전송하여 비교 연산을 요청하는 단계;

상기 사용자 단말에서, 상기 클라우드 서버로부터 상기 아이디에 대한 상기 제1 암호문과 상기 제2 암호문 간의 비교 연산 결과를 수신하는 단계; 및

상기 사용자 단말에서, 확장된 제1 암호문과 상기 제2 암호문 간의 비교 연산 결과에 따라 사용자 인증을 처리하는 단계

를 더 포함하는 원격 바이오 인증 방법.

청구항 4

제3항에 있어서,

상기 사용자 단말에서, 아이디 등록 요청에 따라 동형 암호화 키(homomorphic encryption key)를 생성하여 상기 사용자 단말 상에 저장하는 단계

를 더 포함하고,

상기 사용자 인증을 처리하는 단계는,

상기 동형 암호화 키를 이용하여 상기 제1 암호문과 상기 제2 암호문 간의 비교 연산 결과에 대한 해독 연산(decryption)을 수행한 후 상기 해독 연산의 결과에 따라 상기 아이디의 로그인을 허용하는 것

을 특징으로 하는 원격 바이오 인증 방법.

청구항 5

적어도 하나의 프로그램이 로딩된 메모리; 및

적어도 하나의 프로세서

를 포함하고,

상기 적어도 하나의 프로세서는, 상기 프로그램의 제어에 따라,

아이디 등록 요청에 따라 동형 암호화 키(homomorphic encryption key)를 생성하여 저장하는 과정;

등록하고자 하는 아이디와 생체 정보를 포함하는 제1 이미지가 입력되면 상기 제1 이미지로부터 특징점을 추출하여 상기 특징점으로 구성된 제1 템플릿을 생성하는 과정;

상기 동형 암호화 키를 이용하여 상기 제1 템플릿을 암호화한 제1 암호문을 생성하는 과정;

상기 제1 암호문을 상기 아이디와 함께 클라우드 서버로 전송하여 상기 클라우드 서버 상에 등록하는 과정;

상기 아이디에 대한 인증 요청으로서 상기 아이디와 함께 생체 정보를 포함하는 제2 이미지가 입력되면 상기 제2 이미지로부터 특징점을 추출하여 상기 특징점으로 구성된 제2 템플릿을 생성하는 과정;

상기 동형 암호화 키를 이용하여 상기 제2 템플릿을 암호화한 제2 암호문을 생성하는 과정;

상기 아이디와 상기 제2 암호문을 상기 클라우드 서버로 전송하여 비교 연산을 요청하는 과정;

상기 클라우드 서버로부터 상기 아이디에 대한 상기 제1 암호문과 상기 제2 암호문 간의 비교 연산 결과를 수신하는 과정;

상기 동형 암호화 키를 이용하여 상기 제1 암호문과 상기 제2 암호문 간의 비교 연산 결과에 대한 해독 연산(decryption)을 수행하는 과정; 및

상기 해독 연산의 결과에 따라 상기 아이디를 이용한 사용자 인증을 처리하는 과정

을 처리하고,

상기 클라우드 서버는,

상기 암호화한 제1 암호문을 대상으로, 암호화된 특정 수의 암호문을 동형 뺄셈하여 상기 제1 템플릿과 관련하여 확장된 암호화 좌표 값 순서쌍을 생성하고,

상기 확장된 암호화 좌표 값 순서쌍에 기초하여 제2 암호문과의 비교 연산을 수행하고,

상기 제2 암호문은,

사용자 단말에서 인증 요청 시 입력된 생체정보를 포함하는 제2 이미지로부터 추출된 특징점으로 구성된 제2 템플릿을 암호화하여 생성된 암호문인 것

을 특징으로 하는 원격 바이오 인증 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 신체 정보를 이용한 바이오 인증 기술에 관한 것이다.

배 경 기 술

[0002] 사용자 정보를 내장하고 있는 시스템은 허가된 사용자의 접근만을 허용해야 하며, 접근이 허가된 적법한 사용자인지를 판단하는 기술을 사용자 인증 기술이라 한다. 이러한 사용자 인증 기술은 인터넷 사이트의 로그인, 인터넷 뱅킹, 사용자 단말기 등에서 보안을 위해 널리 사용되고 있다.

[0003] 또한, 오늘날 노트북, 스마트폰, 태블릿 PC 등의 사용자 단말기의 보급이 확산되면서 공공장소에서 이러한 단말기들을 이용한 인증 절차가 빈번하게 이뤄지고 있다.

[0004] 이러한 장치들에서는 사용자 인증을 위해 패스워드(password) 및 개인 식별 번호(Personal Identification Number: 이하 PIN)를 입력하는 방식이 보편적으로 사용되고 있다. 하지만 이러한 장치들에서 사용되고 있는 패스워드나 PIN은 4자리로 제한되는 경우가 많고 자리 수의 제한이 없더라도 사용자가 편의를 위하여 짧은 패스워드나 PIN을 사용하기 때문에 공격, 특히 엿보기 공격이나 카메라가 촬영하는 공격에 취약하다.

[0005] 이러한 패스워드나 PIN 입력을 이용한 사용자 인증 방법의 취약성에 대한 대안으로는 지문이나 홍채 등 신체 정보를 이용한 바이오 인증, 카드나 동글 등 하드웨어를 이용한 소유 기반 인증 등이 이용되고 있다. 이 중 바이오 인증, 특히 지문 인식 기반 인증은 그 편의성으로 인해 점차 많은 곳에서 활용되고 있으며, 최근에는 건물 또는 가정의 출입구 개폐 장치와 스마트폰 등에서도 지문 인식이 쓰이고 있다.

[0006] 지문 인식 기반 인증 기술의 일 예로서, 한국공개특허 제10-2005-0055164호(공개일 2005년 06월 13일)에는 지문 인식 기능을 이용하여 인식한 지문 데이터에 상응하는 사용자 제한 메뉴를 설정하여 사용자에 따라 서비스를 제한하도록 하는 기술이 개시되어 있다.

발명의 내용

해결하려는 과제

[0007] 다양한 형태의 공격으로부터 바이오 데이터를 보호할 수 있는 원격 바이오 인증 방법 및 시스템을 제공한다.

[0008] 동형 암호를 이용하여 바이오 데이터를 원격에서 관리할 수 있는 원격 바이오 인증 방법 및 시스템을 제공한다.

과제의 해결 수단

[0009] 사용자 단말에서, 등록하고자 하는 아이디와 생체 정보를 포함하는 제1 이미지를 입력 받는 단계; 상기 사용자 단말에서, 상기 제1 이미지로부터 특징점을 추출하여 상기 특징점으로 구성된 제1 템플릿을 생성하는 단계; 상기 사용자 단말에서, 동형 암호(homomorphic encryption)를 이용하여 상기 제1 템플릿을 암호화 한 제1 암호문을 생성하는 단계; 및 상기 사용자 단말에서, 상기 제1 암호문을 상기 아이디와 함께 클라우드 서버로 전송하여 상기 클라우드 서버 상에 등록하는 단계를 포함하는 원격 바이오 인증 방법을 제공한다.

[0010] 일 측면에 따르면, 원격 바이오 인증 방법은, 상기 사용자 단말에서, 아이디 등록 요청에 따라 동형 암호화 키(homomorphic encryption key)를 생성하여 상기 사용자 단말 상에 저장하는 단계를 더 포함할 수 있다.

[0011] 다른 측면에 따르면, 원격 바이오 인증 방법은, 상기 사용자 단말에서, 상기 아이디에 대한 인증 요청으로서 상기 아이디와 함께 생체 정보를 포함하는 제2 이미지가 입력되면 상기 제2 이미지로부터 특징점을 추출하여 상기 특징점으로 구성된 제2 템플릿을 생성하는 단계; 상기 사용자 단말에서, 동형 암호를 이용하여 상기 제2 템플릿을 암호화 한 제2 암호문을 생성하는 단계; 상기 사용자 단말에서, 상기 아이디와 상기 제2 암호문을 상기 클라우드 서버로 전송하여 비교 연산을 요청하는 단계; 상기 사용자 단말에서, 상기 클라우드 서버로부터 상기 아이디에 대한 상기 제1 암호문과 상기 제2 암호문 간의 비교 연산 결과를 수신하는 단계; 및 상기 사용자 단말에서, 상기 제1 암호문과 상기 제2 암호문 간의 비교 연산 결과에 따라 사용자 인증을 처리하는 단계를 더 포함할 수 있다.

[0012] 또 다른 측면에 따르면, 원격 바이오 인증 방법은, 상기 사용자 단말에서, 아이디 등록 요청에 따라 동형 암호

화 키(homomorphic encryption key)를 생성하여 상기 사용자 단말 상에 저장하는 단계를 더 포함할 수 있으며, 상기 사용자 인증을 처리하는 단계는, 상기 동형 암호화 키를 이용하여 상기 제1 암호문과 상기 제2 암호문 간의 비교 연산 결과에 대한 해독 연산(decryption)을 수행한 후 상기 해독 연산의 결과에 따라 상기 아이디의 로그인을 허용할 수 있다.

[0013] 적어도 하나의 프로그램이 로딩된 메모리; 및 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 상기 프로그램의 제어에 따라, 아이디 등록 요청에 따라 동형 암호화 키(homomorphic encryption key)를 생성하여 저장하는 과정; 등록하고자 하는 아이디와 생체 정보를 포함하는 제1 이미지가 입력되면 상기 제1 이미지로부터 특징점을 추출하여 상기 특징점으로 구성된 제1 템플릿을 생성하는 과정; 상기 동형 암호화 키를 이용하여 상기 제1 템플릿을 암호화 한 제1 암호문을 생성하는 과정; 상기 제1 암호문을 상기 아이디와 함께 클라우드 서버로 전송하여 상기 클라우드 서버 상에 등록하는 과정; 상기 아이디에 대한 인증 요청으로서 상기 아이디와 함께 생체 정보를 포함하는 제2 이미지가 입력되면 상기 제2 이미지로부터 특징점을 추출하여 상기 특징점으로 구성된 제2 템플릿을 생성하는 과정; 상기 동형 암호화 키를 이용하여 상기 제2 템플릿을 암호화 한 제2 암호문을 생성하는 과정; 상기 아이디와 상기 제2 암호문을 상기 클라우드 서버로 전송하여 비교 연산을 요청하는 과정; 상기 클라우드 서버로부터 상기 아이디에 대한 상기 제1 암호문과 상기 제2 암호문 간의 비교 연산 결과를 수신하는 과정; 상기 동형 암호화 키를 이용하여 상기 제1 암호문과 상기 제2 암호문 간의 비교 연산 결과에 대한 해독 연산(decryption)을 수행하는 과정; 및 상기 해독 연산의 결과에 따라 상기 아이디를 이용한 사용자 인증을 처리하는 과정을 처리하는 원격 바이오 인증 시스템을 제공한다.

발명의 효과

[0014] 본 발명의 실시예에 따르면, 바이오 데이터를 원격 서버에 저장하는 클라우드 형태로 관리하고, 특히 동형 암호를 이용하여 암호화 된 형태로 바이오 데이터를 원격 서버에 저장함으로써 바이오 데이터의 유출을 보다 근본적으로 차단하여, 원격 서버를 완전히 신뢰할 수 없는 상황에서도 외부 공격에 대한 저항성과 안전성을 향상시킬 수 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 일 실시예에 있어서, 사용자 인증 환경의 예를 설명하기 위한 도면이다.

도 2는 본 발명의 일 실시예에 있어서, 원격 관리 서버의 내부 구성을 설명하기 위한 블록도이다.

도 3은 본 발명의 일 실시예에 있어서, 컴퓨터 시스템의 내부 구성의 일례를 설명하기 위한 블록도이다.

도 4는 본 발명의 일 실시예에 있어서, 바이오 데이터에 대한 템플릿을 설명하기 위한 예시 도면이다.

도 5는 본 발명의 일 실시예에 있어서, 바이오 데이터의 원격 관리를 통한 사용자 등록 과정을 도시한 순서도이다.

도 6은 본 발명의 일 실시예에 있어서, 바이오 데이터의 원격 관리를 통한 사용자 인증 과정을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0016] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0017] 본 실시예들은 신체 정보를 이용한 바이오 인증 기술에 관한 것으로, 상세하게는 사용자 인증을 위한 바이오 데이터를 원격에서 관리할 수 있는 원격 바이오 인증 방법 및 시스템에 관한 것이다.

[0018] 본 명세서에서, '바이오 데이터'는 사용자 인증을 위해 입력 받는 생체 정보로서, 지문이나 홍채, 음성, 필체 등을 의미할 수 있으며, 이에 한정되는 것은 아니며 사용자를 식별하는데 사용되는 모든 형태의 정보로 쉽게 확장이 가능하다. 이하에서는 지문을 바이오 데이터의 대표적인 예로 하여 설명하기로 한다.

[0019] 사용자 인증은 특정 시스템(컴퓨터, 웹 서버, 스마트폰 등)에 접근을 시도하는 사용자가 접근 권한이 있는지를 확인하여 접근을 허용하는 일련의 절차로서, 지문 인식을 포함한 바이오 인증 기술을 이용할 수 있다.

[0020] 지문 인식을 포함한 바이오 인증은 안전성 측면에서 한 가지 문제점을 가지고 있다. 지식 기반 인증에서 패스워드 유출 시에는 패스워드를 교체하면 되고, 소유 기반 인증에서도 인증용 하드웨어의 도난 또는 분실 시에는

새로운 하드웨어로 대체하면 되지만, 지문 데이터 유출 시에는 적절한 대응 방안이 없기 때문이다. 손가락의 지문을 바꾸는 것이 불가능하므로 한 번 유출된 지문은 해당 사용자의 지문 인증 자체를 무력화시킬 수 있다. 따라서, 바이오 인증에서는 지문, 홍채 등 바이오 데이터 원본을 시스템에서 안전하게 관리하는 것이 다른 종류의 인증에 비해 더 중요한 조건이다.

[0021] 이러한 문제에 대한 대안으로, 바이오 데이터를 로컬 시스템보다는 좀더 안전하게 관리되는 원격 서버에 저장하는 클라우드 형태의 개선 방안을 고려할 수 있다. 다만, 원격 클라우드 서버가 바이오 데이터를 무단으로 활용할 가능성을 배제할 수 없으므로 클라우드 서버에 바이오 데이터를 원본(예: 지문이나 홍채의 비트맵 이미지)이 아닌 변환된 형태로 저장하도록 하여야 한다. 이 경우 원격 클라우드 서버가 데이터를 악용하려고 시도하여도 해당 데이터는 바이오 데이터 원본이 아닌 변환된 형태이므로 유출 시 쓸모가 없게 된다.

[0022] 본 발명은 동형 암호(homomorphic encryption) 기술을 이용하여 상기 문제를 해결하는 방안을 제시한다. 본 발명에 의하면, 원격 클라우드 서버에 바이오 데이터를 암호화된 형태로 저장함으로써 해당 서버 측에서 바이오 데이터 원본에 대한 정보를 알 수 없으며, 암호화된 상태에서의 바이오 데이터 간 비교 서비스를 제공할 수 있다.

[0023] 도 1은 본 발명의 일 실시예에 있어서, 사용자 인증 환경의 예를 설명하기 위한 도면이다. 도 1은 사용자 단말(101) 및 원격 관리 서버(100)를 나타내고 있다. 도 1에서 화살표는 구성 요소 간에 유/무선 네트워크(10)를 이용하여 데이터가 송수신될 수 있음을 의미한다.

[0024] 사용자 단말(101)은 본 명세서에서 설명되는 특징들 중 하나 이상의 특징을 수행하도록 구성된 하나 이상의 프로세스들을 실행할 수 있다. 사용자 단말(101)은 원격 관리 서버(100)에 접속 가능한 모든 단말 장치를 의미할 수 있다.

[0025] 사용자 단말(101)의 예로는 스마트폰(smart phone), 태블릿(tablet), 웨어러블 컴퓨터(wearable computer), PC(personal computer), 노트북 컴퓨터(laptop computer), 랩탑 컴퓨터(laptop computer) 등을 포함할 수 있지만 이러한 것으로만 한정되는 것은 아니다.

[0026] 사용자 단말(101)은 네트워크(10)(예를 들어, 인터넷 혹은 로컬 영역 네트워크 등)에 직접적으로 혹은 간접적으로 결합될 수 있다. 예를 들어, 개인용 컴퓨터와 노트북 컴퓨터는 유선 네트워크 연결을 통해 네트워크(10)에 직접적으로 결합될 수 있다. 랩탑 컴퓨터는 랩탑 컴퓨터와 무선 액세스 포인트(Wireless Access Point)(즉, WAP) 간에 확립된 무선 통신 채널을 통해 네트워크(10)에 무선으로 결합될 수 있다. 스마트폰은 스마트폰과 셀룰러 네트워크/브리지 간에 확립된 무선 통신 채널을 통해 네트워크(10)에 무선으로 결합될 수 있다. 이때, 네트워크(10)는 하나 이상의 2차 네트워크들(미도시)과 통신할 수 있으며, 2차 네트워크들의 예로는 로컬 영역 네트워크(Local Area Network), 와이드 영역 네트워크(Wide Area Network), 또는 인트라넷(intranet)을 포함할 수 있지만 이러한 것으로만 한정되는 것은 아니다.

[0027] 사용자 단말(101)은 상기에서 설명한 네트워크(10)를 통해 원격 관리 서버(100)와 서로 인터페이스 할 수 있다.

[0028] 원격 관리 서버(100)는 원격의 클라우드 환경에서 바이오 데이터를 관리하기 위한 원격 클라우드 서버로서, 본 명세서에서 설명되는 특징들 중 하나 이상의 특징을 수행하도록 구성된 하나 이상의 프로세스들을 실행할 수 있다. 이때, 원격 관리 서버(100)는 사용자 별 아이디와 바이오 데이터를 저장 및 유지하는 관리 서버 역할을 할 수 있다. 이때, 바이오 데이터는 동형 암호를 이용하여 암호화 된 형태로 저장될 수 있다.

[0029] 원격 관리 서버(100)는 서버 컴퓨터에 해당되는 것으로, 서버 컴퓨터의 예로는 서버 컴퓨팅 디바이스, 개인용 컴퓨터, 서버 컴퓨터, 일련의 서버 컴퓨터들, 미니 컴퓨터, 및/또는 메인프레임 컴퓨터를 포함할 수 있지만 이러한 것으로만 한정되는 것은 아니다. 서버 컴퓨터는 분산형 시스템일 수 있고, 그리고 서버 컴퓨터의 동작들은 하나 이상의 프로세서들 상에서 동시에 그리고/또는 순차적으로 실행될 수 있다.

[0030] 도 2는 본 발명의 일 실시예에 있어서, 원격 관리 서버의 내부 구성을 설명하기 위한 블록도이다.

[0031] 도 2에 도시한 바와 같이, 본 실시예에 따른 원격 관리 서버(100)는 프로세서(210), 버스(220), 네트워크 인터페이스(230), 메모리(240) 및 데이터베이스(250)를 포함할 수 있다. 메모리(240)는 운영체제(241) 및 바이오 데이터 관리 루틴(242)를 포함할 수 있다. 다른 실시예들에서 원격 관리 서버(100)는 도 2의 구성요소들보다 더 많은 구성요소들을 포함할 수도 있다.

[0032] 메모리(240)는 컴퓨터에서 판독 가능한 기록 매체로서, RAM(random access memory), ROM(read only memory) 및 디스크 드라이브와 같은 비소멸성 대용량 기록장치(permanent mass storage device)를 포함할 수 있다. 또한,

메모리(240)에는 운영체제(241)와 바이오 데이터 관리 루틴(242)을 위한 프로그램 코드가 저장될 수 있다. 이러한 소프트웨어 구성요소들은 드라이브 메커니즘(drive mechanism, 미도시)을 이용하여 메모리(240)와는 별도의 컴퓨터에서 판독 가능한 기록 매체로부터 로딩될 수 있다. 이러한 별도의 컴퓨터에서 판독 가능한 기록 매체는 플로피 드라이브, 디스크, 테이프, DVD/CD-ROM 드라이브, 메모리 카드 등의 컴퓨터에서 판독 가능한 기록 매체(미도시)를 포함할 수 있다. 다른 실시예에서 소프트웨어 구성요소들은 컴퓨터에서 판독 가능한 기록 매체가 아닌 네트워크 인터페이스(230)를 통해 메모리(240)에 로딩될 수도 있다.

[0033] 버스(220)는 원격 관리 서버(100)의 구성요소들간의 통신 및 데이터 전송을 가능하게 할 수 있다. 버스(220)는 고속 시리얼 버스(high-speed serial bus), 병렬 버스(parallel bus), SAN(Storage Area Network) 및/또는 다른 적절한 통신 기술을 이용하여 구성될 수 있다.

[0034] 네트워크 인터페이스(230)는 원격 관리 서버(100)를 컴퓨터 네트워크에 연결하기 위한 컴퓨터 하드웨어 구성요소일 수 있다. 네트워크 인터페이스(230)는 원격 관리 서버(100)를 무선 또는 유선 커넥션을 통해 컴퓨터 네트워크에 연결시킬 수 있다.

[0035] 데이터베이스(250)는 바이오 데이터를 저장 및 유지하는 역할을 한다. 이때, 데이터베이스(250)는 사용자 별로(아이디, 바이오 데이터) 쌍을 저장하며, 특히 바이오 데이터는 동형 암호를 이용하여 암호화 된 형태로 저장될 수 있다.

[0036] 프로세서(210)는 기본적인 산술, 로직 및 원격 관리 서버(100)의 입출력 연산을 수행함으로써, 컴퓨터 프로그램의 명령을 처리하도록 구성될 수 있다. 명령은 메모리(240) 또는 네트워크 인터페이스(230)에 의해, 그리고 버스(220)를 통해 프로세서(210)로 제공될 수 있다. 프로세서(210)는 본 명세서에서 설명되는 특징들 중 하나 이상의 특징을 수행하기 위한 프로그램 코드를 실행하도록 구성될 수 있다. 이러한 프로그램 코드는 메모리(240)와 같은 기록 장치에 저장될 수 있다.

[0037] 도 3은 본 발명의 일 실시예에 있어서, 컴퓨터 시스템의 내부 구성의 일례를 설명하기 위한 블록도이다. 컴퓨터 시스템(300)은 적어도 하나의 프로세서(processor)(310), 메모리(memory)(320), 주변장치 인터페이스(peripheral interface)(330), 입/출력 서브시스템(I/O subsystem)(340), 전력 회로(350) 및 통신 회로(360)를 적어도 포함할 수 있다. 이때, 컴퓨터 시스템(300)은 사용자 단말(101)에 해당될 수 있다.

[0038] 메모리(320)는, 일례로 고속 랜덤 액세스 메모리(high-speed random access memory), 자기 디스크, 에스램(SRAM), 디램(DRAM), 롬(ROM), 플래시 메모리 또는 비휘발성 메모리를 포함할 수 있다. 메모리(320)는 컴퓨터 시스템(300)의 동작에 필요한 소프트웨어 모듈, 명령어 집합 또는 그밖에 다양한 데이터를 포함할 수 있다. 이때, 프로세서(310)나 주변장치 인터페이스(330) 등의 다른 컴포넌트에서 메모리(320)에 액세스하는 것은 프로세서(310)에 의해 제어될 수 있다.

[0039] 주변장치 인터페이스(330)는 컴퓨터 시스템(300)의 입력 및/또는 출력 주변장치를 프로세서(310) 및 메모리(320)에 결합시킬 수 있다. 프로세서(310)는 메모리(320)에 저장된 소프트웨어 모듈 또는 명령어 집합을 실행하여 컴퓨터 시스템(300)을 위한 다양한 기능을 수행하고 데이터를 처리할 수 있다.

[0040] 입/출력 서브시스템(340)은 다양한 입/출력 주변장치들을 주변장치 인터페이스(330)에 결합시킬 수 있다. 예를 들어, 입/출력 서브시스템(340)은 모니터나 키보드, 마우스, 프린터 또는 필요에 따라 터치스크린이나 센서 등의 주변장치를 주변장치 인터페이스(330)에 결합시키기 위한 컨트롤러를 포함할 수 있다. 특히, 본 발명에 의하면 주변 장치는 지문 인식을 위한 지문 인식 센서를 포함할 수 있다. 다른 측면에 따르면, 입/출력 주변장치들은 입/출력 서브시스템(340)을 거치지 않고 주변장치 인터페이스(330)에 결합될 수도 있다.

[0041] 전력 회로(350)는 단말기의 컴포넌트의 전부 또는 일부로 전력을 공급할 수 있다. 예를 들어 전력 회로(350)는 전력 관리 시스템, 배터리나 교류(AC) 등과 같은 하나 이상의 전원, 충전 시스템, 전력 실패 감지 회로(power failure detection circuit), 전력 변환기나 인버터, 전력 상태 표시자 또는 전력 생성, 관리, 분배를 위한 임의의 다른 컴포넌트들을 포함할 수 있다.

[0042] 통신 회로(360)는 적어도 하나의 외부 포트를 이용하여 다른 컴퓨터 시스템과 통신을 가능하게 할 수 있다. 또는 상술한 바와 같이 필요에 따라 통신 회로(360)는 RF 회로를 포함하여 전자기 신호(electromagnetic signal)라고도 알려진 RF 신호를 송수신함으로써, 다른 컴퓨터 시스템과 통신을 가능하게 할 수도 있다.

[0043] 이러한 도 3의 실시예는, 컴퓨터 시스템(300)의 일례일 뿐이고, 컴퓨터 시스템(300)은 도 3에 도시된 일부 컴포넌트가 생략되거나, 도 3에 도시되지 않은 추가의 컴포넌트를 더 구비하거나, 2개 이상의 컴포넌트를 결합시키

는 구성 또는 배치를 가질 수 있다. 예를 들어, 모바일 환경의 통신 단말을 위한 컴퓨터 시스템은 도 3에 도시된 컴포넌트들 외에도, 터치스크린이나 센서 등을 더 포함할 수도 있으며, 통신 회로(360)에 다양한 통신 방식(WiFi, 3G, LTE, Bluetooth, NFC, Zigbee 등)의 RF 통신을 위한 회로가 포함될 수도 있다. 컴퓨터 시스템(300)에 포함 가능한 컴포넌트들은 하나 이상의 신호 처리 또는 어플리케이션에 특화된 집적 회로를 포함하는 하드웨어, 소프트웨어, 또는 하드웨어 및 소프트웨어 양자의 조합으로 구현될 수 있다.

[0044] 이하에서는 본 발명에 따른 바이오 데이터를 기반으로 한 사용자 인증 절차의 구체적인 실시예를 설명하기로 한다.

[0045] 동형 암호란 평문(plaintext)에 특정 연산을 수행하여 암호화한 결과와, 평문에 바로 암호화를 한 후 같은 연산을 적용한 결과가 서로 같은 암호이다.

[0046] 예를 들어, 덧셈에 대한 동형 암호는 평문 m_1, m_2의 암호화 연산 E 및 복호화 연산 D에 대해 $D(E(m_1+m_2))=D(E(m_1)+E(m_2))$를 만족하는 암호이며, 곱셈에 대한 동형 암호는 $D(E(m_1\times m_2))=D(E(m_1)\times E(m_2))$를 만족하는 암호이다. 덧셈과 곱셈에 대해 모두 동형인 암호를 완전 동형 암호(fully homomorphic encryption)라 한다.

[0047] 본 발명에서는 평문 m_1, m_2가 이진수 비트인 경우, 즉 평문 m_1, $m_2\in\{0, 1\}$인 경우를 고려하며, 평문의 덧셈 및 곱셈 연산은 mod 2로 수행하고, 암호문의 덧셈 및 곱셈은 mod 연산 없이 수행하는 경우를 고려한다. 즉, $D(E((m_1+m_2)\mathrm{mod}2))=D(E(m_1)+E(m_2))$, $D(E((m_1\times m_2)\mathrm{mod}2))=D(E(m_1)\times E(m_2))$가 성립하는 완전 동형 암호를 고려한다.

[0048] Mod 2에 대한 덧셈 및 곱셈은 각각 배타적 논리합(Exclusive OR: 기호 $\oplus$)과 논리곱(Logical AND: 기호 $\wedge$) 연산과 동치이므로, $D(E(m_1\oplus m_2))=D(E(m_1)+E(m_2))$, $D(E(m_1\wedge m_2))=D(E(m_1)\times E(m_2))$를 만족한다.

[0049] 이하에서는 동형 암호를 이용하여 안전하게 바이오 인식 기반 인증을 수행하는 방법을 설명한다. 설명의 편의상 지문 인식을 이용한 인증만을 설명하나, 홍채, 음성, 필체 등 기타 다른 바이오 인식 기반 인증에도 동일하게 적용할 수 있다.

[0050] 일반적으로 지문 인식 기반 인증은 사용자 등록 단계와 사용자 인증 단계로 구성된다.

[0051] 먼저, 사용자 등록 단계는 다음과 같은 과정으로 이루어진다.

[0052] 1. 사용자 단말(101)은 사용자 등록을 위해 사용자로부터 아이디(ID)를 입력 받고 사용자가 바이오 데이터의 등록을 위해 손가락을 지문 인식 센서에 위치시키면 지문 인식 센서를 통해 지문 원본 이미지를 획득할 수 있다. 예를 들어, 지문 원본 이미지는 도 4의 (a)와 같이 비트맵 이미지로 생성될 수 있다.

[0053] 2. 사용자 단말(101)은 지문 원본 이미지를 변환하여 특징점들로 구성된 템플릿 T을 생성한다. 사용자 단말(101)은 메모리 상에 저장된 비트맵 이미지(도 4의 (a))로부터 특징점들을 추출함으로써 도 4의 (b)와 같이 특징점들로 구성된 지문 템플릿을 생성할 수 있다. 이때, 특징점이란 지문의 골이 둘로 갈라지는 점(도 4의 (c): 분기점(ridge bifurcation)), 지문의 골이 끝나는 점(도 4의 (d): 종점(ridge ending)) 등 해당 지문을 구분하는 특성이 될 수 있는 점을 의미하며, 각 특징점은 (x, y, Θ, t)로 구성된다. x, y는 이미지 상에서 해당 특징점의 위치를 나타내는 좌표, Θ는 특징점에 접촉한 지문 골과 기준선(예를 들면, x축)과의 각도, t는 특징점의 타입(예를 들어, 0: 분기점, 1: 종점)을 의미한다. 템플릿이란 이러한 특징점들을 모아놓은 집합(도 4의 (b)에서 작은 동그라미들)이다.

[0054] 3. 사용자 단말(101)은 사용자로부터 입력된 아이디(ID)와 상기 2. 과정에서 생성된 지문 템플릿 T을 (ID, T) 쌍으로 사용자 단말(101) 내의 저장소에 저장한다.

[0055] 다음으로, 사용자 인증 단계는 아래와 같다.

[0056] 1. 사용자 단말(101)은 사용자로부터 아이디(ID)를 입력 받고, 사용자가 인증을 위하여 손가락을 지문 인식 센서에 위치시키면 지문 인식 센서에서 지문 원본 이미지를 얻어 비트맵을 생성한다.

[0057] 2. 사용자 단말(101)은 메모리 상의 지문 비트맵을 변환하여 특징점들로 구성된 템플릿 T'를 생성한다.

[0058] 3. 사용자 단말(101)은 저장소에서 사용자가 입력한 아이디(ID)에 해당하는 순서쌍 (ID, T)를 찾아 지문 템플릿 T을 추출한다.

[0059] 4. 사용자 단말(101)은 저장소에서 추출한 지문 템플릿 T와 사용자 인증 요청 과정에서 생성한 지문 템플릿 T'를 비교(match)하여 비교 점수(matching score)가 정해진 기준 값(threshold score) 이상이면 해당 아이디(ID)의 로그인을 허용하며, 비교 점수가 기준 값 미만이면 로그인을 거부한다.

[0060] 이때, 비교 점수는 두 템플릿 T와 T'를 구성하는 특징점들 중 어느 정도가 일치하는지를 나타내는 점수이다. 지문의 특성 상 이미지 획득 시 센서 오차, 습도나 조도, 손가락의 이물질 등 주변 환경 변화, 지문 센서에 손가락을 누르는 순간의 압력 차이, 지문 일부 영역이 센서에 찍히지 않음에 의한 특정 이미지 영역 손실 등에 의해 같은 지문이라도 지문 획득 시마다 이미지 왜곡 및 손상 등 약간의 오차가 발생할 수 있는데, 이를 감안하여 두 템플릿 간의 특징점들이 100% 일치하지 않더라도 기준 값을 넘으면 같은 지문으로 간주할 수 있다. 한편, 전혀 다른 손가락이라도 우연히 몇 개의 특징점들이 일치할 수 있으므로 기준 값을 너무 낮게 설정할 경우 타 사용자의 지문을 맞는 것으로 승인하는 오류가 생길 수 있다. 따라서, 기준 점수는 정상 사용자의 지문 인식 오차를 감내하면서 타 사용자는 인식하지 않도록 하는 적절한 수준에서 결정하게 된다.

[0061] 일반적인 지문 인식 기반 인증 방식의 사용자 등록 단계에서 지문 템플릿 T를 로컬 시스템인 사용자 단말(101) 내에 저장하므로 만약 시스템이 해킹 등 외부 공격에 노출될 경우 템플릿이 유출될 수 있다. 공격자는 템플릿을 역변환하여 지문 원본 이미지 또는 이와 유사한 이미지를 획득할 수 있으며, 이렇게 획득된 이미지를 실리콘 등의 재질에 입히면 사용자의 손가락과 거의 같은 지문을 갖는 가짜 손가락을 만들어낼 수 있다. 이는 사용자의 지문이 사용되는 스마트폰, 출입구 개폐 장치 등 다양한 곳에 악용됨으로써 피해를 양산할 수 있다.

[0062] 본 발명에서는 로컬 시스템에 대한 해킹 시 피해를 최소화하기 위해 지문 템플릿을 클라우드 서버인 원격 관리 서버(100)에 저장하며, 원격 관리 서버(100)에서 지문 템플릿을 악용하는 것을 방지하기 위해 템플릿에 동형 암호를 적용하여 암호문만을 저장하도록 한다.

[0063] 두 템플릿 간의 비교는 원격 관리 서버(100)가 암호문 상에서 수행한다. 일반적으로 비교 점수를 결정하는 데에는 각 특징점의 좌표(x, y)와 각도(Θ), 타입(t) 등이 이용되나, 이 중 특히 좌표가 가장 중요한 역할을 하며 나머지 두 가지 정보는 보조적인 역할을 하므로 이하에서는 설명의 편의상 특징점 좌표(x, y)만을 이용한 비교에 대해 설명한다. 다만, 각도(Θ)와 타입(t)을 추가로 이용하는 방법도 유사한 방법으로 가능하다.

[0064] 본 발명의 일 실시예에 따른 지문 인식 기반 인증은 사용자 등록과 사용자 인증 과정으로 구성된다.

[0065] 먼저, 도 5를 참조하여 사용자 등록 단계의 구체적인 과정을 설명하기로 한다.

[0066] 1. 로컬 시스템인 사용자 단말(101)은 지문 등록 과정에서 동형 암호를 위한 키 K를 생성한 후 생성된 동형 암호화 키 K를 사용자 단말(101) 상의 저장소에 저장한다(S51).

[0067] 2. 사용자 단말(101)은 사용자로부터 아이디(ID)를 입력 받고 사용자가 등록을 위하여 손가락을 지문 인식 센서에 위치시키면 지문 인식 센서에서 지문 이미지를 획득한다(S52). 예를 들어, 지문 이미지는 도 4의 (a)와 같이 비트맵 이미지로 생성될 수 있다.

[0068] 3. 사용자 단말(101)은 지문 이미지를 변환하여 특징점들로 구성된 지문 템플릿 T을 생성한다(S53). 단, 템플릿의 각 특징점 i는 x와 y 좌표를 각각 n 비트의 비트 열로 표현한 (x_{i1}, …, x_{in}, y_{i1}, …, y_{in})로 구성된다.

[0069] 4. 사용자 단말(101)은 각 특징점 i를 구성하는 2n비트들을 각각 동형 암호에 의해 암호화하여 암호문 ep_i=(E(x_{i1}), …, E(x_{in}), E(y_{i1}), …, E(y_{in}))을 생성한다(S54).

[0070] 5. 사용자 단말(101)은 사용자로부터 입력된 아이디(ID)와 단계(S54)에서 동형 암호를 이용하여 암호화 된 암호문(ep_1, …, ep_m)(여기서, m은 특징점의 개수)를 사용자의 (아이디, 암호문) 쌍으로 구성하여 원격 관리 서버(100)로 전송한다(S55).

[0071] 6. 원격 관리 서버(100)는 사용자 단말(101)로부터 수신된 사용자의 (아이디, 암호문) 쌍인 (ID, ep_1, …, ep_m)를 데이터베이스에 저장함으로써 사용자 인증 정보를 등록한다(S56).

[0072] 도 6을 참조하여, 사용자 인증 단계의 구체적인 과정을 설명하기로 한다. 이하는, 아이디가 ID인 사용자가 자신의 지문을 입력하고 인증을 수행하는 단계를 설명한 것이다.

[0073] 1. 사용자 단말(101)은 사용자 인증을 위해 사용자가 아이디(ID)를 입력하고 손가락을 지문 인식 센서에 위치시키면 지문 인식 센서에서 지문 이미지(비트맵 이미지)를 획득한다(S61).

[0074] 2. 사용자 단말(101)은 지문 이미지를 변환하여 특징점들로 구성된 지문 템플릿 T'을 생성한다(S62). 단, 템플릿의 각 특징점 i는 해당 특징점을 나타내는 x와 y 좌표를 각각 n 비트의 비트 열로 표현한 (x'_{i1}, …, x'_{in}, y'_{i1}, …, y'_{in})로 구성된다.

[0075] 3. 사용자 단말(101)은 지문 템플릿 T'의 각 특징점 i를 구성하는 x, y 좌표를 각각 n 비트로 표현한 (x'_{i1}, …, x'_{in}, y'_{i1}, …, y'_{in})를 동형 암호로 암호화 하여 암호문 ep'_i=(E(x'_{i1}), …, E(x'_{in}), E(y'_{i1}), …, E(y'_{in}))을 생성한다(S63).

[0076] 4. 사용자 단말(101)은 사용자로부터 입력된 아이디(ID)와 단계(S63)에서 동형 암호를 이용하여 암호화 된 암호문(ep'_1, …, $ep'_{m'}$)(여기서, m'은 특징점의 개수를 의미하고, 지문 인증의 특성 상 정상적인 지문이라도 m=m' 혹은 m≠m'일 수 있다.)을 (아이디, 암호문) 쌍으로 구성하여 원격 관리 서버(100)로 전송한다(S64).

[0077] 5. 원격 관리 서버(100)는 사용자 단말(101)로부터 사용자의 (아이디, 암호문) 쌍인 (ID, ep'_1, …, $ep'_{m'}$)가 수신되면 수신된 아이디 ID에 대해 이전에 저장한 (ID, ep_1, …, ep_m)를 데이터베이스로부터 추출한다(S65).

[0078] 6. 원격 관리 서버(100)는 아이디 ID에 대해 사용자 단말(101)로부터 수신된 암호문 ep'_1, …, $ep'_{m'}$과 데이터베이스로부터 추출된 암호문 ep_1, …, ep_m을 이용하여 두 암호문 간의 비교 연산을 수행한다(S66). 단, 정상 지문에서 특징점 좌표의 미세한 오류(좌표 값±1)를 허용하기 위해 다음과 같이 확장 비교를 수행한다.

[0079] 6-1. (ep_1, …, ep_m)=((E(x_{11}), …, E(x_{1n}), E(y_{11}), …E(y_{1n})), …(E(x_{m1}), …, E(x_{mn}), E(y_{m1}), …E(y_{mn})))을 구성하는 ep_i의 암호화 된 x좌표 (x_{i1}, …, x_{in})에 1의 암호문을 동형 덧셈하여 $(E(x_{i1}^{+1}),\ldots,E(x_{in}^{+1}))$ 을 생성하고, (x_{i1}, …, x_{in})에 1의 암호문을 동형 뺄셈하여 $(E(x_{i1}^{-1}),\ldots,E(x_{in}^{-1}))$ 을 생성한다.

[0080] 6-2. ep_i의 암호화 된 y좌표 (y_{i1}, …, y_{in})에 1의 암호문을 동형 덧셈하여 $(E(y_{i1}^{+1}),\ldots,E(y_{in}^{+1}))$ 을 생성하고, (y_{i1}, …, y_{in})에 1의 암호문을 동형 뺄셈하여 $(E(y_{i1}^{-1}),\ldots,E(y_{in}^{-1}))$ 을 생성한다.

[0081] 6-3. 표기 상의 편의를 위해

[0082] $$\left(E(x_{i1}^{0}),\ldots,E(x_{in}^{0})\right)=\left(E(x_{i1}),\ldots,E(x_{in})\right),$$

[0083] $(E(y_{i1}^{0}),\ldots,E(y_{in}^{0}))=(E(y_{i1}),\ldots,E(y_{in}))$ 라 하면,

[0084] 원래의 ep_i로부터 6-1과 6-2에 의해 다음과 같이 확장된 암호화 좌표 값 순서쌍 9개를 얻을 수 있다.

[0085] $$\left\{\left(E(x_{i1}^{0}),\ldots,E(x_{in}^{0})\right),\left(E(x_{i1}^{+1}),\ldots,E(x_{in}^{+1})\right),\left(E(x_{i1}^{-1}),\ldots,E(x_{in}^{-1})\right)\right\}$$

[0086] $$\times\left\{\left(E(y_{i1}^{0}),\ldots,E(y_{in}^{0})\right),\left(E(y_{i1}^{+1}),\ldots,E(y_{in}^{+1})\right),\left(E(y_{i1}^{-1}),\ldots,E(y_{in}^{-1})\right)\right\}$$

[0087] 6-4. i=1, …, m에 대해 6-1부터 6-3의 과정을 반복하여 확장된 암호화 좌표 값 순서쌍 9m개를 얻을 수 있다.

[0088] 6-5. i=1, …, m, j=1, …, m', s=-1, 0, +1, t=-1, 0, +1에 대해 다음 비교 연산을 수행한다.

[0089] $$E(r_{ijst})=\left(\mathrm{E}(1)+E(x_{i1}^{s})+E(x'_{j1})\right)\times\cdots\times\left(\mathrm{E}(1)+E(x_{in}^{s})+E(x'_{jn})\right)$$
$$\times\left(\mathrm{E}(1)+E(y_{i1}^{t})+E\left(y'_{j1}\right)\right)\times\cdots\times\left(\mathrm{E}(1)+E(y_{in}^{t})+E\left(y'_{jn}\right)\right)$$

[0090] 6-6. 전가산기를 동형으로 수행하여 (E(a_z), …, E(a_0))= $\sum_{i=1,..,m,j=1,..,m',s=-1,0,+1,t=-1,0,+1}E(r_{ijst})$ 를 계산한다.

[0091] 7. 원격 관리 서버(100)는 두 암호문 간의 비교 연산 결과인 ($E(a_z)$, …, $E(a_0)$)를 사용자 단말(101)로 전송한다(S67).

[0092] 8. 사용자 단말(101)은 원격 관리 서버(100)로부터 암호문 비교 연산 결과 ($E(a_z)$, …, $E(a_0)$)가 수신되면 지문 등록 과정에서 생성된 동형 암호화 키 K를 이용하여 암호문 비교 연산 결과 ($E(a_z)$, …, $E(a_0)$)에 대한 해독 연산(decryption)을 수행한다(S68). 이때, 암호문 비교 연산 결과 ($E(a_z)$, …, $E(a_0)$)는 동형 암호화 키 K에 의해 (a_z), …, (a_0)와 같이 복호화 된다.

[0093] 9. 사용자 단말(101)은 해독 연산 결과 (a_z), …, (a_0)에 따라 사용자 인증을 처리할 수 있다(S69). 다시 말해, 사용자 단말(101)은 해독 연산 결과 (a_z), …, (a_0)를 이진수 정수로 해석하여 이 값이 미리 정해진 기준 값 이상이면 사용자의 로그인을 허용하고, 기준 값 미만이면 사용자의 로그인을 거부한다.

[0094] 본 발명에 의한 다른 실시예로서, x, y 좌표 값에 각각 ±1의 오류가 아닌 ±?의 오류를 허용할 경우에는 6-1에서 6-3단계를 변형하여 원래의 ep_i로부터

$$\left\{\left(E(x_{i1}^{-\epsilon}),\dots,E(x_{in}^{-\epsilon})\right),\dots,\left(E(x_{i1}^{0}),\dots,E(x_{in}^{0})\right),\dots,\left(E(x_{i1}^{+\epsilon}),\dots,E(x_{in}^{+\epsilon})\right)\right\}$$
$$\times\left\{\left(E(y_{i1}^{-\epsilon}),\dots,E(y_{in}^{-\epsilon})\right),\dots,\left(E(y_{i1}^{0}),\dots,E(y_{in}^{0})\right),\dots,\left(E(y_{i1}^{+\epsilon}),\dots,E(y_{in}^{+\epsilon})\right)\right\}$$

와 같은 확장된 암호화 좌표 값 순서쌍 $(2\epsilon+1)^2$개를 얻도록 할 수 있으며, 이 경우 6-4 단계에 의해 확장된 암호화 좌표 값 순서쌍 $(2\epsilon+1)^2\times$m개를 얻고, 6-5와 6-6 단계는 s=-ϵ, 0, +ϵ, t=-ϵ, 0, +ϵ에 대해 수행하게 된다.

[0095] 본 발명에 의한 또 다른 실시예로서, 단계 6-1부터 6-4를 사용자 인증 과정이 아닌 사용자 등록 과정에서 사전에 수행함으로써 인증 시간을 단축하도록 하는 변형도 가능하다.

[0096] 본 발명에 의한 또 다른 실시예로, 템플릿 확장을 원격 관리 서버(100)가 하지 않고 로컬 시스템인 사용자 단말(101)이 평문 상태에서 수행 후 그 결과를 암호화하여 각 암호문을 전송하는 방법도 가능하다. 이 경우 원격 관리 서버(100)가 수행하는 단계 6-1부터 6-4를 생략하고 대신 사용자 등록 과정에서 사용자 단말(101)이 수행하도록 해야 하는데, 사용자 등록의 4 단계 내지 5단계를 다음과 같이 변형하면 된다.

[0097] 4. 사용자 단말(101)은 다음 과정을 수행한다.

[0098] 4-1. 특징점 i를 구성하는 x 좌표에 1을 더하여 $(x_{i1}^{+1},\dots,x_{in}^{+1})$를 생성하고, x좌표에 1을 빼서 $(x_{i1}^{-1},\dots,x_{in}^{-1})$를 생성한다.

[0099] 4-2. 특징점 i를 구성하는 y 좌표에 1을 더하여 $(y_{i1}^{+1},\dots,y_{in}^{+1})$를 생성하고, y좌표에 1을 빼서 $(y_{i1}^{-1},\dots,y_{in}^{-1})$를 생성한다.

[0100] 4-3. 표기 상의 편의를 위해

[0101] $(x_{i1}^{0},\dots,x_{in}^{0})=(x_{i1},\dots,x_{in})$, $(y_{i1}^{0},\dots,y_{in}^{0})=(y_{i1},\dots,y_{in})$라 할 때,

[0102] 원래의 좌표 및 4-1과 4-2단계에서 확장된 좌표들을 비트 별로 동형 암호화하여 암호화 좌표 값 순서쌍 9개를 얻을 수 있다.

[0103]
$$\left\{\left(E(x_{i1}^{0}),\dots,E(x_{in}^{0})\right),\left(E(x_{i1}^{+1}),\dots,E(x_{in}^{+1})\right),\left(E(x_{i1}^{-1}),\dots,E(x_{in}^{-1})\right)\right\}$$
$$\times\left\{\left(E(y_{i1}^{0}),\dots,E(y_{in}^{0})\right),\left(E(y_{i1}^{+1}),\dots,E(y_{in}^{+1})\right),\left(E(y_{i1}^{-1}),\dots,E(y_{in}^{-1})\right)\right\}$$

[0104] 4-4. i=1, …, m에 대해 4-1부터 4-3의 과정을 반복하여 확장된 암호화 좌표 값 순서쌍 9m개(총 9m×2n개의 암호문)를 얻을 수 있다.

[0105] 5. 사용자 단말(101)은 4.단계에서 계산된 총 9m×2n개의 암호문을 아이디 ID와 함께 원격 관리 서버(100)에 전송하고, 원격 관리 서버(100)는 이를 저장할 수 있다.

[0106] 본 발명에 따른 지문 인식 기반 사용자 인증 방법은 다음과 같은 성질을 만족한다.

[0107] 1. 정상적인 사용자 인증 기능 제공: 만약 사용자가 정상적인 지문을 지문 센서에 인식시켰다면 사용자 인증 단계에서 로컬 시스템이 복호화 하여 얻은 (a_z), …, (a_0) 값은 기준 값 이상일 것이므로 로그인이 허용된다. 반면에, 잘못된 지문을 입력한다면 매우 높은 확률로 (a_z), …, (a_0)는 0에 가까운 값이므로 로그인이 거부된다.

[0108] 2. 로컬 시스템 공격 시 지문 원본 보호: 로컬 시스템에 저장된 정보는 동형 암호를 위한 키 K밖에 없으므로, 로컬 시스템이 해커에 의해 공격 당하는 경우에도 사용자의 지문은 안전하게 보호된다. 지문 원본 및 이를 변환한 템플릿 모두 로컬 시스템에는 저장되지 않는다.

[0109] 3. 클라우드 서버에 의한 지문 복원 불가: 클라우드 서버는 지문 원본 또는 템플릿을 직접 저장하는 것이 아니라 지문 템플릿 특징점들의 암호문만을 저장하고 있으므로 템플릿을 복원할 수 없다. 특징점 좌표를 얻어내기 위해서는 동형 암호 키 K를 정확히 알아야 하는데, 이 키는 로컬 시스템만이 알고 있기 때문이다. 만약 로컬 시스템을 해킹하여 동형 암호 키 K를 획득한 공격자가 클라우드 서버까지 공격에 성공한 경우에는 템플릿 특징점 좌표들을 복원할 수 있으므로 사전 공격이 가능하나, 현실적으로 두 시스템 모두 공격 당하는 상황은 발생하기 어렵다.

[0110] 이와 같이, 본 발명의 실시예에 따르면, 바이오 데이터를 원격 서버에 저장하는 클라우드 형태로 관리하고, 특히 동형 암호를 이용하여 암호화 된 형태로 바이오 데이터를 원격 서버에 저장함으로써 바이오 데이터의 유출을 보다 근본적으로 차단하여 원격 서버를 완전히 신뢰할 수 없는 상황에서도 외부 공격에 대한 저항성과 안전성을 향상시킬 수 있다.

[0111] 본 발명의 실시예에 따른 방법들은 다양한 컴퓨터 시스템을 통하여 수행될 수 있는 프로그램 명령(instruction) 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 본 실시예에 따른 프로그램은 PC 기반의 프로그램 또는 모바일 단말 전용의 어플리케이션으로 구성될 수 있다.

[0112] 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.

[0113] 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 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 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.

[0114] 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 수행하도

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. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0115] 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.

[0116] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

부호의 설명

[0117] 100: 원격 관리 서버

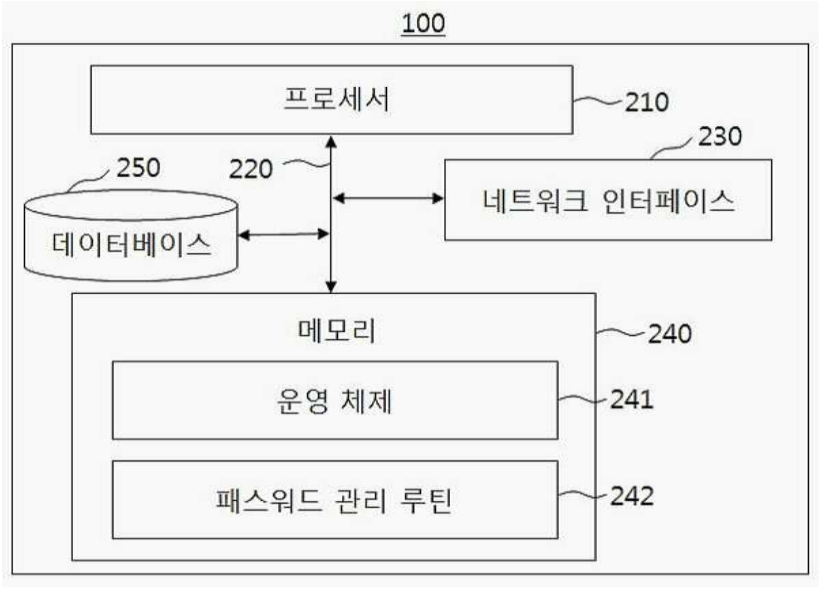
101: 사용자 단말

도면

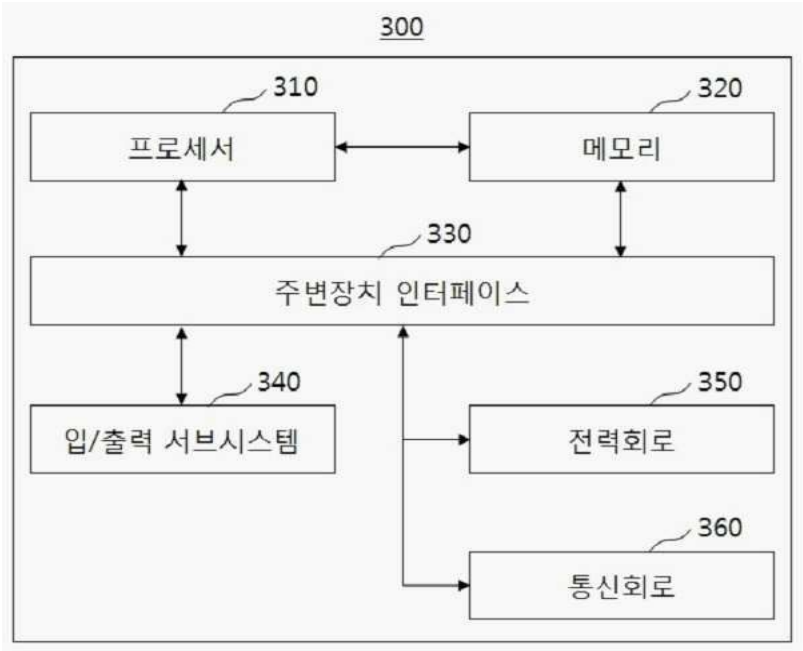
도면1



도면2



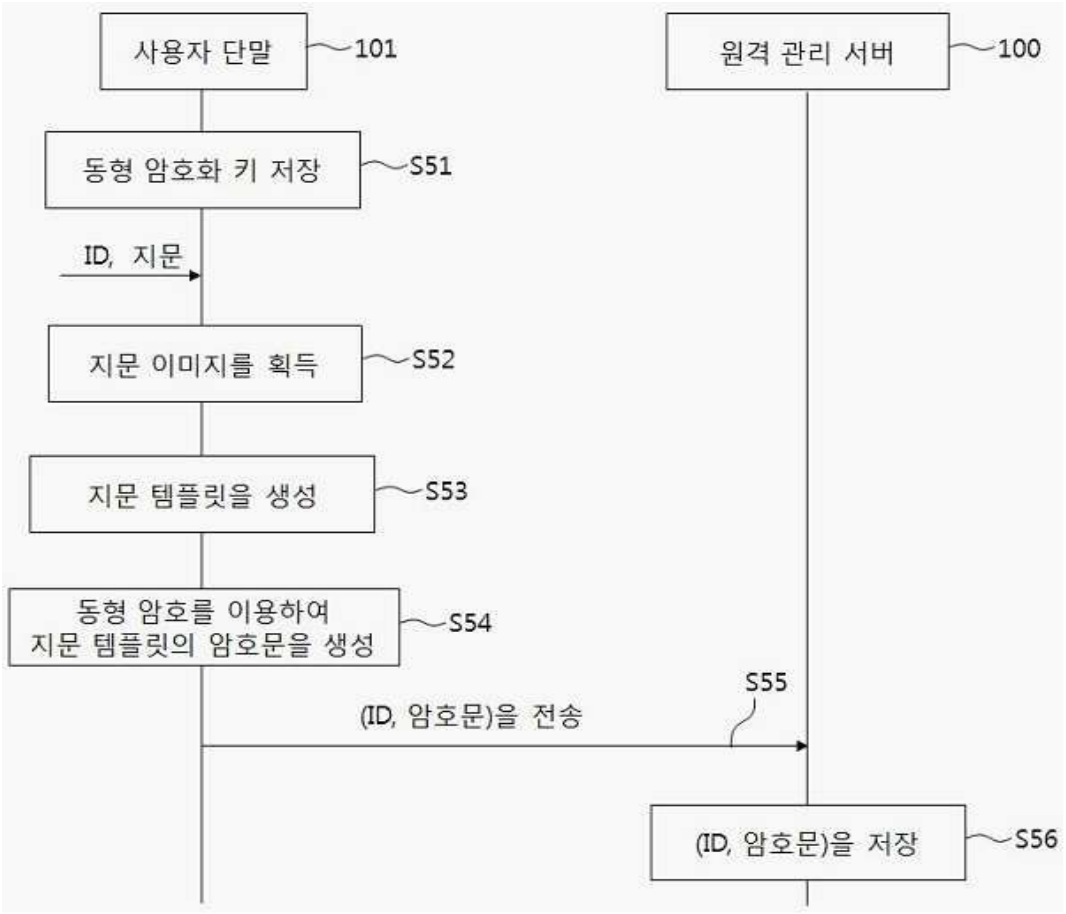
도면3


300
310
프로세서
320
메모리
330
주변장치 인터페이스
340
입/출력 서브시스템
350
전력회로
360
통신회로

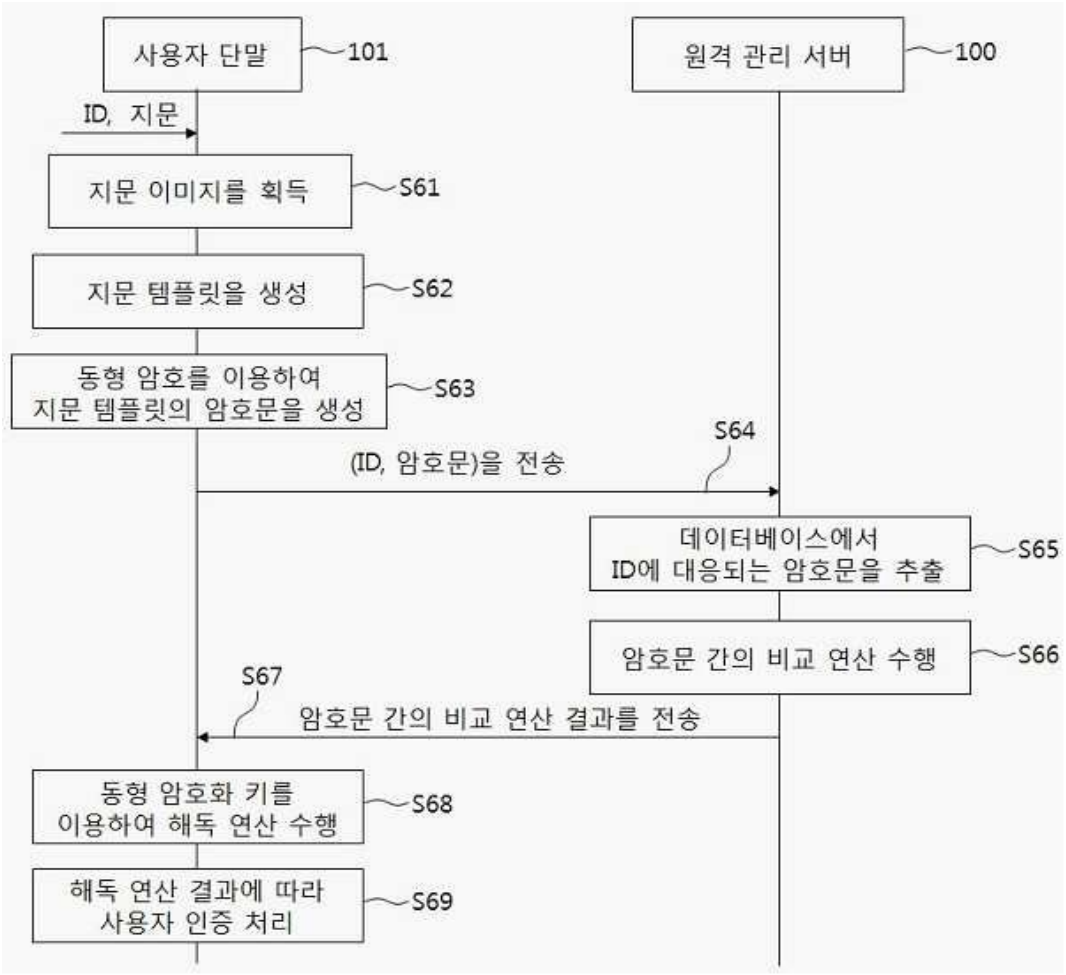
도면4


(a) 지문 원본 이미지
(b) 지문 템플릿
(c) 특징점(분기점)
(d) 특징점(종점)

도면5


사용자 단말
101
원격 관리 서버
100
동형 암호화 키 저장
S51
ID, 지문
지문 이미지를 획득
S52
지문 템플릿을 생성
S53
동형 암호를 이용하여
지문 템플릿의 암호문을 생성
S54
S55
(ID, 암호문)을 전송
(ID, 암호문)을 저장
S56

도면6



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 5

【변경전】

상기 사용자 단말에서

【변경후】

사용자 단말에서