(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년05월19일
(11) 등록번호 10-1622253
(24) 등록일자 2016년05월12일

(51) 국제특허분류(Int. Cl.)
G06F 21/32 (2013.01)
(21) 출원번호 10-2014-0085958
(22) 출원일자 2014년07월09일
심사청구일자 2014년07월09일
(65) 공개번호 10-2016-0006836
(43) 공개일자 2016년01월20일
(56) 선행기술조사문헌
KR1020060044801 A
KR1020080022729 A
KR100787114 B1
JP2009205391 A

(73) 특허권자
전남대학교 산학협력단
광주광역시 북구 용봉로 77 (용봉동)
(72) 발명자
최덕재
광주 북구 설죽로 595, 106동 101호 (일곡동, 롯데아파트)
황민탕
광주 북구 용봉로 77, 생활관 6동 407호 (용봉동, 전남대학교)
(74) 대리인
박종한

전체 청구항 수 : 총 10 항 심사관 : 문남두

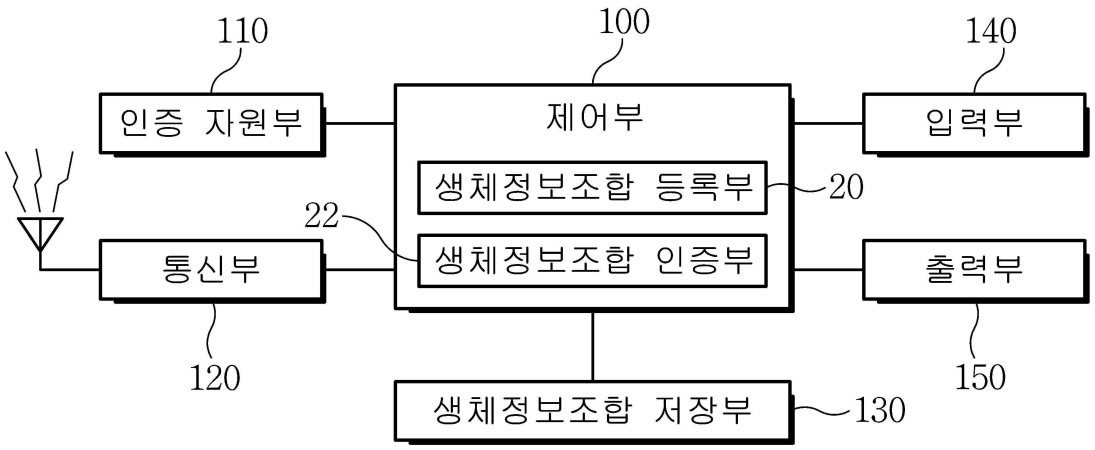
(54) 발명의 명칭 **생체정보 또는 생체정보로부터 파생된 정보 또는 사용자 특징 정보를 이용한 안전한 인증 시스템, 그 시스템에서의 인증 제어를 위한 장치 및 방법**

(57) 요 약

본 발명은 생체정보 또는 생체정보로부터 파생된 정보 또는 사용자 특징 정보를 이용한 안전한 인증 시스템, 그 시스템에서의 인증 제어를 위한 장치 및 방법에 관한 것으로, 이를 위해 인증 제어 장치는 생체정보 또는 이들의 조합 또는 사용자 특징 정보인 생체정보조합을 다양한 센서를 통해 얻고 임의의 키(key)로부터 오류 정정 코드

(뒷면에 계속)

대 표 도 - 도1



(Error Correction Code)의 인코딩을 수행하여 얻어진 코드워드(codeword)와 생체정보조합(ω)과 연산(XOR)을 통해 결과 값(인증 데이터:δ)을 얻어 이 δ와 이에 사용된 키(Key)를 해시하여 저장한다. 또한, 인증을 수행할 경우 인증 데이터 δ과 키를 해싱 한 값을 저장할 때 사용한 방법과 동일한 방식으로 생체정보조합(ω')을 획득하고, 이 획득된 생체정보조합(ω')과 저장된 인증 데이터(δ)과 연산을 통해 코드워드(codeword (c'))를 얻는다. 저장할 때, 사용한 인코딩 방식의 역함수 디코딩 방식을 코드워드 c'에 적용 사용하여 k'을 얻는다. 그리고, 여기에 해시 함수를 적용한 Hash(k')와 저장된 Hash(k) 값이 동일한 지 확인하여 인증을 수행한다. 생체정보의 경우 등록할 때와 인증을 수행할 때 측정한 값이 상이할 수 있으며, 이의 허용정도를 조절하기 위해 오류정정 코드(Error Correcting Code)의 오류허가비트 매개변수를 사용한다. 그러므로, 오류허가 비트의 개념이 있는 모든 오류 정정 코드(Error Correcting Code) 방식이 이 목적에 사용될 수 있다.

이 발명을 지원한 국가연구개발사업

과제고유번호	2012R1A1A2007014
부처명	교육부
연구관리전문기관	한국연구재단
연구사업명	일반연구자지원사업/기본연구지원사업
연구과제명	사용자프로필을 이용한 이동단말용 응용서비스를 위한 자동인증기술
기 여 율	1/1
주관기관	전남대학교
연구기간	2014.05.01 ~ 2015.04.30

명 세 서

청구범위

청구항 1

인증을 위한 데이터를 저장하는 저장부;

등록 요구에 따라 적어도 하나의 측정 메카니즘 및 이들의 조합으로 생성된 생체정보조합을 생성하고, 생성한 생체정보조합을 연산을 위해 전처리를 통해 생체정보조합 템플릿(ω)을 생성하고, 랜덤 키(random key) 발생 함수를 사용하여 키(key)를 생성하고, 생성된 키(Key)를 오류 정정 코드(Error Correction Code)로 인코딩하여 코드워드(codeword(c))를 생성한 후 상기 코드워드(codeword(c))와 생체정보조합 템플릿(ω)와 조합(exclusive OR)을 통해 인증 데이터(δ)를 얻어, 상기 인증 데이터(δ)와 키(key)에 해시 함수를 적용한 해시값((Hash(key))을 상기 저장부에 저장하는 생체정보조합 등록부;

를 포함하는 것을 특징으로 하는 인증 제어 장치.

청구항 2

제 1항에 있어서, 상기 인증 데이터(δ)는,

하기 <수학식 1>과 같이 표현할 수 있는 것을 특징으로 하는 인증 제어 장치.

[수학식 1]

$$\delta = c \text{ XOR } \omega$$

ω: 생체정보조합으로부터 가공된 디지털 정보,

c: 랜덤 키(K)를 오류 정정 코드(Error Correction Code)를 사용하여 인코딩한 결과 생성된 코드워드

청구항 3

제 1항에 있어서, 상기 오류 정정 코드(Error Correction Code)는,

데이터 길이(n), 정보길이(k), 오류 인정 길이(t)를 갖고, 상기 t 값을 조정하여 인증 강도를 조절하는 것을 특징으로 하는 인증 제어 장치.

청구항 4

제 1항에 있어서, 상기 생체정보조합 등록부는,

상기 생체정보조합의 길이는 상기 코드워드(codeword(c))의 길이와 같은 길이가 되도록 전처리하는 것을 특징으로 하는 인증 제어 장치.

청구항 5

등록된 가공생체정보조합인 인증 데이터(δ) 및 해시값(Hash(key))을 저장하는 저장부;

등록 시 사용한 방식으로 생체정보 또는 생체로부터 파생한 정보인 생체정보조합(ω' 를 얻고)를 획득하여 상기 저장된 인증 데이터(δ)와 연산을 통해 코드워드(codeword c')을 얻고, 등록 시 사용된 인코딩 방식과 대응되는 디코딩 방식을 사용하여 키(key k')를 얻고, 상기 키(key k')에 해시 함수를 적용하여 저장된 해시값(Hash(key))와 비교하여 일치여부에 따라 인증을 허용하는 생체정보조합 인증부;

를 포함하는 것을 특징으로 하는 인증 제어 장치.

청구항 6

제 5항에 있어서, 상기 코드워드(codeword c')는,

하기 <수학식 2>과 같이 표현할 수 있는 것을 특징으로 하는 인증 제어 장치.

[수학식 2]

c' = ω' XOR δ

ω' :인증수행시 획득한 생체정보로부터 파생된 생체정보조합

k' = BCH-Decoding(c')

청구항 7

적어도 하나의 물리적 센서나 이의 조합 또는 로지컬 센서를 통해 측정된 사용자 특징 정보를 포함하는 사용자의 생체정보조합 신호를 획득하는 과정;

상기 획득한 생체정보조합 신호에 대하여 전처리 및 분할 처리 후 실제 가치 있는 값을 가진 생체정보조합 템플릿을 추출하는 과정;

상기 생체정보조합 템플릿을 이진화 시키고, 신뢰성 있는 비트를 추출하는 과정;

인코딩을 위한 이진 암호화 키를 생성하여 인코딩하는 과정;

상기 생성한 암호화 키를 해시 함수가 적용시킨 해시값을 저장하는 과정;

상기 인코딩 된 암호화 키를 이용하여 추출한 이진화된 생체정보조합 템플릿을 바인딩하는 과정;

상기 바인딩처리된 생체정보조합 템플릿을 인증 데이터로 등록하는 과정;

을 포함하고,

상기 사용자 특징 정보는 사용자의 핸드폰 사용 패턴 및 로그 정보 중 적어도 하나를 포함하는 것을 특징으로 하는 생체정보 또는 생체정보로부터 파생된 정보 또는 사용자 특징 정보를 이용한 안전한 인증 방법.

청구항 8

제 7항에 있어서, 상기 인코딩하는 과정은

이때, 암호화 키를 생성하여 이를 이용하여 이진화된 생체정보조합 템플릿의 길이와 동일한 길이를 가지는 코드워드를 생성하기 위해 미리 설정된 인코딩 방식으로 인코딩하는 과정을 포함하는 것을 특징으로 하는 생체정보 또는 생체정보로부터 파생된 정보 또는 사용자 특징 정보를 이용한 안전한 인증 방법.

청구항 9

적어도 하나의 물리적 센서나 이의 조합 또는 로지컬 센서를 통해 측정된 사용자 특징 정보를 포함하는 사용자의 생체정보조합 신호를 획득하는 과정;

상기 획득한 생체정보조합 신호에 대하여 전처리 및 분할 처리 후 실제 가치 있는 값을 가진 생체정보조합 템플릿을 추출하는 과정;

상기 추출한 생체정보조합 템플릿을 이진화 시키는 과정;

상기 이진화된 생체정보조합 템플릿에 대해 보안 처리 후 저장된 인증 데이터(δ)에 바인딩시키는 과정;

암호화 키(k)를 획득하기 위해 미리 설정된 디코딩 방식으로 디코딩하는 과정;

상기 디코딩된 키의 해시값을 확인하고, 확인된 해시값과 생체정보조합 등록 시 미리 저장된 해시값을 비교하여 일치하는 경우 사용자를 인증 결정하는 과정;

을 포함하고,

상기 사용자 특징 정보는 사용자의 핸드폰 사용 패턴 및 로그 정보 중 적어도 하나를 포함하는 것을 특징으로 하는 생체정보 또는 생체정보로부터 파생된 정보 또는 사용자 특징 정보를 이용한 안전한 인증 방법.

청구항 10

제 7항 또는 9항에 있어서, 상기 생체정보조합 신호는,

임의의 단일 생체정보, 한 개 이상의 생체정보의 조합 신호, 생체정보로부터 파생된 정보나 이들의 조합 신호,

상기 사용자 특징 정보 중 하나의 신호인 것을 특징으로 하는 생체정보 또는 생체정보로부터 파생된 정보 또는 사용자 특징 정보를 이용한 안전한 인증 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 생체정보 또는 생체정보로부터 파생된 정보 또는 사용자 특징 정보를 이용한 안전한 인증 시스템, 그 시스템에서의 인증 제어를 위한 장치 및 방법에 관한 것으로, 더욱 상세하게는 정보단말기나 원격의 정보서비스를 이용하기 위하여 사용자 인증이 필요한 경우 인증을 위해 생체정보 또는 생체정보로부터 파생된 정보 또는 사용자 특징 정보를 사용하는 경우에 이 생체정보 또는 사용자 특징 정보가 정보단말기의 도난, 원격서비스를 제공하는 서버의 해킹으로 말미암아 생체정보 또는 사용자 특징 정보가 유출되지 않고 안전하게 인증에 사용될 수 있도록 하기 위한 인증 시스템, 그 시스템에서의 인증 제어를 위한 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 스마트폰 등 정보단말기를 사용할 때 그리고, 원격의 서비스를 이용할 때, 합법적인 사용자 외의 사용을 방지하기 위해서 인증이라는 절차를 거치는 경우가 많다.

[0003] 일반적인 인증 방법으로 아이디와 패스워드를 사용하는데 이는 공격자의 추측 및 암호화된 정보의 해독 기술로 안전성이 의심받고 있다. 이를 극복하기 위해 사용자만 가지고 있는 생체정보를 이용하는 방법이 확산되고 있다.

[0004] 인증을 위해 현재 많이 사용되고 있는 생체정보는 지문인식, 홍채인식, 얼굴인식, 걸음걸이 등이 있으며 하나 이상의 생체정보를 조합하여 인증에 사용하는 것을 멀티모달 생체정보 인증방식이라고 한다.

[0005] 직접적인 생체정보가 아닌 생체의 반응 정보를 이용하는 방법도 있다. 예를 들면, 단말 화면에 특정 패턴을 그리거나, 반응형 어플리케이션(application)에 반응하기 위한 손가락 놀림 속도, 터치(Touch) 압력, 걸음걸이 등 다양한 정보가 사용될 수 있다.

[0006] 기본적인 방식은 이러한 생체정보, 또는 생체정보의 조합, 생체로부터 발생하는 반응 정보, 사용자특징정보 등을 단말이나 서비스를 제공하는 서버에 저장, 또는 관련 인증 서버에 저장하고, 인증이 필요한 시점에서 이런 정보를 다시 획득하여 저장된 정보와 비교하여 저장된 정보와 같거나 허락할 정도의 근소한 차이가 있을 때, 인증을 허가하는 방식이다.

[0007] 인증을 위해 생체정보나 생체정보의 조합, 또는 생체정보에서 파생한 정보를 단말이나 서버에 등록(저장)하여 인증 수행 시점에서 동일한 정보를 획득하여 비교하는 방식은 저장된 정보의 유출이 발생할 경우, 생체정보의 유일한 특성 때문에 그 피해가 훨씬 심각하다.

[0008] 이와 같이 생체정보나 생체정보의 조합, 또는 생체정보에서 파생한 정보에 대한 유출이 발생할 수 있는 경로는 다양하다. 예를 들면, 생체정보를 저장하고 있는 단말 또는 서버의 분실, 도난, 해킹 등이 그 경로가 될 수 있다.

[0009] 그러므로, 생체정보나 관련 파생정보의 강력한 인증 능력을 유지하면서 동시에 유출을 방지할 수 있는 기술이 개발이 필요하다. 또한 생체 관련 정보는 측정 시 마다 항상 동일하지 않고 변이가 있으며, 어느 정도 변이가 있을지라도 동일한 사용자로 인증할 수 있는 기술 개발이 필요하다.

발명의 내용

해결하려는 과제

[0010] 이에 본 발명은 생체정보나 관련 파생정보 또는 사용자 특징 정보의 강력한 인증 능력을 유지하면서 동시에 유출을 방지할 수 있는 인증 시스템, 그 시스템에서의 인증 제어를 위한 장치 및 방법을 제공함에 있다.

[0011] 또한 본 발명은 측정 시 마다 항상 동일하지 않고 변이가 있을 수 있는 생체 관련 정보 또는 사용자 특징 정보에 대하여 어느 정도 변이가 있을지라도 동일한 사용자로 인증할 수 있도록 할 수 있는 인증 시스템, 그 시스템에서의 인증 제어를 위한 장치 및 방법을 제공함에 있다.

과제의 해결 수단

[0012] 상술한 과제의 해결 수단으로, 본 발명에 따른 생체정보 또는 사용자 특징 정보 기반의 인증 제어 장치는 인증을 위한 데이터를 저장하는 저장부; 등록 요구에 따라 센서 등 다양한 수집 또는 측정 메카니즘 및 이들의 조합으로 생성된 생체정보조합을 생성하고, 생성한 생체정보조합을 연산을 위해 전처리를 통해 생체정보조합 템플릿(ω)을 생성하고, 랜덤 키(random key) 발생 함수를 사용하여 키(key)를 생성하고, 생성된 키(Key)를 오류 정정 코드(Error Correction Code)로 인코딩하여 코드워드(codeword(c))를 생성한 후 코드워드(codeword(c))와 생체정보조합 템플릿(ω)와 조합(exclusive OR)을 통해 인증 데이터(δ)를 얻어, 인증 데이터(δ)와 키(key)에 해시함수를 적용한 해시값((Hash(key))을 저장부에 저장하는 생체정보조합 등록부를 포함하는 것을 특징으로 한다.

[0013] 여기서, 인증 데이터(δ)는, 하기 <수학식 1>과 같이 표현할 수 있는 것을 특징으로 한다.

[0014] [수학식 1]

[0015] $\delta = c \text{ XOR } \omega$

[0016] ω: 생체정보조합으로부터 가공된 디지털 정보

[0017] c: 랜덤키 K를 오류정정코드(Error Correction Code)로 인코딩한 결과

[0018] 또한, 오류 정정 코드(Error Correction Code)는, 데이터 길이(n), 정보길이(k), 오류 인정 길이(t)를 갖고, t 값을 조정하여 인증 강도를 조절하는 것을 특징으로 한다.

[0019] 또한, 본 발명에 따른 인증 제어 장치의 생체정보조합 등록부는, 생체정보조합의 길이는 코드워드(codeword(c))의 길이와 같은 길이가 되도록 전처리하는 것을 특징으로 한다.

[0020] 상술한 과제의 해결 수단으로, 본 발명에 따른 생체정보 또는 사용자 특징 정보 기반의 인증 제어 장치는 등록된 가공생체정보조합인 인증 데이터(δ) 및 해시값(Hash(key))을 저장하는 저장부; 등록 시 사용한 방식으로 생체정보 또는 생체로부터 파생한 정보 또는 사용자 특징 정보인 생체정보조합(ω’를 얻고)를 획득하여 저장된 인증 데이터(δ)와 연산을 통해 코드워드(codeword c’)을 얻고, 등록 시 사용된 인코딩 방식과 대응되는 디코딩 방식을 사용하여 키(key k’)를 얻고, 키(key k’)에 해시 함수를 적용하여 저장된 해시값(Hash(key))와 비교하여 일치여부에 따라 인증을 허용하는 생체정보조합 인증부를 포함하는 것을 특징으로 한다.

[0021] 여기서, 코드워드(codeword c’)는 하기 <수학식 2>과 같이 표현할 수 있는 것을 특징으로 한다.

[0022] [수학식 2]

[0023] $c' = \omega' \text{ XOR } \delta$

[0024] ω’:인증 수행 시 획득한 생체정보로부터 파생된 생체정보조합 또는 사용자 특징 정보

[0025] k’ = Error Correcting Code-Decoding(c’)

[0026] 상술한 과제의 해결 수단으로, 본 발명에 따른 인증 제어를 위한 생체정보 또는 생체정보로부터 파생된 정보 및 이의 조합 또는 사용자 특징 정보 등록 방법은 적어도 하나의 물리적 센서나 이의 조합 또는 로지컬 센서를 통해 사용자의 핸드폰 사용 패턴 및 로그 정보 등과 같은 사용자 특징 정보를 포함하는 사용자의 생체정보조합 신호를 획득하는 과정; 획득한 생체정보조합 신호에 대하여 전처리 및 분할 처리 후 실제 가치 있는 값을 가진 생체정보조합 템플릿을 추출하는 과정; 생체정보조합 템플릿을 이진화 시키고, 신뢰성 있는 비트를 추출하는 과정; 인코딩을 위한 이진 암호화 키를 생성하여 인코딩하는 과정; 생성한 암호화 키를 해시 함수가 적용시킨 해시값을 저장하는 과정; 인코딩 된 암호화 키를 이용하여 추출한 이진화된 생체정보조합 템플릿을 바인딩하는 과정; 바인딩 처리된 생체정보조합 템플릿을 인증 데이터로 등록하는 과정을 포함하는 것을 특징으로 한다.

[0027] 여기서, 인코딩하는 과정은 이진화된 생체정보조합 템플릿의 길이와 동일한 길이를 가지는 암호화 키를 생성하여 미리 설정된 인코딩 방식으로 인코딩하는 과정을 포함하는 것을 특징으로 한다.

[0028] 또한, 인증 제어를 위한 생체정보조합 등록 방법에서 미리 설정된 인코딩 방식은, 오류 정정 코드(Error Correcting Code)인 것을 특징으로 한다.

[0029] 상술한 과제의 해결 수단으로, 본 발명에 따른 생체정보 또는 생체정보로부터 파생된 정보를 이용한 인증 방법은 물리적 센서나 이의 조합 또는 로지컬 센서를 통해 사용자의 핸드폰 사용 패턴 및 로그 정보 등과 같은 사용자 특징 정보를 포함하는 사용자의 생체정보조합 신호를 획득하는 과정; 획득한 생체정보조합 신호에 대하여 전

처리 및 분할 처리 후 실제 가치 있는 값을 가진 생체정보조합 템플릿을 추출하는 과정; 추출한 생체정보조합 템플릿을 이진화 시키는 과정; 이진화된 생체정보조합 템플릿에 대해 보완 처리 후 저장된 인증 데이터(δ)에 바인딩시키는 과정; 암호화 키(k)를 획득하기 위해 미리 설정된 디코딩 방식으로 디코딩하는 과정; 디코딩된 키의 해시값을 확인하고, 확인된 해시값과 생체정보조합 등록 시 미리 저장된 해시값을 비교하여 일치하는 경우 사용자를 인증 결정하는 과정을 포함하는 것을 특징으로 한다.

[0030] key의 인코딩과 디코딩은 오류정정코드를 사용하는 것을 특징으로 하며, 설명의 편의를 위해 BCH 코딩을 예로 사용한다.

[0031] 또한, 생체정보조합 신호는 임의의 단일 생체정보, 한 개 이상의 생체정보의 조합 신호, 생체정보로부터 파생된 정보나 이들의 조합 신호, 단말로부터 얻은 사용자의 단말 사용 패턴 및 로그 정보와 같은 사용자의 특징 정보 중 하나의 신호인 것을 특징으로 한다.

발명의 효과

[0032] 본 발명은 강력한 인증에 사용될 수 있는 생체정보나 생체정보로부터 파생된 정보 및 정보의 조합 또는 사용자의 핸드폰 사용 패턴 및 로그 정보 등과 같은 사용자 특징 정보의 유출 위험이 없이 안전하게 사용할 수 있도록 해 주는 효과가 있다. 이런 인증 방식은 사용자의 의도적 입력 없이 암묵적으로 인증을 수행할 수 있는 장점이 있다. 암묵적 인증이 안전하게 가능하면 많은 모바일 응용 분야에 적용이 가능하다.

도면의 간단한 설명

[0033] 도 1은 본 발명의 실시예에 따라 단말 내에서 생체인증정보의 등록 및 검증이 수행되는 인증 제어 장치의 내부 구성을 도시하는 도면이다.

도 2는 본 발명의 실시예에 따라 인증을 수행하는 객체와 인증을 요청하는 객체가 서로 다른 인증 시스템을 도시하는 도면이다.

도 3은 본 발명의 실시예에 따른 오류 정정 코드(Error Correcting Code)의 예로 사용된 BCH 코드(Code)의 (n,k,t) 조합을 도시하는 표를 나타내는 예시도이다.

도 4는 본 발명의 실시예에 따른 생체정보조합 기반의 인증 제어 장치의 등록 및 인증의 전체적 과정을 나타내는 흐름도이다.

도 5는 본 발명의 실시예에 따른 생체정보조합 기반의 인증 제어 장치에서 생체정보조합을 등록하는 과정을 나타내는 흐름도이다.

도 6은 본 발명의 실시예의 BCH(511, 157,51)에 대한 FAR(False Acceptance Rate) 및 FRR(False Reject Rate)를 나타내는 도면이다.

도 7은 본 발명의 실시예에 따른 생체정보조합 기반의 인증 제어 장치에서 생체정보조합을 인증하는 과정을 나타내는 흐름도이다.

도 8은 본 발명의 실시예에 따라 생체정보조합 및 해시값(Hash(key))를 등록하는 과정을 나타내는 도면이다.

도 9는 본 발명의 실시예에 따라 생체정보조합 기반으로 인증 처리하는 과정을 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0034] 이하 본 발명의 바람직한 실시예를 첨부한 도면을 참조하여 상세히 설명한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 이는 불필요한 설명을 생략함으로써 본 발명의 핵심을 흐리지 않고 더욱 명확히 전달하기 위함이다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 도면 부호로 나타내고 있음에 유의하여야 한다.

[0035] 이하에서 설명되는 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이거나 사전적인 의미로 한정해서 해석되어서는 아니 되며, 발명자는 그 자신의 발명을 가장 최선의 방법으로 설명하기 위한 용어의 개념으로 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야만 한다. 따라서 본 명세서에 기재된 실시예와 도면에 도시된 구성은 본 발명의 가장 바람직한 하나의 실시예에 불과할 뿐이고, 본 발명의 기술적 사상을 모두 대변하는 것은 아니므로, 본 출원시점에 있어서 이들을 대체할 수

있는 다양한 균등물과 변형 예들이 있을 수 있음을 이해하여야 한다.

[0036] 본 발명에서는 생체정보, 생체정보로부터 파생된 정보 및 이의 조합 정보 또는 사용자의 핸드폰 사용 패턴 및 로그 정보 등과 같은 사용자 특징 정보를 이용한 안전한 인증체계를 제안한다.

[0037] 이하, 본 발명을 설명함에 앞서 물리적 센서는 단말 내부에 구비되는 센서로, 생체정보 또는 생체정보로부터 파생된 정보를 획득할 수 있는 물리적인 구성이고, 로지컬 센서는 사용자의 핸드폰 사용 패턴 및 로그 정보 등과 같은 사용자 특징 정보를 획득할 수 있는 논리적인 구성을 말한다.

[0038] 또한, 본 발명에서 사용되는 생체정보조합이라는 용어는 물리적 센서를 통해 획득한 생체정보 또는 생체정보로부터 파생된 정보와 로지컬 센서를 통해 획득한 사용자 특징 정보를 모두 포함할 것이다.

[0039] 또한, 본 발명에서는 생체정보와 다른 정보와 조합하여 암호화할 시 생체정보조합 특성의 변화를 완화하기 위해서 이진 BCH 코드를 사용하는 실시 예로 한정하여 설명하지만, BCH 인코딩 방식에 한정되는 것이 아니다. 즉, 오류정정코드의 특성을 갖춘 다양한 인코딩 방식이 적용 가능할 것이다.

[0040] 기존에 지문인식, 홍채인식, 걸음걸이 인식 등 다양한 생체정보를 이용하여 인증하는 시스템은 이미 널리 보급되어 있고, 또 확산되고 있는 실정이다. 이 방식은 사용자에게 고유한 생체정보를 저장해놓고, 인증이 필요할 때, 동일한 생체정보를 획득하여 저장된 정보와 비교함으로써 동일인 유무, 즉 인증 유무를 결정한다. 이때, 생체정보를 저장하는 곳은 단말기이거나, 아니면 다른 서버에 등록되어 있을 수 있다. 이와 같은 기존 방식의 문제점은 저장된 생체정보가 유출되면 강력한 인증효과에 비례하여 그 피해가 크게 발생할 수 있다는 점이다.

[0041] 이를 위해 본 발명에서는 생체정보 또는 생체정보로부터 파생된 정보 또는 사용자의 핸드폰 사용 패턴 및 로그 정보 등과 같은 사용자 특징 정보를 등록하는 절차, 인증수행절차, 측정 시 마다 어느 정도 변이가 존재하는 생체정보 처리 방법으로 구성되며 이에 대해 구체적으로 설명한다.

[0042] 이하, 본 발명에 따른 인증 시스템은 임의의 단일 생체정보, 또는 한 개 이상의 생체정보의 조합, 또는 생체정보로부터 파생된 정보나 이들의 조합 또는 사용자의 핸드폰 사용 패턴 및 로그 정보 등과 같은 사용자 특징 정보 등에 적용이 가능하며, 본 발명의 상세한 설명에서는 이러한 정보들을 생체정보조합으로 칭하여 설명하도록 한다.

[0043] 그래서, 본 발명에서는 이런 생체정보 또는 사용자 특징 정보를 인증에 사용하지만 유출 피해를 염려하지 않아도 되는 안전한 생체정보 인증시스템을 제안하며, 주요 내용은 생체정보 또는 생체정보로부터 파생된 정보 또는 사용자 특징 정보를 등록하는 절차, 인증수행절차, 측정 시 마다 어느정도 변이가 존재하는 생체정보 처리 방법으로 구성되며 이에 대해 구체적으로 설명한다. 본 시스템은 임의의 단일 생체정보, 또는 한 개 이상의 생체정보의 조합, 또는 생체정보로부터 파생된 정보나 이들의 조합 또는 사용자 특징 정보 등에 적용되며, 설명의 편의상 이 모든 경우를 본 출원서에는 생체정보조합으로 칭한다.

[0044] 먼저, 도 1을 참조하여 본 발명의 실시 예에 따라 독립 단말내에서 생체인증정보의 등록 및 검증이 수행되는 인증 시스템 구성에 대하여 살펴보도록 한다.

[0045] 도 1은 본 발명의 실시예에 따라 단말 내에서 생체인증정보의 등록 및 검증이 수행되는 인증 제어 장치의 내부 구성을 도시하는 도면이다.

[0046] 도 1을 참조하면, 본 발명에 따른 생체정보조합 기반의 인증 제어 장치는, 제어부(100), 인증 자원부(110), 통신부(120), 생체정보조합 저장부(130), 입력부(140), 출력부(150)을 포함하여 이루어지며, 이들이 기능적으로 연동할 수 있다.

[0047] 먼저, 제어부(100)는 생체정보조합 기반의 인증 제어 장치의 전반적인 동작을 제어한다. 기본적으로, 제어부(100)는 저장부(130)에 저장된 OS 프로그램을 실행하여, 다양한 어플리케이션이 구동할 수 있는 실행 환경을 구축하고, 구축된 실행 환경을 통해서 사용자의 요청 혹은 설정된 알고리즘에 따라 특정 어플리케이션 혹은 기능을 수행한다.

[0048] 특히, 본 발명에 따른 제어부(100)는 생체정보조합 등록 처리를 위한 생체정보조합 등록부(20)와 생체정보조합 인증 처리를 위한 생체정보조합 인증부(22)를 포함하여 구성된다.

[0049] 먼저, 생체정보조합 등록부(20)는 생체정보조합 유출 방지를 위한 등록을 위한 동작을 수행한다. 본 발명에서는 생체정보조합 유출 방지를 위해 생체정보조합을 직접적으로 저장하지 않는다. 직접 저장하는 대신 생체정보조합과 인증 시스템을 위한 다른 정보와 조합하여 저장하며, 저장된 정보로부터 생체정보조합을 추출할 수 없는 방

식으로 조합하여 저장한다.

[0050] 여기서, 생체정보조합의 예는 지문인식, 홍체인식, 걸음걸이인식 등 단일 생체정보를 이용할 수 있으며, 이들의 다양한 조합 즉 지문인식과 홍체인식, 지문인식과 걸음걸이인식, 등 다양한 생체정보의 가중치를 적용한 결합 등 다양한 생체정보조합 또는 사용자의 핸드폰 사용 패턴 및 로그 정보 등과 같은 사용자 특징 정보가 가능하다.

[0051] 이하, 본 발명의 실시 예에서는 BCH(Key)를 한 예로 설명하지만, BCH는 오류정정코드(Error Correcting Code)의 하나의 예시일 뿐, BCH에 한정되지 않는다. 즉, BCH 이외의 오류정정코드들 중 다른 코드를 사용해도 적용 가능할 것이다.

[0052] 본 발명에 따른 생체정보조합 등록부(20)는 랜덤으로 생성한 키(Key(k))를 BCH 코드(Code)로 인코딩한 결과(BCH-Encoding(k):c)와 생체정보조합으로부터 파생시킨 디지털 정보(ω)를 조합(exclusive OR)한 인증 데이터(δ)를 생체정보조합 저장부(130)에 저장한다. 또한, 생체정보조합 등록부(20)는 두 정보를 조합(exclusive OR)하기 위해서 비트(bit)수를 맞춘 후 조합한다. 그리고, 랜덤키(key(k))에 원웨이(one way) 함수인 해시 함수를 적용한 결과 H(k)를 저장한다. 해시 함수는 원웨이(one way)이기 때문에 H(k)로부터 랜덤키(key(k))를 유추할 수 없다. 이와 같은 인증 데이터(δ)는 하기 <수학식 1>과 같은 표현할 수 있다.

수학식 1

[0053] $$\delta = c \ \mathrm{XOR} \ \omega$$

[0054] 상기 <수학식 1>에서 ω는 생체정보조합으로부터 가공된 디지털 정보이고, c는 오류정정코드(ECC)를 랜덤키 k에 적용한 결과이다.

[0055] 그러므로, 생체정보조합 등록부(20)에서 저장부(130)에 저장하는 등록정보는 인증 데이터(δ)와 해시값(Hash(k))이다.

[0056] 이와 같은 등록절차는 도 1에서는 생체정보조합 등록부(20)에서 수행되고, 이하 설명할 도 2에서는 인증 서버의 생체정보조합 등록부(26)에서 수행될 것이다.

[0057] 본 발명에서의 인증 제어 장치는 도 1과 같이 사용자 단말 내에 구현될 수 있고, 이러한 사용자 단말은 다양한 형태로 구현될 수 있는데, 예를 들어, 휴대폰, 스마트 폰(smart phone), 디지털방송용 단말기, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 네비게이션, MP3 플레이어 등의 이동 단말기로서 생체정보조합을 획득할 수 있는 기능을 내장한 단말기가 사용될 수 있다. 또, 다른 형태는 도 2와 같이 원격 서버와 같은 별도의 인증 서버를 통해 구현될 수 있다.

[0058] 본 발명은 어디에서 인증제어가 이루어지는 것인가에 있지 않고, 생체정보조합을 사용하지만 유출되어도 안전한 방식에 있으므로, 도 1과 도 2와 같이 생체정보조합 등록부(20, 26)에 제한되지 않고, 인증 제어부 위치는 모든 가능한 경우를 다 포함할 수 있을 것이다.

[0059] 이와 같은 생체정보조합 등록부(20)의 동작에 따른 구성은 도 5와 같이 도시할 수 있다.

[0060] 도 5를 참조하면, 생체정보조합 등록부(20)는 신호 획득부(200), 특징 추출부(210), 바이너리 생성부(220), 비트 추출부(230), 랜덤키 생성부(240),인코딩부(250)를 포함하여 구성될 수 있다.

[0061] 신호 획득부(200)는 등록 요구에 따라 물리적 센서 또는 로지컬 센서 등 다양한 측정 또는 수집 메카니즘 및 이들의 조합으로 생성된 생체정보조합 신호를 획득한다.

[0062] 특징 추출부(210)는 수집 생성한 생체정보조합을 연산을 위해 전처리를 통해 생체정보조합 템플릿(ω)를 만든다.

[0063] 바이너리 생성부(220)는 생체정보조합 템플릿을 이진화 시킨다.

[0064] 비트 추출부(230)는 이진화된 생체정보조합 템플릿에서 신뢰성이 큰 비트를 추출한다. 여기서, 신뢰성이 큰 비트를 추출하는 방법에 대하여 구체적으로 설명하면, 예를 들어 생체정보조합이 100개의 속성으로 구성되어 있고, 샘플이 50개라고 하면, 먼저 각 속성에 대해 50개 샘플값의 평균을 구하고, 이 각 속성에 대한 평균값과

전체 비교대상 사용자의 속성에 대한 평균값과 비교하여 전자가 후자보다 크면 1, 아니면 0을 할당하고, 각 속성에 대한 표준오차함수를 적용하여 오차가 큰 속성에 대한 비트를 추출한다.

[0065] 랜덤키 생성부(240)는 임의의 랜덤 키(random key) 발생 함수를 사용하여 키(key)를 생성한다. 즉, 랜덤키 생성부(240)는 생체정보조합 템플릿과 바인딩하여 암호화 처리하기 위한 암호화 키를 랜덤 방식으로 생성한다. 이때, 랜덤키 생성부(240)는 미리 설정된 길이로 이진 암호화 키(k)를 각 해당 사용자에게 임의로 생성한다.

[0066] 인코딩부(250)는 생성된 키(Key)를 오류 정정 코드(Error Correction Code)로 인코딩(encoding)하여 코드워드(codeword(c))를 생성하고, 생성된 코드워드(codeword c)와 생체정보조합(ω)과 연산을 통해 인증 데이터(δ)를 얻어, 이 인증 데이터(δ)와 키(key)에 해시 함수를 적용한 해시값(Hash(key))을 생체정보조합 저장부(130)에 저장하여 등록한다.

[0067] 이러한 인코딩부(250)는 랜덤키 생성부(240)를 통해 생성된 암호화 키를 BCH (nc, k, t)를 사용하여 길이 nc의 워드 c로 인코딩하고, 생체정보조합 템플릿과 암호화 키를 exclusive-OR과 같은 연산을 통해 바인딩한다. 또한, 인코딩부(250)는 키 바인딩 방식을 이용하여 이진 BCH 코드를 나타내기 위해 BCH(nc, k, t)를 사용한다. 이때, BCH오류정정코드는 k비트의 key를 입력으로 받아 t비트의 오류를 허용하는 nc 비트 길이의 코드워드 C를 생성한다. 반드시 BCH 방식을 적용해야 되는 것은 아니며, 오류 정정 코드(Error Correction Code)로서 (n, k, t) 개념을 갖고 있으면 임의의 오류 정정 코드(Error Correction Code)도 가능하다.

[0068] 또한, 인코딩부(250)는 생체정보조합 템플릿을 암호화 키와 바인딩할 시 exclusive-OR 연산 방법을 사용하여 바인딩한다. 반드시 exclusive-OR를 적용할 필요는 없으며, 임의의 연산이 가능하나, 연산 결과로부터 연산에 사용된 피연산자를 추정할 수 없어야 한다. 인코딩부(250)는 생체정보조합 등록을 위해 이와 같이 바인딩처리되어 암호화된 생체정보조합 템플릿을 인증 데이터(δ)로 저장부(130)에 저장한다.

[0069] 예를 들어, 길이 n_c=127, 255, 511 3가지의 코드워드 크기에 대해 이진 템플릿의 해밍 거리 분포 및 적절한 길이의 암호키를 갖는 이러한 템플릿을 바인딩 했을 경우 인증 제어 장치의 FAR (False Acceptance Rate)과 FRR(False Rejection Rate)는 도 6과 같이 도시할 수 있을 것이다. 이와 같은 생체정보조합 등록 과정은 도 4와 같이 도시할 수 있을 것이다. 도 4를 참조하면, 생체정보조합 등록 동작을 수행하는 생체정보조합 등록부(Enrollment Phase)와 인증 동작을 수행하는 생체정보조합 인증부 (Authentication Phase)로 구분되어 도시되어 있다.

[0070] 생체정보조합 등록부는 신호획득부(Biometric acquisition)(41), 특징추출부(Template extraction)(42), 바이너리생성부(Binarization)(43), 신뢰적 비트 추출부(Reliable Bit Extraction)(44), 조합부(45), 오류정정코드를 이용한 키 암호화부(key Encoding using ECC)(46), 랜덤 키 k 생성부(Random key k Generation)(47), 해쉬함수(Hash Function)(48), 저장부(Storage)(49), 키 k의 해쉬 결과(Hash Code h(k))(50) 및 인증 데이터(secured(δ))(51)를 포함한다. 또한, 생체정보조합 인증부는 신호획득부(Biometric acquisition)(61), 특징추출부(Template extraction)(62), 바이너리생성부(Binarization)(63), 신뢰적 비트 추출부(Reliable Bit Extraction)(64), 조합부(65), 오류정정코드를 이용한 키 암호화부(key Decoding using ECC)(66), 해쉬함수(Hash Function)(67), 키 k'의 해쉬 결과(Hash Code h(k'))(68), 인증키 매칭부(Matching)(69), 인증여부판단부(Decision)(70)을 포함한다.

[0071] 한편, 다시 도 1로 돌아가서 설명하면 생체정보조합 인증부(22)는 인증 수행을 위해 등록 시 사용한 방식으로 생체정보조합 (ω')을 획득하여 인증을 위해 저장된 인증 데이터(δ)와 역연산(XOR)을 통해 c' 을 얻고, 이 c' 에서 등록 시 사용한 k로부터 c를 얻은 방식의 짝함수를 사용하여 k' 을 얻으며, k' 에 해시 함수를 적용하여 저장된 H(k) 동일 여부를 확인한다.

[0072] 예를 들어, 등록 시에서 BCH 인코딩(BCH-Encoding) 방식을 사용한 경우에는 인증 시에는 BCH 디코딩(BCH-Decoding) 방식을 적용하여 k' 을 얻으며, 얻어진 k' 에 해시 함수를 적용하여 시스템에 저장된 H(k)와 비교하여 값이 같으면 인증을 허용하고 그렇지 않으면 인증을 허용하지 않는다.

[0073] 이때, c' 는 하기의 <수학식 2>와 같이 표현할 수 있을 것이다.

수학식 2

[0074] $$c' = \omega' \text{ XOR } \delta$$

[0075] 상기의 <수학식 2>에서 ω'는 인증 수행 시 획득한 생체정보로부터 파생된 정보이고, k'는 BCH-Decoding(c')이다. 또한, 만약 H(k')와 H(k)가 일치하면 인증 허용하고, 그렇지 않으면 불허한다.

[0076] 이와 같은 인증수행은 도 1의 22, 도 2의 28에서 수행되지만, 이는 설명을 위한 것일 뿐 인증 수행의 위치는 본 발명의 핵심이 아니고, 인증 수행 방식이 핵심이므로 어디에서 수행되어도 모두 이 출원범위에 포함된다고 보아야 할 것이다.

[0077] 한편, 도 1의 생체정보조합 인증부(22)와 도 2의 생체정보조합 인증부(28)에서 수행되는 인증 처리는 인증 요구에 따라 측정된 측정 데이터나 이들의 조합 또는 수집한 사용자 특징 정보를 통해 생체정보조합을 얻고 이를 전처리하여 현재 사용자의 생체정보조합 템플릿(ω')을 생성하고, 생성한 템플릿을 저장된 인증 데이터(δ)에 바인딩하여 코드워드(codeword(c'))을 얻고, 이 코드워드(c')를 인코딩 때 사용한 동일한 오류 정정 코드(Error Correction Code)로 디코딩하여 디코딩된 키(k')를 얻고 여기에 해시함수를 적용한 해시값(Hash(k'))과 저장된 해시값(Hash(k))를 비교하여 인증을 결정한다.

[0078] 이와 같은 생체정보조합 인증부(22)의 동작에 따른 구성은 도 7과 같이 도시할 수 있다.

[0079] 도 7을 참조하면, 생체정보조합 인증부(22)는 신호 획득부(300), 특징 추출부(310), 바이너리 생성부(320), 비트 추출부(330), 디코딩부(340), 인증키 매칭부(350), 생체정보조합 인증 확인부(360)를 포함하여 구성될 수 있다.

[0080] 신호 획득부(300)는 다양한 센서나 측정 또는 수집 메카니즘을 통해 획득한 생체정보조합에 대한 전처리 및 분할 동작을 수행한다. 이때, 신호 획득부(300)가 측정 및 수집하는 신호는 임의의 단일 생체정보, 한 개 이상의 생체정보의 조합 신호, 생체정보로부터 파생된 정보나 이들의 조합 신호, 단말로부터 얻은 사용자의 단말 사용 패턴 및 로그 정보와 같은 사용자의 특징 정보 중 하나의 신호가 될 것이다.

[0081] 이후, 특징 추출부(310)는 미리 설정된 길이로 생체정보조합 템플릿을 샘플링한다. 이때, 미리 설정된 길이는 암호화 키(k)와 바인딩 가능하도록 하기 위한 길이로 설정될 것이다.

[0082] 바이너리 생성부(320)는 특징 추출부(310)에 의해 추출한 생체정보조합 템플릿을 이진화 처리한다.

[0083] 본 발명의 실시예에서는 생체정보조합 등록 시 인코딩 방식과 대응하여 생체정보조합 인증 시에는 BCH 디코딩을 이용하여 디코딩하였지만, 설정에 따라 다른 인코딩 및 디코딩 방식을 사용할 수도 있을 것이다.

[0084] 인증키 매칭부(350)는 디코딩된 키의 해시값을 확인하고, 확인된 해시값과 저장된 해시값(H(k)을 비교한다.

[0085] 생체정보조합 인증 확인부(360)는 인증키 매핑부(350)를 통해 비교한 결과 해시값이 일치하면 사용자를 인증한다.

[0086] 본 발명에서는 생체정보나 여러 생체정보의 조합 또는 이에서 파생된 정보 또는 사용자의 특징 정보를 인증에 사용하면 생체정보조합을 등록할 때와 인증을 위해 새로 수집 또는 측정한 정보는 동일할 수 없다. 동일하지는 않지만, 다른 사용자와 구분할 수 있을 정도의 유사성을 가지고 있기 때문에 이와 같은 상이점을 수용하기 위한 방안도 제안한다.

[0087] 어느 정도의 상이한 점을 허용하기 위해 본 발명에서는 오류 정정 코드(Error Correcting Code)를 사용한다. 예를 들면, 오류 정정 코드(Error Correcting Code)의 일종인 BCH 방식은 인코딩 때와 디코딩 때 어느 정도 오류 정정 코드(Error Correcting Code)의 능력에 따라, 그 이내의 상이점은 정정(Correction) 연산을 통해 상이하여도 동일한 것으로 인식할 수 있다. 어느 정도 다른 것까지 인정할지 여부는 설정에 따라 달라질 수 있을 것이며, 오류 정정 코드(Error Correcting Code)에는 이러한 특성이 잠재해 있다. 오류 정정 코드(Error Correcting Code)로는 BCH, Cyclic Code, Reed-Solomon Code, Golay, Reed-Muller Code 등이 있으며, 이들 오류 정정 코드(Error Correcting Code)는 공통적으로 다음과 같은 매개변수 (n, k, t)를 가지고 있으며, 이런 특징을 가지고 있는 어떤 종류의 오류 정정 코드(Error Correcting Code)를 사용해도 등록 시와 인증수행 시 생체정보조합의 상이점을 극복할 수 있다.

[0088] 여기서, n은 코드워드(codeword)의 길이이고, k는 정보(information(key))의 길이이고, t는 에러(error)를 수정할 수 있는 비트 수를 말한다.

[0089] 도 3은 본 발명에서 예시로 제시하고 있는 BCH Code의 (n, k, t)의 조합을 보여주는 표이며, 어느 정도 상이점을 허용할 것인가는 이 표의 't' 값에 따라 사용자가 선택할 수 있다.

[0090] 상기한 생체정보조합 등록, 인증 및 등록 시의 생체정보조합 신호와 인증 수행 시 사용된 생체정보조합 신호 간의 어느 정도 상이점을 수용하는 방식으로 인증을 수행하면, 단말이나 서버의 도난, 분실, 해킹 등이 발생하여도 직접적 생체정보 또는 사용자 특징 정보가 저장되어 있지 않기 때문에 생체정보 또는 사용자 특징 정보의 유출 가능성이 없을 것이다. 또한, 원웨이(one way) 해시 함수를 사용하여 키(key)를 저장하기 때문에 키(key) 자체가 유출될 가능성이 없다. 예를 들어 BCH(n=511, k=157, t=51)을 사용하면 임의의 랜덤(random) 함수를 사용하여 157bit key를 생성하여 BCH-encoding을 하면 511bit의 코드워드(codeword(c))가 생성된다. 이 511bit의 코드워드(codeword)와 생체정보조합(ω)과 XOR(exclusive OR)한 결과 δ를 Hash(k)와 함께 저장할 것이기 때문에 ω 역시 511bit가 되도록 생성한다. 그러나, 본 발명에서는 특정 오류 정정 코드(Error Correction Code) 알고리즘으로 제한하지 않고, (n:codeword size, k:information length, t:allowable error size) 개념을 포함하는 임의의 오류 정정 코드(Error Correction Code) 또는 알고리즘(algorithm)이면 가능하다. 생체정보조합(ω) 역시 특정 생체정보에 국한 되지 않고, 지문, 홍채, 걸음걸이, 정맥 등 단일 생체정보 또는 이런 단일 생체정보의 몇 개의 다양한 조합으로 생성 가능한 생체정보조합이 가능하며, 단 δ를 만들어야하기 때문에 ω와 c(codeword: Error Correction Code 연산 결과값)와 적절한 연산이 가능하도록 하는 준비 작업을 포함한다. 이 연산은 반드시 exclusive OR일 필요는 없으며, 연산 결과 δ를 만들 수 있으면 가능하다.

[0091] 한편, 다시 도 1로 돌아가서 설명하면 인증 자원부(110)는 센서를 포함한 인증을 위한 신호를 획득하기 위한 구성으로, 다양한 센서나 측정 메카니즘을 통해 획득한 생체정보조합 신호를 제어부(100)로 제공한다.

[0092] 통신부(120)는 통신망에 접속하여, 통신망을 통해서 데이터를 송수신하기 위한 구성이다. 이러한 통신부(120)는 통신망의 구조 및 통신 프로토콜에 따라서 그 구성 및 동작이 달라진다. 예를 들어 통신부(120)는 1G, 2G, 3G 방식 등 다양한 이동 통신 방식 또는 유선 통신 방식 또는 Wi-Fi와 같은 무선 통신 방식 중 어느 하나를 지원하는 통신 모듈 중 적어도 하나 또는 하나 이상으로 구성될 수 있다.

[0093] 저장부(130)는 인증 제어 장치의 동작에 필요한 프로그램 및 데이터 및 동작 결과로서 발생되는 데이터를 저장하는 것으로서 크게 프로그램 영역과 데이터 영역을 포함할 수 있다. 특히, 본 발명에 따른 저장부(130)는 생체정보조합 등록을 위한 등록 정보인 인증 데이터(δ)와 해시값(Hash(k))을 저장한다.

[0094] 입력부(140)는 인증 제어 장치에 대한 혹은 인증 제어 장치에서 실행되는 특정 기능에 대한 사용자 입력 신호를 생성하는 수단으로서, 숫자 또는 다양한 문자 정보를 입력 받고, 각종 기능들의 설정 및 인증 제어 장치의 기능 제어를 위한 입력 키 및 기능 키들을 포함할 수 있다. 이러한 입력부(140)는 키보드, 키패드, 마우스, 모션 센서 등과 같은 다양한 종류의 입력 수단으로 형성될 수 있으며, 인증 제어 장치가 터치스크린으로 제작되는 경우, 터치스크린 상에 구현되는 소프트 키 및 사이드 키나 별도의 핫 키, 단축 키 등을 포함하여 구성될 수 있다.

[0095] 출력부(150)는 표시부와 음성 처리부를 포함하여 구성되는데, 표시부는 인증 제어 장치의 동작 상태 및 동작 결과를 표시하거나 소정의 정보를 사용자에게 제공하기 위한 출력 수단으로서, 각종 메뉴를 비롯하여 사용자가 입력한 정보 또는 사용자에게 제공하는 정보를 출력한다. 특히, 표시부는 인증 제어 장치의 동작 상태에 따른 다양한 사용자 인터페이스 화면을 출력한다. 이러한 표시부는 액정 표시 장치(Liquid Crystal Display), OLED(Organic Light Emitted Diode) 등의 평판 표시 패널의 형태로 형성될 수 있다. 또한, 표시부는 제조 형태에 따라 표시 패널과 터치 패널을 포함하는 구조로 제작될 수 있다. 그리고 음성 처리부는 마이크 및 스피커 등의 가청음 인식 수단이나 가청음 출력 수단에 연결되어, 인식된 음성을 음성 데이터로 변환하여 제어부(100)로 출력하거나, 제어부(100)를 통해 입력된 음성 데이터를 스피커를 통해 가청음으로 출력되도록 처리한다.

[0096] 도 2는 인증을 수행하는 객체와 인증을 요청하는 객체가 서로 다른 경우, 인증을 요청하는 단말, 인증을 수행하는 인증 서버를 나타내는 도면이다. 인증을 수행하는 인증 서버는 인증을 필요로 하는 어플리케이션(application)이 실행되는 서버이거나 또는 인증을 필요로 하는 서버로부터 인증 기능만 위임받은 인증 전용 서버의 경우를 포함한다.

[0097] 인증 서버(170)는 생체정보 유출 방지를 위한 등록 및 인증 동작을 수행한다. 이를 위해 인증 서버(170)는 생체정보조합 등록부(26) 및 생체정보조합 인증부(28)를 포함하여 구성된다.

[0098] 생체정보조합 등록부(26)는 제1 단말(24)로부터 전송되는 생체정보조합 신호를 획득하면, 랜덤으로 생성한 키(Key(k))를 BCH 코드(Code)로 인코딩한 결과(BCH-Encoding(k):c)와 생체정보조합으로부터 파생시킨 디지털 정보(ω)를 조합(exclusive OR)한 인증 데이터(δ)를 저장한다. 또한, 생체정보조합 등록부(26)는 두 정보를 조합(exclusive OR)하기 위해서 비트(bit)수를 맞춘 후 조합한다. 그리고, 랜덤키(key(k))에 원웨이(one way) 함수인 해시 함수를 적용한 결과 H(k)를 저장한다. 해시 함수는 원웨이(one way)이기 때문에 H(k)로부터 랜덤키(key(k))를 유추할 수 없다. 이와 같은 인증 데이터(δ)는 상기 <수학식 1>과 같은 표현할 수 있다. 그러므로, 생체정보조합 등록부(26)에서 저장부에 저장하는 등록정보는 인증 데이터(δ)와 해시값(Hash(k))이다. 이와 같은 도 2에서의 생체정보조합 등록부(26)에서의 등록 동작은 도 1의 생체정보조합 등록부(20)의 동작과 동일하고, 이를 위한 내부 구성은 도 5와 같이 구성될 수 있을 것이다.

[0099] 또한, 생체정보조합 인증부(28)는 인증을 위한 동작을 수행한다. 이러한 생체정보조합 인증부(28)는 등록 시 사용한 방식으로 생체정보 또는 생체로부터 파생한 정보를 획득하여 인증을 위해 저장된 δ와 연산을 통해 c'을 얻고, 이 c'에서 등록 시 사용한 k로부터 c를 얻은 방식의 짝함수를 사용하여 k'을 얻으며, k'에 해시 함수를 적용하여 저장된 H(k)와 동일 여부를 확인한다. 예를 들어, 등록 시 BCH-Encoding 방식을 사용한 경우라면 BCH-Decoding을 적용하여 k'을 얻으며, 얻어진 k'에 해시 함수를 적용하여 시스템에 저장된 H(k)와 비교하여 값이 같으면 인증을 허용하고 그렇지 않으면 인증을 허용하지 않는다. 이와 같은 도 2에서의 생체정보조합 인증부(28)에서의 등록 동작은 도 1의 생체정보조합 인증부(22)의 동작과 동일하고, 이를 위한 내부 구성은 도 7과 같이 구성될 수 있을 것이다.

[0100] 상기한 바와 같은 방식으로 인증을 수행하면 단말이나 서버의 도난, 분실, 해킹 등이 발생하여도 직접적 생체정보가 저장되어 있지 않기 때문에 생체정보의 유출 가능성이 없으며, 원웨이(one way) 해시 함수를 사용하여 키(key)를 저장하기 때문에 키(key) 자체가 유출될 가능성이 없다.

[0101] 그러면 이제 상기와 같이 구성되는 생체정보조합 기반의 인증 제어 장치에서 생체정보조합 등록을 위한 과정에 대하여 도 8을 참조하여 설명하도록 한다.

[0102] 도 8은 본 발명의 실시 에에 따른 생체정보조합 기반의 인증 제어 장치에서 생체정보조합 등록을 위한 과정을 나타내는 흐름도이다.

[0103] 도 8를 참조하면, 인증 제어 장치는 물리적 센서 또는 로지컬 센서나 이의 조합으로 사용자의 생체정보조합 신호를 획득한다.(S800)

[0104] 이후, 인증 제어 장치는 획득한 생체정보조합 신호에 대하여 전처리 및 분할 처리 후 실제 가치 있는 값을 가진 생체정보조합 템플릿을 추출한다.(S802)

[0105] 이후, 인증 제어 장치는 생체정보조합 템플릿을 이진화 시키고, 신뢰성 있는 비트를 추출한다.(S804 ~ S806) 이때, 신뢰성 있는 비트를 추출하기 위한 방법은 상기의 도 2의 설명에서 설명하였으므로 여기서 구체적인 설명은 생략하도록 한다.

[0106] 이후, 인증 제어 장치는 인코딩을 위한 이진 암호화 키를 생성하여 인코딩하고, 생성한 암호화 키를 해시 함수가 적용시킨 해시값을 저장한다.(S808) 이때, 이진화된 생체정보조합 템플릿의 길이와 동일한 길이를 가지는 암호화 키를 생성한다.

[0107] 또한, 인증 제어 장치는 인코딩 된 암호화 키를 이용하여 추출한 이진화된 생체정보조합 템플릿을 바인딩하고, 바인딩처리된 생체정보조합 템플릿을 인증 데이터로 등록한다.(S810 ~ S812)

[0108] 즉, 암호화 키는 생체정보조합 특성의 변화를 완화하기 위해서 이진 BCH 코드와 같은 오류 정정 코드를 사용하여 인코딩된다. 인코딩된 암호화 키는 이진 생체정보조합 템플릿과 함께 바인딩된다.

[0109] 그러면 이제 상기와 같이 구성되는 생체정보조합 기반의 인증 제어 장치에서 생체정보조합 인증을 위한 과정에 대하여 도 9를 참조하여 설명하도록 한다.

[0110] 도 9는 본 발명의 실시 에에 따른 생체정보조합 기반의 인증 제어 장치에서 생체정보조합 인증을 위한 과정을 나타내는 흐름도이다.

[0111] 도 9를 참조하면, 인증 제어 장치는 물리적 센서 또는 로지컬 센서 및 이의 조합으로 사용자의 생체정보조합 신호를 획득한다.(S900) 이때, 사용자의 생체정보조합 신호는 인증 요청이 있은 후 새로 발생한 정보 뿐 아니라 인증 목표를 달성할 수 있으면, 기존에 누적된 자료를 사용할 수 있다.

[0112] 인증 제어 장치는 획득한 생체정보조합 신호에 대하여 전처리 및 분할 처리 후 실제 가치 있는 값을 가진 생체정보조합 템플릿을 추출하고, 생체정보조합 템플릿을 이진화 시킨다.(S902) 이때, 생체정보조합 템플릿 추출 방법은 상기의 도 2의 설명에서 설명하였으므로 여기서 구체적인 설명은 생략하도록 한다.

[0113] 이후, 인증 제어 장치는 이진화된 생체정보조합 템플릿에 대해 보완 처리 후 저장된 인증 데이터(δ)에 Exclusive OR를 사용하여 바인딩시켜 코드워드를 생성하고, 생성된 코드워드에 BCH 디코딩을 사용하여 암호화 키(k)를 획득한다.(S904 ~ S906)

[0114] 이후, 인증 제어 장치는 디코딩된 키의 해시값을 확인하고, 확인된 해시값과 저장된 해시값을 비교하여 일치하는 경우 사용자를 인증 결정한다.

[0115] 본 발명에 따른 생체정보조합 기반의 인증 제어 방법은 다양한 컴퓨터 수단을 통하여 판독 가능한 소프트웨어 형태로 구현되어 컴퓨터로 판독 가능한 기록매체에 기록될 수 있다. 여기서, 기록매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 기록매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 예컨대 기록매체는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 롬(ROM), 램(RAM, Random Access Memory), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함한다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 이러한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0116] 이상과 같이, 본 명세서와 도면에는 본 발명의 바람직한 실시예에 대하여 개시하였으나, 여기에 개시된 실시 예 외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 자명한 것이다. 또한, 본 명세서와 도면에서 특정 용어들이 사용되었으나, 이는 단지 본 발명의 기술 내용을 쉽게 설명하고 발명의 이해를 돕기 위한 일반적인 의미에서 사용된 것이지, 본 발명의 범위를 한정하고자 하는 것은 아니다.

[0117] 또한, 본 발명에 따른 장치에 탑재되고 본 발명에 따른 생체정보조합 기반의 인증 제어 방법을 실행하는 컴퓨터 프로그램(프로그램, 소프트웨어, 소프트웨어 어플리케이션, 스크립트 혹은 코드로도 알려져 있음)은 컴파일 되거나 해석된 언어나 선험적 혹은 절차적 언어를 포함하는 프로그래밍 언어의 어떠한 형태로도 작성될 수 있으며, 독립형 프로그램이나 모듈, 컴포넌트, 서브루틴 혹은 컴퓨터 환경에서 사용하기에 적합한 다른 유닛을 포함하여 어떠한 형태로도 전개될 수 있다. 컴퓨터 프로그램은 파일 시스템의 파일에 반드시 대응하는 것은 아니다. 프로그램은 요청된 프로그램에 제공되는 단일 파일 내에, 혹은 다중의 상호 작용하는 파일(예컨대, 하나 이상의 모듈, 하위 프로그램 혹은 코드의 일부를 저장하는 파일) 내에, 혹은 다른 프로그램이나 데이터를 보유하는 파일의 일부(예컨대, 마크업 언어 문서 내에 저장되는 하나 이상의 스크립트) 내에 저장될 수 있다. 컴퓨터 프로그램은 하나의 사이트에 위치하거나 복수의 사이트에 걸쳐서 분산되어 통신 네트워크에 의해 상호 접속된 다중 컴퓨터나 하나의 컴퓨터 상에서 실행되도록 전개될 수 있다.

[0118] 아울러, 본 발명에 따른 생체정보조합 기반의 인증 제어 방법을 설명하는데 있어서, 특정한 순서로 도면에서 동작들을 묘사하고 있지만, 이는 바람직한 결과를 얻기 위하여 도시된 그 특정한 순서나 순차적인 순서대로 그러한 동작들을 수행하여야 한다거나 모든 도시된 동작들이 수행되어야 하는 것으로 이해되어서는 안 된다. 특정한 경우, 멀티태스킹과 병렬 프로세싱이 유리할 수 있다. 또한, 상술한 실시형태의 다양한 시스템 컴포넌트의 분리는 그러한 분리를 모든 실시형태에서 요구하는 것으로 이해되어서는 안되며, 설명한 프로그램 컴포넌트와 시스템들은 일반적으로 단일의 소프트웨어 제품으로 함께 통합되거나 다중 소프트웨어 제품에 패키징될 수 있다는 점을 이해하여야 한다.

산업상 이용가능성

[0119] 본 발명을 통해 얻게 되는 생체정보조합 기반의 인증 기술은 이동통신을 이용한 다양한 서비스를 이용할 때, 인증을 위해 등록된 생체정보조합 템플릿과 같은 사용자 개인 정보를 안전하게 관리할 수 있도록 함으로써 생체정보조합 인증 기술 시장 선점에 기여가 예상된다.

부호의 설명

[0120] 100: 제어부 110: 인증자원부

120: 통신부 130: 생체정보조합 저장부

140: 입력부 150: 출력부

20: 생체정보조합 등록부 22: 생체정보조합 인증부

24: 제1 단말 26: 생체정보조합 등록부

28: 생체정보조합 인증부 30: 제2 단말

160: 통신망 170: 인증 서버

200: 신호 획득부 210: 특징 추출부

220: 바이너리 생성부 230: 비트 추출부

240: 랜덤키 생성부 250: 인코딩부

300: 신호 획득부 310: 특징 추출부

320: 바이너리 생성부 330: 비트 추출부

340: 디코딩부 350: 인증키 매칭부

360: 생체정보조합 인증 확인부

41: 신호획득부(Biometric acquisition)

42: 특징추출부(Template extraction)

43: 바이너리생성부(Binarization)

44: 신뢰적 비트 추출부(Reliable Bit Extraction)

45: 조합부

46: 오류정정코드를 이용한 키 암호화부(key Encoding using ECC)

47: 랜덤 키 k 생성부(Random key k Generation)

48: 해쉬함수(Hash Function)

49: 저장부(Storage)

50: 키 k의 해쉬 결과(Hash Code h(k))

51: 인증 데이터(secured(δ))

61: 신호획득부(Biometric acquisition)

62: 특징추출부(Template extraction)

63: 바이너리생성부(Binarization)

64: 신뢰적 비트 추출부(Reliable Bit Extraction)

65: 조합부

66: 오류정정코드를 이용한 키 암호화부(key Decoding using ECC)

67: 해쉬함수(Hash Function)

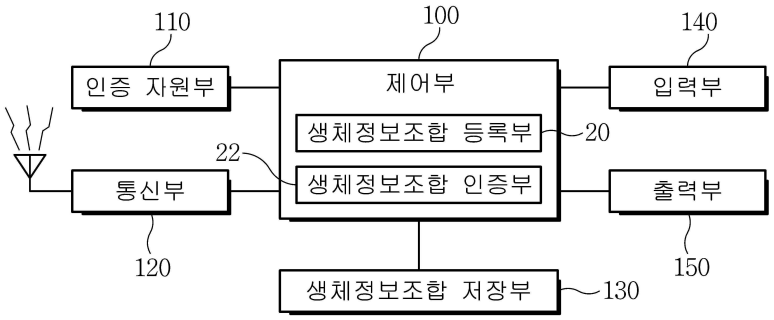
68: 키 k'의 해쉬 결과(Hash Code h(k'))

69: 인증키 매칭부(Matching)

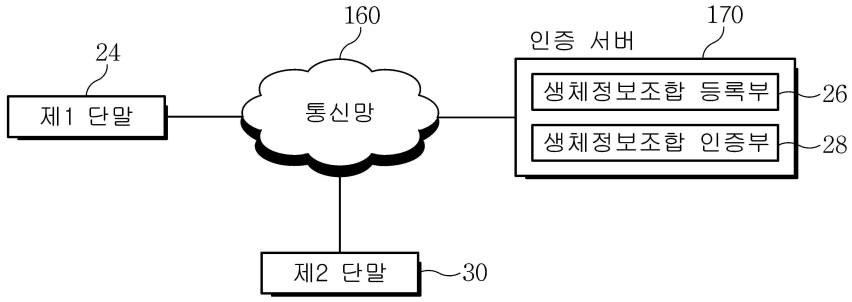
70: 인증여부판단부(Decision)

도면

도면1



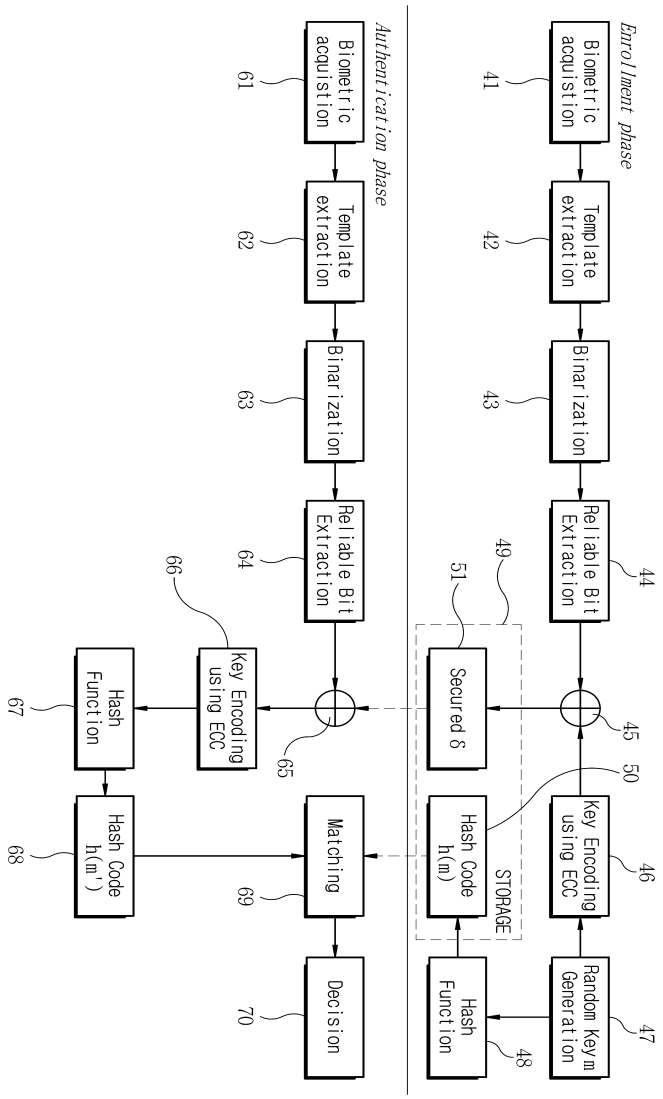
도면2



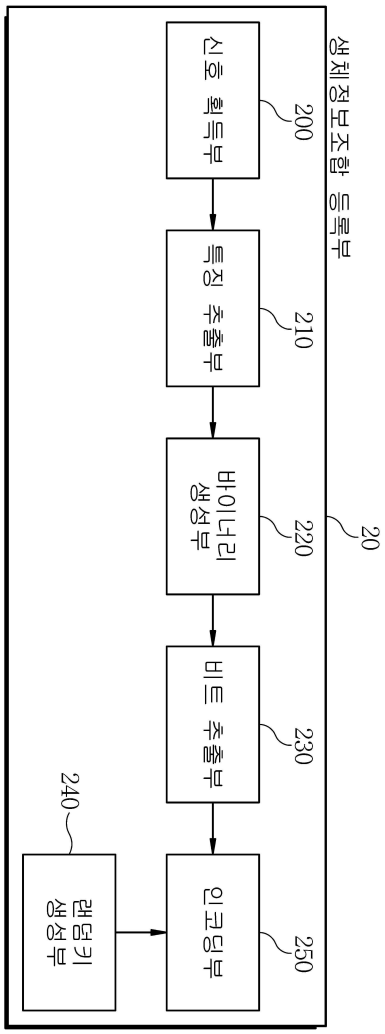
도면3

n	k	t	n	k	t	n	k	t
7	4	1	255	163	12	511	268	29
15	11	1		155	13		259	30
	7	2		147	14		250	31
	5	3		139	15		241	36
31	26	1		131	18		238	37
	21	2		123	19		229	38
	16	3		115	21		220	39
	11	5		107	22		211	41
	6	7		99	23		202	42
63	57	1		91	25		193	43
	51	2		87	26		184	45
	45	3		79	27		175	46
	39	4		71	29		166	47
	36	5		63	30		157	51
	30	6		55	31		148	53
	24	7		47	42		139	54
	18	10		45	43		130	55
	16	11		37	45		121	58
	10	13		29	47		112	59
	7	15		21	55		103	61
127	120	1		13	59		94	62
	113	2		9	63		85	63
	106	3	511	502	1		76	85
	99	4		493	2		67	87
	92	5		484	3		58	91
	85	6		475	4		49	93
	78	7		466	5		40	95
	71	9		457	6		31	109
	64	10		448	7		28	111
	57	11		439	8		19	119
	50	13		430	9		10	121
	43	14		421	10	1023	1013	1
	36	15		412	11		1003	2
	29	21		403	12		993	3
	22	23		394	13		983	4
	15	27		385	14		973	5
	8	31		376	15		963	6
255	247	1		367	16		953	7
	239	2		358	18		943	8
	231	3		349	19		933	9
	223	4		340	20		923	10
	215	5		331	21		913	11
	207	6		322	22		903	12
	199	7		313	23		893	13
	191	8		304	25		883	14
	187	9		295	26		873	15
	179	10		286	27		863	16
	171	11		277	28		858	17

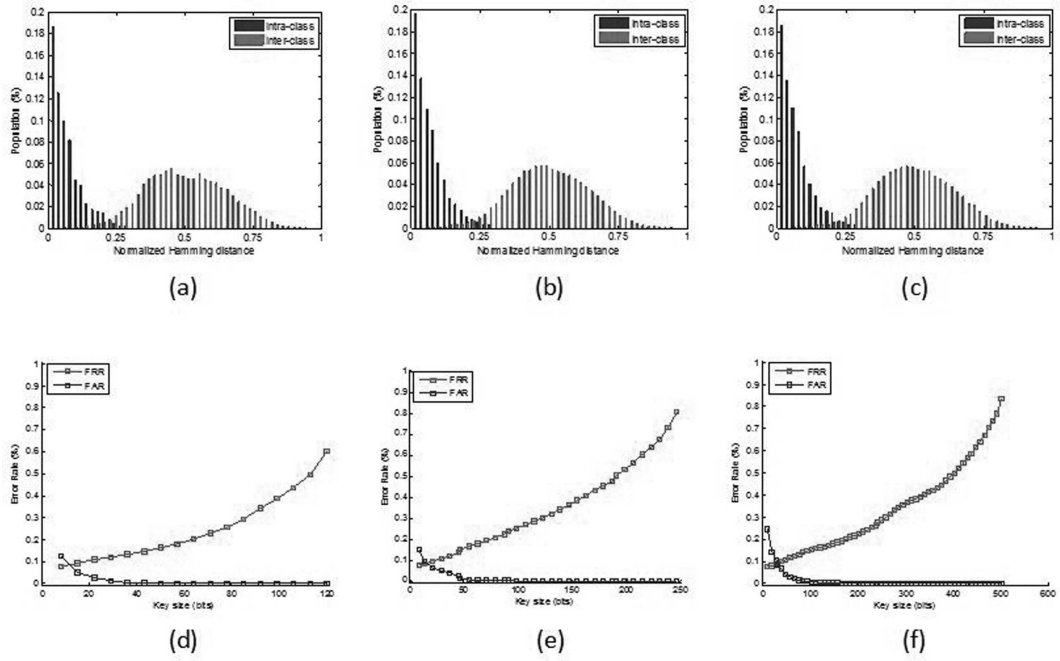
도면4


Enrollment phase
Biometric acquistion
41
Template extraction
42
Binarization
43
Reliable Bit Extraction
44
45
50
Key Encoding using ECC
46
Random Key m Generation
47
Hash Function
48
49
STORAGE
Secured δ
51
Hash Code h(m)
Authentication phase
Biometric acquistion
61
Template extraction
62
Binarization
63
Reliable Bit Extraction
64
65
66
Key Encoding using ECC
Hash Function
67
Hash Code h(m')
68
Matching
69
Decision
70

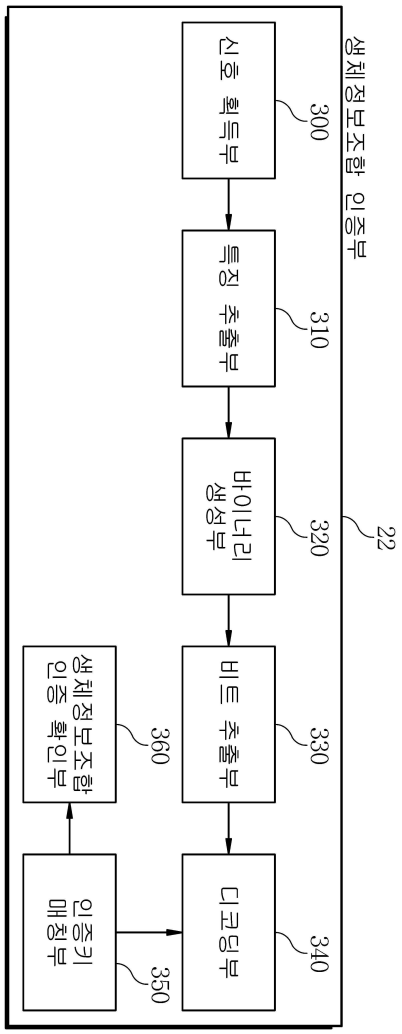
도면5


생체정보조합 등록부
20
신호 획득부
200
특징 추출부
210
바이너리 생성부
220
비트 추출부
230
인코딩부
250
랜덤키 생성부
240

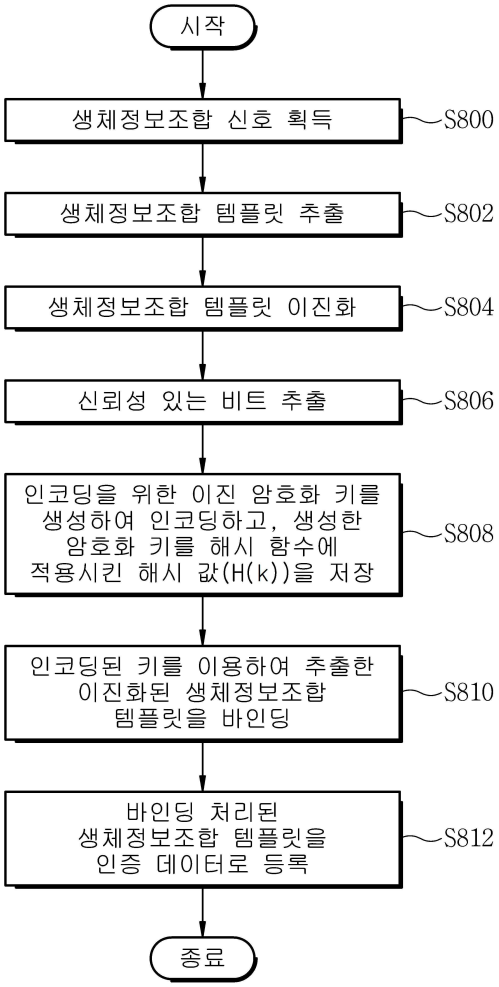
도면6


intra-class
inter-class
Population (%)
Normalized Hamming distance
(a)
(b)
(c)
FRR
FAR
Error Rate (%)
Key size (bits)
(d)
(e)
(f)

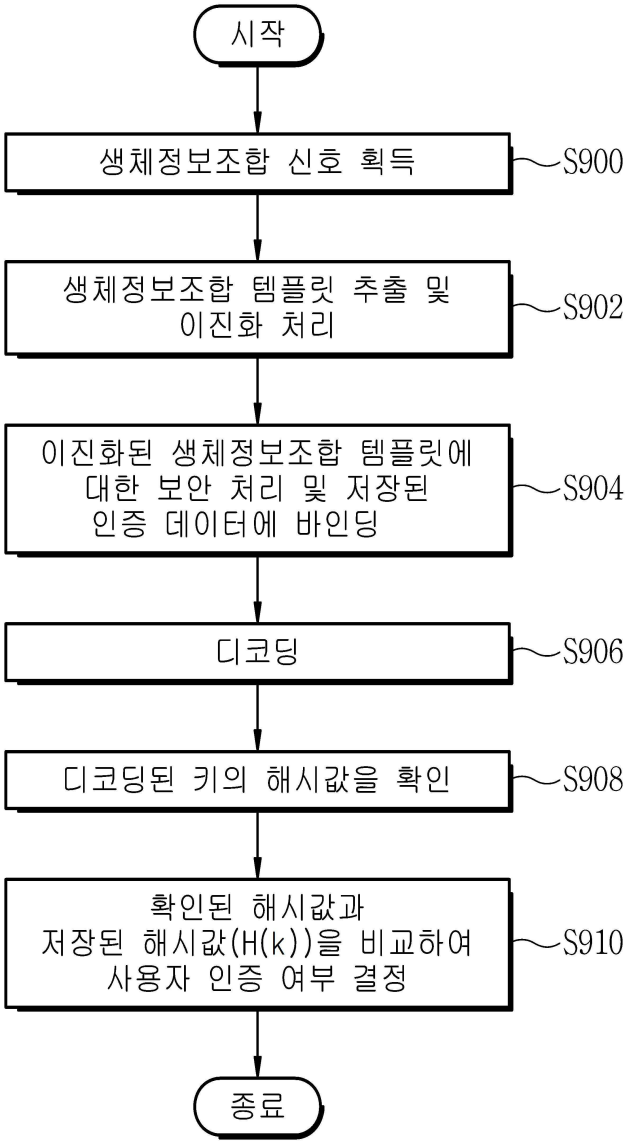
도면7


생체정보조합 인증부
22
신호 획득부
300
특징 추출부
310
바이너리 생성부
320
비트 추출부
330
디코딩부
340
인증키 매칭부
350
생체정보조합 인증 확인부
360

도면8


시작
생체정보조합 신호 획득
S800
생체정보조합 템플릿 추출
S802
생체정보조합 템플릿 이진화
S804
신뢰성 있는 비트 추출
S806
인코딩을 위한 이진 암호화 키를 생성하여 인코딩하고, 생성한 암호화 키를 해시 함수에 적용시킨 해시 값(H(k))을 저장
S808
인코딩된 키를 이용하여 추출한 이진화된 생체정보조합 템플릿을 바인딩
S810
바인딩 처리된 생체정보조합 템플릿을 인증 데이터로 등록
S812
종료

도면9


시작
생체정보조합 신호 획득
S900
생체정보조합 템플릿 추출 및 이진화 처리
S902
이진화된 생체정보조합 템플릿에 대한 보안 처리 및 저장된 인증 데이터에 바인딩
S904
디코딩
S906
디코딩된 키의 해시값을 확인
S908
확인된 해시값과 저장된 해시값(H(k))을 비교하여 사용자 인증 여부 결정
S910
종료