(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014 년 4 월 24 일 (24.04.2014)

WIPO | PCT

(10) 국제공개번호
WO 2014/061895 A1

(51) 국제특허분류:
G06F 17/21 (2006.01) *G06F 21/32* (2013.01)
G06K 9/46 (2006.01)

(21) 국제출원번호: PCT/KR2013/005491

(22) 국제출원일: 2013 년 6 월 21 일 (21.06.2013)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2012-0114739 2012 년 10 월 16 일 (16.10.2012) KR

(71) 출원인: **주식회사 시큐에프엔 (SECUFN CO LTD.,)** [KR/KR]; 133-834 서울시 성동구 아차산로 113 8 층, Seoul (KR).

(72) 발명자: **신준호 (SHIN, Joon Ho)**; 446-858 경기도 용인시 기흥구 죽현로 12 309 동 1202 호, Gyeonggi-do (KR).

(74) 대리인: **특허법인 수 (SU INTELLECTUAL PROPERTY)**; 135-907 서울시 강남구 논현로 101 길 8, 2 층, Seoul (KR).

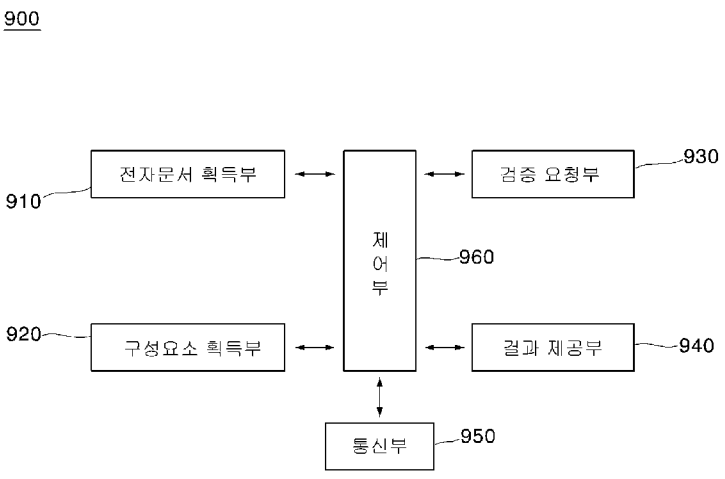
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[다음 쪽 계속]

(54) **Title**: ELECTRONIC SIGNING METHOD BASED ON BIOMETRIC INFORMATION RECOGNITION AND METHOD FOR VERIFYING ELECTRONICALLY SIGNED ELECTRONIC DOCUMENT BASED ON SAID BIOMETRIC INFORMATION RECOGNITION, AND TERMINAL, SERVER, AND COMPUTER-READABLE RECORDING MEDIUM USING SAME

(54) **발명의 명칭** : 생체정보인식 기반의 전자서명 방법 및 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법, 이와 같은 방법을 이용한 단말, 서버 및 컴퓨터 판독 가능한 기록 매체



910 ... Electronic document obtaining unit
920 ... Element obtaining unit
960 ... Controller
950 ... Communicating unit
930 ... Verification request unit
940 ... Result providing unit

(57) **Abstract**: According to one embodiment of the present invention, a method is provided which includes the steps of: (a) obtaining an original electronic document comprising biometric information that is electronically signed in the original electronic document to be verified or feature point information obtained from the biometric information, the hash value of the original electronic document, and time information in which the biometric information is electronically signed in the original electronic document is obtained and information on an encoded state with a biometric data standard is associated with a metafield; (b) obtaining the information on the encoded state with the biometric data standard in the metafield of the obtained original electronic document; (c) decoding the information on the encoded state with the biometric data standard and extracting the biometric information or the feature point information about the biometric information, the hash value of the original electronic document, and the time information that the biometric information electronically signed on the original electronic document is obtained; (d) comparing the extracted hash value from the information on the encoded state with the biometric data standard with a hash value directly obtained from the original electronic document, and comparing biometric information or biometric information about the feature point information extracted from the information on the encoded state with the biometric data standard with biometric information received from a user who has actually signed the original electronic document or feature point information obtained from the biometric information.

(57) **요약서**:

[다음 쪽 계속]

WO 2014/061895 A1

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

— 청구범위 보정서 및 설명서와 함께 (조약 제 19 조(1))

본 발명의 일 실시예에 따르면 (a) 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 생체정보로부터 획득된 특징점 정보, 전자문서의 원문의 해쉬값 및 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 단계, (b) 획득된 전자문서의 원문의 메타필드 내에서 생체데이터 표준으로 인코딩한 상태의 정보를 획득하는 단계, (c) 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 생체정보 또는 생체정보에 대한 특징점 정보, 전자문서의 원문의 해쉬값 및 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 단계, 및 (d) 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 생체정보 또는 생체정보에 대한 특징점 정보를 전자문서의 원문에 실제로 전자서명을 했던 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 단계를 포함하는 방법이 제공된다.

명세서

발명의 명칭: 생체정보인식 기반의 전자서명 방법 및 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법, 이와 같은 방법을 이용한 단말, 서버 및 컴퓨터 판독 가능한 기록 매체

기술분야

[1] 본 발명은 생체정보인식 기반의 전자서명 방법 및 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법, 이와 같은 방법을 이용한 단말, 서버 및 컴퓨터 판독 가능한 기록 매체에 관한 것이다.

배경기술

[2] 한국공개특허공보 제10-2009-0016886호에는, 서명과 패스워드를 입력 받은 후 입력된 패스워드를 암호화하여 서명에 추가될 가짜획과 가짜획의 삽입위치정보를 생성하고 가짜획의 삽입위치정보를 기초로 가짜획을 서명에 추가하여 암호화된 서명을 생성하는 방법이 기재되어 있다. 여기서, 가짜획이란 서명자로부터 입력된 서명 이외에 패스워드에 의해 별도로 생성되는 획을 의미한다고 기재되어 있다. 이에 따르면, 전자서명의 재현가능성을 제거할 수 있게 되는 특징이 있다.

[3] 하지만, 이와 같이 한국공개특허공보 제10-2009-0016886호는 암호화된 서명을 생성하는데에 주목적이 있었기에, 전자문서의 원문 자체의 진정성을 파악할 수 없다는 한계가 있었다. 또한, 상기 제10-2009-0016886호는 생체신호를 이용한 전자서명에 대해서는 전혀 개시하고 있지 아니하므로, 개개인 고유의 생체신호를 효과적으로 사용하여 간편하게 전자서명의 위조를 방지하고자 하는 생각을 하지 못하였고, 단지 일반 전자서명에 대하여 복잡한 암호화를 수행하여 전자서명의 위조를 방지해야 하였다.

발명의 상세한 설명

기술적 과제

[4] 본 발명은 상술한 문제점을 모두 해결하는 것을 그 목적으로 한다.

[5] 또한, 본 발명은 생체신호인식 기반의 전자서명을 삽입하여 전자문서를 생성하고 이를 통하여 추후 상기 전자문서의 무결성을 담보하는 것을 다른 목적으로 한다.

[6] 또한, 본 발명은 생체신호 기반의 전자서명을 통해 부인방지를 효과적으로 수행할 수 있는 것을 전자문서를 생성하는 것을 또 다른 목적으로 한다.

과제 해결 수단

[7] 상기 목적을 달성하기 위한 본 발명의 대표적인 구성은 다음과 같다.

[8] 본 발명의 일 태양에 따르면, 생체정보인식 기반의 전자서명 방법에 있어서, (a) 전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보를

획득하는 단계, (b) 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬 값 및 상기 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 단계, 및 (c) 상기 생체데이터 표준으로 인코딩된 정보를 마크 형태로 변환한 후 상기 전자문서의 원문과 상기 마크 형태를 결합하거나, 상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 결합하는 단계를 포함하는 방법이 제공된다.

[9] 본 발명의 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법에 있어서, (a) 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보를 변환하여 생성된 마크 형태가 결합된 전자문서의 원문을 획득하는 단계, (b) 상기 획득된 전자문서의 원문에 결합된 마크 형태의 부분을 변환하여 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하는 단계, (c) 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 단계, 및 (d) 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 단계를 포함하는 방법이 제공된다.

[10] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법에 있어서, (a) 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 단계, (b) 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하는 단계, (c) 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 단계, 및 (d) 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기

전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 단계를 포함하는 방법이 제공된다.

[11] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반의 전자서명 방법에 있어서, (a) 전자문서에 삽입될 생체정보를 획득하는 단계, (b) 상기 전자문서의 원문에 대한 해쉬 값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보에 워터마크로 삽입하는 단계, (c) 상기 워터마크를 포함하는 생체정보를 마크 형태로 변환하는 단계, 및 (d) 상기 전자문서의 원문과 상기 마크 형태를 결합하는 단계를 포함하는 방법이 제공된다.

[12] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반의 전자서명 방법에 있어서, (a) 전자문서에 삽입될 생체정보를 제1 이미지 형태로 획득하는 단계, (b) 상기 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하는 단계, (c) 상기 추출된 특징점 정보를 제2 이미지 형태로 변환하는 단계, (d) 상기 전자문서의 원문에 대한 해쉬 값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보로부터 추출된 특징점 정보로부터 변환된 상기 제2 이미지에 워터마크로 삽입하는 단계, 및 (e) 상기 워터마크를 포함하는 상기 제2 이미지를 마크 형태로 변환한 후 상기 전자문서의 원문과 상기 마크 형태를 결합하거나, 상기 워터마크를 포함하는 상기 제2 이미지를 상기 전자문서의 원문의 메타필드에 결합하는 단계를 포함하는 방법이 제공된다.

[13] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반의 전자서명 방법에 있어서, (a) 전자문서에 삽입될 생체정보를 획득하는 단계, (b) 상기 전자문서의 원문에 대한 해쉬 값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보에 워터마크로 삽입하는 단계, 및 (c) 상기 워터마크를 포함하는 생체정보를 상기 전자문서의 원문의 메타필드(meta field)에 결합하는 단계를 포함하는 방법이 제공된다.

[14] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법에 있어서, (a) 검증을 요하는 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로서 삽입되어 있는 상태의 생체정보를 변환하여 생성된 마크 형태가 결합된 전자문서의 원문을 획득하는 단계, (b) 상기 획득된 전자문서의 원문에 결합된 상기 마크 형태 부분을 변환하여 상기 워터마크를 포함하는 생체정보를 획득하는 단계, (c) 워터마크 모듈을 통해 상기 워터마크를 포함하는 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 단계, 및 (d) 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교되도록 하는 단계를 포함하는 방법이 제공된다.

[15] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법에 있어서, (a) 검증을 요하는 전자문서의 원문에 사용자에 의해 직접 전자서명에 사용된 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하고 상기 추출된 특징점 정보를 제2 이미지 형태로 변환한 경우, 상기 전자문서의 원문에 전자서명된 상기 제1 이미지 형태의 생체정보가 획득된 시점 정보 및 상기 전자문서의 원문의 해쉬값이 워터마크로서 삽입되어 있는 상태의 상기 제2 이미지 형태의 생체정보를 변환하여 생성된 마크 형태가 결합된 전자문서의 원문; 또는 검증을 요하는 전자문서의 원문에 사용자에 의해 직접 전자서명에 사용된 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하고 상기 추출된 특징점 정보를 제2 이미지 형태로 변환한 경우, 상기 전자문서의 원문에 전자서명된 상기 제1 이미지 형태의 생체정보가 획득된 시점 정보 및 상기 전자문서의 원문의 해쉬값이 워터마크로서 삽입되어 있는 상태의 상기 제2 이미지 형태의 생체정보가 메타필드에 결합되어 있는 전자문서의 원문을 획득하는 단계, (b) 상기 획득된 전자문서의 원문에 결합된 상기 마크 형태 부분을 변환하여 상기 워터마크를 포함하는 상기 제2 이미지 형태의 생체정보를 획득하거나 상기 획득된 전자문서의 원문의 메타필드에 결합되어 있는 상기 제2 이미지 형태의 생체정보를 획득하는 단계, (c) 워터마크 모듈을 통해 상기 워터마크를 포함하는 제2 이미지 형태의 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 제1 이미지 형태의 생체정보가 획득된 시점 정보를 추출하는 단계, 및 (d) 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 워터마크 모듈을 통해 획득된 상기 제1 이미지 형태의 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교되도록 하는 단계를 포함하는 방법이 제공된다.

[16] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법에 있어서, (a) 검증을 요하는 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로서 삽입되어 있는 상태의 생체정보를 메타필드에 결합된 상태로 포함하고 있는 전자문서의 원문을 획득하는 단계, (b) 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 워터마크를 포함하는 생체정보를 획득하는 단계, (c) 워터마크 모듈을 통해 상기 워터마크를 포함하는 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 단계, 및 (d) 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교되도록 하는 단계를 포함하는 방법이 제공된다.

[17] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반의 전자서명을 위한 단말 장치에 있어서, 전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보를 획득하는 생체정보 획득부, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬 값 및 상기 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 생체정보 가공부, 및 상기 생체데이터 표준으로 인코딩된 정보가 상기 생체정보 가공부에 의해 마크 형태로 변환되면 상기 전자문서의 원문과 상기 마크 형태를 결합하거나, 상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 결합하는 전자서명 결합부를 포함하는 단말 장치가 제공된다.

[18] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 단말 장치에 있어서, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보를 변환하여 생성된 마크 형태가 결합된 전자문서의 원문을 획득하는 전자문서 획득부, 상기 획득된 전자문서의 원문에 결합된 마크 형태의 부분을 변환하여 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 비교 요청부를 포함하는 단말 장치가 제공된다.

[19] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 단말 장치에 있어서, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 전자문서 획득부, 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는

구성요소 획득부, 및 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 비교 요청부를 포함하는 단말 장치가 제공된다.

[20] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반의 전자서명을 위한 단말 장치에 있어서, 전자문서에 삽입될 생체정보를 획득하는 생체정보 획득부, 상기 전자문서의 원문에 대한 해쉬 값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보에 워터마크로 삽입하고, 상기 워터마크를 포함하는 생체정보를 마크 형태로 변환하는 생체정보 가공부, 및 상기 전자문서의 원문과 상기 마크 형태를 결합하는 전자서명 결합부를 포함하는 단말 장치가 제공된다.

[21] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반의 전자서명을 위한 단말 장치에 있어서, 전자문서에 삽입될 생체정보를 제1 이미지 형태로 획득하는 생체정보 획득부, 상기 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하고, 상기 추출된 특징점 정보를 제2 이미지 형태로 변환한 후, 상기 전자문서의 원문에 대한 해쉬 값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보로부터 추출된 특징점 정보로부터 변환된 상기 제2 이미지에 워터마크로 삽입하는 생체정보 가공부, 및 상기 워터마크를 포함하는 상기 제2 이미지를 마크 형태로 변환한 후 상기 전자문서의 원문과 상기 마크 형태를 결합하거나, 상기 워터마크를 포함하는 상기 제2 이미지를 상기 전자문서의 원문의 메타필드에 결합하는 전자서명 결합부를 포함하는 단말 장치가 제공된다.

[22] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반의 전자서명을 위한 단말 장치에 있어서, 전자문서에 삽입될 생체정보를 획득하는 생체정보 획득부, 상기 전자문서의 원문에 대한 해쉬 값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보에 워터마크로 삽입하는 생체정보 가공부, 및 상기 워터마크를 포함하는 생체정보를 상기 전자문서의 원문의 메타필드(meta field)에 결합하는 전자서명 완결부를 포함하는 단말 장치가 제공된다.

[23] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 단말 장치에 있어서, 검증을 요하는 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로서 삽입되어 있는 상태의 생체정보를 변환하여 생성된 마크 형태가 결합된 전자문서의 원문을 획득하는 전자문서 획득부, 상기 획득된 전자문서의 원문에 결합된 상기 마크 형태 부분을 변환하여 상기 워터마크를 포함하는 생체정보를 획득하고, 워터마크 모듈을 통해 상기 워터마크를 포함하는 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의

원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교되도록 하는 비교 요청부를 포함하는 단말 장치가 제공된다.

[24] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 단말 장치에 있어서, 검증을 요하는 전자문서의 원문에 사용자에 의해 직접 전자서명에 사용된 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하고 상기 추출된 특징점 정보를 제2 이미지 형태로 변환한 경우, 상기 전자문서의 원문에 전자서명된 상기 제1 이미지 형태의 생체정보가 획득된 시점 정보 및 상기 전자문서의 원문의 해쉬값이 워터마크로서 삽입되어 있는 상태의 상기 제2 이미지 형태의 생체정보를 변환하여 생성된 마크 형태가 결합된 전자문서의 원문; 또는 검증을 요하는 전자문서의 원문에 사용자에 의해 직접 전자서명에 사용된 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하고 상기 추출된 특징점 정보를 제2 이미지 형태로 변환한 경우, 상기 전자문서의 원문에 전자서명된 상기 제1 이미지 형태의 생체정보가 획득된 시점 정보 및 상기 전자문서의 원문의 해쉬값이 워터마크로서 삽입되어 있는 상태의 상기 제2 이미지 형태의 생체정보가 메타필드에 결합되어 있는 전자문서의 원문을 획득하는 전자문서 획득부, 상기 획득된 전자문서의 원문에 결합된 상기 마크 형태 부분을 변환하여 상기 워터마크를 포함하는 상기 제2 이미지 형태의 생체정보를 획득하거나 상기 획득된 전자문서의 원문의 메타필드에 결합되어 있는 상기 제2 이미지 형태의 생체정보를 획득한 후, 워터마크 모듈을 통해 상기 워터마크를 포함하는 제2 이미지 형태의 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 제1 이미지 형태의 생체정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 워터마크 모듈을 통해 획득된 상기 제1 이미지 형태의 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교되도록 하는 비교 요청부를 포함하는 단말 장치가 제공된다.

[25] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 단말 장치에 있어서, 검증을 요하는 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로서 삽입되어 있는 상태의 생체정보를 메타필드에 결합된 상태로 포함하고 있는 전자문서의 원문을 획득하는 전자문서 획득부, 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 워터마크를 포함하는 생체정보를 획득한 후, 워터마크 모듈을 통해 상기 워터마크를 포함하는

생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교되도록 하는 비교 요청부를 포함하는 단말 장치가 제공된다.

[26] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반의 전자서명을 위한 서버에 있어서, 전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬 값 및 상기 생체정보가 획득된 시점 정보를 단말 장치로부터 수신하는 구성요소 획득부, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬 값 및 상기 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 생체정보 가공부, 및 상기 생체데이터 표준으로 인코딩된 정보가 상기 생체정보 가공부에 의해 마크 형태로 변환되면 상기 전자문서의 원문과 상기 마크 형태를 결합하거나, 상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 결합하는 전자서명 결합부를 포함하는 서버가 제공된다.

[27] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 서버에 있어서, 단말 장치로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보를 변환하여 생성된 마크 형태가 결합된 전자문서의 원문을 획득하는 전자문서 획득부, 상기 획득된 전자문서의 원문에 결합된 마크 형태의 부분을 변환하여 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교하는 구성요소 비교부를 포함하는 서버가 제공된다.

[28] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 서버에 있어서, 단말 장치로부터 특정 전자문서에

대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 전자문서 획득부, 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 비교하는 구성요소 비교부를 포함하는 서버가 제공된다.

[29] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반의 전자서명을 위한 서버에 있어서, 전자문서에 삽입될 생체정보, 상기 전자문서의 원문에 대한 해쉬값, 및 상기 생체정보가 획득된 시점 정보를 단말 장치로부터 수신하는 구성요소 획득부, 상기 전자문서의 원문에 대한 해쉬 값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보에 워터마크로 삽입하고, 상기 워터마크를 포함하는 생체정보를 마크 형태로 변환하는 생체정보 가공부, 및 상기 전자문서의 원문과 상기 마크 형태를 결합하는 전자서명 결합부를 포함하는 서버가 제공된다.

[30] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반의 전자서명을 위한 서버에 있어서, 단말 장치로부터 전자문서에 삽입될 생체정보를 제1 이미지 형태 또는 이로부터 추출된 특징점 정보 형태로 획득하고, 상기 전자문서의 원문에 대한 해쉬 값과 상기 생체정보가 획득된 시점 정보를 획득하는 구성요소 획득부, 상기 제1 이미지 형태의 생체정보에서 추출된 특징점 정보를 제2 이미지 형태로 변환한 후, 상기 전자문서의 원문에 대한 해쉬 값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보로부터 추출된 특징점 정보로부터 변환된 상기 제2 이미지에 워터마크로 삽입하는 생체정보 가공부, 및 상기 워터마크를 포함하는 상기 제2 이미지를 마크 형태로 변환한 후 상기 전자문서의 원문과 상기 마크 형태를 결합하거나, 상기 워터마크를 포함하는 상기 제2 이미지를 상기 전자문서의 원문의 메타필드에 결합하는 전자서명 결합부를 포함하는 서버가 제공된다.

[31] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반의 전자서명을 위한 서버에 있어서, 단말 장치로부터 전자문서에 삽입될 생체정보, 상기 전자문서의 원문에 대한 해쉬 값, 및 상기 생체정보가 획득된 시점 정보를 획득하는

구성요소 획득부, 상기 전자문서의 원문에 대한 해쉬 값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보에 워터마크로 삽입하는 생체정보 가공부, 및 상기 워터마크를 포함하는 생체정보를 상기 전자문서의 원문의 메타필드(meta field)에 결합하는 전자서명 완결부를 포함하는 서버가 제공된다.

[32]

[33] *본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 서버에 있어서, 단말 장치로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로서 삽입되어 있는 상태의 생체정보를 변환하여 생성된 마크 형태가 결합된 전자문서의 원문을 획득하는 전자문서 획득부, 상기 획득된 전자문서의 원문에 결합된 상기 마크 형태 부분을 변환하여 상기 워터마크를 포함하는 생체정보를 획득하고, 워터마크 모듈을 통해 상기 워터마크를 포함하는 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교하는 구성요소 비교부를 포함하는 서버가 제공된다.

[34]

[35] *본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 서버에 있어서, 단말 장치로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문에 사용자에 의해 직접 전자서명에 사용된 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하고 상기 추출된 특징점 정보를 제2 이미지 형태로 변환한 경우, 상기 전자문서의 원문에 전자서명된 상기 제1 이미지 형태의 생체정보가 획득된 시점 정보 및 상기 전자문서의 원문의 해쉬값이 워터마크로서 삽입되어 있는 상태의 상기 제2 이미지 형태의 생체정보를 변환하여 생성된 마크 형태가 결합된 전자문서의 원문; 또는 검증을 요하는 전자문서의 원문에 사용자에 의해 직접 전자서명에 사용된 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하고 상기 추출된 특징점 정보를 제2 이미지 형태로 변환한 경우, 상기 전자문서의 원문에 전자서명된 상기 제1 이미지 형태의 생체정보가 획득된 시점 정보 및 상기 전자문서의 원문의 해쉬값이 워터마크로서 삽입되어 있는 상태의 상기 제2 이미지 형태의 생체정보가 메타필드에 결합되어 있는 전자문서의 원문을 획득하는 전자문서 획득부, 상기 획득된 전자문서의 원문에 결합된 상기 마크 형태 부분을 변환하여 상기 워터마크를 포함하는 상기 제2 이미지 형태의 생체정보를 획득하거나 상기 획득된 전자문서의 원문의 메타필드에 결합되어 있는 상기 제2 이미지 형태의 생체정보를 획득한 후, 워터마크 모듈을 통해 상기

워터마크를 포함하는 제2 이미지 형태의 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 제1 이미지 형태의 생체정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 워터마크 모듈을 통해 획득된 상기 제1 이미지 형태의 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교하는 구성요소 비교부를 포함하는 서버가 제공된다.

[36] 본 발명의 또 다른 태양에 따르면, 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 서버에 있어서, 단말 장치로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로서 삽입되어 있는 상태의 생체정보를 메타필드에 결합된 상태로 포함하고 있는 전자문서의 원문을 획득하는 전자문서 획득부, 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 워터마크를 포함하는 생체정보를 획득한 후, 워터마크 모듈을 통해 상기 워터마크를 포함하는 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교하는 구성요소 비교부를 포함하는 서버가 제공된다.

발명의 효과

[37] 본 발명에 의하면, 생체신호인식 기반으로 전자서명을 삽입하여 효과적으로 전자문서를 생성할 수 있는 효과를 달성할 수 있다.

[38] 본 발명에 의하면, 생체신호인식 기반의 전자서명이 삽입된 전자문서의 원문에 대하여 추후 그 진위가 논란이 되었을 때 효과적으로 원문의 무결성을 확보할 수 있는 효과를 달성할 수 있다.

[39] 또한, 본 발명에 의하면, 이미지 편집 등을 통해 쉽게 위조가 가능하였던 생체신호 기반의 전자서명에 대하여 위조를 방지하고 본인의 전자서명에 대한 부인을 방지할 수 있는 효과를 달성할 수 있다.

도면의 간단한 설명

[40] 도 1은 본 발명의 일 실시예에 따라 생체정보인식 기반의 전자서명을 전자문서에 삽입하기 위한 전체 시스템의 구성을 개략적으로 나타내는 도면이다.

[41] 도 2는 본 발명의 일 실시예에 따라 단말 장치(100)의 구성을 나타내는 도면이다.

[42] 도 3은 본 발명의 일 실시예에 따라, 지문서명에 의한 전자문서의 생성 절차를 나타내는 일례를 나타낸다.

[43] 도 4는 본 발명의 일 실시예에 따라 생체정보인식 기반으로 전자서명이 삽입된 전자문서를 검증하기 위한 전체 시스템의 구성을 개략적으로 나타내는 도면이다.

[44] 도 5는 본 발명의 일 실시예에 따라 단말 장치(900)의 구성을 나타내는 도면이다.

[45] 도 6은 본 발명의 일 실시예에 따라, 전자문서의 검증 절차를 나타내는 일례를 나타낸다.

[46] <부호의 설명>

[47] 10: 생체정보 획득장치

[48] 100: 전자문서 생성용 단말 장치

[49] 200: 저장부

[50] 300: 서버

[51] 110: 생체정보 획득부

[52] 120: 생체정보 가공부

[53] 130: 전자서명 결합부

[54] 140: 전자문서 저장 관리부

[55] 150: 통신부

[56] 160: 제어부

[57] 900: 전자문서 검증용 단말 장치

[58] 910: 전자문서 획득부

[59] 920: 구성요소 획득부

[60] 930: 검증 요청부

[61] 940: 결과 제공부

[62] 950: 통신부

[63] 960: 제어부

발명의 실시를 위한 형태

[64] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예에 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의

범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[65] 이하에서는, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있도록 하기 위하여, 본 발명의 바람직한 실시예들에 관하여 첨부된 도면을 참조하여 상세히 설명하기로 한다.

[66] 본 명세서에 있어서, "생체정보"는 인간의 몸으로부터 획득된 식별 가능한 정보를 나타내는 것으로서, 지문, 손금, DNA, 홍채, 얼굴, 전신 등으로부터 획득된 정보를 포함하는 개념이다. 다만, 본 명세서에서는 설명의 편의상 주로 지문으로부터 획득된 정보를 이용하여 전자문서를 생성하고 이를 검증하는 것을 예로 들어 설명할 것이다.

[67] 본 명세서에 있어서, "생체데이터 표준"은 획득된 생체정보를 인코딩하고 디코딩하기 위하여 사용되는 일종의 규약으로서, CBEFF(Common Biometric Exchange Formats Framework)를 포함하는 개념이다. 다만, 이에 한정되는 것은 아니며, x.984, XCBF 등 다양한 후속 표준도 포함한다 할 것이다.

[68] 본 명세서에 있어서, "마크"는 바코드, QR 코드뿐만 아니라 시각화하여 나타낼 수 있는 각종 표장 등을 포함하는 개념이다. 또한, 여기서 "시각화"란 육안으로 식별 가능한 상태뿐만 아니라 장치의 힘을 빌려 식별 가능한 상태도 포함하는 개념이다.

[69] 생체정보인식 기반의 전자서명을 전자문서에 삽입하기 위한 전체 시스템의 구성

[70] 도 1은 본 발명의 일 실시예에 따라 생체정보인식 기반의 전자서명을 전자문서에 삽입하기 위한 전체 시스템의 구성을 개략적으로 나타내는 도면이다.

[71] 도 1에 도시되어 있는 바와 같이 본 발명의 일 실시예에 따른 전체 시스템은, 생체정보 획득장치(10), 전자문서 생성용 단말 장치(100)(이하, 편의상 단말 장치(100)로 기술함), 저장부(200), 서버(300)로 구성될 수 있다. 물론, 상기 구성요소들이 전부 필수적인 것은 아니며, 단말 장치(100)와 서버(300) 간의 업무 수행 분담 정도에 따라 구성요소의 변경이 있을 수도 있을 것이다.

[72] 먼저, 상기 구성요소들 사이 중 적어도 일부를 연결하기 위한 통신망은 유선 및 무선과 같은 그 통신 양태를 가리지 않고 구성될 수 있다.

[73] 다음으로, 본 발명의 일 실시예에 따르면, 단말 장치(100)는 사용자가 통신망을 통하여 저장부(200) 및/또는 서버(300)에 접속한 후 통신할 수 있도록 하는 기능을 포함하는 디지털 기기이다. 이하에서는 단말 장치(100)의 예로서 주로 모바일 폰을 상정하여 설명하지만, 반드시 이에 한정되는 것은 아니다. 예를 들어, 개인용 컴퓨터(예를 들어, 데스크탑 컴퓨터, 노트북 컴퓨터 등), 워크스테이션, PDA, 웹 패드, 스마트 폰, 태블릿 PC 등과 같이 메모리 수단을 구비하고 마이크로 프로세서를 탑재하여 연산 능력을 갖춘 디지털 기기라면

얼마든지 본 발명에서 말하는 단말 장치(100)로서 채택될 수 있다.

[74] 이러한 단말 장치(100)는 생체정보가 획득되면 소정의 전자문서에 생체정보를 전자서명으로서 삽입하여 전자문서를 완성하는 기능을 수행할 수 있다. 이에 대해서는 추후 보다 구체적으로 살펴보도록 한다.

[75] 다음으로, 생체정보 획득장치(10)는 단말 장치(100)에 연결될 수 있는 기기이며, 사용자로부터 생체정보를 수집하는 기능을 수행할 수 있다. 이때, 생체정보 획득장치(10)가 반드시 필요한 것은 아니며, 단말 장치(100)의 터치스크린 또는 카메라 모듈 등을 통하여 직접적으로 획득할 수도 있을 것이다.

[76] 다음으로, 저장부(200)는 단말 장치(100)에 의해 전자서명이 삽입되어 완성된 전자문서를 보관하는 기능을 수행할 수 있다. 저장부(200)는 단말 장치(100)의 내부에 있을 수도 있지만, 단말 장치(100)의 외부에 존재하여 통신망을 통하여 단말 장치(100)와 통신할 수도 있음은 물론이라 할 것이다.

[77]

[78] *다음으로, 서버(300)는 추후 도 3을 참조로 설명할 키(key)와 전자문서의 식별번호 등을 저장하는 기능을 수행할 수 있으며, 이들을 저장함으로써 추후 서버(300)가 지문특징점을 매칭하여 사용자의 신원을 확인하고 전자문서에 삽입된 전자서명에 대한 부인을 방지하는 역할을 할 수 있다.

[79] 도 2는 본 발명의 일 실시예에 따라 단말 장치(100)의 구성을 나타내는 도면이다.

[80] 도 2에 도시되어 있는 바와 같이, 본 발명의 일 실시예에 따른 단말 장치(100)는, 생체정보 획득부(110), 생체정보 가공부(120), 전자서명 결합부(130), 전자문서 저장관리부(140), 통신부(150) 및 제어부(160)를 포함할 수 있다. 본 발명의 일 실시예에 따르면, 생체정보 획득부(110), 생체정보 가공부(120), 전자서명 결합부(130), 전자문서 저장관리부(140), 통신부(150) 및 제어부(160)는 그 중 적어도 일부가 단말 장치(100)와 통신하는 프로그램 모듈들일 수도 있다. 이러한 프로그램 모듈들은 운영 시스템, 응용 프로그램 모듈 및 기타 프로그램 모듈의 형태로 단말 장치(100)에 포함될 수 있으며, 물리적으로는 여러 가지 공지의 기억 장치 상에 저장될 수 있다. 또한, 이러한 프로그램 모듈들은 단말 장치(100)와 통신 가능한 원격 기억 장치에 저장될 수도 있다. 한편, 이러한 프로그램 모듈들은 본 발명에 따라 후술할 특정 업무를 수행하거나 특정 추상 데이터 유형을 실행하는 루틴, 서브루틴, 프로그램, 오브젝트, 컴포넌트, 데이터 구조 등을 포괄하지만, 이에 제한되지는 않는다.

[81] 먼저, 본 발명의 일 실시예에 따르면, 생체정보 획득부(110)는 전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보를 획득하는 기능을 수행할 수 있다. 이때, 생체정보 획득부(110)는 생체정보를 단말 장치(100)에 연결된 생체정보 수집용 기기를 통해 획득되거나 단말 장치(100)의 터치스크린 또는 카메라 모듈을 통해 획득할 수 있으며, 이와 같은 생체정보로부터 추출된 특징점을 획득하는 기능을 수행할 수도 있을 것이다. 물론, 단말 장치(100)의

생체정보 획득부(110)가 직접 특징점을 추출할 수도 있겠지만, 이미 다른 장치에서 추출된 상태로 생체정보 획득부(110)로 입력될 수도 있을 것이다(이에 대해서는 별도의 말이 없어도 본 명세서의 유사한 실시예에 적용될 수 있다 할 것이다).

[82] 다음으로, 본 발명의 일 실시예에 따르면, 생체정보 가공부(120)는 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 기능을 수행할 수 있다. 가령, 생체데이터 표준이 CBEFF(Common Biometric Exchange File Format)일 때, CBEFF 내에 (i) 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, (ii) 상기 전자문서의 원문에 대한 해쉬값과 (iii) 상기 생체정보가 획득된 시점 정보를 삽입하여 인코딩을 수행하는 기능을 수행할 수 있다. 이때, CBEFF 내에는 (iv) 생체정보의 획득 기관에 대한 정보도 포함되어 인코딩될 수 있으나, 반드시 필수적인 것은 아니다(이에 대해서도 별도의 말이 없어도 본 명세서의 유사한 실시예에 적용될 수 있다 할 것이다).

[83] 본 발명의 일 실시예에 따르면, 경우에 따라서, 생체정보 획득부(110)가 생체정보에 대한 암호화된 상태의 정보 또는 상기 생체정보의 특징점 정보에 대한 암호화된 상태의 정보를 획득할 수도 있는데, 이 경우 생체정보 가공부(120)는 상기 암호화된 상태의 생체정보(또는, 상기 암호화된 상태의 생체정보의 특징점 정보), 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하게 될 것이다(이에 대해서도 별도의 말이 없어도 본 명세서의 유사한 실시예에 적용될 수 있다 할 것이다).

[84] 다음으로, 본 발명의 일 실시예에 따르면, 상기 생체데이터 표준으로 인코딩된 정보가 상기 생체정보 가공부(120)에 의해 마크 형태로 변환되면, 전자서명 결합부(130)는 상기 전자문서의 원문과 상기 마크를 결합하는 기능을 수행할 수 있다. 이 경우 전자문서의 원문에 시각적으로 드러나는 마크가 결합되어 전자문서가 완성되게 된다.

[85] 또 다른 경우에, 전자서명 결합부(130)는 상기 생체데이터 표준으로 인코딩된 정보를 (마크 형태로 변환하지 않고) 상기 전자문서의 원문의 메타필드(meta field)에 결합하는 기능을 수행할 수도 있다. 이 경우에는 전자문서의 원문에 시각적으로 드러나지 않는 형태로 생체정보가 녹아들게 되며, 이와 같은 상태로 전자문서가 완성되게 된다. 여기서, 메타필드는 메타데이터가 기록되기 위한 영역을 의미한다.

[86] 본 발명의 일 실시예에 따르면, 이와 같이 전자서명이 삽입되어 완성된 버전의 전자문서는 전자문서 저장관리부(140)에 의해 저장부(200)에 전송되어 저장될 수 있다.

[87] 한편, 본 발명의 다른 실시예에 따르면, 생체정보 획득부(110)가 전자문서에 삽입될 생체정보를 획득하면, 생체정보 가공부(120)는 전자문서의 원문에 대한

해쉬값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보에 워터마크로 삽입하고, 상기 워터마크를 포함하는 생체정보를 마크로 변환하는 기능을 수행할 수 있다. 이후, 전자서명 결합부(130)는 상기 전자문서의 원문과 상기 마크를 결합하여 전자문서를 완성할 수 있다. 마찬가지로, 완성된 전자문서는 전자문서 저장관리부(140)를 통해 저장부(200)에 저장되도록 할 수 있다.

[88] 여기서, 생체정보 가공부(120)는, 상기 워터마크를 포함하는 생체정보를 생체데이터 표준으로 인코딩하는 기능을 더 수행할 수 있다. 이 경우 생체정보 가공부(120)는 상기 생체데이터 표준으로 인코딩된 워터마크를 포함하는 생체정보를 마크 형태로 변환하면, 전자서명 결합부(130)는 이와 같은 마크를 전자문서 원문과 결합할 수 있을 것이다(이에 대해서도 별도의 말이 없어도 본 명세서의 유사한 실시예에 적용될 수 있다 할 것이다).

[89] 또한, 생체정보 가공부(120)가 상기 워터마크를 포함하는 생체정보를 생체데이터 표준으로 인코딩할 때, 상기 워터마크를 포함하는 생체정보뿐만 아니라 상기 서명시점, 상기 전자문서의 원문에 대한 해쉬값을 추가적으로 생체데이터 표준으로 인코딩할 수도 있고, 추가적으로 생체정보의 획득기관 정보를 포함하여 생체데이터 표준으로 인코딩할 수도 있을 것이다(이에 대해서도 별도의 말이 없어도 본 명세서의 유사한 실시예에 적용될 수 있다 할 것이다).

[90] 한편, 생체정보 가공부(120)는, 상기 워터마크를 포함하는 생체정보를 압축 알고리즘으로 압축하는 기능을 더 수행할 수도 있는데, 이 경우 생체정보 가공부(120)는 상기 워터마크를 포함하는 생체정보를 압축한 상태의 정보를 마크로 변환할 수 있을 것이다(이에 대해서도 별도의 말이 없어도 본 명세서의 유사한 실시예에 적용될 수 있다 할 것이다).

[91] 한편, 본 발명의 또 다른 실시예에 따르면, 생체정보 획득부(110)가 전자문서에 삽입될 생체정보를 제1 이미지 형태로 획득하면, 생체정보 가공부(120)는 상기 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하고, 상기 추출된 특징점 정보를 제2 이미지 형태로 변환한 후, 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보로부터 추출된 특징점 정보로부터 변환된 상기 제2 이미지에 워터마크로 삽입하는 기능을 수행할 수 있다. 이때, 생체정보 가공부(120)는 생체정보를 제1 이미지 형태로 획득할 수도 있지만, 제1 이미지 형태로부터 특징점이 추출된 상태를 수신할 수도 있을 것이고, 제1 이미지 형태로부터 특징점이 추출된 상태를 제2 이미지 형태로 변환한 후 수신할 수도 있을 것이다(이에 대해서도 별도의 말이 없어도 본 명세서의 유사한 실시예에 적용될 수 있다 할 것이다). 이때, 전자서명 결합부(130)는 상기 워터마크를 포함하는 상기 제2 이미지를 마크로 변환한 후 상기 전자문서의 원문과 상기 마크를 결합할 수도 있고, 다른 예로서, 상기 워터마크를 포함하는 상기 제2 이미지를 상기 전자문서의 원문의 메타필드에 결합할 수도 있을 것이다. 이와 같이 완성된 전자문서는 전자문서

저장관리부(140)에 의해 저장부(200)에 저장될 것이다.

[92] 한편, 본 발명의 또 다른 실시예에 따르면, 생체정보 획득부(110)가 전자문서에 삽입될 생체정보를 획득하면, 생체정보 가공부(120)는 전자문서의 원문에 대한 해쉬값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보에 워터마크로 삽입하고, 전자서명 완결부(130)는 상기 워터마크를 포함하는 생체정보를 상기 전자문서의 원문의 메타필드(meta field)에 결합할 수 있다. 마찬가지로, 이와 같이 완성된 전자문서는 전자문서 저장관리부(140)에 의해 저장부(200)에 저장될 것이다. 그런데, 이 경우에도, 생체정보 가공부(120)는 상기 워터마크를 포함하는 생체정보를 생체데이터 표준으로 인코딩하는 기능을 수행할 수도 있으며, 이 경우 전자서명 결합부(130)는 상기 생체데이터 표준으로 인코딩된 워터마크를 포함하는 생체정보를 상기 전자문서의 원문의 메타필드에 결합할 수 있을 것이다.

[93] 다음으로, 본 발명의 일 실시예에 따르면, 통신부(150)는 본 발명의 단말 장치(100)가 외부 장치와 통신할 수 있도록 하는 기능을 수행할 수 있다.

[94] 마지막으로, 본 발명의 일 실시예에 따르면, 제어부(160)는 생체정보 획득부(110), 생체정보 가공부(120), 전자서명 결합부(130), 전자문서 저장관리부(140) 및 통신부(150)의 데이터의 흐름을 제어하는 기능을 수행한다. 즉, 제어부(160)는 외부로부터의 또는 단말 장치(100)의 각 구성요소 간의 데이터의 흐름을 제어함으로써, 생체정보 획득부(110), 생체정보 가공부(120), 전자서명 결합부(130), 전자문서 저장관리부(140), 및 통신부(150)에서 각각 고유 기능을 수행하도록 제어한다.

[95] 한편, 상기 실시예들은 전자문서의 완성을 위한 단계들을 단말 장치(100)에서 수행하는 것으로 설명하였으나, 반드시 이에 한정되는 것은 아니며, 서버(300)에서 이와 같은 단계들을 수행할 수도 있을 것이다.

[96] 예를 들어, 서버(300)에 포함된 구성요소 획득부(미도시)는 전자문서에 삽입될 (i) 생체정보 또는 상기 생체정보에 대한 특징점 정보, 그리고 (ii) 상기 전자문서의 원문에 대한 해쉬값 및 (iii) 상기 생체정보가 획득된 시점 정보를 단말 장치(100)로부터 수신하는 기능을 수행할 수 있다. 구성요소 획득부가 이와 같은 데이터들을 수신하면, 서버(300)에 포함된 생체정보 가공부(미도시)는 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 그리고 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 기능을 수행할 수 있으며, 상기 생체데이터 표준으로 인코딩된 정보가 상기 생체정보 가공부에 의해 마크로 변환되면 서버(300)에 포함된 전자서명 결합부(미도시)가 상기 전자문서의 원문과 상기 마크를 결합하여 전자문서를 완성할 수도 있고, 마크 형태로 변환 없이 전자서명 결합부가 상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 결합하여 전자문서를 완성할 수도 있을 것이다. 이때, 전자서명 결합부에 의해 상기 전자문서의 원문과 상기 마크가 결합되거나 상기

전자문서의 원문의 메타필드에 상기 생체데이터 표준으로 인코딩된 정보가 결합되면, 서버(300)에 포함된 전자문서 저장관리부(미도시)는 이를 서명완료된 전자문서로서 저장부(200)에 저장되도록 할 수 있을 것이다.

[97] 전자문서의 완성을 위한 단계들을 서버(300)에서 수행하는 다른 예를 살펴보면, 서버(300)에 포함된 구성요소 획득부(미도시)가 (i) 전자문서에 삽입될 생체정보, (ii) 상기 전자문서의 원문에 대한 해쉬값, 및 (iii) 상기 생체정보가 획득된 시점 정보를 단말 장치(100)로부터 수신하면, 서버(300)에 포함된 생체정보 가공부(미도시)가 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보에 워터마크로 삽입하고, 상기 워터마크를 포함하는 생체정보를 마크로 변환하면, 서버(300)에 포함된 전자서명 결합부는 상기 전자문서의 원문과 상기 마크를 결합하는 기능을 수행할 수도 있을 것이다. 이때, 상기 생체정보 가공부는, 상기 워터마크를 포함하는 생체정보를 생체데이터 표준으로 인코딩하는 기능을 더 수행할 수도 있는데, 이 경우 생체정보 가공부는 상기 생체데이터 표준으로 인코딩된 워터마크를 포함하는 생체정보를 마크로 변환할 수 있을 것이다.

[98] 전자문서의 완성을 위한 단계들을 서버(300)에서 수행하는 또 다른 예를 살펴보면, 서버(300)에 포함된 구성요소 획득부(미도시)가 단말 장치(100)로부터 전자문서에 삽입될 생체정보를 제1 이미지 형태 또는 이로부터 추출된 특징점 정보 형태로 획득하고, 이와 더불어 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보가 획득된 시점 정보를 획득하면, 서버(300)에 포함된 생체정보 가공부는 상기 제1 이미지 형태의 생체정보에서 추출된 특징점 정보를 제2 이미지 형태로 변환한 후, 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보로부터 추출된 특징점 정보로부터 변환된 상기 제2 이미지에 워터마크로 삽입하는 기능을 수행할 수 있다. 이후, 서버(300)에 포함된 전자서명 결합부는 상기 워터마크를 포함하는 상기 제2 이미지를 마크로 변환한 후 상기 전자문서의 원문과 상기 마크를 결합하여 전자문서를 완성할 수도 있고, 마크 형태로의 변환 없이 곧바로 상기 워터마크를 포함하는 상기 제2 이미지를 상기 전자문서의 원문의 메타필드에 결합하여 전자문서를 완성할 수도 있다.

[99] 전자문서의 완성을 위한 단계들을 서버(300)에서 수행하는 또 다른 예를 살펴보면, 서버(300)에 포함된 구성요소 획득부(미도시)가 단말 장치로부터 전자문서에 삽입될 생체정보, 상기 전자문서의 원문에 대한 해쉬값, 및 상기 생체정보가 획득된 시점 정보를 획득하면, 서버(300)에 포함된 생체정보 가공부가 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보가 획득된 시점 정보를 상기 생체정보에 워터마크로 삽입하는 기능을 수행할 수 있다. 이후, 서버(300)에 포함된 전자서명 완결부는 상기 워터마크를 포함하는 생체정보를 상기 전자문서의 원문의 메타필드(meta field)에 결합하여 전자문서를 완성할 수도 있다. 이때, 상기 생체정보 가공부는, 상기 워터마크를 포함하는

생체정보를 생체데이터 표준으로 인코딩하는 기능을 더 수행할 수도 있고, 이 경우 상기 전자서명 결합부는, 상기 생체데이터 표준으로 인코딩된 워터마크를 포함하는 생체정보를 상기 전자문서의 원문의 메타필드에 결합하여 전자문서를 완성할 수도 있을 것이다.

[100] 도 3은 본 발명의 일 실시예에 따라, 지문서명에 의한 전자문서의 생성 절차를 나타내는 일례를 나타낸다. 참고로, 도 3은 도 1에 나타난 각 구성요소인 생체정보 획득장치(10), 전자문서 생성용 단말장치(100), 저장부(200), 서버(300)의 일례로서, 각각 지문인식기, 스마트패드, 공전소(공인 전자문서 보관소), HSM을 예시적으로 나타내었다. 도 3을 참조로 설명되는 내용 중 암호화 단계 및 종류 라든가 복호화 단계 및 종류, 인코딩 단계 및 종류, 특징점 추출 단계 등은 (위에서 다양한 실시예를 통해 누차 설명하였듯이) 필수적인 단계는 아니며, 예시적으로 나타낸 것에 불과함을 미리 밝혀둔다.

[101] 우선, 스마트패드에서 지문인식기에 지문서명을 요청한다는 신호를 보내면(단계 3-1), 지문인식기는 사용자의 지문을 스캔하고 품질이 기설정된 선명도 이상이라고 확인되면 지문 이미지로부터 특징점을 추출해 낸다(소위 지문템플릿)(단계 3-2). 이때, 난수를 사용하여 지문템플릿을 암호화하기 위한 AES(Advanced Encryption Standard) 키를 생성하고(단계 3-3), 이를 사용하여 지문템플릿을 암호화하게 된다(단계 3-4). 다음으로, AES키 자체를 비대칭키로 암호화한 후(단계 3-5), 암호화된 지문템플릿(즉, 지문 특징점)과 비대칭키로 암호화된 AES키를 스마트패드에 전송한다(단계 3-6).

[102] 상기 데이터들을 전송받은 스마트패드는, 상기 데이터들과 전자문서 원문으로부터 추출된 해쉬값과 안드로이드 시간 정보를 통해 획득된 지문서명 시점정보를 CBEFF에 입력하여 CBEFF 인코딩을 수행하고(단계 3-7), 이를 시각화하기 위하여 PDF 인코딩을 수행하여 마크를 생성하며(단계 3-8), 마크 부분을 전자문서 원문과 결합하여 전자문서를 완성하고 이를 공전소에 저장되도록 공전소에 전송한다(단계 3-9). 이와 동시에 스마트패드가 비대칭키 암호화된 AES키와 완성된 전자문서에 대한 식별번호(가령, 계약서 번호)를 HSM에 전송하면, HSM은 이를 수신한 후 비대칭키 암호화된 AES키를 복호화하고(단계 3-10), 복호화된 AES키와 완성된 전자문서의 식별번호를 저장하게 된다(단계 3-11).

[103] 생체정보인식 기반으로 전자서명이 삽입된 전자문서를 검증하기 위한 전체 시스템의 구성

[104] 도 4는 본 발명의 일 실시예에 따라 생체정보인식 기반으로 전자서명이 삽입된 전자문서를 검증하기 위한 전체 시스템의 구성을 개략적으로 나타내는 도면이다.

[105] 도 4에 도시되어 있는 바와 같이 본 발명의 일 실시예에 따른 전체 시스템은, 생체정보 획득장치(10), 전자문서 검증용 단말 장치(900)(이하, 편의상 단말 장치(900)로 기술함), 저장부(200), 서버(300)로 구성될 수 있다. 다만, 여기서

단말 장치(100)와 단말 장치(900)는 동일한 단말 장치로 구현될 수도 있음은 물론이라 할 것이다.

[106] 물론, 상기 구성요소들이 전부 필수적인 것은 아니며, 단말 장치(900)와 서버(300) 간의 업무 수행 분담 정도에 따라 구성요소의 변경이 있을 수도 있을 것이다.

[107] 먼저, 상기 구성요소들 사이 중 적어도 일부를 연결하기 위한 통신망은 유선 및 무선과 같은 그 통신 양태를 가리지 않고 구성될 수 있다.

[108] 다음으로, 본 발명의 일 실시예에 따르면, 단말 장치(900)는 사용자가 통신망을 통하여 저장부(200) 및/또는 서버(300)에 접속한 후 통신할 수 있도록 하는 기능을 포함하는 디지털 기기이다. 이하에서는 단말 장치(900)의 예로서 주로 모바일 폰을 상정하여 설명하지만, 반드시 이에 한정되는 것은 아니다. 예를 들어, 개인용 컴퓨터(예를 들어, 데스크탑 컴퓨터, 노트북 컴퓨터 등), 워크스테이션, PDA, 웹 패드, 스마트 폰, 태블릿 PC 등과 같이 메모리 수단을 구비하고 마이크로 프로세서를 탑재하여 연산 능력을 갖춘 디지털 기기라면 얼마든지 본 발명에서 말하는 단말 장치(900)로서 채택될 수 있다.

[109] 이러한 단말 장치(900)는 생체정보가 전자서명으로서 삽입된 전자문서가 검증 대상으로서 획득되면 해당 전자문서의 원문의 무결성을 확보하고 전자서명을 한 자의 부인을 방지하기 위하여 검증하는 기능을 수행할 수 있다. 이에 대해서는 추후 보다 구체적으로 살펴보도록 한다.

[110] 다음으로, 생체정보 획득장치(10)는 단말 장치(900)에 연결될 수 있는 기기이며, 상기 전자문서의 전자서명을 한 사람으로 생각되는 사용자로부터 직접 생체정보를 수집하는 기능을 수행할 수 있다. 이때, 생체정보 획득장치(10)가 반드시 필요한 것은 아니며, 단말 장치(900)의 터치스크린 또는 카메라 모듈 등을 통하여 직접적으로 획득할 수도 있을 것이다.

[111] 다음으로, 저장부(200)는 단말 장치(900)의 요청에 의해 그 동안 보관하고 있던 전자서명이 삽입된 전자문서를 단말 장치(900)로 송신하는 기능을 수행할 수 있다. 저장부(200)는 단말 장치(900)의 내부에 있을 수도 있지만, 단말 장치(900)의 외부에 존재하여 통신망을 통하여 단말 장치(900)와 통신할 수도 있음은 물론이라 할 것이다.

[112] 다음으로, 서버(300)는 단말 장치(900)로부터의 요청에 의해 전자문서에 전자서명으로서 삽입되어 있는 생체정보와 생체정보 획득장치(10)로부터 직접 획득된 생체정보를 비교하고 이의 결과를 단말 장치(900)에 제공하는 기능을 수행할 수 있다. 서버(300)에 대해서는 추후 도 6을 참조로 보다 자세히 설명하도록 한다.

[113] 도 5는 본 발명의 일 실시예에 따라 단말 장치(900)의 구성을 나타내는 도면이다.

[114] 도 5에 도시되어 있는 바와 같이, 본 발명의 일 실시예에 따른 단말 장치(900)는, 전자문서 획득부(910), 구성요소 획득부(920), 검증 요청부(930), 결과

제공부(940), 통신부(950) 및 제어부(960)를 포함할 수 있다. 본 발명의 일 실시예에 따르면, 전자문서 획득부(910), 구성요소 획득부(920), 검증 요청부(930), 결과 제공부(940), 통신부(950) 및 제어부(960)는 그 중 적어도 일부가 단말 장치(900)와 통신하는 프로그램 모듈들일 수도 있다. 이러한 프로그램 모듈들은 운영 시스템, 응용 프로그램 모듈 및 기타 프로그램 모듈의 형태로 단말 장치(900)에 포함될 수 있으며, 물리적으로는 여러 가지 공지의 기억 장치 상에 저장될 수 있다. 또한, 이러한 프로그램 모듈들은 단말 장치(900)와 통신 가능한 원격 기억 장치에 저장될 수도 있다. 한편, 이러한 프로그램 모듈들은 본 발명에 따라 후술할 특정 업무를 수행하거나 특정 추상 데이터 유형을 실행하는 루틴, 서브루틴, 프로그램, 오브젝트, 컴포넌트, 데이터 구조 등을 포괄하지만, 이에 제한되지는 않는다.

[115] 본 발명의 일 실시예에 따르면, 전자문서 획득부(910)는 검증을 요하는 전자문서의 원문을 획득하는 기능을 수행할 수 있는데, 구체적으로는, 복수의 정보(즉, (i) 해당 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, (ii) 상기 전자문서의 원문의 해쉬값 및 (iii) 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보)를 생체데이터 표준으로 인코딩한 상태의 정보를 변환하여 생성된 마크가 결합되어 있는 상태의 전자문서를 획득할 수 있다. 전자문서의 원문이 획득되면, 구성요소 획득부(920)는, 상기 획득된 전자문서의 원문에 결합된 마크의 부분을 변환하여 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 (i) 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, (ii) 상기 전자문서의 원문의 해쉬값 및 (iii) 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 기능을 수행할 수 있다. 이와 같이 추출된 데이터는 전자문서의 무결성 확보와 사용자의 부인 방지를 위한 검증에 사용되므로, 소위 검증을 위한 "구성요소"로 불리울 수 있을 것이다. 다음으로, 검증 요청부(930)는 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교되도록 요청하는 기능을 수행할 수 있다. 가령, 검증 요청부(930)는 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교되도록 별도의 서버(300)에 요청할 수도 있을 것이다(다만, 반드시 이에 한정되는 것은 아니며, 서버(300)의 업무와 단말 장치(900)의 업무가 적절하게 분담되도록 조정할 수

있음은 물론이라 할 것이다. 이에 대해서는 본 명세서의 유사한 실시예에 그대로 적용될 수 있다 할 것이다). 이때, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우, 결과 제공부(940)는 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 일치하는 경우, 결과 제공부(940)는 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지한다는 결과를 제공할 수 있다. 여기서, 상기 생체데이터 표준으로 인코딩한 상태의 정보는, CBEFF(Common Biometric Exchange File Format) 내에 상기 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보가 획득된 시점 정보를 삽입하여 인코딩을 수행하여 획득되는 것을 포함하는 개념이나, 반드시 이에 한정되는 것은 아닐 것이다.

[116] 본 발명의 다른 실시예에 따르면, 전자문서 획득부(910)는 검증을 요하는 전자문서의 원문을 획득하는 기능을 수행할 수 있는데, 구체적으로는, 복수의 정보(즉, 해당 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보)를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 기능을 수행할 수 있다. 이와 같이 전자문서의 원문이 획득되면, 구성요소 획득부(920)는 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 기능을 수행할 수 있다. 다음으로, 검증 요청부(930)는 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 비교되도록 서버(300) 등에 요청하는 기능을 수행할 수 있을 것이다. 이때, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우, 결과 제공부(940)는 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의

원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 일치하는 경우, 결과 제공부(940)는 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 제공할 수 있다.

[117] 본 발명의 또 다른 실시예에 따르면, 전자문서 획득부(910)는 검증을 요하는 전자문서의 원문을 획득하는 기능을 수행할 수 있는데, 구체적으로는, 검증을 요하는 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로서 삽입되어 있는 상태의 생체정보를 변환하여 생성된 마크가 결합된 전자문서의 원문을 획득하는 기능을 수행할 수 있다. 이와 같이 전자문서의 원문이 획득되면, 구성요소 획득부(920)는 상기 획득된 전자문서의 원문에 결합된 상기 마크 부분을 변환하여 상기 워터마크를 포함하는 생체정보를 획득하고, 워터마크 모듈을 통해 상기 워터마크를 포함하는 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 기능을 수행할 수 있다. 다음으로, 검증 요청부(930)는 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교되도록 서버(300) 등에 요청하는 기능을 수행할 수 있다. 이때, 상기 워터마크 모듈을 통해 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우, 결과 제공부(940)는 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 직접 현장에서 입력 받은 생체정보와 일치하는 경우, 결과 제공부(940)는 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 제공할 수 있다. 한편, 상기 전자문서 획득부(910)는, 검증을 요하는 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로 삽입된 생체정보를 생체데이터 표준으로 인코딩한 후 상기 생체데이터 표준으로 인코딩된 상태로부터 변환하여 생성된 마크가 결합된 상태의 전자문서의 원문을 획득할 수도 있는 등 다양한 변형예를 상정할 수 있을 것이다. 또한, 이 경우, 상기 구성요소 획득부(920)는, 상기 획득된 전자문서의 원문에 결합된 상기 마크 부분을 변환하여 상기 생체데이터 표준으로 인코딩된 상태의 생체정보를 획득한 후, 상기 생체데이터 표준으로 인코딩된 상태의 생체정보를 디코딩하여 상기 생체데이터 표준으로 인코딩되기 전의 생체정보를 복원함으로써, 상기 워터마크를 포함하는 생체정보를 획득할 수 있을 것이다. 또 다른 예로서, 상기 전자문서 획득부(910)는, 검증을 요하는 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점

정보가 워터마크로 삽입된 생체정보를 압축 알고리즘으로 압축한 후 상기 압축된 상태를 변환하여 생성된 마크가 결합된 상태의 전자문서의 원문을 획득할 수도 있을 것이고, 이 경우 상기 구성요소 획득부(920)는, 상기 획득된 전자문서의 원문에 결합된 상기 마크 부분을 변환하여 상기 압축된 상태의 생체정보를 획득한 후, 상기 압축된 상태의 생체정보에서 압축되기 전의 생체정보를 복원함으로써, 상기 워터마크를 포함하는 생체정보를 획득할 수 있을 것이다.

[118] 본 발명의 또 다른 실시예에 따르면, 전자문서 획득부(910)는 검증을 요하는 전자문서의 원문을 획득하는 기능을 수행할 수 있는데, 구체적으로는, 검증을 요하는 전자문서의 원문에 사용자에 의해 직접 전자서명에 사용된 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하고 상기 추출된 특징점 정보를 제2 이미지 형태로 변환한 경우, 전자문서 획득부(910)는, 상기 전자문서의 원문에 전자서명된 상기 제1 이미지 형태의 생체정보가 획득된 시점 정보 및 상기 전자문서의 원문의 해쉬값이 워터마크로서 삽입되어 있는 상태의 상기 제2 이미지 형태의 생체정보를 변환하여 생성된 마크가 결합된 전자문서의 원문을 획득할 수도 있고, 또 다른 예로서, 상기 전자문서의 원문에 전자서명된 상기 제1 이미지 형태의 생체정보가 획득된 시점 정보 및 상기 전자문서의 원문의 해쉬값이 워터마크로서 삽입되어 있는 상태의 상기 제2 이미지 형태의 생체정보가 메타필드에 결합되어 있는 전자문서의 원문을 획득할 수도 있을 것이다. 전자문서의 원문이 획득되면, 구성요소 획득부(920)는 상기 획득된 전자문서의 원문에 결합된 상기 마크 부분을 변환하여 상기 워터마크를 포함하는 상기 제2 이미지 형태의 생체정보를 획득하거나 상기 획득된 전자문서의 원문의 메타필드에 결합되어 있는 상기 제2 이미지 형태의 생체정보를 획득한 후, 워터마크 모듈을 통해 상기 워터마크를 포함하는 제2 이미지 형태의 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 제1 이미지 형태의 생체정보가 획득된 시점 정보를 추출하는 기능을 수행할 수 있다. 다음으로, 검증 요청부(930)는 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 워터마크 모듈을 통해 획득된 상기 제1 이미지 형태의 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교되도록 서버(300) 등에 요청하는 기능을 수행할 수 있다.

[119] 본 발명의 또 다른 실시예에 따르면, 전자문서 획득부(910)는 검증을 요하는 전자문서의 원문을 획득하는 기능을 수행할 수 있는데, 구체적으로는, 전자문서 획득부(910)는, 검증을 요하는 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로서 삽입되어 있는 상태의 생체정보를 메타필드에 결합된 상태로 포함하고 있는 전자문서의 원문을 획득하는 기능을 수행할 수 있다. 전자문서의 원문이 획득되면, 구성요소

획득부(920)는, 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 워터마크를 포함하는 생체정보를 획득한 후, 워터마크 모듈을 통해 상기 워터마크를 포함하는 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 기능을 수행할 수 있다. 다음으로, 검증 요청부(930)는, 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교되도록 서버(300) 등에 요청하는 기능을 수행할 수 있다. 이때, 상기 워터마크 모듈을 통해 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우, 결과 제공부(940)는 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 직접 현장에서 입력 받은 생체정보와 일치하는 경우, 결과 제공부(940)는 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 제공하는 기능을 수행할 수 있다. 이때, 상기 전자문서 획득부(910)는, 검증을 요하는 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로 삽입된 생체정보를 생체데이터 표준으로 인코딩한 후 상기 생체데이터 표준으로 인코딩된 상태의 생체정보를 메타필드에 결합된 상태로 포함하고 있는 전자문서의 원문을 획득할 수도 있을 것이다. 그렇게 되면, 상기 구성요소 획득부(920)는, 상기 획득된 전자문서의 메타필드 내에서 상기 생체데이터 표준으로 인코딩된 상태의 생체정보를 획득한 후, 상기 생체데이터 표준으로 인코딩된 상태의 생체정보를 디코딩하여 상기 생체데이터 표준으로 인코딩되기 전의 생체정보를 복원함으로써, 상기 워터마크를 포함하는 생체정보를 획득하는 기능을 수행할 수도 있을 것이다.

[120] 한편, 상기 실시예들은 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 단계들을 단말 장치(900)에서 수행하는 것으로 설명하였으나, 반드시 이에 한정되는 것은 아니며, 서버(300)에서 이와 같은 단계들을 수행할 수도 있을 것이다.

[121] 예를 들어, 본 발명의 일 실시예에 따르면, 서버(300)에 포함된 전자문서 획득부(미도시)는, 단말 장치(900)로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보를 변환하여 생성된 마크가 결합된 전자문서의 원문을 획득하는 기능을 수행할 수 있다. 이때, 전자문서의 원문을 저장부(200)로부터 직접 수신할 수도 있고, 저장부(200)로부터 단말 장치(900)를

경유하여 수신할 수도 있는 등 다양한 변형예를 상정할 수 있을 것이다(이에 대해서도 별도의 말이 없어도 본 명세서의 유사한 실시예에 적용될 수 있다 할 것이다). 이후, 서버(300)에 포함된 구성요소 획득부(미도시)가 상기 획득된 전자문서의 원문에 결합된 마크의 부분을 변환하여 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 (i) 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, (ii) 상기 전자문서의 원문의 해쉬값 및 (iii) 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 기능을 수행할 수 있다. 다음으로, 서버(300)에 포함된 구성요소 비교부(미도시)는, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교하는 기능을 수행할 수 있다. 여기서, 서버(300)에 포함된 결과 제공부(미도시)는, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 상기 단말장치(900)에 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 상기 단말장치(900)에 제공하는 기능을 수행할 수 있다.

[122] 전자문서의 검증을 위한 단계들을 서버(300)에서 수행하는 다른 예를 살펴보면, 서버(300)에 포함된 전자문서 획득부(미도시)는, 단말장치(900)로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 기능을 수행할 수 있다. 이후, 서버(300)에 포함된 구성요소 획득부(미도시)는, 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 기능을 수행할 수 있다. 다음으로, 서버(300)에 포함된 구성요소

비교부(미도시)는, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 비교하는 기능을 수행할 수 있다. 여기서, 서버(300)에 포함된 결과 제공부(미도시)는, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 상기 단말 장치(900)에 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 상기 단말 장치(900)에 제공하는 기능을 수행할 수 있다.

[123] 전자문서의 검증을 위한 단계들을 서버(300)에서 수행하는 또 다른 예를 살펴보면, 서버(300)에 포함된 전자문서 획득부(미도시)는, 단말 장치(900)로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로서 삽입되어 있는 상태의 생체정보를 변환하여 생성된 마크가 결합된 전자문서의 원문을 획득하는 기능을 수행할 수 있다. 이후, 서버(300)에 포함된 구성요소 획득부(미도시)는, 상기 획득된 전자문서의 원문에 결합된 상기 마크 부분을 변환하여 상기 워터마크를 포함하는 생체정보를 획득하고, 워터마크 모듈을 통해 상기 워터마크를 포함하는 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 기능을 수행할 수 있다. 다음으로, 서버(300)에 포함된 구성요소 비교부(미도시)는, 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교하는 기능을 수행할 수 있다. 여기서, 서버(300)에 포함된 결과 제공부(미도시)는, 상기 워터마크 모듈을 통해 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 상기 단말 장치(900)에 제공하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 직접 현장에서 입력 받은 생체정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 상기 단말 장치(900)에 제공하는

기능을 수행할 수 있다. 이때, 상기 전자문서 획득부는, 검증을 요하는 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로 삽입된 생체정보를 생체데이터 표준으로 인코딩한 후 상기 생체데이터 표준으로 인코딩된 상태로부터 변환하여 생성된 마크가 결합된 상태의 전자문서의 원문을 획득할 수도 있을 것인데, 이 경우, 상기 구성요소 획득부는, 상기 획득된 전자문서의 원문에 결합된 상기 마크 부분을 변환하여 상기 생체데이터 표준으로 인코딩된 상태의 생체정보를 획득한 후, 상기 생체데이터 표준으로 인코딩된 상태의 생체정보를 디코딩하여 상기 생체데이터 표준으로 인코딩되기 전의 생체정보를 복원함으로써, 상기 워터마크를 포함하는 생체정보를 획득하게 될 것이다.

[124] 전자문서의 검증을 위한 단계들을 서버(300)에서 수행하는 또 다른 예를 살펴보면, 단말 장치(900)로부터 특정 전자문서에 대한 검증 요청이 수신될 때, 검증을 요하는 전자문서의 원문에 사용자에 의해 직접 전자서명에 사용된 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하고 상기 추출된 특징점 정보를 제2 이미지 형태로 변환하는 경우를 상정한다면, 서버(300)에 포함된 전자문서 획득부(미도시)는, 상기 전자문서의 원문에 전자서명된 상기 제1 이미지 형태의 생체정보가 획득된 시점 정보 및 상기 전자문서의 원문의 해쉬값이 워터마크로서 삽입되어 있는 상태의 상기 제2 이미지 형태의 생체정보를 변환하여 생성된 마크가 결합된 전자문서의 원문을 획득할 수도 있고, 또 다른 예로서, 검증을 요하는 전자문서의 원문에 사용자에 의해 직접 전자서명에 사용된 제1 이미지 형태의 생체정보에서 특징점 정보를 추출하고 상기 추출된 특징점 정보를 제2 이미지 형태로 변환한 경우를 상정한다면, 서버(300)에 포함된 전자문서 획득부(미도시)는, 상기 전자문서의 원문에 전자서명된 상기 제1 이미지 형태의 생체정보가 획득된 시점 정보 및 상기 전자문서의 원문의 해쉬값이 워터마크로서 삽입되어 있는 상태의 상기 제2 이미지 형태의 생체정보가 메타필드에 결합되어 있는 전자문서의 원문을 획득할 수도 있을 것이다. 이후, 서버(300)에 포함된 구성요소 획득부(미도시)는, 상기 획득된 전자문서의 원문에 결합된 상기 마크 부분을 변환하여 상기 워터마크를 포함하는 상기 제2 이미지 형태의 생체정보를 획득하거나 상기 획득된 전자문서의 원문의 메타필드에 결합되어 있는 상기 제2 이미지 형태의 생체정보를 획득한 후, 워터마크 모듈을 통해 상기 워터마크를 포함하는 제2 이미지 형태의 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 제1 이미지 형태의 생체정보가 획득된 시점 정보를 추출하는 기능을 수행할 수 있을 것이다. 다음으로, 서버(300)에 포함된 구성요소 비교부(미도시)는, 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 워터마크 모듈을 통해 획득된 상기 제1 이미지 형태의 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은

생체정보와 비교하는 기능을 수행할 수 있을 것이다.

[125] 전자문서의 검증을 위한 단계들을 서버(300)에서 수행하는 또 다른 예를 살펴보면, 서버(300)에 포함된 전자문서 획득부(미도시)는, 단말 장치(900)로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로서 삽입되어 있는 상태의 생체정보를 메타필드에 결합된 상태로 포함하고 있는 전자문서의 원문을 획득하는 기능을 수행할 수 있다. 이후, 서버(300)에 포함된 구성요소 획득부(미도시)는, 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 워터마크를 포함하는 생체정보를 획득한 후, 워터마크 모듈을 통해 상기 워터마크를 포함하는 생체정보에서 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보를 추출하는 기능을 수행할 수 있다. 다음으로, 서버(300)에 포함된 구성요소 비교부(미도시)는, 상기 워터마크 모듈을 통해 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보와 비교하는 기능을 수행할 수 있다. 이때, 서버(300)에 포함된 결과 제공부(미도시)는, 상기 워터마크 모듈을 통해 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 상기 단말 장치에 제공하고, 상기 워터마크 모듈을 통해 획득된 상기 생체정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 직접 현장에서 입력 받은 생체정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 상기 단말 장치에 제공하는 기능을 수행할 수 있을 것이다. 한편, 상기 전자문서 획득부는, 검증을 요하는 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보가 획득된 시점 정보가 워터마크로 삽입된 생체정보를 생체데이터 표준으로 인코딩한 후 상기 생체데이터 표준으로 인코딩된 상태의 생체정보를 메타필드에 결합된 상태로 포함하고 있는 전자문서의 원문을 획득할 수도 있을 것인데, 이 경우, 상기 구성요소 획득부는, 상기 획득된 전자문서의 메타필드 내에서 상기 생체데이터 표준으로 인코딩된 상태의 생체정보를 획득한 후, 상기 생체데이터 표준으로 인코딩된 상태의 생체정보를 디코딩하여 상기 생체데이터 표준으로 인코딩되기 전의 생체정보를 복원함으로써, 상기 워터마크를 포함하는 생체정보를 획득할 수 있을 것이다.

[126] 도 6은 본 발명의 일 실시예에 따라, 전자문서의 검증 절차를 나타내는 일례를 나타낸다. 참고로, 도 6은 도 4에 나타난 각 구성요소인 생체정보 획득장치(10), 전자문서 검증용 단말장치(900), 저장부(200), 서버(300)의 일례로서, 각각 지문인식기, 스마트패드, 공전소(공인전자 문서 보관소), HSM을 예시적으로

나타내었다. 도 6을 참조로 설명되는 내용 중 암호화 단계 및 종류 라든가 복호화 단계 및 종류, 인코딩 단계 및 종류, 특징점 추출 단계 등은 (위에서 다양한 실시예를 통해 설명하였듯이) 필수적인 단계는 아니며, 예시적으로 나타낸 것에 불과함을 미리 밝혀둔다.

[127] 도 6을 참조하면, 스마트패드가 검증의 대상이 되는 전자문서의 원본을 공전소에 요청하면(단계 6-1), 전자문서를 저장하고 있던 공전소는 전자문서의 식별번호와 전자문서의 원본을 스마트패드에 전송한다(단계 6-2). 스마트패드가 검증의 대상이 되는 전자문서의 원본을 획득하면, 해당 전자문서에 결합되어 있는 마크에 대해 PDF 디코딩을 수행하고(단계 6-3), CBEFF 디코딩을 수행하여(단계 6-4), 암호화된 지문특징점을 추출한다(단계 6-5). 이때, 실시예에 따라 암호화되지 않은 상태의 지문특징점이 추출될 수도 있음은 앞서 설명한 바와 같다. 상기 단계 6-5에서 추출되는 것은 지문특징점 이외에도 전자문서 원문의 해쉬값, 지문이 획득된 시점 정보 등이 있을 수 있다. 이후, 스마트패드는 전자문서의 원문이 본인이 전자서명했다고 주장하는 사용자로 하여금 지문인식기를 통하여 지문을 스캐닝하도록 요청할 수 있다(단계 6-6). 지문인식기가 사용자의 지문을 스캐닝하고 소정 이상의 선명도를 만족하면 이로부터 지문특징점을 추출할 수 있다(단계 6-7). 이후, 지문인식기는 난수를 사용하여 AES 키를 생성하고(단계 6-8), 이를 사용하여 지문템플릿을 암호화한다(단계 6-9). 이후, 지문인식기는 AES 키를 비대칭키 암호화한 후(단계 6-10), 암호화된 지문특징점(사용자로부터 직접 채취한 지문특징점)와 비대칭키 암호화된 AES키를 스마트패드로 전송한다(단계 6-11). 다음으로, 스마트패드는 지문인식기로부터 수신한 암호화된 지문특징점과 공전소로부터 획득된 전자문서의 원본에서 직접 추출한 암호화된 지문특징점을 지문인식기로부터 수신한 비대칭키 암호화된 AES키와 더불어 HSM으로 전송한다(단계 6-12). 이에, HSM은 기존에 저장하고 있던 AES키를 인출하고 이를 사용하여 전자문서의 원문으로부터 추출한 지문특징점을 복호화하고(단계 6-13), 지문인식기로부터 흘러온 AES키를 복호화한 후(단계 6-14), 이를 사용하여 마찬가지로 지문인식기로부터 흘러온 지문특징점(사용자로부터 직접 채취한 지문특징점)을 복호화한다(단계 6-15). 이에 따라, HSM은 전자문서의 원문으로부터 추출한 지문특징점과 사용자로부터 직접 채취한 지문특징점을 매칭하는 작업을 수행하고(단계 6-16), 매칭 결과를 스마트패드로 전송하는 기능을 수행한다(단계 6-17). 참고로, 도 6에서는 지문특징점의 매칭에 의해 사용자의 신원을 확인하고 부인을 방지하는 프로세스를 중점적으로 설명하였으나, 해당 전자문서에 결합되어 있는 마크에 대해 PDF 디코딩을 수행하고(단계 6-3), CBEFF 디코딩을 수행함으로써(단계 6-4) 지문특징점과 같이 추출된 전자문서 원문의 해쉬값을 전자문서로부터 직접 추출된 해쉬값과 비교함으로써 원문의 무결성도 검증할 수 있는데, 이에 대해서는 도 6에서 설명을 생략한 것임을 밝혀둔다.

[128] 이상 설명된 본 발명에 따른 실시예들은 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[129] 이상에서 본 발명이 구체적인 구성요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나, 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명이 상기 실시예들에 한정되는 것은 아니며, 본 발명이 속하는 기술분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형을 꾀할 수 있다.

[130] 따라서, 본 발명의 사상은 상기 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등하게 또는 등가적으로 변형된 모든 것들은 본 발명의 사상의 범주에 속한다고 할 것이다.

청구범위

[청구항 1] 생체정보인식 기반의 전자서명 방법에 있어서,
(a) 생체정보 획득부가, 전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보를 획득하는 단계,
(b) 생체정보 가공부가, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 단계, 및
(c) 전자서명 결합부가, 상기 생체데이터 표준으로 인코딩된 정보에 대해 시각화하기 위한 추가적인 인코딩을 수행하여 마크를 생성한 후 상기 전자문서의 원문과 상기 마크를 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 전자문서 상에서 시각화된 상태로, 상기 전자문서를 완성하는 단계
를 포함하는 방법.

[청구항 2] 제1항에 있어서,
상기 (b) 단계는,
상기 생체정보 가공부가, CBEFF(Common Biometric Exchange File Format) 내에 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 삽입하여 인코딩을 수행하는 것을 특징으로 하는 방법.

[청구항 3] 제1항에 있어서,
상기 (a) 단계는,
상기 생체정보 획득부가, 상기 생체정보 또는 상기 생체정보의 특징점 정보에 대한 암호화된 상태의 정보를 획득하는 단계인 것을 특징으로 하고,
상기 (b) 단계는,
상기 생체정보 가공부가, 상기 암호화된 상태의 생체정보 또는 상기 암호화된 상태의 생체정보의 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 단계인 것을 특징으로 하는 방법.

[청구항 4] 제1항에 있어서,
상기 생체정보는 지문을 스캐닝한 전자적 지문 서명인 것을 특징으로 하는 방법.

[청구항 5] 제4항에 있어서,

상기 (a) 단계는,
상기 생체정보 획득부가, 상기 전자적 지문 서명의 품질을 확인하여 선명도가 기설정된 임계치 이상인 경우에만 상기 전자적 지문 서명으로부터 특징점 정보를 획득하는 것을 특징으로 하는 방법.

[청구항 6] 제1항에 있어서,
상기 (a) 단계에서,
상기 생체정보는 소정의 단말 장치에 연결된 생체정보 수집용 기기를 통해 획득되거나 소정의 단말 장치의 터치스크린 또는 카메라 모듈을 통해 획득되는 것을 특징으로 하는 방법.

[청구항 7] 제1항에 있어서,
상기 (b) 단계는,
상기 생체정보 가공부가, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보에 더하여 상기 생체정보의 획득기관에 대한 정보를 추가적으로 상기 생체데이터 표준으로 인코딩하는 것을 특징으로 하는 방법.

[청구항 8] 제1항에 있어서,
상기 (c) 단계에서,
상기 마크는 바코드, QR코드, 시각화된 표장 중 적어도 하나를 포함하는 것을 특징으로 하는 방법.

[청구항 9] 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법에 있어서,
(a) 전자문서 획득부가, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보에 대해 시각화하기 위한 추가적인 인코딩을 수행하여 생성된 마크가 일체로 결합된 전자문서의 원문을 획득하는 단계 - 상기 획득된 전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 획득된 전자문서의 원문 상에서 시각화된 상태로 결합되어 완성된 상태임 - ,
(b) 구성요소 획득부가, 상기 획득된 전자문서의 원문에 일체로 결합된 마크의 부분을 디코딩하여 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하는 단계,

(c) 상기 구성요소 획득부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 추가적으로 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 추출하는 단계, 및

(d) 검증 요청부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 단계를 포함하는 방법.

[청구항 10] 제9항에 있어서,

(e) 결과 제공부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 제공하는 단계

를 더 포함하는 방법.

[청구항 11] 제9항에 있어서,

상기 생체데이터 표준으로 인코딩한 상태의 정보는,

CBEFF(Common Biometric Exchange File Format) 내에 상기 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 삽입하여 인코딩을 수행하여 획득되는 것을 특징으로 하는 방법.

[청구항 12] 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법에 있어서,

(a) 전자문서 획득부가, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가

획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 일체로 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 단계 - 상기 획득된 전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 전자문서의 원문 상에서 시각화되지 않은 상태로 결합되어 완성된 상태임 - ,

(b) 구성요소 획득부가, 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하는 단계,

(c) 상기 구성요소 획득부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 추출하는 단계, 및

(d) 검증 요청부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 단계

를 포함하는 방법.

[청구항 13] 제12항에 있어서,

(e) 결과 제공부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 제공하는 단계

를 더 포함하는 방법.

[청구항 14] 생체정보인식 기반의 전자서명을 위한 단말 장치에 있어서,

전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보를 획득하는 생체정보 획득부,

상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 생체정보 가공부, 및

상기 생체데이터 표준으로 인코딩된 정보에 대해 상기 생체정보 가공부에 의해 시각화하기 위한 추가적인 인코딩이 수행되어 마크가 생성되면 상기 전자문서의 원문과 상기 마크를 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 전자문서 상에서 시각화된 상태로, 상기 전자문서를 완성하는 전자서명 결합부를 포함하는 단말 장치.

[청구항 15] 제14항에 있어서,

상기 생체정보 가공부는,

CBEFF(Common Biometric Exchange File Format) 내에 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 삽입하여 인코딩을 수행하는 것을 특징으로 하는 단말 장치.

[청구항 16] 제14항에 있어서,

상기 생체정보 획득부는,

상기 생체정보 또는 상기 생체정보의 특징점 정보에 대한 암호화된 상태의 정보를 획득하고,

상기 생체정보 가공부는,

상기 암호화된 상태의 생체정보 또는 상기 암호화된 상태의 생체정보의 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 것을 특징으로 하는 단말 장치.

[청구항 17] 제14항에 있어서,

상기 생체정보는 지문을 스캐닝한 전자적 지문 서명인 것을 특징으로 하는 단말 장치.

[청구항 18] 제14항에 있어서,

상기 생체정보 획득부는,

상기 생체정보를 상기 단말 장치에 연결된 생체정보 수집용 기기를 통해 획득되거나 상기 단말 장치의 터치스크린 또는 카메라 모듈을 통해 획득하는 것을 특징으로 하는 단말 장치.

[청구항 19] 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 단말 장치에 있어서,

검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보에 대해 시각화하기 위한 추가적인 인코딩을 수행하여 생성된 마크가 일체로 결합된 전자문서의 원문을 획득하는 전자문서 획득부 - 상기 획득된 전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 획득된 전자문서의 원문 상에서 시각화된 상태로 결합되어 완성된 상태임 - ,

상기 획득된 전자문서의 원문에 일체로 결합된 마크의 부분을 디코딩하여 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 추가적으로 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 검증 요청부

를 포함하는 단말 장치.

[청구항 20] 제19항에 있어서,

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 제공하는 결과 제공부

를 더 포함하는 단말 장치.

[청구항 21] 제19항에 있어서,
상기 생체데이터 표준으로 인코딩한 상태의 정보는,
CBEFF(Common Biometric Exchange File Format) 내에 상기 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 삽입하여 인코딩을 수행하여 획득되는 것을 특징으로 하는 단말 장치.

[청구항 22] 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 단말 장치에 있어서,
검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 일체로 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 전자문서 획득부 - 상기 획득된 전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 전자문서의 원문 상에서 시각화되지 않은 상태로 결합되어 완성된 상태임 - ,
상기 획득된 전자문서의 원문의 메타필드 내에서 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및
상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 검증 요청부
를 포함하는 단말 장치.

[청구항 23] 제22항에 있어서,
상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과

일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 제공하는 결과 제공부

를 더 포함하는 단말 장치.

[청구항 24] 생체정보인식 기반의 전자서명을 위한 서버에 있어서,

전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보가 획득된 시점 정보를 단말 장치로부터 수신하는 구성요소 획득부,

상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 생체정보 가공부, 및

상기 생체데이터 표준으로 인코딩된 정보에 대해 상기 생체정보 가공부에 의해 시각화하기 위한 추가적인 인코딩이 수행되어 마크가 생성되면 상기 전자문서의 원문과 상기 마크를 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 전자문서 상에서 시각화된 상태로, 상기 전자문서를 완성하는 전자서명 결합부

를 포함하는 서버.

[청구항 25] 제24항에 있어서,

상기 전자서명 결합부에 의해 상기 전자문서의 원문과 상기 마크가 일체로 결합되면, 이를 서명완료된 전자문서로서 저장하도록 하는 전자문서 저장 관리부를 더 포함하는 서버.

[청구항 26] 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 서버에 있어서,

단말 장치로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보에 대해 시각화하기 위한 추가적인 인코딩을 수행하여 생성된 마크가 일체로 결합된 전자문서의 원문을 획득하는 전자문서 획득부 - 상기 획득된

전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 획득된 전자문서의 원문 상에서 시각화된 상태로 결합되어 완성된 상태임 - ,

상기 획득된 전자문서의 원문에 일체로 결합된 마크의 부분을 디코딩하여 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 추가적으로 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교하는 구성요소 비교부

를 포함하는 서버.

[청구항 27] 제26항에 있어서,

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 상기 단말 장치에 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 상기 단말 장치에 제공하는 결과 제공부

를 더 포함하는 서버.

[청구항 28] 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 서버에 있어서,

단말 장치로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는

상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 일체로 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 전자문서 획득부 - 상기 획득된 전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 전자문서의 원문 상에서 시각화되지 않은 상태로 결합되어 완성된 상태임 - ,

상기 획득된 전자문서의 원문의 메타필드 내에서 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 비교하는 구성요소 비교부

를 포함하는 서버.

[청구항 29] 제28항에 있어서,

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 상기 단말 장치에 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 상기 단말 장치에 제공하는 결과 제공부

를 더 포함하는 서버.

[청구항 30] 제1항 내지 제13항 중 어느 한 항에 따른 방법을 실행하기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

[청구항 31] 생체정보인식 기반의 전자서명 방법에 있어서,

(a) 생체정보 획득부가, 전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보를 획득하는 단계,
(b) 생체정보 가공부가, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 단계, 및
(c) 전자서명 결합부가, 상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서 상에서 시각화되지 않은 상태로, 상기 전자문서를 완성하는 단계
를 포함하는 방법.

[청구항 32] 생체정보인식 기반의 전자서명을 위한 단말 장치에 있어서,
전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보를 획득하는 생체정보 획득부,
상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 생체정보 가공부, 및
상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서 상에서 시각화되지 않은 상태로, 상기 전자문서를 완성하는 전자서명 결합부
를 포함하는 단말 장치.

[청구항 33] 생체정보인식 기반의 전자서명을 위한 서버에 있어서,
전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보가 획득된 시점 정보를 단말 장치로부터 수신하는 구성요소 획득부,
상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 생체정보 가공부, 및
상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서 상에서 시각화되지 않은 상태로, 상기 전자문서를 완성하는 전자서명 결합부

를 포함하는 서버.

[청구항 34] 제33항에 있어서,
상기 전자문서의 원문의 메타필드에 상기 생체데이터 표준으로 인코딩된 정보가 일체로 결합되면, 이를 서명완료된 전자문서로서 저장하도록 하는 전자문서 저장 관리부를 더 포함하는 서버.

[청구항 35] 제31항에 따른 방법을 실행하기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

청구범위 보정서
국제사무국 접수일: 2013 년 10 월 31 일 (31.10.2013)

【청구항 1】(정정)

생체정보인식 기반의 전자서명 방법에 있어서,

(a) 생체정보 획득부가, 전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보를 획득하는 단계,

(b) 생체정보 가공부가, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 단계, 및

(c) 전자서명 결합부가, 상기 생체데이터 표준으로 인코딩된 정보에 대해 시각화하기 위한 추가적인 인코딩을 수행하여 마크를 생성한 후 상기 전자문서의 원문과 상기 마크를 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 전자문서 상에서 시각화된 상태로, 상기 전자문서를 완성하거나, 상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서 상에서 시각화되지 않은 상태로, 상기 전자문서를 완성하는 단계

를 포함하는 방법.

【청구항 2】(유지)

제1항에 있어서,

상기 (b) 단계는,

상기 생체정보 가공부가, CBEFF(Common Biometric Exchange File Format) 내에 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 삽입하여 인코딩을 수행하는 것을 특징으로 하는 방법.

【청구항 3】(유지)

제1항에 있어서,

상기 (a) 단계는,

상기 생체정보 획득부가, 상기 생체정보 또는 상기 생체정보의 특징점 정보에 대한 암호화된 상태의 정보를 획득하는 단계인 것을 특징으로 하고,

상기 (b) 단계는,

상기 생체정보 가공부가, 상기 암호화된 상태의 생체정보 또는 상기 암호화된 상태의 생체정보의 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 단계인 것을 특징으로 하는 방법.

【청구항 4】(유지)

제1항에 있어서,

상기 생체정보는 지문을 스캐닝한 전자적 지문 서명인 것을 특징으로

하는 방법.

【청구항 5】(유지)

제4항에 있어서,

상기 (a) 단계는,

상기 생체정보 획득부가, 상기 전자적 지문 서명의 품질을 확인하여 선명도가 기설정된 임계치 이상인 경우에만 상기 전자적 지문 서명으로부터 특징점 정보를 획득하는 것을 특징으로 하는 방법.

【청구항 6】(유지)

제1항에 있어서,

상기 (a) 단계에서,

상기 생체정보는 소정의 단말 장치에 연결된 생체정보 수집용 기기를 통해 획득되거나 소정의 단말 장치의 터치스크린 또는 카메라 모듈을 통해 획득되는 것을 특징으로 하는 방법.

【청구항 7】(유지)

제1항에 있어서,

상기 (b) 단계는,

상기 생체정보 가공부가, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보에 더하여 상기 생체정보의

획득기관에 대한 정보를 추가적으로 상기 생체데이터 표준으로 인코딩하는 것을 특징으로 하는 방법.

【청구항 8】(유지)

제1항에 있어서,

상기 (c) 단계에서,

상기 마크는 바코드, QR코드, 시각화된 표장 중 적어도 하나를 포함하는 것을 특징으로 하는 방법.

【청구항 9】(유지)

생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법에 있어서,

(a) 전자문서 획득부가, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보에 대해 시각화하기 위한 추가적인 인코딩을 수행하여 생성된 마크가 일체로 결합된 전자문서의 원문을 획득하는 단계 - 상기 획득된 전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 획득된 전자문서의 원문 상에서 시각화된 상태로 결합되어 완성된 상태임 - ,

(b) 구성요소 획득부가, 상기 획득된 전자문서의 원문에 일체로 결합된 마크의 부분을 디코딩하여 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하는 단계,

(c) 상기 구성요소 획득부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 추가적으로 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 추출하는 단계, 및

(d) 검증 요청부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 단계

를 포함하는 방법.

【청구항 10】(유지)

제9항에 있어서,

(e) 결과 제공부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는

경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 제공하는 단계

를 더 포함하는 방법.

【청구항 11】(유지)

제9항에 있어서,

상기 생체데이터 표준으로 인코딩한 상태의 정보는,

CBEFF(Common Biometric Exchange File Format) 내에 상기 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 삽입하여 인코딩을 수행하여 획득되는 것을 특징으로 하는 방법.

【청구항 12】(유지)

생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 방법에 있어서,

(a) 전자문서 획득부가, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의

원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 일체로 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 단계 - 상기 획득된 전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 전자문서의 원문 상에서 시각화되지 않은 상태로 결합되어 완성된 상태임 - ,

(b) 구성요소 획득부가, 상기 획득된 전자문서의 원문의 메타필드 내에서 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하는 단계,

(c) 상기 구성요소 획득부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 추출하는 단계, 및

(d) 검증 요청부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 단계

를 포함하는 방법.

【청구항 13】(유지)

제12항에 있어서,

(e) 결과 제공부가, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 제공하는 단계

를 더 포함하는 방법.

【청구항 14】(정정)

생체정보인식 기반의 전자서명을 위한 단말 장치에 있어서,

전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보를 획득하는 생체정보 획득부,

상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 생체정보 가공부, 및

상기 생체데이터 표준으로 인코딩된 정보에 대해 상기 생체정보 가공부에

의해 시각화하기 위한 추가적인 인코딩이 수행되어 마크가 생성되면 상기 전자문서의 원문과 상기 마크를 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 전자문서 상에서 시각화된 상태로, 상기 전자문서를 완성하거나, 상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서 상에서 시각화되지 않은 상태로, 상기 전자문서를 완성하는 전자서명 결합부

를 포함하는 단말 장치.

【청구항 15】(유지)

제14항에 있어서,

상기 생체정보 가공부는,

CBEFF(Common Biometric Exchange File Format) 내에 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 삽입하여 인코딩을 수행하는 것을 특징으로 하는 단말 장치.

【청구항 16】(유지)

제14항에 있어서,

상기 생체정보 획득부는,

상기 생체정보 또는 상기 생체정보의 특징점 정보에 대한 암호화된 상태의 정보를 획득하고,

상기 생체정보 가공부는,

상기 암호화된 상태의 생체정보 또는 상기 암호화된 상태의 생체정보의 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 것을 특징으로 하는 단말 장치.

【청구항 17】(유지)

제14항에 있어서,

상기 생체정보는 지문을 스캐닝한 전자적 지문 서명인 것을 특징으로 하는 단말 장치.

【청구항 18】(유지)

제14항에 있어서,

상기 생체정보 획득부는,

상기 생체정보를 상기 단말 장치에 연결된 생체정보 수집용 기기를 통해 획득되거나 상기 단말 장치의 터치스크린 또는 카메라 모듈을 통해 획득하는 것을 특징으로 하는 단말 장치.

【청구항 19】(유지)

생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 단말

장치에 있어서,

검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보에 대해 시각화하기 위한 추가적인 인코딩을 수행하여 생성된 마크가 일체로 결합된 전자문서의 원문을 획득하는 전자문서 획득부 - 상기 획득된 전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 획득된 전자문서의 원문 상에서 시각화된 상태로 결합되어 완성된 상태임 - ,

상기 획득된 전자문서의 원문에 일체로 결합된 마크의 부분을 디코딩하여 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 추가적으로 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기

생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 검증 요청부

를 포함하는 단말 장치.

【청구항 20】(유지)

제19항에 있어서,

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 제공하는 결과 제공부

를 더 포함하는 단말 장치.

【청구항 21】(유지)

제19항에 있어서,

상기 생체데이터 표준으로 인코딩한 상태의 정보는,

CBEFF(Common Biometric Exchange File Format) 내에 상기 특징점 정보,

상기 전자문서의 원문에 대한 해쉬값과 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 삽입하여 인코딩을 수행하여 획득되는 것을 특징으로 하는 단말 장치.

【청구항 22】(유지)

생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 단말 장치에 있어서,

검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 일체로 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 전자문서 획득부 - 상기 획득된 전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 전자문서의 원문 상에서 시각화되지 않은 상태로 결합되어 완성된 상태임 - ,

상기 획득된 전자문서의 원문의 메타필드 내에서 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를

추출하는 구성요소 획득부, 및

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교되도록 하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 비교되도록 하는 검증 요청부

를 포함하는 단말 장치.

【청구항 23】(유지)

제12항에 있어서,

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 제공하는 결과 제공부

를 더 포함하는 단말 장치.

【청구항 24】(정정)

생체정보인식 기반의 전자서명을 위한 서버에 있어서,

전자문서에 삽입될 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보가 획득된 시점 정보를 단말 장치로부터 수신하는 구성요소 획득부,

상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문에 대한 해쉬값 및 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩하는 생체정보 가공부, 및

상기 생체데이터 표준으로 인코딩된 정보에 대해 상기 생체정보 가공부에 의해 시각화하기 위한 추가적인 인코딩이 수행되어 마크가 생성되면 상기 전자문서의 원문과 상기 마크를 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 전자문서 상에서 시각화된 상태로, 상기 전자문서를 완성하거나, 상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서 상에서 시각화되지 않은 상태로, 상기 전자문서를 완성하는 전자서명 결합부

를 포함하는 서버.

【청구항 25】(정정)

제24항에 있어서,

상기 전자서명 결합부에 의해 상기 전자문서의 원문과 상기 마크가 일체로 결합되거나 상기 전자문서의 원문의 메타필드에 상기 생체데이터 표준으로 인코딩된 정보가 일체로 결합되면, 이를 서명완료된 전자문서로서 저장하도록 하는 전자문서 저장 관리부를 더 포함하는 서버.

【청구항 26】(유지)

생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 서버에 있어서,

단말 장치로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보에 대해 시각화하기 위한 추가적인 인코딩을 수행하여 생성된 마크가 일체로 결합된 전자문서의 원문을 획득하는 전자문서 획득부 - 상기 획득된 전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 상태로부터 변형되어 상기 획득된 전자문서의 원문 상에서 시각화된 상태로 결합되어 완성된 상태임 - ,

상기 획득된 전자문서의 원문에 일체로 결합된 마크의 부분을 디코딩하여 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터

표준으로 인코딩한 상태의 정보를 추가적으로 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 생체정보로부터 획득된 특징점 정보와 비교하는 구성요소 비교부

를 포함하는 서버.

【청구항 27】(유지)

제26항에 있어서,

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 상기 단말장치에 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보

또는 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의 원문에 대한 전자서명에 대한 부인을 방지하는 결과를 상기 단말 장치에 제공하는 결과 제공부

를 더 포함하는 서버.

【청구항 28】(유지)

생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 서버에 있어서,

단말 장치로부터 특정 전자문서에 대한 검증 요청이 수신되면, 검증을 요하는 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 생체데이터 표준으로 인코딩한 상태의 정보가 메타필드에 일체로 결합된 상태로 포함되어 있는 전자문서의 원문을 획득하는 전자문서 획득부 - 상기 획득된 전자문서의 원문은 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 획득된 전자문서의 원문 상에서 시각화되지 않은 상태로 결합되어 완성된 상태임 - ,

상기 획득된 전자문서의 원문의 메타필드 내에서 상기 생체데이터 표준으로 인코딩한 상태의 정보를 획득하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보를 디코딩하여 상기 생체정보 또는 상기 생체정보에 대한 특징점

정보, 상기 전자문서의 원문의 해쉬값 및 상기 전자문서의 원문에 전자서명된 생체정보 또는 상기 생체정보에 대한 특징점 정보가 획득된 시점 정보를 추출하는 구성요소 획득부, 및

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값을 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 비교하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보를 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 비교하는 구성요소 비교부

를 포함하는 서버.

【청구항 29】(유지)

제28항에 있어서,

상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 해쉬값이 상기 전자문서의 원문으로부터 직접 획득된 해쉬값과 일치하는 경우 상기 전자문서의 원문이 변조되지 않았다는 무결성을 인정하는 결과를 상기 단말장치에 제공하고, 상기 생체데이터 표준으로 인코딩한 상태의 정보에서 추출된 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서의 원문에 실제로 전자서명을 했다고 주장하는 사용자로부터 입력 받은 생체정보 또는 상기 생체정보로부터 획득된 특징점 정보와 일치하는 경우 상기 전자문서의

원문에 대한 전자서명에 대한 부인을 방지하는 결과를 상기 단말 장치에 제공하는 결과 제공부

를 더 포함하는 서버.

【청구항 30】(유지)

제1항 내지 제13항 중 어느 한 항에 따른 방법을 실행하기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

【청구항 31】(삭제)

【청구항 32】(삭제)

【청구항 33】(삭제)

【청구항 34】(삭제)

【청구항 35】(삭제)

조약 제19조(1) 규정의 설명서

Claim 1 amended; claims 2 to 13 unchanged; claim 14 amended; claims 15 to 23 unchanged; claims 24 and 25 amended; claims 26 to 31 unchanged; claims 31 to 35 cancelled.

(i) Basis for the amendment: Claim 1 has been amended at lines 12 to 15. Concerning the amended Claim 1, the indication of "상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서 상에서 시각화되지 않은 상태로, 상기 전자문서를 완성하는" is in original claim 31 as filed.

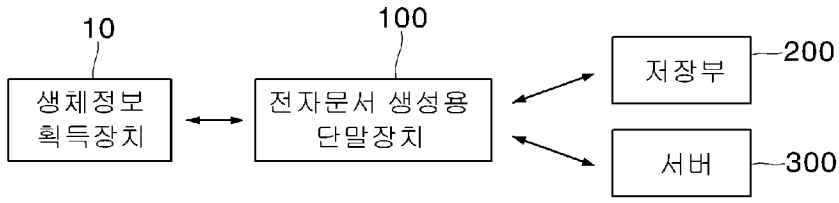
(ii) Basis for the amendment: Claim 14 has been amended at lines 11 to 14. Concerning the amended Claim 14, the indication of "상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기

전자문서 상에서 시각화되지 않은 상태로, 상기 전자문서를 완성하는" is in original claim 32 as filed.

(iii) Basis for the amendment: Claim 24 has been amended at lines 12 to 15. Concerning the amended Claim 24, the indication of "상기 생체데이터 표준으로 인코딩된 정보를 상기 전자문서의 원문의 메타필드(meta field)에 일체로 결합함으로써, 상기 생체정보 또는 상기 생체정보에 대한 특징점 정보가 상기 전자문서 상에서 시각화되지 않은 상태로, 상기 전자문서를 완성하는" is in original claim 33 as filed.

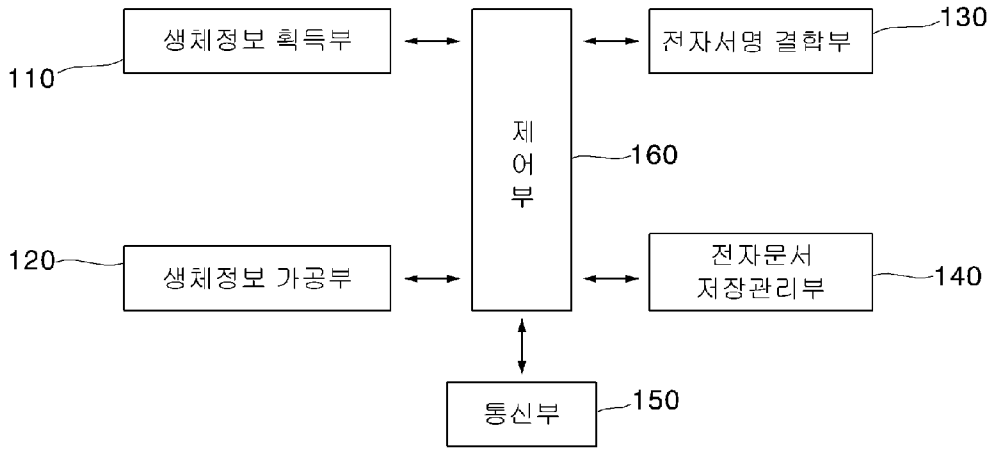
(iv) Basis for the amendment: Claim 25 has been amended at lines 3 to 4. Concerning the amended Claim 25, the indication of "상기 전자문서의 원문의 메타필드에 상기 생체데이터 표준으로 인코딩된 정보가 일체로 결합되면" is in original claim 34 as filed.

[Fig. 1]

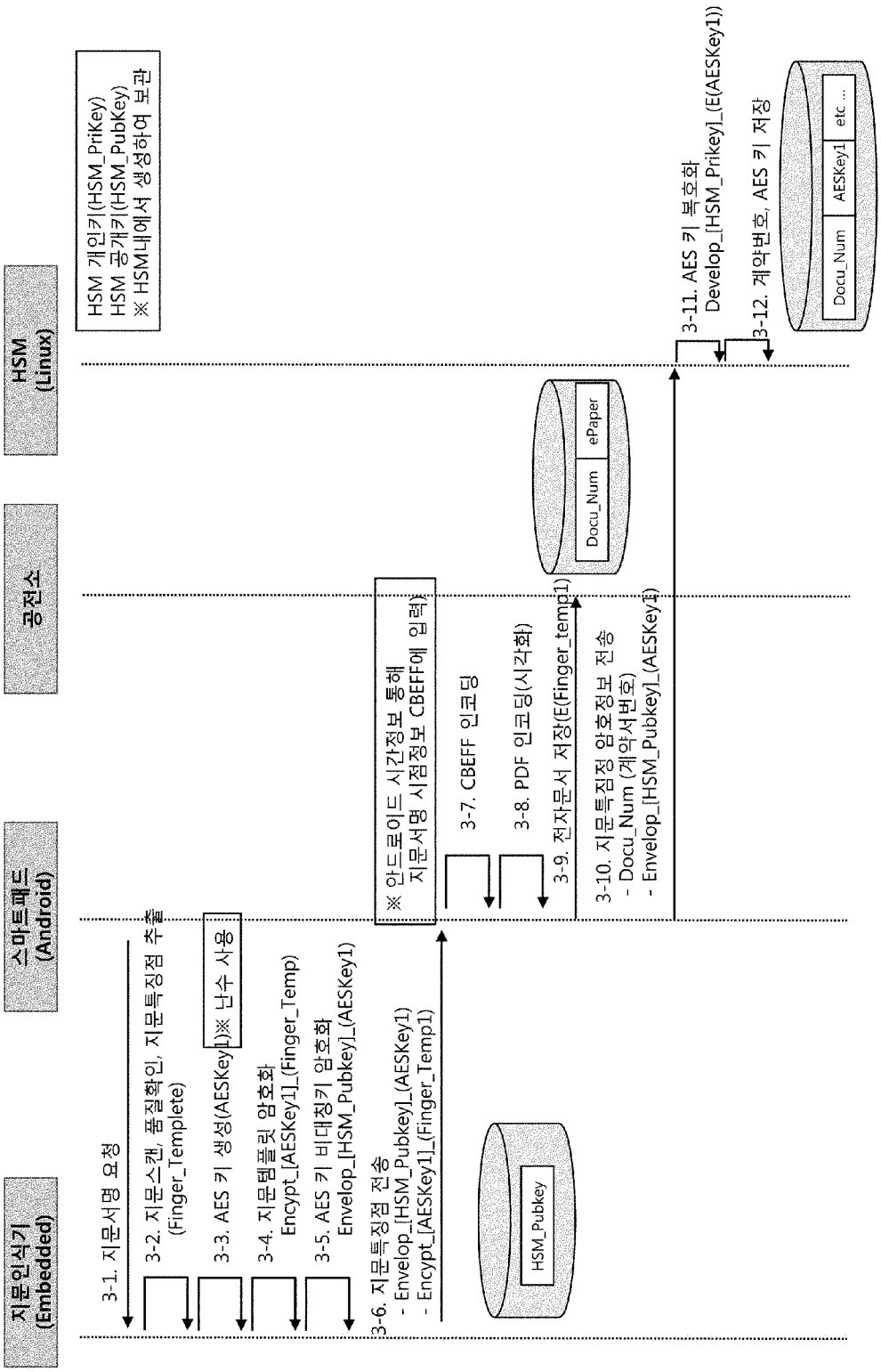


[Fig. 2]

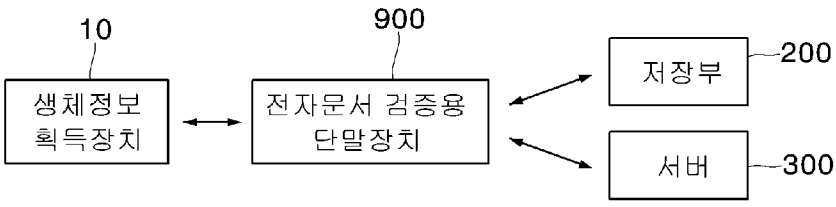
100



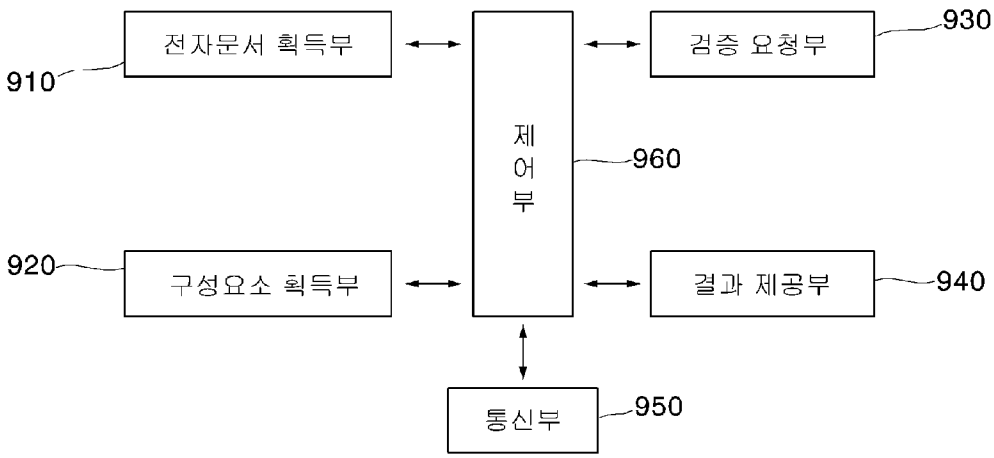
[Fig. 3]


지문인식기 (Embedded)
스마트패드 (Android)
공전소
HSM (Linux)
HSM 개인키(HSM_PriKey)
HSM 공개키(HSM_PubKey)
※ HSM내에서 생성하여 보관
3-1. 지문서명 요청
3-2. 지문스캔, 품질확인, 지문특징점 추출 (Finger_Templete)
3-3. AES 키 생성(AESKey1)※ 난수 사용
3-4. 지문템플릿 암호화 Encypt_[AESKey1]_(Finger_Temp)
3-5. AES 키 비대칭키 암호화 Envelop_[HSM_Pubkey]_(AESKey1)
3-6. 지문특징점 전송
- Envelop_[HSM_Pubkey]_(AESKey1)
- Encypt_[AESKey1]_(Finger_Temp1)
※ 안드로이드 시간정보 통해 지문서명 시점정보 CBEFF에 입력
3-7. CBEFF 인코딩
3-8. PDF 인코딩(시각화)
3-9. 전자문서 저장(E(Finger_temp1)
3-10. 지문특징점 암호정보 전송
- Docu_Num (계약서번호)
- Envelop_[HSM_Pubkey]_(AESKey1)
HSM_Pubkey
Docu_Num
ePaper
3-11. AES 키 복호화
Develop_[HSM_Prikey]_(E(AESKey1))
3-12. 계약번호, AES 키 저장
Docu_Num
AESKey1
etc ...

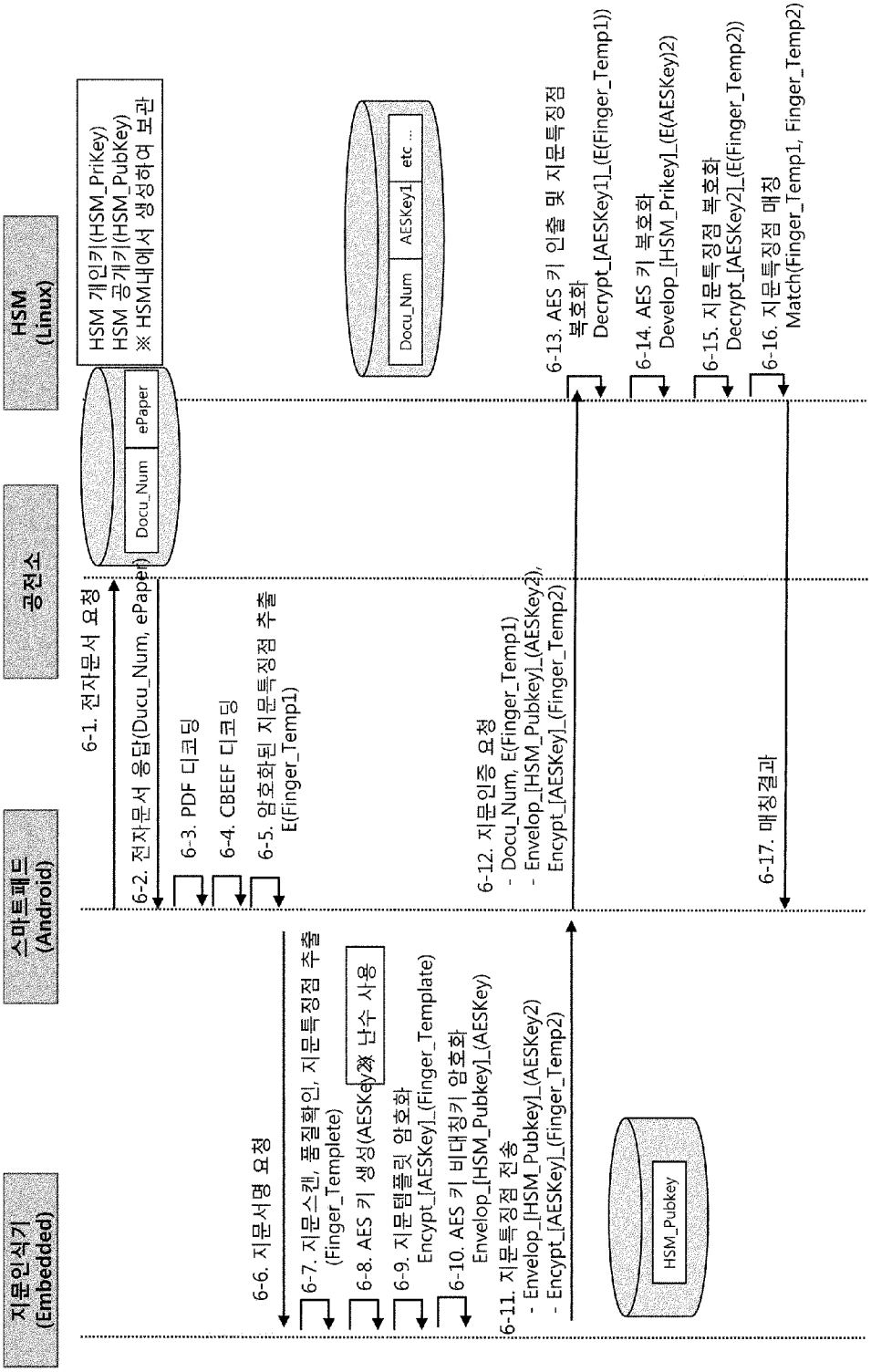
[Fig. 4]


10
생체정보 획득장치
900
전자문서 검증용 단말장치
저장부
200
서버
300

[Fig. 5]


900
전자문서 획득부
910
제어부
960
검증 요청부
930
구성요소 획득부
920
결과 제공부
940
통신부
950

[Fig. 6]


지문인식기 (Embedded)
스마트패드 (Android)
공전소
HSM (Linux)
HSM 개인키(HSM_PriKey)
HSM 공개키(HSM_PubKey)
※ HSM내에서 생성하여 보관
Docu_Num
ePaper
Docu_Num
AESKey1
etc ...
HSM_Pubkey
6-1. 전자문서 요청
6-2. 전자문서 응답(Ducu_Num, ePaper)
6-3. PDF 디코딩
6-4. CBEEF 디코딩
6-5. 암호화된 지문특징점 추출
E(Finger_Temp1)
6-6. 지문서명 요청
6-7. 지문스캔, 품질확인, 지문특징점 추출
(Finger_Templete)
6-8. AES 키 생성(AESKey)※ 난수 사용
6-9. 지문템플릿 암호화
Encypt_[AESKey]_(Finger_Template)
6-10. AES 키 비대칭키 암호화
Envelop_[HSM_Pubkey]_(AESKey)
6-11. 지문특징점 전송
- Envelop_[HSM_Pubkey]_(AESKey2)
- Encypt_[AESKey]_(Finger_Temp2)
6-12. 지문인증 요청
- Docu_Num, E(Finger_Temp1)
- Envelop_[HSM_Pubkey]_(AESKey2),
Encypt_[AESKey]_(Finger_Temp2)
6-13. AES 키 인출 및 지문특징점
복호화
Decrypt_[AESKey1]_(E(Finger_Temp1))
6-14. AES 키 복호화
Develop_[HSM_Prikey]_(E(AESKey2)
6-15. 지문특징점 복호화
Decrypt_[AESKey2]_(E(Finger_Temp2))
6-16. 지문특징점 매칭
Match(Finger_Temp1, Finger_Temp2)
6-17. 매칭결과

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2013/005491

A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/21(2006.01)i, G06K 9/46(2006.01)i, G06F 21/32(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 17/21; G06F 17/00; H04L 9/32; G06K 9/00; H04L 9/00; G06K 9/46; G06F 21/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: virtual-sign formation, electronic document, watermark, encoding, hash, meta, point<or>time<or>time

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2004-0027649 A (PASSSIGN CO., LTD) 01 April 2004 See: page 2, line 35 - page 3, line 50; claims 1-3; figures 2-4.	1-35
A	KR 10-2006-0009205 A (SOFTFORUM CO., LTD.) 31 January 2006 See: page 2, line 36 - page 3, line 37; page 4, line 34 - page 8, line 14; claims 1-4; figures 1-4.	1-35
A	KIM, Hak Il et al., International Standardization Trend for Fingerprint Recognition, The Magazine of the IEEK, vol. 33, no. 1, 30 January 2006 See: pages 17 - 33.	1-35
A	KIM, Seung-Hee et al., Study for Biometrics System Using Watermark, KSII, Journal of 2004 Fall Conference, vol. 5, no. 1, 30 May 2004 See: pages 451 - 454.	1-35
A	KR 10-2003-0045419 A (KIM, Young Je) 11 June 2003 See: page 2, line 23 - page 5, line 34; figures 1-8.	1-35

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 AUGUST 2013 (27.08.2013)	**28 AUGUST 2013 (28.08.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2013/005491

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002-0056043 A1 (GLASS, Randal W.) 09 May 2002 See: paragraphs 31 - 83; figures 2-13.	1-35

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2013/005491

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2004-0027649 A	01/04/2004	NONE	
KR 10-2006-0009205 A	31/01/2006	NONE	
KR 10-2003-0045419 A	11/06/2003	NONE	
US 2002-0056043 A1	09/05/2002	AU 2000-26154 A1	01/08/2000
		AU 2000-26154 B2	27/01/2005
		AU 2002-365086 A1	09/07/2003
		CA 2358535 A1	20/07/2000
		CA 2358535 C	14/04/2009
		CA 2465227 A1	03/07/2003
		EP 1147493 A1	24/10/2001
		EP 1449086 A2	25/08/2004
		EP 1449086 A4	31/05/2006
		JP 04741081 B2	03/08/2011
		JP 2002-535761 A	22/10/2002
		JP 2005-513641 A	12/05/2005
		KR 10-0407900 B1	03/12/2003
		KR 10-2004-0053253 A	23/06/2004
		US 06332193 B1	18/12/2001
		US 2002-0056043 A1	09/05/2002
		WO 2000-042577 A1	20/07/2000
		WO 2003-053123 A2	03/07/2003
		WO 2003-053123 A3	11/03/2004

국 제 조 사 보 고 서

국제출원번호
PCT/KR2013/005491

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 17/21(2006.01)i, G06K 9/46(2006.01)i, G06F 21/32(2013.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 17/21; G06F 17/00; H04L 9/32; G06K 9/00; H04L 9/00; G06K 9/46; G06F 21/32

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드:생체정보,전자문서,워터마크,인코딩,해쉬,메타,시점<or>시간<or>time

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2004-0027649 A ((주)패스싸인) 2004.04.01 참조: 페이지 2, 라인 35 - 페이지 3, 라인 50; 청구항 1-3; 도면 2-4.	1-35
A	KR 10-2006-0009205 A (소프트포럼 주식회사) 2006.01.31 참조: 페이지 2, 라인 36 - 페이지 3, 라인 37; 페이지 4, 라인 34 - 페이지 8, 라인 14; 청구항 1-4; 도면 1-4.	1-35
A	김학일 외, 지문인식 호환을 위한 국제 표준화 동향, 전자공학회지 제33권 제1호, 2006.01.30 참조: 페이지 17 - 페이지 33.	1-35
A	김승희 외, 워터마크를 이용한 생체 인식 시스템에 관한 연구, 한국인터넷정보학회 2004 춘계학술발표대회 논문집 제5권 제1호, 2004.05.30 참조: 페이지 451 - 페이지 454.	1-35
A	KR 10-2003-0045419 A (김영제) 2003.06.11 참조: 페이지 2, 라인 23 - 페이지 5, 라인 34; 도면 1-8.	1-35

☒ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2013년 08월 27일 (27.08.2013)	2013년 08월 28일 (28.08.2013)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-472-7140

심사관
박상현
전화번호 +82-42-481-8263

국 제 조 사 보 고 서

국제출원번호
PCT/KR2013/005491

C (계속). 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	US 2002-0056043 A1 (RANDAL W. GLASS) 2002.05.09 참조: 단락 31 - 단락 83; 도면 2-13.	1-35

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2013/005491

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2004-0027649 A	2004/04/01	없음	
KR 10-2006-0009205 A	2006/01/31	없음	
KR 10-2003-0045419 A	2003/06/11	없음	
US 2002-0056043 A1	2002/05/09	AU 2000-26154 A1	2000/08/01
		AU 2000-26154 B2	2005/01/27
		AU 2002-365086 A1	2003/07/09
		CA 2358535 A1	2000/07/20
		CA 2358535 C	2009/04/14
		CA 2465227 A1	2003/07/03
		EP 1147493 A1	2001/10/24
		EP 1449086 A2	2004/08/25
		EP 1449086 A4	2006/05/31
		JP 04741081 B2	2011/08/03
		JP 2002-535761 A	2002/10/22
		JP 2005-513641 A	2005/05/12
		KR 10-0407900 B1	2003/12/03
		KR 10-2004-0053253 A	2004/06/23
		US 06332193 B1	2001/12/18
		US 2002-0056043 A1	2002/05/09
		WO 2000-042577 A1	2000/07/20
		WO 2003-053123 A2	2003/07/03
		WO 2003-053123 A3	2004/03/11