(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2023 년 7 월 6 일 (06.07.2023)

WIPO | PCT

(10) 국제공개번호
WO 2023/128345 A1

(51) 국제특허분류:
G06F 21/32 (2013.01) *G06V 40/16* (2022.01)
H04L 9/00 (2006.01) *G06V 10/10* (2022.01)

(21) 국제출원번호: PCT/KR2022/019485

(22) 국제출원일: 2022 년 12 월 2 일 (02.12.2022)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2021-0192467 2021 년 12 월 30 일 (30.12.2021) KR

(71) 출원인: 주식회사 디사일로 (**DESILO INC.**) [KR/KR]; 06619 서울특별시 서초구 서운로 138, 6층, Seoul (KR).

(72) 발명자: 안용대 (**AN, Yong Dae**); 06762 서울특별시 서초구 바우뫼로 33, 105동 101호, Seoul (KR). 박준홍 (**PARK, Jun Hong**); 13644 경기도 성남시 수정구 위례동이로 24, 5904동 404호, Gyeonggi-do (KR).

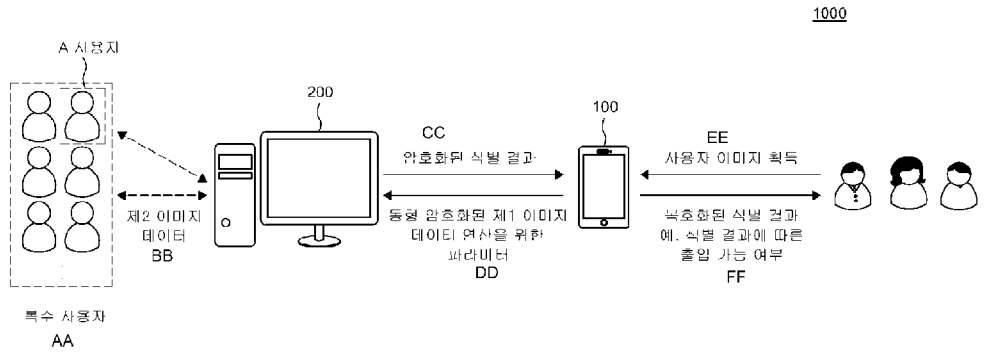
(74) 대리인: 특허법인 인벤싱크 (**INVENSYNC INTELLECTUAL PROPERTY GROUP**); 06222 서울특별시 강남구 언주로 425 재송빌딩 5층, Seoul (KR).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, 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,

(54) **Title:** PERSONAL IDENTIFICATION METHOD AND SYSTEM USING HOMOMORPHICALLY ENCRYPTED IMAGE

(54) **발명의 명칭:** 동형 암호화된 이미지를 이용한 개인 식별 방법 및 시스템



A ... User
AA ... Multiple users
BB ... Second image data
CC ... Encrypted identification result
DD ... Parameter for calculating homomorphically encrypted first image data
EE ... Obtain user image
FF ... Decrypted identification result, for example, able or unable to access in accordance with identification result

(57) **Abstract:** The present invention relates to a personal identification method using a homomorphically encrypted image, the method comprising the steps of: obtaining first image data of a user; homomorphically encrypting the first image data; transmitting the homomorphically encrypted first image data to an image calculation server; receiving a homomorphically encrypted identification result calculated on the basis of the homomorphically encrypted first image data and pre-stored second image data of another user from the image calculation server; and decrypting the homomorphically encrypted identification result.

(57) **요약서:** 본 발명은, 동형 암호화된 이미지를 이용한 개인 식별 방법으로서, 상기 방법은, 사용자의 제1 이미지 데이터를 획득하는 단계, 상기 제1 이미지 데이터를 동형 암호화하는 단계, 이미지 연산 서버로 동형 암호화된 제1 이미지 데이터를 송신하는 단계, 상기 이미지 연산 서버로부터 상기 동형 암호화된 제1 이미지 데이터와 미리 저장된 다른 사용자의 제2 이미지 데이터를 기초로 계산된 동형 암호화된 식별 결과를 수신하는 단계 및 상기 동형 암호화된 식별 결과를 복호화하는 단계를 포함하도록 구성된다.

WO 2023/128345 A1

[다음 쪽 계속]

FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, 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).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 동형 암호화된 이미지를 이용한 개인 식별 방법 및 시스템

기술분야

[1] 본 발명은 동형 암호화된 이미지를 이용한 개인 식별 방법 및 시스템에 관한 것이다.

배경기술

[2] 컴퓨터, 노트북, 키오스크(KIOSK) 단말기, 출입 통제 설비, 은행 단말기(ATM), 웹사이트, 인터넷 뱅킹 등을 사용하는 데 있어 사용자의 신원을 증명하기 위해 대표적으로 3가지의 개인 식별 방법이 사용되고 있다.

[3] 첫 번째는, 사용자가 인증을 위해 알파벳 및 숫자를 이용한 패스워드나 숫자만으로 구성된 개인 식별 번호를 입력하여, 올바른 사용자인지 식별하는 방법이다. 두 번째는, 사용자의 지문, 홍채, 얼굴, 목소리 등 사용자 고유의 바이오 정보를 인식해 올바른 사용자인지 식별하는 방법이다. 세 번째는, 인터넷 뱅킹의 OTP(One-Time Password) 생성 장치, 사원증과 같이 사용자가 인증만을 위한 추가적인 디바이스를 가지고 다니면서 인증이 요구될 시 디바이스를 사용해 올바른 사용자인지 식별하는 방법이다.

[4] 이 중 첫 번째 방법이 가장 많이 사용되고 있지만, 사용자가 시스템마다 다른 패스워드를 지정하고, 기억하기 힘들기 때문에, 편의성을 위해 많은 사람들이 짧고 공통적인 패스워드를 사용하고 있어, 보안 상 취약하다.

[5] 또한, 세 번째 방법은 사용자가 인증을 위해 디바이스를 항상 소지하고 있어야 하며, 소지하는 동안 디바이스를 분실할 경우 이를 재발급하는 과정이 번거롭다는 단점이 있다.

[6] 발명의 배경이 되는 기술은 본 발명에 대한 이해를 보다 용이하게 하기 위해 작성되었다. 발명의 배경이 되는 기술에 기재된 사항들이 선행기술로 존재한다고 인정하는 것으로 이해되어서는 안 된다.

발명의 상세한 설명

기술적 과제

[7] 그에 따라, 분실의 우려가 없고, 변경되지 않는 사용자 고유의 바이오 정보를 이용한 두 번째 식별 방법이 안전한 방법이지만, 노트북과 같은 개인 디바이스 외에 공용 출입 설비와 같은 외부 장치에서 사용자를 식별하기 위해서는 식별 장치와 데이터를 구축하기 위한 상당한 시간과 비용이 소모될 뿐만 아니라, 사용자의 이미지(고유의 바이오 정보)가 노출되는 문제가 있다.

[8] 이에, 공용 공간에서 사용자의 이미지를 이용하여 빠르고, 보안 상 안전하게 사용자를 식별할 수 있는 새로운 방법이 요구된다.

[9] 그 결과, 본 발명의 발명자들은 사용자의 이미지를 획득할 수 있는

장치만으로도, 사용자의 이미지가 노출될 우려 없이 안전하게 사용자를 식별할 수 있는 방법 및 이를 수행하는 시스템을 개발하고자 하였다.

[10] 특히, 본 발명의 발명자들은 사용자로부터 획득된 이미지 데이터를 동형 암호화한 뒤, 사용자 식별 결과에 대한 동형 암호화한 연산 결과를 얻음으로써, 사용자 고유의 바이오 정보가 노출되지 않도록 방법을 구성하였다.

[11] 본 발명의 과제들은 이상에서 언급한 과제들로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

[12] 전술한 바와 같은 과제를 해결하기 위하여 본 발명의 일 실시예에 따른 동형 암호화된 이미지를 이용한 개인 식별 방법이 제공된다. 상기 방법은, 사용자의 제1 이미지 데이터를 획득하는 단계, 상기 제1 이미지 데이터를 동형 암호화하는 단계, 이미지 연산 서버로 동형 암호화된 제1 이미지 데이터를 송신하는 단계, 상기 이미지 연산 서버로부터 상기 동형 암호화된 제1 이미지 데이터와 미리 저장된 다른 사용자의 제2 이미지 데이터를 기초로 계산된 동형 암호화된 식별 결과를 수신하는 단계 및 상기 동형 암호화된 식별 결과를 복호화하는 단계를 포함하도록 구성된다.

[13] 본 발명의 특징에 따르면, 상기 동형 암호화된 제1 이미지 데이터를 송신하는 단계는, 상기 제1 이미지 데이터를 동형 암호화하기 위해 사용된, 동형 암호화 연산을 위한 파라미터를 상기 이미지 연산 서버로 송신하는 단계를 더 포함할 수 있다.

[14] 본 발명의 다른 특징에 따르면, 상기 동형 암호화된 식별 결과는, 상기 동형 암호화된 제1 이미지 데이터와 상기 파라미터를 기초로 동형 암호화된 제2 이미지 데이터를 기초로 계산된 식별 결과일 수 있다.

[15] 본 발명의 또 다른 특징에 따르면, 상기 제2 이미지 데이터는, 상기 이미지 연산 서버에 미리 저장된 복수의 다른 사용자의 이미지 데이터이고, 상기 복호화하는 단계는, 상기 복수의 다른 사용자 중에서 상기 사용자와 매칭되는 다른 사용자에 대한 식별 결과를 획득하는 단계를 더 포함할 수 있다.

[16] 본 발명의 또 다른 특징에 따르면, 상기 제1 이미지 데이터 및 상기 제2 이미지 데이터는, 식별자 디바이스를 통해 촬영된 이미지, 상기 이미지에서 추출된 복수의 특징 좌표 값 및 상기 이미지의 픽셀 별 RGB 값 중 적어도 하나를 포함할 수 있다.

[17] 본 발명의 또 다른 특징에 따르면, 상기 동형 암호화하는 단계는, 부분 동형 암호(Partial Homomorphic Encryption), 준동형 암호(Somewhat Homomorphic Encryption) 및 완전 동형 암호(Fully Homomorphic Encryption) 중 어느 하나의 암호화 방법을 이용하여 동형 암호화하는 단계일 수 있다.

[18] 전술한 바와 같은 과제를 해결하기 위하여 본 발명의 다른 실시예에 따른 동형

암호화된 이미지를 이용한 개인 식별 방법이 제공된다. 상기 방법은, 식별자 디바이스로부터 동형 암호화된 사용자의 제1 이미지 데이터를 포함하는 연산 요청을 수신하는 단계, 상기 연산 요청에 따라 미리 저장된 다른 사용자의 제2 이미지 데이터를 획득하는 단계, 상기 동형 암호화된 제1 이미지 데이터와 상기 제2 이미지 데이터를 기초로 동형 암호화된 식별 결과를 산출하는 단계 및 상기 동형 암호화된 식별 결과를 상기 식별자 디바이스로 송신하는 단계를 포함하도록 구성된다.

[19] 본 발명의 특징에 따르면, 상기 연산 요청을 수신하는 단계는, 상기 식별자 디바이스로부터 상기 제1 이미지 데이터를 동형 암호화하기 위해 사용된, 동형 암호화 연산을 위한 파라미터를 수신하는 단계를 더 포함하며, 상기 획득하는 단계는, 상기 파라미터를 기초로 상기 제2 이미지 데이터를 동형 암호화하는 단계를 더 포함할 수 있다.

[20] 본 발명의 다른 특징에 따르면, 상기 동형 암호화된 식별 결과를 산출하는 단계는, 상기 동형 암호화된 제1 이미지 데이터에 대응되는 제1 위치와 상기 제2 이미지 데이터에 대응되는 제2 위치를 결정하는 단계와 상기 식별 결과에 대응되는 상기 제1 위치와 제2 위치 사이의 거리 값을 계산하는 단계를 더 포함할 수 있다.

[21] 본 발명의 또 다른 특징에 따르면, 상기 동형 암호화된 식별 결과를 산출하는 단계는, 상기 수신된 연산 요청의 종류에 따라, 상기 복수의 다른 사용자의 제2 이미지 데이터와 상기 동형 암호화된 제1 이미지 데이터를 기초로 암호화된 식별 결과를 산출하는 단계일 수 있다.

[22] 기타 실시예의 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

발명의 효과

[23] 본 발명은 공용 공간에서의 사용자 식별을 위해 사용자 고유의 바이오 정보(얼굴 이미지)를 외부 서버에 공유하지 않고도, 사용자를 식별할 수 있다. 특히, 본 발명은 사용자가 어떠한 사용자인지 식별하거나, 사용자가 다른 사용자와 동일한지 여부를 판단할 수 있다.

[24] 또한, 본 발명은 사용자의 이미지 데이터가 동형 암호화된 상태로 연산되고, 사용자의 이미지를 획득한 디바이스에서는 연산 결과만을 복호화하여 확인함으로써, 사용자의 얼굴 이미지가 안전하게 보호될 수 있다.

[25] 또한, 본 발명은 사용자 식별, 사용자 본인 인증을 위해 별도의 디바이스를 소지하거나, 고유의 식별 번호를 기억할 필요가 없어, 사용자 편의성이 향상될 수 있다.

[26] 본 발명에 따른 효과는 이상에서 예시된 내용에 의해 제한되지 않으며, 더욱 다양한 효과들이 본 발명 내에 포함되어 있다.

도면의 간단한 설명

[27] 도 1은 본 발명의 일 실시예에 따른 개인 식별 시스템의 개략도이다.

[28] 도 2는 본 발명의 일 실시예에 따른 식별자 디바이스의 구성을 나타낸 블록도이다.

[29] 도 3은 본 발명의 일 실시예에 따른 식별자 디바이스의 개인 식별 방법에 대한 순서도이다.

[30] 도 4 및 도 5는 본 발명의 일 실시예에 따른 식별자 디바이스에 출력되는 개인 식별 인터페이스 화면을 설명하기 위한 개략도이다.

[31] 도 6은 본 발명의 일 실시예에 따른 동형 암호화 연산을 수행하는 이미지 연산 서버의 구성을 나타낸 블록도이다.

[32] 도 7은 본 발명의 일 실시예에 따른 이미지 연산 서버의 개인 식별 방법에 대한 순서도이다.

[33] 도 8 및 도 9는 본 발명의 일 실시예에 따른 데이터 식별 방법에 대한 개략적인 순서도이다.

발명의 실시를 위한 형태

[34] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 도면의 설명과 관련하여, 유사한 구성요소에 대해서는 유사한 참조부호가 사용될 수 있다.

[35] 본 문서에서, "가진다," "가질 수 있다," "포함한다," 또는 "포함할 수 있다" 등의 표현은 해당 특징(예: 수치, 기능, 동작, 또는 부품 등의 구성요소)의 존재를 가리키며, 추가적인 특징의 존재를 배제하지 않는다.

[36] 본 문서에서, "A 또는 B," "A 또는/및 B 중 적어도 하나," 또는 "A 또는/및 B 중 하나 또는 그 이상" 등의 표현은 함께 나열된 항목들의 모든 가능한 조합을 포함할 수 있다. 예를 들면, "A 또는 B," "A 및 B 중 적어도 하나," 또는 "A 또는 B 중 적어도 하나"는, (1) 적어도 하나의 A를 포함, (2) 적어도 하나의 B를 포함, 또는(3) 적어도 하나의 A 및 적어도 하나의 B 모두를 포함하는 경우를 모두 지칭할 수 있다.

[37] 본 문서에서 사용된 "제1," "제2," "첫째," 또는 "둘째," 등의 표현들은 다양한 구성요소들을, 순서 및/또는 중요도에 상관없이 수식할 수 있고, 한 구성요소를 다른 구성요소와 구분하기 위해 사용될 뿐 해당 구성요소들을 한정하지 않는다. 예를 들면, 제1 사용자 기기와 제2 사용자 기기는, 순서 또는 중요도와 무관하게, 서로 다른 사용자 기기를 나타낼 수 있다. 예를 들면, 본 문서에 기재된 권리범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 바꾸어 명명될 수 있다.

[38] 어떤 구성요소(예: 제1 구성요소)가 다른 구성요소(예: 제2 구성요소)에 "(기능적으로 또는 통신적으로) 연결되어((operatively or communicatively) coupled with/to)" 있다거나 "접속되어(connected to)" 있다고 언급된 때에는, 상기 어떤 구성요소가 상기 다른 구성요소에 직접적으로 연결되거나, 다른 구성요소(예: 제3 구성요소)를 통하여 연결될 수 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소(예: 제1 구성요소)가 다른 구성요소(예: 제2 구성요소)에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 상기 어떤 구성요소와 상기 다른 구성요소 사이에 다른 구성요소(예: 제3 구성요소)가 존재하지 않는 것으로 이해될 수 있다.

[39] 본 문서에서 사용된 표현 "~하도록 구성된(또는 설정된)(configured to)"은 상황에 따라, 예를 들면, "~에 적합한(suitable for)," "~하는 능력을 가지는(having the capacity to)," "~하도록 설계된(designed to)," "~하도록 변경된(adapted to)," "~하도록 만들어진(made to)," 또는 "~ 를 할 수 있는(capable of)"과 바꾸어 사용될 수 있다. 용어 "~하도록 구성된(또는 설정된)"은 하드웨어적으로 "특별히 설계된(specifically designed to)" 것만을 반드시 의미하지 않을 수 있다. 대신, 어떤 상황에서는, "~하도록 구성된 장치"라는 표현은, 그 장치가 다른 장치 또는 부품들과 함께 "~할 수 있는" 것을 의미할 수 있다. 예를 들면, 문구 "A, B, 및 C를 수행하도록 구성된(또는 설정된)프로세서"는 해당 동작을 수행하기 위한 전용 프로세서(예: 임베디드 프로세서), 또는 메모리 장치에 저장된 하나 이상의 소프트웨어 프로그램들을 실행함으로써, 해당 동작들을 수행할 수 있는 범용 프로세서(generic-purpose processor)(예: CPU 또는 application processor)를 의미할 수 있다.

[40] 본 문서에서 사용된 용어들은 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 다른 실시예의 범위를 한정하려는 의도가 아닐 수 있다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함할 수 있다. 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 용어들은 본 문서에 기재된 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가질 수 있다. 본 문서에 사용된 용어들 중 일반적인 사전에 정의된 용어들은, 관련 기술의 문맥상 가지는 의미와 동일 또는 유사한 의미로 해석될 수 있으며, 본 문서에서 명백하게 정의되지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다. 경우에 따라서, 본 문서에서 정의된 용어일지라도 본 문서의 실시예들을 배제하도록 해석될 수 없다.

[41] 본 발명의 여러 실시예들의 각각 특징들이 부분적으로 또는 전체적으로 서로 결합 또는 조합 가능하며, 당업자가 충분히 이해할 수 있듯이 기술적으로 다양한 연동 및 구동이 가능하며, 각 실시예들이 서로에 대하여 독립적으로 실시 가능할 수도 있고 연관 관계로 함께 실시 가능할 수도 있다.

[42] 본 명세서의 해석의 명확함을 위해, 이하에서는 본 명세서에서 사용되는 용어들을 정의하기로 한다.

[43] 도 1은 본 발명의 일 실시예에 따른 개인 식별 시스템의 개략도이다.

[44] 도 1을 참조하면, 개인 식별 시스템(1000)은 사용자의 개인 식별 결과를 표시하는 식별자 디바이스(100) 및 사용자의 개인 식별 결과를 산출하는 이미지 연산 서버(200)를 포함할 수 있다.

[45] 개인 식별 시스템(1000)은 사용자의 이미지를 이용하여 사용자를 식별할 수 있는 시스템일 수 있다. 본 발명에서, 사용자를 식별한다는 것은 두 명의 사용자 간의 고유의 바이오 정보(사용자의 이미지)를 비교하여, 사용자가 어떠한 사용자인지 인식하거나, 사용자가 다른 사용자와 동일한지 여부를 판단하는 것으로 이해될 수 있다.

[46] 본 발명에서 사용자를 식별하기 위한 비교 대상이 되는 다른 사용자들은 사용자가 속한 그룹의 사용자일 수 있다. 예를 들어, 사용자가 속한 회사, 학교, 지역의 DB 서버(미도시)(또는 이미지 연산 서버(200))에 등록된 사용자들 또는 사용자가 참여하는 컨퍼런스에 등록된 사용자들이 비교 대상이 되는 다른 사용자가 될 수 있다. 식별자 디바이스(100)는 개인 식별 결과의 정확도를 높이고, 식별 속도를 향상시키기 위해, 개인 식별 서비스를 이용하는 데 사용될 DB 서버를 미리 지정할 수 있다.

[47] 개인 식별 시스템(1000)에서 식별자 디바이스(100)와 이미지 연산 서버(200)는 모든 데이터들을 암호화된 상태로 주고 받을 수 있으며, 식별자 디바이스(100)와 이미지 연산 서버(200)는 암호화된 상태에서의 데이터 연산이 가능하도록, 데이터들을 동형 암호화 기법을 통해 암호화할 수 있다.

[48] 즉, 개인 식별 시스템(1000)에서 식별자 디바이스(100)와 이미지 연산 서버(200) 간에 주고 받는 데이터는 데이터 원본이 아닌, 동형 암호화된 데이터이며, 데이터의 원본은 각자의 디바이스에 저장될 수 있다.

[49] 식별자 디바이스(100) 및 이미지 연산 서버(200)는 동형 암호화 데이터를 처리할 수 있는 웹 페이지 또는 어플리케이션/프로그램을 통해 데이터를 동형 암호화할 수 있으며, 동형 암호화된 데이터 간의 연산을 수행할 수 있다. 식별자 디바이스(100) 및 이미지 연산 서버(200)는 동형 암호문 간에, 또는 동형 암호문과 평문 간의 연산을 수행할 수 있으며, 다양한 동형 암호 알고리즘을 이용하여 이미지 데이터를 동형 암호화할 수 있다. 예를 들어, 식별자 디바이스(100) 및 이미지 연산 서버(200)는 부분 동형 암호(Partial Homomorphic Encryption), 준동형 암호(Somewhat Homomorphic Encryption) 및 완전 동형 암호(Fully Homomorphic Encryption) 중 어느 하나의 암호화 방법을 이용하여 이미지 데이터를 동형 암호화할 수 있다.

[50] 식별자 디바이스(100)는 사용자의 이미지를 획득하여, 이미지 식별 결과를 출력할 수 있는 디바이스로, PC, 태블릿 PC, 스마트 폰, 웨어러블 디바이스 등으로 구현될 수 있다. 여기서, 사용자 고유의 바이오 정보는 사용자의 신체에서 촬영 가능한 다양한 영역에 대한 이미지를 의미하며, 얼굴, 정맥, 홍채, 지문 등에 대한 이미지를 포함할 수 있다.

[51] 본 발명에서는 설명의 편의를 위해, 사용자의 얼굴 이미지를 이용하여 사용자를 식별하는 방식에 대하여 설명하도록 한다.

[52] 식별자 디바이스(100)는 동형 암호화된 제1 이미지 데이터(사용자의 이미지)를 토대로 해당 사용자에 대한 식별 결과를 얻을 수 있도록, 이미지 연산 서버(200)로 동형 암호화 연산을 위한 파라미터를 송신할 수 있다. 구체적으로, 파라미터는 동형 암호화 연산을 위해 사용되는 함수의 차수(polynomial degree), 동형 암호화 연산을 위해 지정되는 스케일 비트(scale bit), 계수(coefficient)), 이미지의 속성 정보(해상도, 크기)일 수 있다.

[53] 식별자 디바이스(100)는 파라미터를 이용하여 동형 암호화 연산된 식별 결과를 수신할 수 있으며, 이를 복호화하여 사용자에 대한 식별 결과를 얻을 수 있다. 예를 들어, 식별자 디바이스(100)가 어떠한 특정 공간에 설치된 경우, 식별자 디바이스(100)는 사용자의 이미지를 촬영한 뒤, 이를 동형 암호화하여 이미지 연산 서버(200)로 송신할 수 있으며, 이미지 연산 서버(200)로부터 수신된 동형 암호화된 연산 결과를 복호화하여, 사용자 각각에게 사용자 식별 결과에 따라 해당 사용자가 출입 가능한 사용자로 등록되었는지 여부, 즉 출입 가능 여부를 출력할 수 있다.

[54] 다양한 실시예에서, 식별자 디바이스(100)는 이미지 연산 서버(200)로부터 동형 암호화된 연산 결과를 수신하지 않고, 직접 연산을 수행할 수 있다. 이 경우, 식별자 디바이스(100)는 이미지 연산 서버(200)로부터 동형 암호화된 다른 사용자의 제2 이미지 데이터를 제공받고, 두 개의 동형 암호화된 데이터 간의 연산을 수행할 수 있으며, 동형 암호화된 데이터 간의 연산 방법은 후술하도록 한다.

[55] 다양한 실시예에서, 식별자 디바이스(100)는 직접 촬영한 이미지 자체를 동형 암호화할 수도 있지만, 관리자의 설정에 따라, 이미지에서 특징점(특징 데이터)들을 추출하고, 이를 동형 암호화할 수 있다. 이러한 경우, 식별자 디바이스(100)는 동형 암호화된 제1 이미지 데이터로 특징 데이터에 대한 메타 데이터를 이미지 연산 서버(200)로 송신할 수 있다.

[56] 이미지 연산 서버(200)는 식별자 디바이스(100)의 연산 요청에 따라, 미리 저장된 이미지 데이터를 이용하여 동형 암호화된 데이터 간의 연산을 수행할 수 있는 서버로, PC, 태블릿 PC, 스마트 폰, 범용 컴퓨터, 랩탑 및 클라우드 서버 등으로 구현될 수 있다.

[57] 이미지 연산 서버(200)는 복수의 제2 이미지 데이터(다른 사용자의 이미지)를 저장할 수 있으며, 연산 요청의 유형에 따라 어느 한 명의 사용자 이미지 데이터와의 동형 암호화 연산을 수행하거나, 복수의 사용자 이미지 데이터를 이용하여 복수 회의 동형 암호화 연산을 수행할 수 있다.

[58] 이미지 연산 서버(200)는 동형 암호화된 연산 결과를 산출할 수 있으며, 연산 결과에 대한 복호화는 식별자 디바이스(100)에서 수행될 수 있다. 즉, 이미지 연산 서버(200)는 식별자 디바이스(100)로부터 동형 암호화된 제1 이미지

데이터를 수신하여 연산을 수행하고, 그 결과 또한 복호화하지 않은 상태로 전달하기 때문에, 이미지 연산 서버(200)는 해당 사용자가 미리 저장된 A 사용자와 일치하는지 혹은 복수의 사용자 중 어느 한 명의 사용자인지에 대한 식별 결과를 확인할 수 없다.

[59] 다양한 실시예에서, 이미지 연산 서버(200)는 동형 암호화된 제1 이미지 데이터와 평문 상태의 제2 이미지 데이터를 기초로 연산을 수행하거나, 식별자 디바이스(100)로부터 수신한 파라미터가 반영된 암호화 키를 이용하여 동형 암호화된 제2 이미지 데이터를 기초로 연산을 수행할 수 있다.

[60] 다양한 실시예에서, 이미지 연산 서버(200)는 식별자 디바이스(100)로 데이터 동형 암호화 및 식별 결과 복호화를 위한 웹 페이지 또는 어플리케이션을 제공할 수 있다.

[61] 다양한 실시예에서, 식별자 디바이스(100) 및 이미지 연산 서버(200)는 동형 암호화를 수행하기 전, 동형 암호화 연산의 부담을 줄이기 위해, 각자의 디바이스에 저장된 이미지 데이터를 전처리할 수 있다. 예를 들어, 식별자 디바이스(100) 및 이미지 연산 서버(200)는 이미지 데이터에 대한 유사도를 계산하기 위해, 이미지 데이터를 위치로 변환할 수 있다. 즉, 각각의 이미지 데이터를 이산화된 격자(grid) 시스템의 지정된 위치로 변환할 수 있다.

[62] 지금까지 본 발명의 일 실시예에 따른 개인 식별 시스템(1000)에 대하여 설명하였다. 본 발명에 따르면, 식별자 디바이스(100)와 이미지 연산 서버(200) 간에 주고 받는 데이터는 모두 동형 암호화된 상태인 바, 개인 식별 서비스가 제공되는 동안 사용자 이미지가 노출될 가능성이 없으며, 개인 정보가 침해되는 상황을 예방할 수 있다.

[63] 이하에서는, 개인 식별 서비스를 제공 받는 식별자 디바이스(100)에 대하여 설명하도록 한다.

[64] 도 2는 본 발명의 일 실시예에 따른 식별자 디바이스의 구성을 나타낸 블록도이다.

[65] 도 2를 참조하면, 식별자 디바이스(100)는 메모리 인터페이스(110), 하나 이상의 프로세서(120) 및 주변 인터페이스(130)를 포함할 수 있다. 식별자 디바이스(100) 내의 다양한 컴포넌트들은 하나 이상의 통신 버스 또는 신호 라인에 의해 연결될 수 있다.

[66] 메모리 인터페이스(110)는 메모리(150)에 연결되어 프로세서(120)로 다양한 데이터를 전할 수 있다. 여기서, 메모리(150)는 플래시 메모리 타입, 하드디스크 타입, 멀티미디어 카드 마이크로 타입, 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램, SRAM, 롬, EEPROM, PROM, 네트워크 저장 스토리지, 클라우드, 블록체인 데이터베이스 중 적어도 하나의 타입의 저장매체를 포함할 수 있다.

[67] 다양한 실시예에서, 메모리(150)는 사용자의 이미지를 획득하고, 개인 식별 결과를 출력하기 위한 개인 식별 인터페이스 화면을 구성하는 데이터, 전처리된

제1 이미지 데이터, 제1 이미지 데이터를 동형 암호화 가능한 형태로 변환하기 위한 함수, 동형 암호화를 위한 알고리즘, 동형 암호화된 제1 이미지 데이터, 동형 암호화 연산을 위한 파라미터 등을 저장할 수 있다.

[68] 다양한 실시예에서, 메모리(150)는 운영 체제(151), 통신 모듈(152), 그래픽 사용자 인터페이스 모듈(GUI)(153), 센서 처리 모듈(154), 전화 모듈(155) 및 애플리케이션 모듈(156) 중 적어도 하나 이상을 저장할 수 있다. 구체적으로, 운영 체제(151)는 기본 시스템 서비스를 처리하기 위한 명령어 및 하드웨어 작업들을 수행하기 위한 명령어를 포함할 수 있다. 통신 모듈(152)은 다른 하나 이상의 디바이스, 컴퓨터 및 서버 중 적어도 하나와 통신할 수 있다. 그래픽 사용자 인터페이스 모듈(GUI)(153)은 그래픽 사용자 인터페이스를 처리할 수 있다. 센서 처리 모듈(154)은 센서 관련 기능(예를 들어, 하나 이상의 마이크(192)를 통해 수신된 음성 입력을 처리함)을 처리할 수 있다. 전화 모듈(155)은 전화 관련 기능을 처리할 수 있다. 애플리케이션 모듈(156)은 사용자 애플리케이션의 다양한 기능들, 예컨대 전자 메시징, 웹 브라우징, 미디어 처리, 탐색, 이미징, 기타 프로세스 기능을 수행할 수 있다. 아울러, 식별자 디바이스(100)는 메모리(150)에 어느 한 종류의 서비스와 연관된 하나 이상의 소프트웨어 애플리케이션(156-1, 156-2)(예. 개인 식별 서비스 어플리케이션)을 저장할 수 있다.

[69] 다양한 실시예에서, 메모리(150)는 디지털 어시스턴트 클라이언트 모듈(157)(이하, DA 클라이언트 모듈)을 저장할 수 있으며, 그에 따라 디지털 어시스턴트의 클라이언트 측의 기능을 수행하기 위한 명령어 및 다양한 사용자 데이터(158)(예. 사용자 맞춤형 어휘 데이터, 선호도 데이터, 사용자의 전자 주소록 등과 같은 기타 데이터)를 저장할 수 있다.

[70] 한편, DA 클라이언트 모듈(157)은 식별자 디바이스(100)에 구비된 다양한 사용자 인터페이스(예. I/O 서브시스템(140))를 통해 사용자의 음성 입력, 텍스트 입력, 터치 입력 및/또는 제스처 입력을 획득할 수 있다.

[71] 또한, DA 클라이언트 모듈(157)은 시청각적, 촉각적 형태의 데이터를 출력할 수 있다. 예를 들어, DA 클라이언트 모듈(157)은 음성, 소리, 알림, 텍스트 메시지, 메뉴, 그래픽, 비디오, 애니메이션 및 진동 중 적어도 둘 하나 이상의 조합으로 이루어진 데이터를 출력할 수 있다. 아울러, DA 클라이언트 모듈(157)은 통신 서브시스템(180)을 이용하여 디지털 어시스턴트 서버(미도시)와 통신할 수 있다.

[72] 다양한 실시예에서, DA 클라이언트 모듈(157)은 사용자 입력과 연관된 상황(context)을 구성하기 위하여 다양한 센서, 서브시스템 및 주변 디바이스로부터 식별자 디바이스(100)의 주변 환경에 대한 추가 정보를 수집할 수 있다. 예를 들어, DA 클라이언트 모듈(157)은 사용자 입력과 함께 상황 정보를 디지털 어시스턴트 서버에 제공하여 사용자의 의도를 추론할 수 있다. 여기서, 사용자 입력에 동반될 수 있는 상황 정보는 센서 정보, 예를 들어, 광(lighting), 주변 소음, 주변 온도, 주변 환경의 이미지, 비디오 등을 포함할 수 있다. 다른

예를 들어, 상황 정보는 식별자 디바이스(100)의 물리적 상태(예. 디바이스 배향, 디바이스 위치, 디바이스 온도, 전력 레벨, 속도, 가속도, 모션 패턴, 셀룰러 신호 강도 등)을 포함할 수 있다. 또 다른 예를 들어, 상황 정보는 식별자 디바이스(100)의 소프트웨어 상태에 관련된 정보(예. 식별자 디바이스(100)에서 실행 중인 프로세스, 설치된 프로그램, 과거 및 현재 네트워크 활동성, 백그라운드 서비스, 오류 로그, 리소스 사용 등)를 포함할 수 있다.

[73] 다양한 실시예에서, 메모리(150)는 추가 또는 삭제된 명령어를 포함할 수 있으며, 나아가 식별자 디바이스(100)도 도 2에 도시된 구성 외에 추가 구성을 포함하거나, 일부 구성을 제외할 수도 있다.

[74] 프로세서(120)는 식별자 디바이스(100)의 전반적인 동작을 제어할 수 있으며, 메모리(150)에 저장된 어플리케이션 또는 프로그램을 구동하여 개인 식별 서비스용 인터페이스를 구현하기 위한 다양한 명령들을 수행할 수 있다.

[75] 프로세서(120)는 CPU(Central Processing Unit)나 AP(Application Processor)와 같은 연산 장치에 해당할 수 있다. 또한, 프로세서(120)는 NPU(Neural Processing Unit)과 같이 기계 학습을 수행하는 다양한 연산 장치가 통합된 SoC(System on Chip)와 같은 통합 칩(Integrated Chip (IC))의 형태로 구현될 수 있다.

[76] 다양한 실시예에서, 프로세서(120)는 이미지를 동형 암호화하고, 이를 기초로 동형 암호화된 사용자의 식별 결과를 획득할 수 있으며, 이하 도 3 내지 5를 참조하여 설명하도록 한다.

[77] 도 3은 본 발명의 일 실시예에 따른 식별자 디바이스의 개인 식별 방법에 대한 순서도이고, 도 4 및 도 5는 본 발명의 일 실시예에 따른 식별자 디바이스에 출력되는 개인 식별 인터페이스 화면을 설명하기 위한 개략도이다.

[78] 도 3을 참조하면, 프로세서(120)는 사용자의 제1 이미지 데이터를 획득할 수 있다(S110). 예를 들어, 프로세서(120)는 카메라 서브 시스템(170)을 통해 촬영된 사용자의 이미지를 획득할 수 있으며, 개인 식별을 위해 사용자의 이미지가 아닌 정맥의 분포 패턴을 활용할 경우, 통신 모듈(152)을 통해 사용자 개인이 소지한 웨어러블 디바이스(미도시)로부터 손가락, 손목의 이미지를 획득할 수도 있다.

[79] 관련하여, 도 4를 참조하면, 식별자 디바이스(100)의 프로세서(120)는 (a)와 같이, 사용자의 제1 이미지 데이터를 획득하기 위한 인터페이스 화면을 제공할 수 있다. 구체적으로, 인터페이스 화면에는 카메라 서브 시스템(170)을 통해서 사용자의 얼굴 이미지를 획득할 수 있는 가이드 라인(10)과 사용자 안내 문구(11)가 포함될 수 있다.

[80] 이 외에도, 인터페이스 화면에는 식별자 디바이스(100)가 배치된 위치 정보와 개인 식별을 수행하는 시간 정보가 함께 표시될 수 있다.

[81] 프로세서(120)는 (b)와 같이, 가이드 라인(10) 내 사용자 이미지(12)를 획득하는 경우, 카메라 서브 시스템(170)을 통해 사용자 이미지를 획득할 수 있다.

[82] 다양한 실시예에서, 프로세서(120)는 이미지 전체를 동형 암호화할 수도 있지만, 관리자의 설정에 따라, 이미지의 특징점을 동형 암호화할 수 있다. 이를

위해, 프로세서(120)는 이미지에서 특징 데이터를 추출할 수 있다. 구체적으로, 프로세서(120)는 이미지의 가로/세로 위치를 기준으로 픽셀 값의 변화율을 계산하고(이미지 미분), 이 값들을 이용하여 엣지 추출(edge detection), 코너 추출(corner detection)을 수행하여 특징 데이터(특징점들의 좌표 값)를 획득하거나, 이미지 히스토그램(image Histogram), 그래디언트 히스토그램 설명자(gradient histogram descriptor), FAST(Features from Accelerated Segment Test), SIFT(Scale-Invariant Feature Transform), SURF(Speed-Up Robust Features) 등의 방법을 통해 특징 데이터(특징점들의 좌표 값)를 획득할 수 있다. 그에 따라, 예를 들어, 프로세서(120)는 이미지에서 사용자의 눈, 코, 입의 좌표 값을 추출할 수 있으며, 이 외에도 이미지의 픽셀 별 RGB 값을 추출할 수도 있다.

[83] 즉, 프로세서(120)는 카메라 서브 시스템(170)을 통해 촬영된 이미지, 이미지에서 추출된 복수의 특징 좌표 값((User1=(E_1, N_1, L_1))), 이미지의 픽셀 별 RGB 값 중 어느 하나를 개인 식별이 필요한 사용자의 제1 이미지 데이터로 사용할 수 있다. 이 중 이미지의 픽셀 별 RGB 값은 이미지의 크기 또는 해상도에 따라 데이터의 크기가 지나치게 커질 수 있으므로, 프로세서(120)는 예를 들어, 복수의 특징 좌표 값에 대응되는 픽셀에서의 RBG 값을 사용자의 제1 이미지 데이터로 사용할 수 있다.

[84] 다양한 실시예에서, 프로세서(120)는 동형 암호화 연산의 부담을 줄이기 위해, 사용자의 제1 이미지 데이터를 전처리할 수 있다. 예를 들어, 프로세서(120)는 제1 이미지 데이터와 비교 대상인 제2 이미지 데이터와의 유사도를 계산하기 위해, 이미지 데이터를 미리 저장된 함수를 이용하여 위치로 변환할 수 있다.

[85] 다시 도 3을 참조하면, S110 단계 이후, 프로세서(120)는 제1 이미지 데이터를 동형 암호화 할 수 있다(S120). 구체적으로, 프로세서(120)는 동형 암호화 연산을 위한 파라미터가 반영된 암호화 키를 이용하여 제1 이미지 데이터를 동형 암호화할 수 있다.

[86] 다양한 실시예에서, 프로세서(120)는 부분 동형 암호(Partial Homomorphic Encryption), 준동형 암호(Somewhat Homomorphic Encryption) 및 완전 동형 암호(Fully Homomorphic Encryption) 중 어느 하나의 암호화 방법을 이용하여 제1 이미지 데이터를 동형 암호화할 수 있다.

[87] S120 단계 이후, 프로세서(120)는 통신 모듈(152)을 통해 동형 암호화된 제1 이미지 데이터를 이미지 연산 서버(200)로 송신할 수 있다(S130). 프로세서(120)는 동형 암호화된 제1 이미지 데이터와 제1 이미지 데이터를 동형 암호화하는 과정에서 사용된 파라미터를 포함하는 연산 요청을 이미지 연산 서버(200)로 송신할 수 있다. 예를 들어, 파라미터는 동형 암호화 연산을 위해 사용되는 함수의 차수(polynomial degree), 동형 암호화 연산을 위해 지정되는 스케일 비트(scale bit), 계수(coefficient)), 이미지의 속성 정보(해상도, 크기)일 수 있다.

[88] S130 단계 이후, 프로세서(120)는 이미지 연산 서버(200)로부터 동형 암호화된

제1 이미지 데이터와 미리 저장된 다른 사용자의 제2 이미지 데이터를 기초로 계산된 동형 암호화된 식별 결과를 수신할 수 있다(S140). 여기서, 동형 암호화된 식별 결과는, 동형 암호화된 제1 이미지 데이터와 S130 단계에서 제공된 파라미터를 기초로 동형 암호화된 제2 이미지 데이터를 기초로 계산된 식별 결과일 수 있다.

[89] 즉, 동일한 파라미터가 반영된 암호화 키를 이용하여 제1 및 제2 이미지 데이터가 동형 암호화된 상태로 연산될 수 있으며, 그에 따라, 이 후 이미지 연산 서버(200)에 의해 연산된 식별 결과가 올바르게 복호화될 수 있다.

[90] 한편, 프로세서(120)는 연산 요청에 따라 미리 저장된 한 명의 다른 사용자의 이미지 데이터와의 식별 결과를 수신하거나, 복수의 다른 사용자 각각의 이미지 데이터와의 식별 결과를 수신할 수 있다.

[91] S140 단계 이후, 프로세서(120)는 동형 암호화된 식별 결과를 복호화할 수 있다(S150). 구체적으로, 프로세서(120)는 연산 요청에 따라 서로 다른 유형의 복호화된 결과를 터치 스크린(143)에 출력할 수 있다. 예를 들어, 프로세서(120)는 사용자가 지정된 다른 사용자와 일치하는지에 대한 식별 결과, 혹은 복수의 사용자 중 어느 한 명의 사용자인지에 대한 식별 결과를 확인할 수 있다.

[92] 관련하여, 도 5를 참조하면, 식별자 디바이스(100)의 프로세서(120)는 (a)와 같이 사용자가 복수의 출입 가능한 사용자 중 어느 하나의 사용자와 일치하는지, 일치하지 않는지에 따라 출입 가능 여부를 나타내는 알림(13)을 제공할 수 있다.

[93] 다시 도 2를 참조하면, 주변 인터페이스(130)는 다양한 센서, 서브 시스템 및 주변 디바이스와 연결되어, 식별자 디바이스(100)가 다양한 기능을 수행할 수 있도록 데이터를 제공해 줄 수 있다. 여기서, 식별자 디바이스(100)가 어떠한 기능을 수행한다는 것은 프로세서(120)에 의해 수행되는 것으로 이해될 수 있다.

[94] 주변 인터페이스(130)는 모션 센서(160), 조명 센서(광 센서)(161) 및 근접 센서(162)로부터 데이터를 제공받을 수 있으며, 이를 통해, 식별자 디바이스(100)는 배향, 광, 및 근접 감지 기능 등을 수행할 수 있다. 다른 예를 들어, 주변 인터페이스(130)는 기타 센서들(163)(포지셔닝 시스템-GPS 수신기, 온도 센서, 생체인식 센서)로부터 데이터를 제공받을 수 있으며, 이를 통해 식별자 디바이스(100)가 기타 센서들(163)과 관련된 기능들을 수행할 수 있다.

[95] 다양한 실시예에서, 식별자 디바이스(100)는 주변 인터페이스(130)와 연결된 카메라 서브시스템(170) 및 이와 연결된 광학 센서(171)를 포함할 수 있으며, 이를 통해 식별자 디바이스(100)는 사진 촬영 및 비디오 클립 녹화 등의 다양한 촬영 기능을 수행할 수 있다.

[96] 다양한 실시예에서, 식별자 디바이스(100)는 주변 인터페이스(130)와 연결된 통신 서브 시스템(180)을 포함할 수 있다. 통신 서브 시스템(180)은 하나 이상의 유/무선 네트워크로 구성되며, 다양한 통신 포트, 무선 주파수 송수신기, 광학 송수신기를 포함할 수 있다.

[97] 다양한 실시예에서, 식별자 디바이스(100)는 주변 인터페이스(130)와 연결된 오디오 서브 시스템(190)을 포함하며, 이러한 오디오 서브 시스템(190)은 하나 이상의 스피커(191) 및 하나 이상의 마이크(192)를 포함함으로써, 식별자 디바이스(100)는 음성 작동형 기능, 예컨대 음성 인식, 음성 복제, 디지털 녹음, 및 전화 기능 등을 수행할 수 있다.

[98] 다양한 실시예에서, 식별자 디바이스(100)는 주변 인터페이스(130)와 연결된 I/O 서브시스템(140)을 포함할 수 있다. 예를 들어, I/O 서브시스템(140)은 터치 스크린 제어기(141)를 통해 식별자 디바이스(100)에 포함된 터치 스크린(143)을 제어할 수 있다. 예를 들어, 터치 스크린 제어기(141)는 정전용량형, 저항형, 적외형, 표면 탄성파 기술, 근접 센서 어레이 등과 같은 복수의 터치 감지 기술 중 어느 하나의 기술을 사용하여 사용자의 접촉 및 움직임 또는 접촉 및 움직임의 중단을 검출할 수 있다. 다른 예를 들어, I/O 서브시스템(140)은 기타 입력 제어기(들)(142)를 통해 식별자 디바이스(100)에 포함된 기타 입력/제어 디바이스(144)를 제어할 수 있다. 일 예로서, 기타 입력 제어기(들)(142)은 하나 이상의 버튼, 로커 스위치(rocker switches), 썸 휠(thumb-wheel), 적외선 포트, USB 포트 및 스타일러스 등과 같은 포인터 디바이스를 제어할 수 있다.

[99] 지금까지 본 발명의 일 실시예에 따른 식별자 디바이스(100)에 대하여 설명하였다. 본 발명에 따르면, 식별자 디바이스(100)는 자신이 가지고 있는 이미지 데이터와 다른 사용자의 이미지 데이터를 비교하기 위해, 이미지 연산 서버(200)로 동형 암호화된 이미지 데이터를 이용한 연산 요청을 할 수 있으며, 그에 따라, 사용자의 초상권은 보호하면서도 사용자에 대한 신원은 빠르게 확인할 수 있다.

[100] 이하에서는 개인 식별 서비스를 제공하는 이미지 연산 서버(200)에 대하여 설명하도록 한다.

[101] 도 6은 본 발명의 일 실시예에 따른 동형 암호화 연산을 수행하는 이미지 연산 서버의 구성을 나타낸 블록도이다.

[102] 도 6을 참조하면, 이미지 연산 서버(200)는 통신 인터페이스(210), 메모리(220), I/O 인터페이스(230) 및 프로세서(240)를 포함할 수 있으며, 각 구성은 하나 이상의 통신 버스 또는 신호 라인을 통해 서로 통신할 수 있다.

[103] 통신 인터페이스(210)는 유/무선 통신 네트워크를 통해 복수의 식별자 디바이스(100)와 연결되어 데이터를 주고받을 수 있다. 예를 들어, 통신 인터페이스(210)는 식별자 디바이스(100)로부터 동형 암호화된 제1 이미지 데이터, 동형 암호화 연산을 위한 파라미터를 포함하는 연산 요청을 수신할 수 있으며, 식별자 디바이스(100)로 동형 암호화된 식별 결과를 송신할 수 있다.

[104] 한편, 이러한 데이터의 송수신을 가능하게 하는 통신 인터페이스(210)는 통신 포드(211) 및 무선 회로(212)를 포함하며, 여기 유선 통신 포트(211)는 하나 이상의 유선 인터페이스, 예를 들어, 이더넷, 범용 직렬 버스(USB), 파이어와이어 등을 포함할 수 있다. 또한, 무선 회로(212)는 RF 신호 또는 광학 신호를 통해

외부 디바이스와 데이터를 송수신할 수 있다. 아울러, 무선 통신은 복수의 통신 표준, 프로토콜 및 기술, 예컨대 GSM, EDGE, CDMA, TDMA, 블루투스, Wi-Fi, VoIP, Wi-MAX, 또는 임의의 기타 적합한 통신 프로토콜 중 적어도 하나를 사용할 수 있다.

[105] 메모리(220)는 이미지 연산 서버(200)에서 사용되는 다양한 데이터를 저장할 수 있다. 예를 들어, 메모리(220)는 복수의 사용자에 대한 제2 이미지 데이터(사용자 이미지, 사용자 이미지에서 추출되는 특징 데이터(좌표 값, RGB 값), 제2 이미지 데이터를 동형 암호화 가능한 형태로 변환하기 위한 함수, 동형 암호화를 위한 알고리즘 등을 저장할 수 있다.

[106] 다양한 실시예에서, 메모리(220)는 각종 데이터, 명령 및 정보를 저장할 수 있는 휘발성 또는 비휘발성 기록 매체를 포함할 수 있다. 예를 들어, 메모리(220)는 플래시 메모리 타입, 하드디스크 타입, 멀티미디어 카드 마이크로 타입, 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램, SRAM, 롬, EEPROM, PROM, 네트워크 저장 스토리지, 클라우드, 블록체인 데이터베이스 중 적어도 하나의 타입의 저장매체를 포함할 수 있다.

[107] 다양한 실시예에서, 메모리(220)는 운영 체제(221), 통신 모듈(222), 사용자 인터페이스 모듈(223) 및 하나 이상의 애플리케이션(224) 중 적어도 하나의 구성을 저장할 수 있다.

[108] 운영 체제(221)(예. LINUX, UNIX, MAC OS, WINDOWS, VxWorks 등의 내장형 운영 체제)는 일반적인 시스템 작업(예. 메모리 관리, 저장 디바이스 제어, 전력 관리 등)를 제어하고 관리하기 위한 다양한 소프트웨어 컴포넌트 및 드라이버를 포함할 수 있으며, 다양한 하드웨어, 펌웨어, 및 소프트웨어 컴포넌트 간의 통신을 지원할 수 있다.

[109] 통신 모듈(223)은 통신 인터페이스(210)를 통해 다른 디바이스와 통신을 지원할 수 있다. 통신 모듈(220)은 통신 인터페이스(210)의 유선 통신 포트(211) 또는 무선 회로(212)에 의해 수신되는 데이터를 처리하기 위한 다양한 소프트웨어 구성 요소들을 포함할 수 있다.

[110] 사용자 인터페이스 모듈(223)은 I/O 인터페이스(230)를 통해 키보드, 터치 스크린, 마이크 등으로부터 사용자의 요청 또는 입력을 수신하고, 디스플레이 상에 사용자 인터페이스를 제공할 수 있다.

[111] 애플리케이션(224)은 하나 이상의 프로세서(230)에 의해 실행되도록 구성되는 프로그램 또는 모듈을 포함할 수 있다. 여기서, 이미지 데이터를 연산하기 위한 어플리케이션은 서버 팜(server farm) 상에서 구현될 수 있다.

[112] I/O 인터페이스(230)는 이미지 연산 서버(200)의 입출력 디바이스(미도시), 예컨대 디스플레이, 키보드, 터치 스크린 및 마이크 중 적어도 하나를 사용자 인터페이스 모듈(223)과 연결할 수 있다. I/O 인터페이스(230)는 사용자 인터페이스 모듈(223)과 함께 사용자 입력(예. 음성 입력, 키보드 입력, 터치 입력 등)을 수신하고, 수신된 입력에 따른 명령을 처리할 수 있다.

[113] 프로세서(240)는 통신 인터페이스(210), 메모리(220) 및 I/O 인터페이스(230)와 연결되어 이미지 연산 서버(200)의 전반적인 동작을 제어할 수 있으며, 메모리(220)에 저장된 애플리케이션 또는 프로그램을 통해 동형 암호화된 데이터가 처리되기 위한 다양한 명령들을 수행할 수 있다.

[114] 프로세서(240)는 CPU(Central Processing Unit)나 AP(Application Processor)와 같은 연산 장치에 해당할 수 있다. 또한, 프로세서(240)는 다양한 연산 장치가 통합된 SoC(System on Chip)와 같은 통합 칩(Integrated Chip (IC))의 형태로 구현될 수 있다. 또는 프로세서(240)는 NPU(Neural Processing Unit)과 같이 인공 신경망 모델을 계산하기 위한 모듈을 포함할 수 있다.

[115] 다양한 실시예에서, 프로세서(240)는 사용자의 개인 정보가 노출되지 않은 상태로 사용자를 식별하는 서비스를 제공할 수 있으며, 이하 도 7을 참조하여 설명하도록 한다.

[116] 도 7은 본 발명의 일 실시예에 따른 이미지 연산 서버의 개인 식별 방법에 대한 순서도이다.

[117] 도 7을 참조하면, 프로세서(240)는 통신 인터페이스(210)를 통해 식별자 디바이스(100)로부터 동형 암호화된 사용자의 제1 이미지 데이터를 포함하는 연산 요청을 수신할 수 있다(S210). 연산 요청에는 제1 이미지 데이터를 동형 암호화하기 위해 사용된, 동형 암호화 연산을 위한 파라미터, 제1 이미지에서 추출된 특징 데이터가 포함될 수 있다.

[118] S210 단계 이후, 프로세서(240)는 연산 요청에 따라 미리 저장된 다른 사용자의 제2 이미지 데이터를 획득할 수 있다(S220). 프로세서(240)는 연산 요청이 한 명의 다른 사용자의 제2 이미지 데이터에 대한 연산 요청인지, 복수의 다른 사용자의 제2 이미지 데이터에 대한 연산 요청인지에 따라, 메모리(220)에 저장된 사용자의 제2 이미지 데이터를 로드(load)할 수 있다.

[119] 아울러, 프로세서(240)는 제1 이미지 데이터가 식별자 디바이스(100)를 통해 촬영된 이미지, 복수의 특징 좌표 값((User1=(E_1, N_1, L_1))) 및 이미지의 픽셀 별 RGB 값(특징 데이터) 중 어느 하나인지 확인하고, 그에 맞는 제2 이미지 데이터를 획득할 수 있다.

[120] 프로세서(240)는 동형 암호화된 제1 이미지 데이터 동일한 파라미터가 반영된 암호화 키를 이용하여 메모리(220)에 저장된 다른 사용자의 제2 이미지 데이터를 동형 암호화할 수 있다. 또한, 프로세서(240)는 연산 요청에 따라 메모리(220)에 저장된 한 명의 다른 사용자의 제2 이미지 데이터를 동형 암호화하거나, 메모리(220)에 저장된 복수의 다른 사용자의 제2 이미지 데이터를 동형 암호화할 수 있다.

[121] 다양한 실시예에서, 프로세서(240)는 부분 동형 암호(Partial Homomorphic Encryption), 준동형 암호(Somewhat Homomorphic Encryption) 및 완전 동형 암호(Fully Homomorphic Encryption) 중 어느 하나의 암호화 방법을 이용하여 동형 암호화할 수 있다.

[122] 한편, 프로세서(240)는 미리 저장된 다른 사용자의 제2 이미지 데이터를 획득하고, 동형 암호화하지 않을 수도 있다.

[123] S220 단계 이후, 프로세서(240)는 동형 암호화된 제1 이미지 데이터와 제2 이미지 데이터를 기초로 동형 암호화된 식별 결과를 산출할 수 있다(S230). 구체적으로, 프로세서(240)는 두 개의 이미지 데이터를 거리 유사도 계산 방법(예. 유클리디안 거리 측정 방법(Euclidean Distance), 민코프스키 거리 측정 방법(Minkowski Distance), 코사인 유사도 계산 방법(Cosine Similarity), 평균 제곱 차이 유사도 계산 방법(Mean Squared Difference Similarity), 피어슨 유사도 계산 방법(Pearson Similarity)) 등을 이용하여 연산하여 이미지 데이터 간의 유사도(이미지 식별 결과)를 산출할 수 있다.

[124] 이를 위해, 프로세서(240)는 동형 암호화된 제1 이미지 데이터에 대응되는 제1 위치와 제2 이미지 데이터에 대응되는 제2 위치를 결정할 수 있다. 예를 들어, 프로세서(240)는 H3(Hexagonal Hierarchical Spatial Index) 시스템을 이용하여 이미지 데이터 각각에 대응되는 위치를 실수(real number) 값 또는 위치 벡터로 결정할 수 있다.

[125] 프로세서(240)는 제1 위치와 제2 위치 사이의 거리 값을 앞서 언급한 거리 유사도 계산 방법을 이용하여 계산하여, 식별 결과에 대응되는 값을 획득할 수 있다. 예를 들어, 프로세서(240)는 계산된 거리 값이 미리 지정된 거리 범위에 포함되는 경우, 두 개의 이미지 데이터가 유사하다는 결과를 포함하는 동형 암호화된 식별 결과를 산출할 수 있으며, 계산된 거리 값이 미리 지정된 거리 범위에 포함되지 않는 경우, 두 개의 이미지 데이터가 유사하지 않다는 결과를 포함하는 동형 암호화된 식별 결과를 산출할 수 있다.

[126] 다양한 실시예에서, 프로세서(240)는 연산 요청의 종류에 따라, 한 명 또는 복수의 다른 사용자의 제2 이미지 데이터와 동형 암호화된 제1 이미지 데이터를 기초로 암호화된 식별 결과를 산출할 수 있다.

[127] 한편, 상술한 식별 결과는 동형 암호화된 상태인 바, 프로세서(240)는 두 개의 이미지 데이터 간의 유사도 결과는 확인할 수 없다.

[128] S230 단계 이후, 프로세서(240)는 동형 암호화된 식별 결과를 식별자 디바이스(100)로 송신할 수 있다(S240). 동형 암호화된 식별 결과는 식별자 디바이스(100)에 의해서 복호화될 수 있으며, 그에 따라, 프로세서(240)는 jpg, png, pdf 과 같은 포맷의 사용자의 이미지를 획득하지 않고도, 메모리(220)에 저장된 복수의 다른 사용자의 이미지와의 비교 및 식별 결과를 산출하여 식별자 디바이스(100)로 제공할 수 있다.

[129] 지금까지 본 발명의 일 실시예에 따른 이미지 연산 서버(200)에 대하여 설명하였다. 본 발명에 따르면, 사용자 고유의 이미지가 각자의 안전한 디바이스 내에 저장된 상태로 동형 암호화 및 복호화되고, 이미지 연산 서버(200)는 동형 암호화된 연산 결과만을 전달해 줌으로써, 민감 정보 처리에 따른 위험 부담을 최소화할 수 있다.

[130] 이하에서는 식별자 디바이스(100) 및 이미지 연산 서버(200)를 포함하는 양자 간의 개인 식별 방법을 개략적으로 설명하도록 한다.

[131] 도 8 및 도 9는 본 발명의 일 실시예에 따른 데이터 식별 방법에 대한 개략적인 순서도이다.

[132] 도 8을 참조하면, 식별자 디바이스(100)는 사용자의 이미지를 획득하거나(S10), 이에 더하여 이미지에서 특징 데이터를 추출할 수 있으며(S11), 이미지 또는 특징 데이터(제1 이미지 데이터)를 동형 암호화할 수 있다(S12).

[133] 식별자 디바이스(100)는 동형 암호화된 제1 이미지 데이터와 함께 동형 암호 연산을 위한 파라미터를 이미지 연산 서버(200)로 송신할 수 있다. 여기서, 동형 암호 연산을 위한 파라미터는 동형 암호화된 제1 이미지 데이터의 암호화 키에 적용된 파라미터일 수 있다.

[134] 이미지 연산 서버(200)는 파라미터를 이용하여 미리 저장된 제2 이미지 데이터를 동형 암호화하고(S14), 동형 암호화된 제1, 제2 이미지 데이터를 기초로 동형 암호화된 식별 결과를 산출할 수 있다(S15)(즉, 동형 암호화된 데이터를 연산할 수 있다). 구체적으로, 이미지 연산 서버(200)는 동형 암호화된 이미지 데이터에 대응되는 위치를 결정하고, 위치 사이의 거리를 계산하여, 동형 암호화된 데이터 간의 연산을 수행할 수 있으며, 식별 결과에 대응되는 값을 획득할 수 있다.

[135] 다양한 실시예에서, 이미지 연산 서버(200)는 미리 저장된 제2 이미지 데이터를 암호화하지 않고, 평문 상태의 제2 이미지 데이터와 동형 암호화된 제1 이미지 데이터 간의 비교 연산을 수행할 수도 있다.

[136] 이미지 연산 서버(200)는 암호화된 연산 결과를 식별자 디바이스(100)로 송신하고(S16), 식별자 디바이스(100)는 연산 결과를 복호화하여(S17), 디스플레이 화면 상에 복호화 결과를 출력할 수 있다(S18).

[137] 한편, 동형 암호화된 데이터 간의 연산은 식별자 디바이스(100)에서도 이미지 연산 서버(200)와 동일한 방식으로 수행될 수 있다.

[138] 관련하여, 도 9를 참조하면, S20 내지 S21 단계는 이전과 동일하나, 식별자 디바이스(100)는 이미지 또는 특징 데이터를 동형 암호화를 선택적으로 수행할 수 있다(S22).

[139] 이 후, 식별자 디바이스(100)는 이미지 연산 서버(200)로 동형 암호 연산을 위한 파라미터를 포함하는 데이터 식별 요청을 송신할 수 있다(S23).

[140] 이미지 연산 서버(200)는 데이터 식별 요청에 따라, 앞서 수신된 파라미터와 동일한 파라미터를 이용하여 미리 저장된 복수의 제2 이미지 데이터를 동형 암호화하여 식별자 디바이스(100)로 송신할 수 있다.

[141] 즉, 이미지 연산 서버(200)가 동형 암호화된 제2 이미지 데이터를 제공함으로써, 식별자 디바이스(100)가 동형 암호화된 제1, 제2 이미지 데이터를 기초로 동형 암호화된 식별 결과를 산출할 수 있다(S25)(즉, 동형 암호화된 데이터를 연산할 수 있다).

[142] 식별자 디바이스(100)는 암호화된 연산 결과를 이미지 연산 서버(200)로 송신할 수 있으며(S26), 이미지 연산 서버(200)는 다시 연산 결과를 복호화하여 전달할 수 있다(S27).

[143] 최종적으로 식별자 디바이스(100)는 복호화된 결과를 출력할 수 있으며(S28), 그 결과는 예를 들어, 사용자와 다른 사용자와의 이미지 일치 여부, 사용자의 식별 정보일 수 있다.

[144] 이상 첨부된 도면을 참조하여 본 발명의 일 실시예들을 더욱 상세하게 설명하였으나, 본 발명은 반드시 이러한 실시예로 국한되는 것은 아니고, 본 발명의 기술사상을 벗어나지 않는 범위 내에서 다양하게 변형 실시될 수 있다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

청구범위

[청구항 1] 사용자의 제1 이미지 데이터를 획득하는 단계;
상기 제1 이미지 데이터를 동형 암호화하는 단계;
이미지 연산 서버로 동형 암호화된 제1 이미지 데이터를 송신하는 단계;
상기 이미지 연산 서버로부터 상기 동형 암호화된 제1 이미지 데이터와 미리 저장된 다른 사용자의 제2 이미지 데이터를 기초로 계산된 동형 암호화된 식별 결과를 수신하는 단계; 및
상기 동형 암호화된 식별 결과를 복호화하는 단계; 를 포함하는 동형 암호화된 이미지를 이용한 개인 식별 방법.

[청구항 2] 제1항에 있어서,
상기 동형 암호화된 제1 이미지 데이터를 송신하는 단계는,
상기 제1 이미지 데이터를 동형 암호화하기 위해 사용된, 동형 암호화 연산을 위한 파라미터를 상기 이미지 연산 서버로 송신하는 단계, 를 더 포함하는 동형 암호화된 이미지를 이용한 개인 식별 방법.

[청구항 3] 제2항에 있어서,
상기 동형 암호화된 식별 결과는,
상기 동형 암호화된 제1 이미지 데이터와 상기 파라미터를 기초로 동형 암호화된 제2 이미지 데이터를 기초로 계산된 식별 결과인, 동형 암호화된 이미지를 이용한 개인 식별 방법.

[청구항 4] 제1항에 있어서,
상기 제2 이미지 데이터는,
상기 이미지 연산 서버에 미리 저장된 복수의 다른 사용자의 이미지 데이터이고,
상기 복호화하는 단계는,
상기 복수의 다른 사용자 중에서 상기 사용자와 매칭되는 다른 사용자에 대한 식별 결과를 획득하는 단계, 를 더 포함하는 동형 암호화된 이미지를 이용한 개인 식별 방법.

[청구항 5] 제1항에 있어서,
상기 제1 이미지 데이터 및 상기 제2 이미지 데이터는,
식별자 디바이스를 통해 촬영된 이미지, 상기 이미지에서 추출된 복수의 특징 좌표 값 및 상기 이미지의 픽셀 별 RGB 값 중 적어도 하나를 포함하는, 동형 암호화된 이미지를 이용한 개인 식별 방법.

[청구항 6] 제1항에 있어서,
상기 동형 암호화하는 단계는,
부분 동형 암호(Partial Homomorphic Encryption), 준동형 암호(Somewhat Homomorphic Encryption) 및 완전 동형 암호(Fully Homomorphic Encryption) 중 어느 하나의 암호화 방법을 이용하여 동형 암호화하는

단계인, 동형 암호화된 이미지를 이용한 개인 식별 방법.

[청구항 7] 식별자 디바이스로부터 동형 암호화된 사용자의 제1 이미지 데이터를 포함하는 연산 요청을 수신하는 단계;
상기 연산 요청에 따라 미리 저장된 다른 사용자의 제2 이미지 데이터를 획득하는 단계;
상기 동형 암호화된 제1 이미지 데이터와 상기 제2 이미지 데이터를 기초로 동형 암호화된 식별 결과를 산출하는 단계; 및
상기 동형 암호화된 식별 결과를 상기 식별자 디바이스로 송신하는 단계;
를 포함하는 동형 암호화된 이미지를 이용한 개인 식별 방법.

[청구항 8] 제7항에 있어서,
상기 연산 요청을 수신하는 단계는,
상기 식별자 디바이스로부터 상기 제1 이미지 데이터를 동형 암호화하기 위해 사용된, 동형 암호화 연산을 위한 파라미터를 수신하는 단계, 를 더 포함하며,
상기 획득하는 단계는,
상기 파라미터를 기초로 상기 제2 이미지 데이터를 동형 암호화하는 단계, 를 더 포함하는, 동형 암호화된 이미지를 이용한 개인 식별 방법.

[청구항 9] 제7항에 있어서,
상기 동형 암호화된 식별 결과를 산출하는 단계는,
상기 동형 암호화된 제1 이미지 데이터에 대응되는 제1 위치와 상기 제2 이미지 데이터에 대응되는 제2 위치를 결정하는 단계, 와
상기 식별 결과에 대응되는 상기 제1 위치와 제2 위치 사이의 거리 값을 계산하는 단계, 를 더 포함하는, 동형 암호화된 이미지를 이용한 개인 식별 방법.

[청구항 10] 제7항에 있어서,
상기 제2 이미지 데이터는,
미리 저장된 복수의 다른 사용자의 제2 이미지 데이터이고,
상기 동형 암호화된 식별 결과를 산출하는 단계는,
상기 수신된 연산 요청의 종류에 따라, 상기 복수의 다른 사용자의 제2 이미지 데이터와 상기 동형 암호화된 제1 이미지 데이터를 기초로 암호화된 식별 결과를 산출하는 단계인, 동형 암호화된 이미지를 이용한 개인 식별 방법.

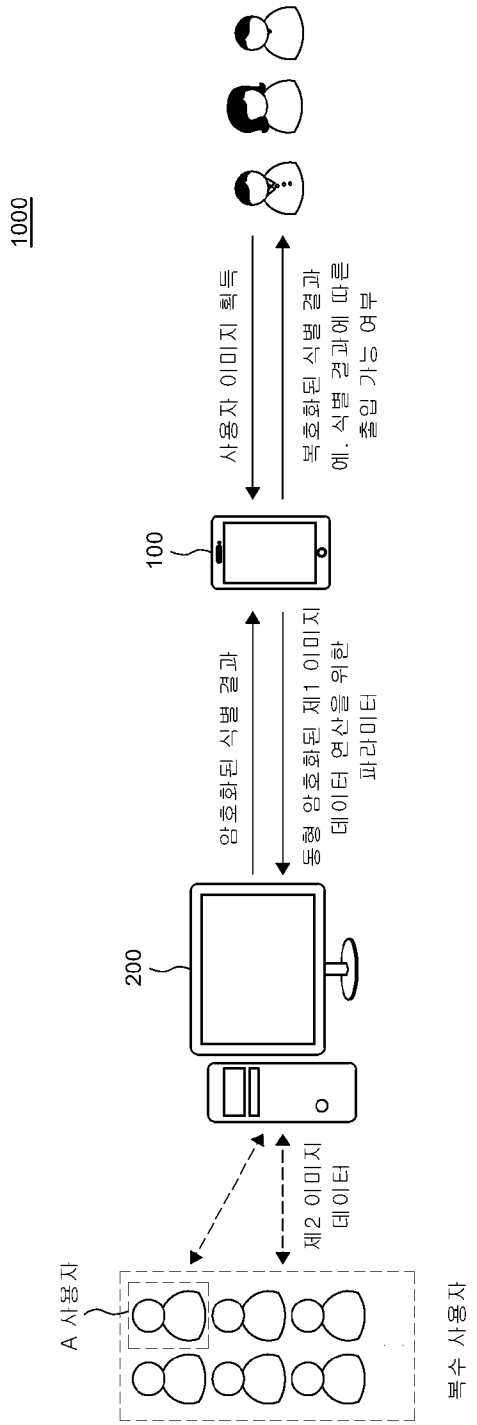
[청구항 11] 제7항에 있어서,
상기 제1 이미지 데이터 및 상기 제2 이미지 데이터는,
상기 식별자 디바이스를 통해 촬영된 이미지, 상기 이미지에서 추출된 복수의 특징점 및 상기 이미지의 픽셀 별 RGB 값 중 적어도 하나를 포함하는, 동형 암호화된 이미지를 이용한 개인 식별 방법.

[청구항 12] 제8항에 있어서,

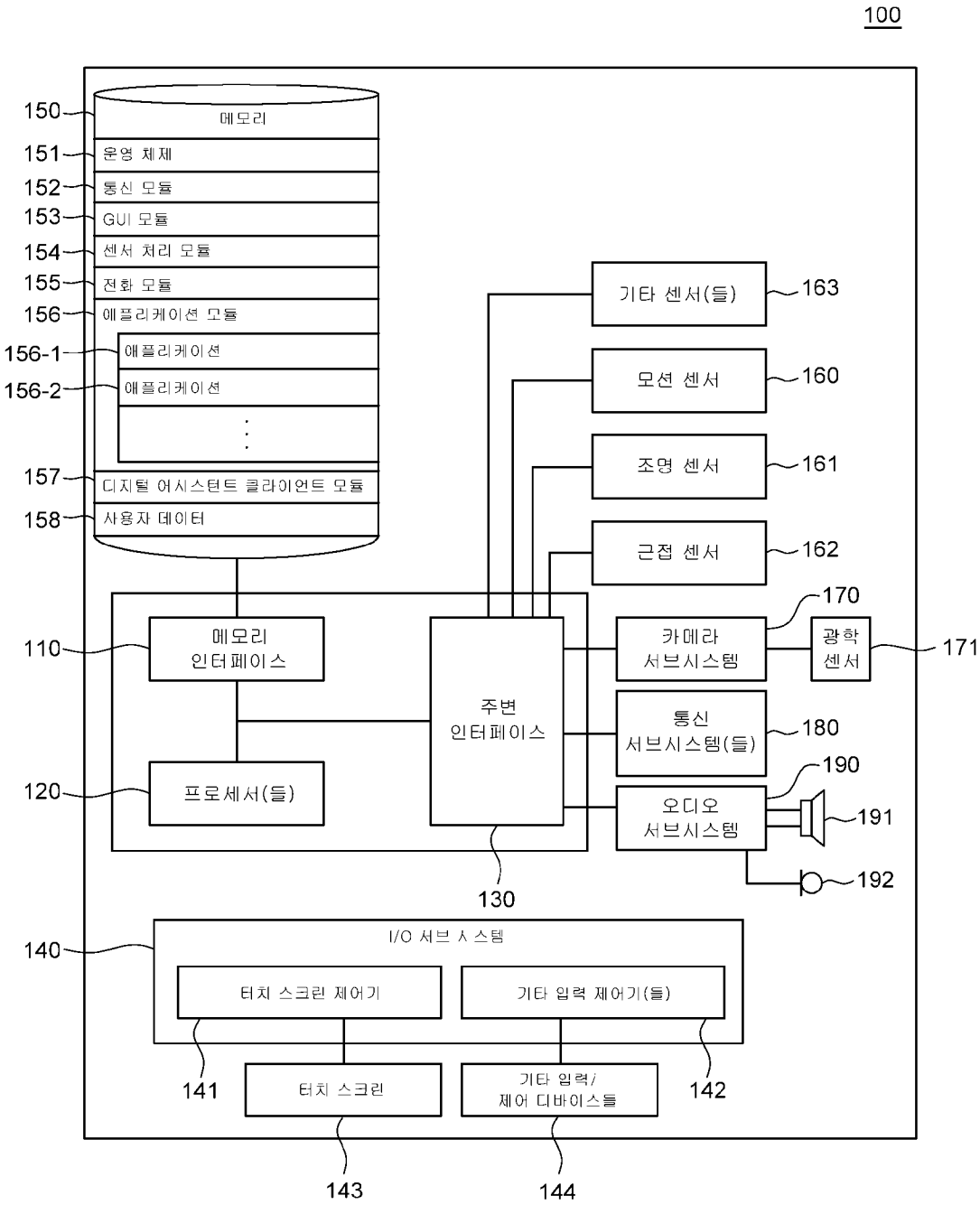
상기 동형 암호화하는 단계는,

부분 동형 암호(Partial Homomorphic Encryption), 준동형 암호(Somewhat Homomorphic Encryption) 및 완전 동형 암호(Fully Homomorphic Encryption) 중 어느 하나의 암호화 방법을 이용하여 동형 암호화하는 단계인, 동형 암호화된 이미지를 이용한 개인 식별 방법.

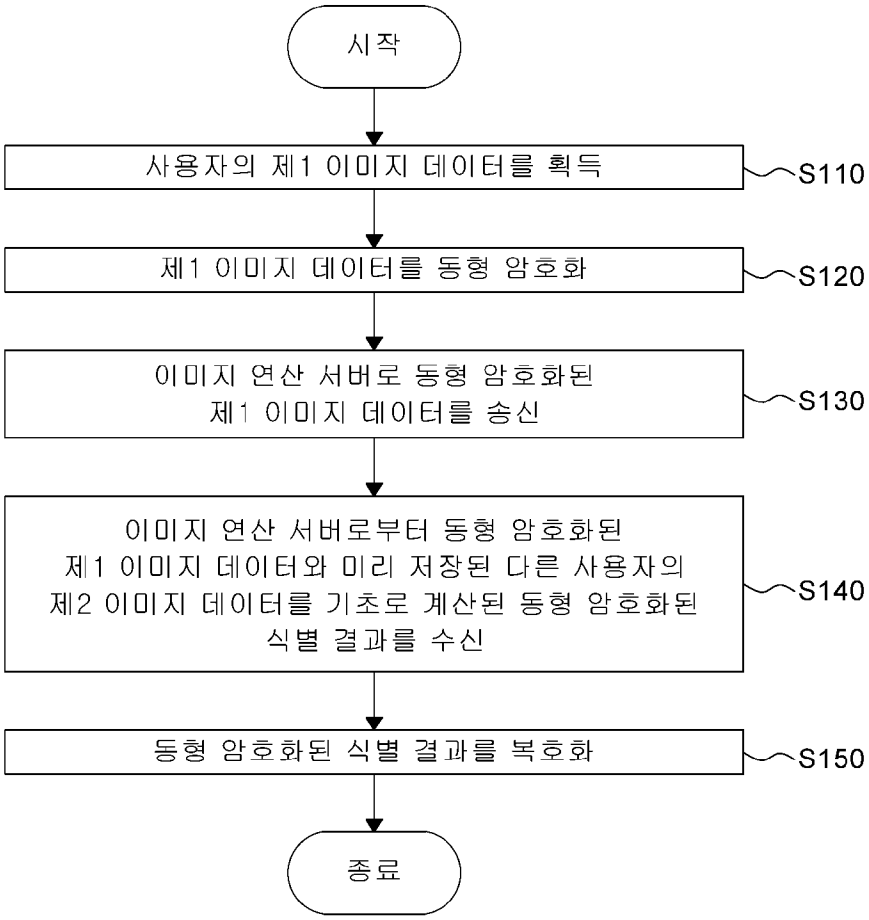
[도1]


1000
사용자 이미지 획득
복호화된 식별 결과
예. 식별 결과에 따른
출입 가능 여부
100
암호화된 식별 결과
동형 암호화된 제1 이미지
데이터 연산을 위한
파라미터
200
제2 이미지
데이터
A 사용자
복수 사용자

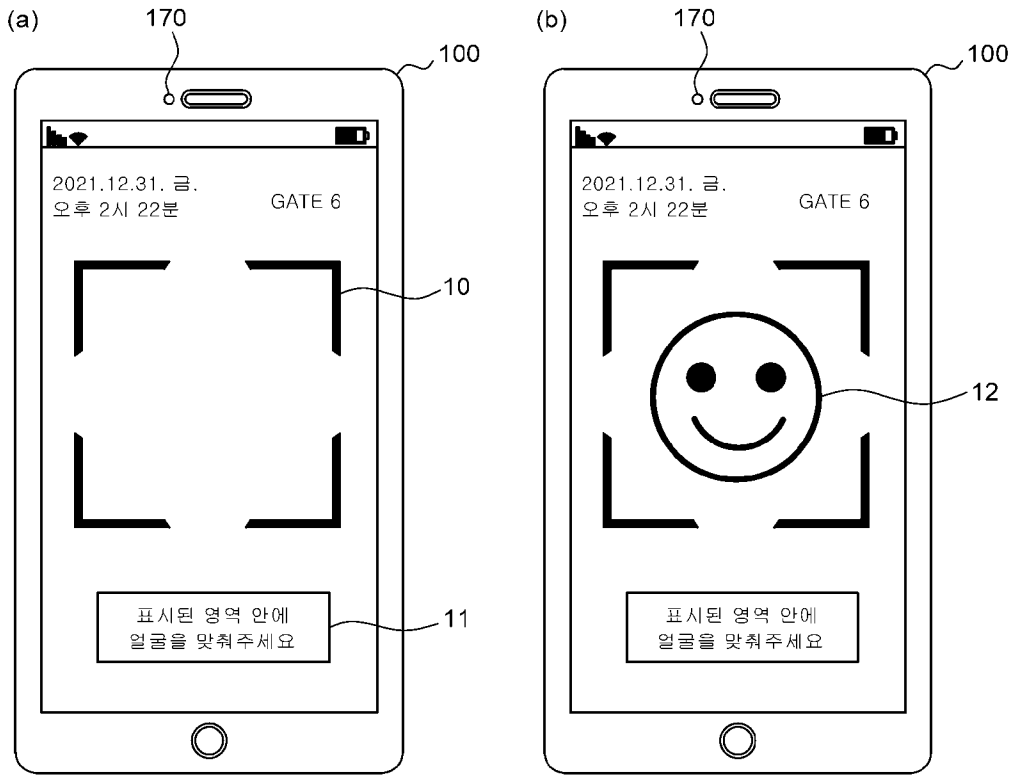
[도2]


100
150
메모리
151
운영 체제
152
통신 모듈
153
GUI 모듈
154
센서 처리 모듈
155
전화 모듈
156
애플리케이션 모듈
156-1
애플리케이션
156-2
애플리케이션
157
디지털 어시스턴트 클라이언트 모듈
158
사용자 데이터
163
기타 센서(들)
160
모션 센서
161
조명 센서
162
근접 센서
170
카메라 서브시스템
171
광학 센서
110
메모리 인터페이스
주변 인터페이스
180
통신 서브시스템(들)
190
오디오 서브시스템
191
192
120
프로세서(들)
130
140
I/O 서브시스템
터치 스크린 제어기
기타 입력 제어기(들)
141
터치 스크린
기타 입력/제어 디바이스들
142
143
144

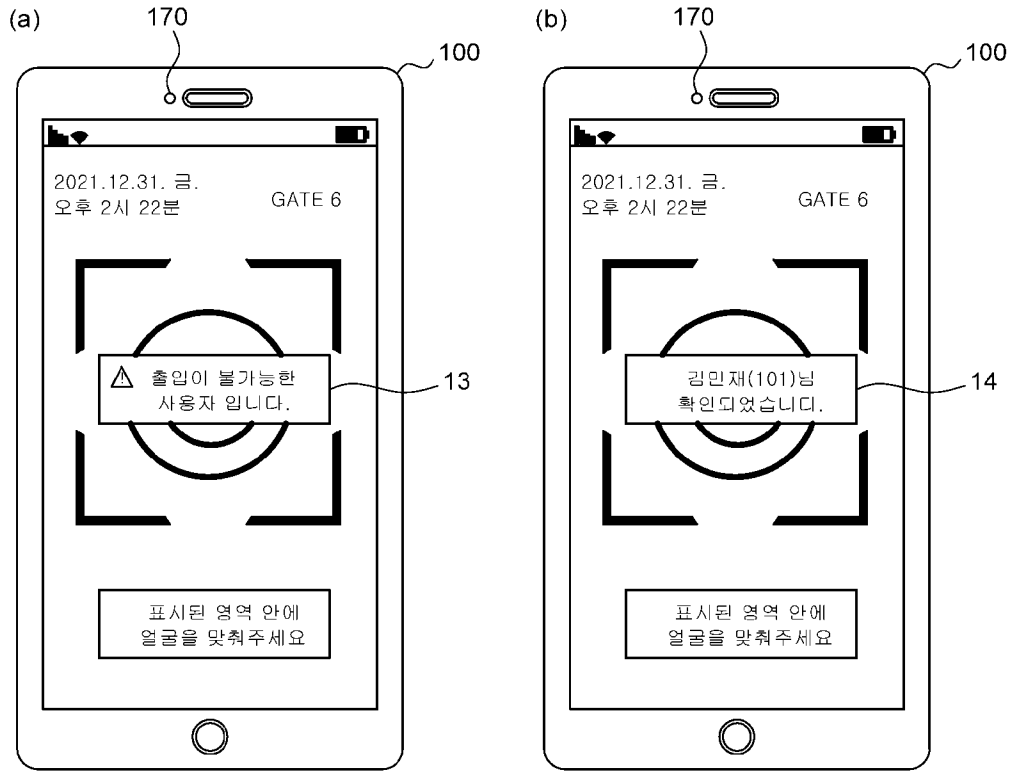
[도3]


시작
사용자의 제1 이미지 데이터를 획득
S110
제1 이미지 데이터를 동형 암호화
S120
이미지 연산 서버로 동형 암호화된
제1 이미지 데이터를 송신
S130
이미지 연산 서버로부터 동형 암호화된
제1 이미지 데이터와 미리 저장된 다른 사용자의
제2 이미지 데이터를 기초로 계산된 동형 암호화된
식별 결과를 수신
S140
동형 암호화된 식별 결과를 복호화
S150
종료

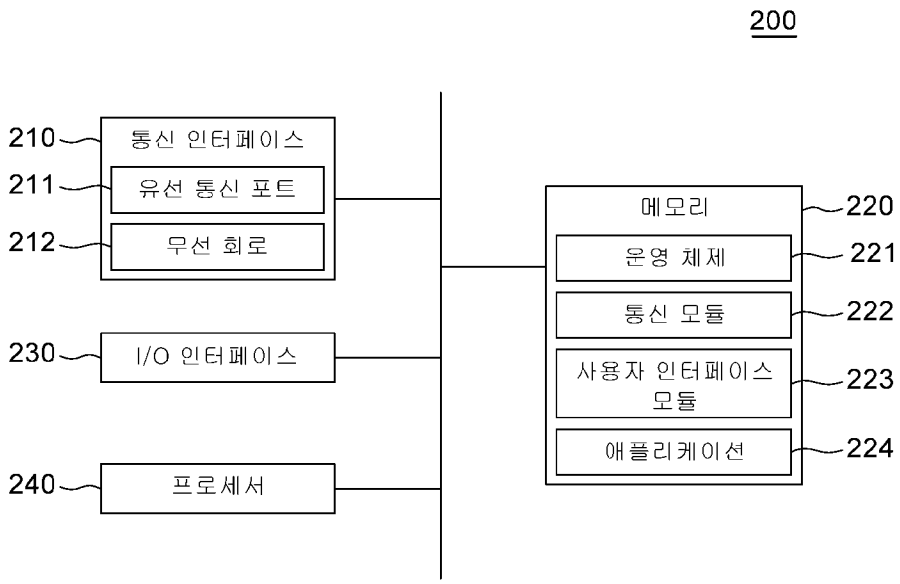
[도4]


(a)
170
100
2021.12.31. 금.
오후 2시 22분
GATE 6
10
표시된 영역 안에
얼굴을 맞춰주세요
11
(b)
170
100
2021.12.31. 금.
오후 2시 22분
GATE 6
12
표시된 영역 안에
얼굴을 맞춰주세요

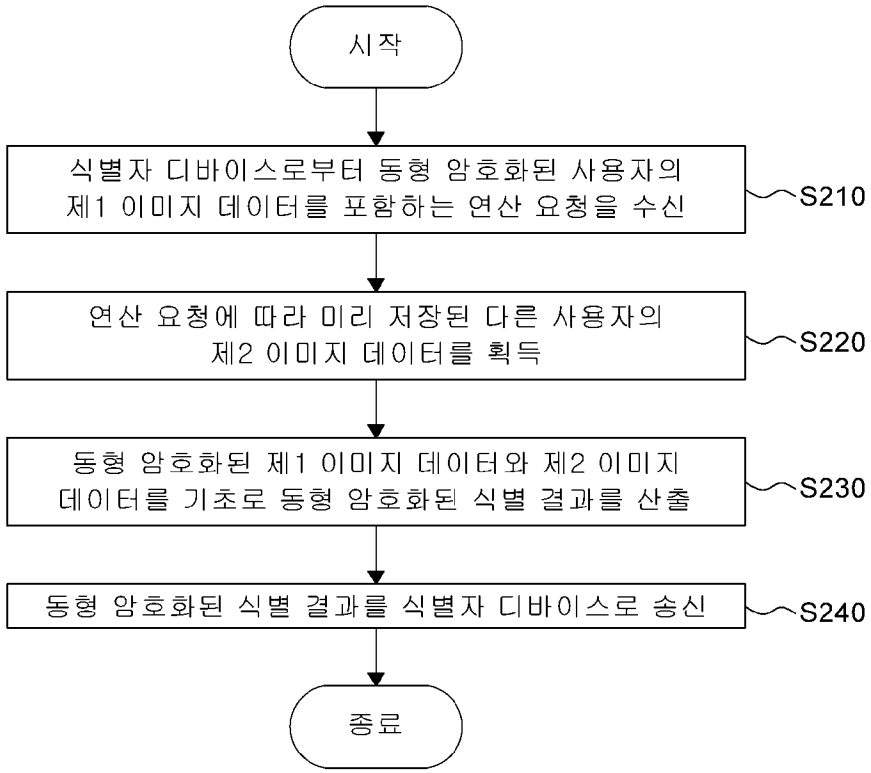
[도5]


(a)
170
100
2021.12.31. 금.
오후 2시 22분
GATE 6
출입이 불가능한
사용자 입니다.
13
표시된 영역 안에
얼굴을 맞춰주세요
(b)
170
100
2021.12.31. 금.
오후 2시 22분
GATE 6
김민재(101)님
확인되었습니다.
14
표시된 영역 안에
얼굴을 맞춰주세요

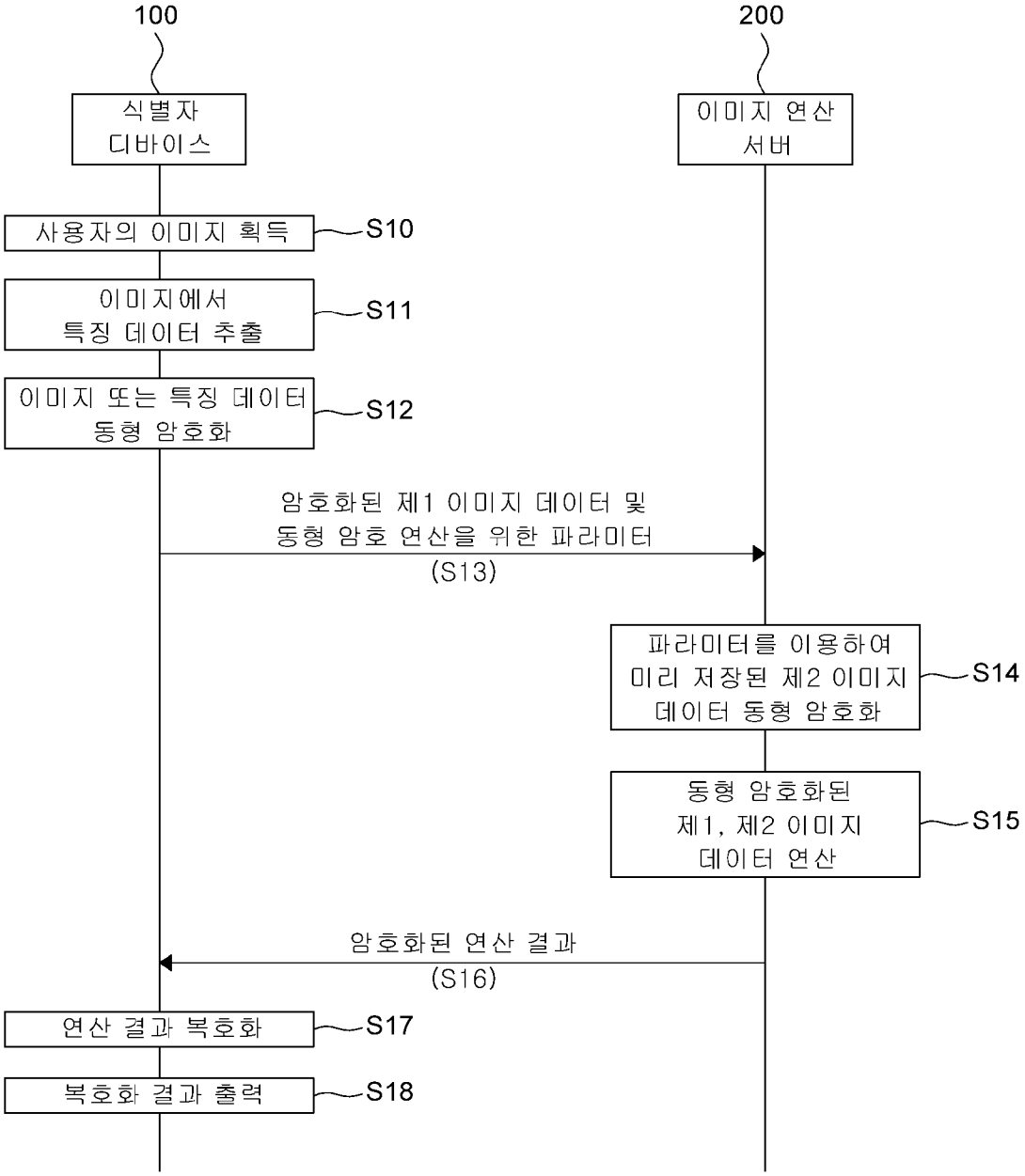
[도6]


200
210
통신 인터페이스
211
유선 통신 포트
212
무선 회로
230
I/O 인터페이스
240
프로세서
메모리
220
운영 체제
221
통신 모듈
222
사용자 인터페이스
모듈
223
애플리케이션
224

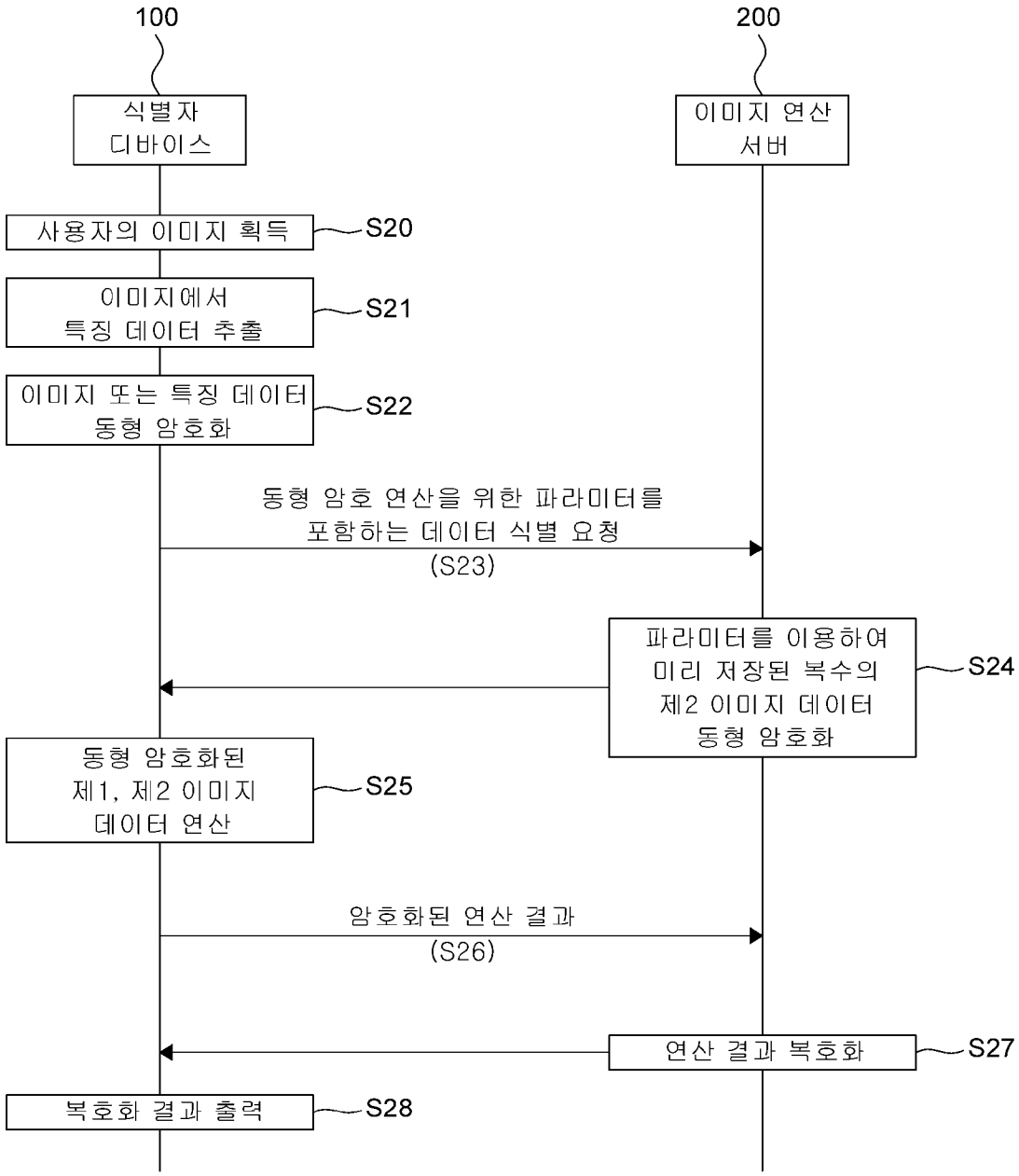
[도7]


시작
식별자 디바이스로부터 동형 암호화된 사용자의 제1 이미지 데이터를 포함하는 연산 요청을 수신
S210
연산 요청에 따라 미리 저장된 다른 사용자의 제2 이미지 데이터를 획득
S220
동형 암호화된 제1 이미지 데이터와 제2 이미지 데이터를 기초로 동형 암호화된 식별 결과를 산출
S230
동형 암호화된 식별 결과를 식별자 디바이스로 송신
S240
종료

[도8]


100
200
식별자 디바이스
이미지 연산 서버
사용자의 이미지 획득
S10
이미지에서 특징 데이터 추출
S11
이미지 또는 특징 데이터 동형 암호화
S12
암호화된 제1 이미지 데이터 및 동형 암호 연산을 위한 파라미터
(S13)
파라미터를 이용하여 미리 저장된 제2 이미지 데이터 동형 암호화
S14
동형 암호화된 제1, 제2 이미지 데이터 연산
S15
암호화된 연산 결과
(S16)
연산 결과 복호화
S17
복호화 결과 출력
S18

[도9]


100
200
식별자 디바이스
이미지 연산 서버
사용자의 이미지 획득
S20
이미지에서 특징 데이터 추출
S21
이미지 또는 특징 데이터 동형 암호화
S22
동형 암호 연산을 위한 파라미터를 포함하는 데이터 식별 요청 (S23)
파라미터를 이용하여 미리 저장된 복수의 제2 이미지 데이터 동형 암호화
S24
동형 암호화된 제1, 제2 이미지 데이터 연산
S25
암호화된 연산 결과 (S26)
연산 결과 복호화
S27
복호화 결과 출력
S28

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2022/019485

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32(2013.01)i; **H04L 9/00**(2006.01)i; **G06V 40/16**(2022.01)i; **G06V 10/10**(2022.01)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 21/32(2013.01); G06F 21/60(2013.01); G06Q 20/32(2012.01); G06Q 20/40(2012.01); G06V 10/10(2022.01); G06V 40/16(2022.01); H04L 29/06(2006.01); H04L 9/32(2006.01)

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: 동형 암호화(homomorphic encryption), 이미지(image), 개인(personal), 식별(identification), 서버(server), 복호화(decryption)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2019-0085674 A (SAMSUNG ELECTRONICS CO., LTD. et al.) 19 July 2019 (2019-07-19) See paragraphs [0119]-[0120], [0127]-[0129] and [0135]; claims 13-14; and figure 4.	1-12
Y	KR 10-1755995 B1 (INHA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) 10 July 2017 (2017-07-10) See paragraphs [0021], [0045], [0050], [0073]-[0074], [0098]-[0099] and [0104]; claim 1; and figures 6 and 8.	1-12
A	US 2019-0220866 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 18 July 2019 (2019-07-18) See paragraphs [0079] and [0099]; and claims 1 and 7.	1-12
A	US 2020-0358611 A1 (INFERATI INC.) 12 November 2020 (2020-11-12) See paragraphs [0029], [0050]-[0051] and [0055]; and claim 1.	1-12
A	CN 110011954 A (ALIBABA GROUP HOLDING LTD.) 12 July 2019 (2019-07-12) See paragraphs [0047]-[0091]; claim 1; and figures 1-3.	1-12

☑ 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
"D" document cited by the applicant in the international application
"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
28 February 2023	**02 March 2023**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **Government Complex-Daejeon Building 4, 189 Cheongsa-ro, Seo-gu, Daejeon 35208**	
Facsimile No. **+82-42-481-8578**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2022/019485

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	KR 10-2404763 B1 (DESILO INC.) 02 June 2022 (2022-06-02) See paragraphs [0012]-[0021]; and claims 1, 6-7 and 12. * This document is a published earlier application that serves as a basis for claiming priority of the present international application.	1-12

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2022/019485

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
KR 10-2019-0085674 A	19 July 2019	KR 10-2411883 B1	22 June 2022
		US 2020-0389303 A1	10 December 2020
		WO 2019-139420 A1	18 July 2019
KR 10-1755995 B1	10 July 2017	None	
US 2019-0220866 A1	18 July 2019	US 11232450 B2	25 January 2022
		US 2022-0108323 A1	07 April 2022
		WO 2019-140157 A1	18 July 2019
US 2020-0358611 A1	12 November 2020	WO 2020-227320 A1	12 November 2020
CN 110011954 A	12 July 2019	CN 110011954 B	14 September 2021
KR 10-2404763 B1	02 June 2022	None	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2022/019485

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/32(2013.01)i; **H04L 9/00**(2006.01)i; **G06V 40/16**(2022.01)i; **G06V 10/10**(2022.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/32(2013.01); G06F 21/60(2013.01); G06Q 20/32(2012.01); G06Q 20/40(2012.01); G06V 10/10(2022.01); G06V 40/16(2022.01); H04L 29/06(2006.01); H04L 9/32(2006.01)

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: 동형 암호화(homomorphic encryption), 이미지(image), 개인(personal), 식별(identification), 서버(server), 복호화(decryption)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2019-0085674 A (삼성전자주식회사 등) 2019.07.19 단락 [0119]-[0120], [0127]-[0129], [0135]; 청구항 13-14; 및 도면 4	1-12
Y	KR 10-1755995 B1 (인하대학교 산학협력단) 2017.07.10 단락 [0021], [0045], [0050], [0073]-[0074], [0098]-[0099], [0104]; 청구항 1; 및 도면 6, 8	1-12
A	US 2019-0220866 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 2019.07.18 단락 [0079], [0099]; 및 청구항 1, 7	1-12
A	US 2020-0358611 A1 (INFERATI INC.) 2020.11.12 단락 [0029], [0050]-[0051], [0055]; 및 청구항 1	1-12
A	CN 110011954 A (ALIBABA GROUP HOLDING LTD.) 2019.07.12 단락 [0047]-[0091]; 청구항 1; 및 도면 1-3	1-12

☑ 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

"D" 본 국제출원에서 출원인이 인용한 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
2023년02월28일(28.02.2023)	**2023년03월02일(02.03.2023)**

ISA/KR의 명칭 및 우편주소

대한민국 특허청
(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)

팩스 번호 **+82-42-481-8578**

심사관

양정록

전화번호 **+82-42-481-5709**

국 제 조 사 보 고 서

국제출원번호
PCT/KR2022/019485

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
PX	KR 10-2404763 B1 (주식회사 디사일로) 2022.06.02 단락 [0012]-[0021]; 및 청구항 1, 6-7, 12 * 위 문헌은 본 국제출원의 우선권주장의 기초가 되는 선출원의 공개된 공보임.	1-12

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2022/019485

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2019-0085674 A	2019/07/19	KR 10-2411883 B1	2022/06/22
		US 2020-0389303 A1	2020/12/10
		WO 2019-139420 A1	2019/07/18
KR 10-1755995 B1	2017/07/10	없음	
US 2019-0220866 A1	2019/07/18	US 11232450 B2	2022/01/25
		US 2022-0108323 A1	2022/04/07
		WO 2019-140157 A1	2019/07/18
US 2020-0358611 A1	2020/11/12	WO 2020-227320 A1	2020/11/12
CN 110011954 A	2019/07/12	CN 110011954 B	2021/09/14
KR 10-2404763 B1	2022/06/02	없음	