

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2018년 5월 17일 (17.05.2018) WIPO | PCT



(10) 국제공개번호
WO 2018/088867 A1

- (51) 국제특허분류:
G06Q 20/32 (2012.01) G06F 21/32 (2013.01)
G06Q 20/40 (2012.01) G06K 9/00 (2006.01)
G06Q 20/38 (2012.01)
- (21) 국제출원번호: PCT/KR2017/012829
- (22) 국제출원일: 2017년 11월 14일 (14.11.2017)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2016-0151016 2016년 11월 14일 (14.11.2016) KR
- (72) 발명자: 겸
- (71) 출원인: 이선관 (LEE, Seon Gwan) [KR/KR]; 61265 광주광역시 북구 북문대로 235, 105동 708호, Gwangju (KR).
- (74) 대리인: 정은열 (JUNG, Eun Youl); 06025 서울시 강남구 논현로154길 16 삼릉빌딩 5층 (정앤김 특허법률사무소), 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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ,

LA, LC, LK, LR, LS, 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, SA, 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.

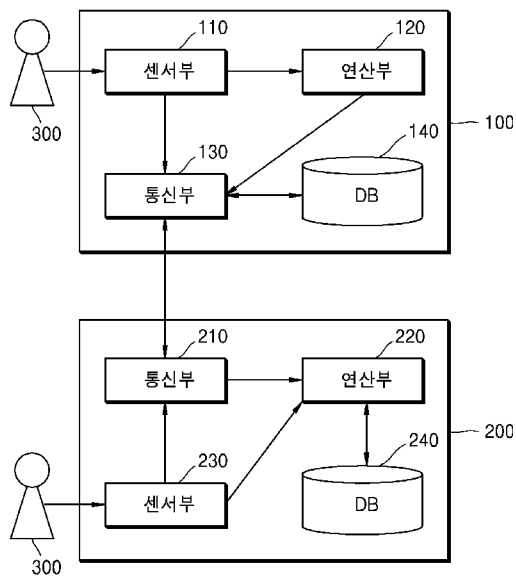
- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,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

공개:

- 국제조사보고서와 함께 (조약 제21조(3))
- 청구범위 보장 기한 만료 전의 공개이며, 보정서를 접수하는 경우 그에 관하여 별도 공개함 (규칙 48.2(h))

(54) Title: FINANCIAL PAYMENT METHOD AND PAYMENT SYSTEM USING MOBILE DEVICE

(54) 발명의 명칭: 모바일 디바이스를 이용한 금융 결제 방법 및 결제 시스템



110, 230 ... Sensor unit
120, 220 ... Computing unit
130, 210 ... Communication unit

(57) Abstract: The present invention relates to a financial payment method using biometric information, in which biometric information of an individual collected in a mobile device of a franchise is transmitted to a mobile device of the individual so that the biometric information can be authenticated in the mobile device of the individual, and after the authentication of the biometric information, a substitute key corresponding to a card password preset by the individual is inputted and a financial payment is requested according to the payment content.

(57) 요약서: 본 발명은 생체정보를 이용하여 금융결제를 하는 방법에 관한 것으로, 가맹점 측의 모바일 디바이스에서 수집된 개인의 생체정보를 해당 개인의 모바일 디바이스에 전송하여, 개인의 모바일 디바이스 내에서 생체정보의 인증이 이루어지고, 생체정보 인증 후 개인이 미리 설정해 놓은 카드 비밀번호에 대응되는 대체키를 입력받아 결제 내용에 따라 금융 결제를 요청하는 방법이다.

WO 2018/088867 A1

명세서

발명의 명칭: 모바일 디바이스를 이용한 금융 결제 방법 및 결제 시스템

기술분야

- [1] 모바일 디바이스를 이용한 금융 결제 방법 및 결제 시스템에 연관되며, 보다 구체적으로는 두 개의 모바일 디바이스에서 생체 정보 및 금융 정보를 상호 확인하여 결제하는 방법 및 시스템에 연관된다.

배경기술

- [2] 2007년 미국에서 처음으로 지문인식을 이용하여 결제하는 시스템이 사기업에 도입되었으나, 개인의 생체 정보가 제3자의 특정 기기에 저장되어 있다거나, 해킹 등의 위험에 노출되어 있는 네트워크를 통해 접근 가능하다는 점이 개인 정보 보호에 미흡한 단점을 가지고 있어 현재 널리 보편화되어 사용되고 있지 못하다. 또한, 지문인식 결제 시스템은 지문인식을 위한 고가의 지문인식 센서를 모든 오프라인 가맹점에 구비되어야 한다는 비용 부담이 있다. 실제로 2007년에 지문인식 결제 시스템을 도입한 해당 기업은 200만 달러에서 300만 달러 정도의 비용이 드는 결제 POS 기기의 설치로 인한 적자 문제로 파산하였다.
- [3] 최근 일본정부에서는 지문 인식을 이용한 또 다른 결제 시스템을 시도하고 있다. 일본을 찾은 여행객이 공항에서 지문 판독 장치에 두 손가락을 인식시키고 신용카드 정보를 입력하면 일본 내 지문인식이 가능한 상점이나 호텔에서 지문 인식만으로 결제할 수 있는 방식이다. 이를 위해 일본 정부는 도쿄 올림픽이 열리는 2020년까지 전국 각지에 지문 인식 결제 인프라를 구축하겠다고 밝혔다. 정부 단계에서 지문인식 결제를 위한 인프라를 구축하고자 시도하는 것으로 보편화 가능성은 높을 수 있지만, 비용 단점 및 개인 정보 보호에 미흡한 문제점은 미국의 경우와 동일한 한계를 가진다.
- [4] (특허문헌 1) 대한민국 특허공보 제10-0997820호 (2010.12.01)

발명의 상세한 설명

기술적 과제

- [5] 실시예들에 따르면, 실물카드 없이 언제 어디서나 모바일 디바이스를 이용하여 금융 결제를 할 수 있다. 또한 별도의 인프라를 구축할 필요 없이 널리 보편화되어 이미 다수가 소지하고 있는 모바일 디바이스를 이용하여 금융 결제를 진행할 수 있다.
- [6] 개인이 소지한 모바일 디바이스에 개인의 주민번호, 지문 등과 같은 개인 정보 및 카드 번호, 카드 비밀번호 등의 금융 정보를 저장해두고, 각각 금융 결제 시에 개인의 모바일 디바이스에서 개인 정보 및 금융 정보를 확인하게 함으로써, 개인 정보 및 금융 정보의 노출 없이 안전한 금융 결제를 할 수 있다.

과제 해결 수단

- [7] 일측에 따르면, 판매자의 제1 모바일 디바이스가 금융 결제를 인증하는 방법에 있어서, 상기 제1 모바일 디바이스에 구비된 센서를 이용하여 구매자의 하나 이상의 생체 정보를 센싱하는 단계; 상기 제1 모바일 디바이스가 미리 지정된 방법으로 상기 구매자에 대응하여 식별되는 제2 모바일 디바이스에 상기 센싱한 생체 정보를 전송하는 단계; 상기 제2 모바일 디바이스로부터 상기 전송한 생체 정보가 상기 구매자의 제2 모바일 디바이스에 미리 저장된 상기 구매자의 생체 정보와 일치하는지 여부를 수신하는 단계; 및 상기 제1 모바일 디바이스가 전송한 생체 정보와 상기 제2 모바일 디바이스에 저장된 생체 정보가 일치하는 경우 상기 제1 모바일 디바이스가 결제 내용을 인증하는 단계를 포함하는 방법이 제공된다.
- [8] 일실시예에서, 상기 생체 정보는 지문 정보, 홍채 정보, 정맥 정보, 심전도 정보, 또는 음성 정보 중 어느 하나 이상을 포함할 수 있다.
- [9] 일실시예에서, 상기 구매자의 제2 모바일 디바이스에 미리 지정된 결제 방식으로 상기 결제 내용을 진행하는 단계를 더 포함하고, 상기 미리 지정된 결제 방식은, 하나 이상의 결제 수단 중에서 상기 구매자가 선택한 제1 결제 수단에 대해서 상기 제1 결제 수단의 비밀번호에 대응하는 대체키로 상기 제1 결제 수단을 사용하기 위한 인증을 수행할 수 있다. 상기 실시예에서 상기 대체키는 상기 제1 모바일 디바이스에 표시되는 입력키 조합 중에서 상기 구매자가 상기 비밀번호의 각 자리에 대응되도록 미리 설정한 것일 수 있다. 또한 상기 실시예에서 상기 제1 결제 수단은 상기 결제 내용에 적응적으로 상기 미리 지정된 하나 이상의 결제 방식 중에서 선택된 것일 수 있다.
- [10] 일실시예에서, 상기 센싱한 생체 정보를 전송하는 단계는, 상기 생체 정보를 미리 설정된 암호화 방법으로 암호화하거나, 상기 생체 정보를 미리 지정된 형태의 파일로 변환하여 전송할 수 있다. 상기 실시예에서, 상기 미리 설정된 암호화 방법은 RC4, OTPad, DES, TDES, AES, IDEA, Diffie-Hellman, DSA, Elgamal, RSA, ECC, SHA, MD5, HAVAL, HMAC, CBC-MAC 중 어느 하나일 수 있고, 상기 미리 지정된 형태의 파일은 이미지 파일, 동영상 파일, 음성 파일 중 어느 하나일 수 있다. 상기 센싱한 생체 정보에 따라 적응적으로 상기 파일의 형태가 결정될 수 있다.
- [11] 다른 일측에 따르면, 구매자에 대응하여 식별되는 제2 모바일 디바이스가 금융 결제를 수행하는 방법에 있어서, 판매자의 제1 모바일 디바이스로부터 구매자의 생체 정보를 수신하는 단계; 상기 수신된 구매자의 생체 정보와 상기 제2 모바일 디바이스에 미리 저장된 상기 구매자의 생체 정보가 일치하는지 확인하는 단계; 상기 수신된 구매자의 생체 정보와 상기 제2 모바일 디바이스에 저장된 구매자의 생체 정보가 일치하는 경우, 상기 제1 모바일 디바이스로부터 인증된 결제 내용을 수신하는 단계; 및 상기 결제 내용에 대하여 미리 설정된 결제 방식으로 결제를 수행하는 단계를 포함하는 방법이 제공된다.
- [12] 일실시예에서, 상기 구매자로부터 하나 이상의 생체 정보 및 하나 이상의 결제

방식을 입력 받는 단계를 더 포함할 수 있다.

- [13] 일실시에에서는 상기 하나 이상의 결제 방식 중 선택된 제1 결제 수단에 대해서, 상기 구매자로부터 입력 받은 상기 제1 결제 수단의 비밀번호에 대응하는 대체키를 이용하여 상기 결제를 수행할 수 있다. 상기 실시예에서, 상기 대체키는 상기 제1 모바일 디바이스에 표시되는 입력키 조합 중에서 상기 구매자의 입력에 의해 상기 비밀번호의 각 자리에 대응되는 것일 수 있다.
- [14] 일실시에에서, 상기 하나 이상의 결제 방식은 결제금액 할인, 포인트 적립, 또는 사용실적 누적금액 중 미리 설정된 우선순위에 의해 결정될 수 있고, 상기 결제 내용에 따라 적응적으로 상기 우선순위를 반영할 수 있다.
- [15] 또 다른 일측에 따르면, 적어도 하나의 프로세서를 포함하는 컴퓨팅 장치에 있어서, 상기 적어도 하나의 프로세서에 의해 적어도 일시적으로 구현되는: 구매자의 하나 이상의 생체 정보를 센싱하는 센서부; 미리 지정된 방법으로 상기 구매자로 식별되는 제2 모바일 디바이스에 상기 센싱한 생체 정보를 전송하고, 상기 전송에 대한 응답으로 상기 제2 모바일 디바이스로부터 상기 전송한 생체 정보가 상기 구매자의 제2 모바일 디바이스에 미리 저장된 상기 구매자의 생체 정보와 일치하는지 여부를 수신하는 통신부; 및 상기 전송한 생체 정보와 상기 제2 모바일 디바이스에 저장된 구매자의 생체 정보가 일치하는 경우 결제 내용을 인증하는 연산부를 포함하는 컴퓨팅 장치가 제공된다.
- [16] 또 다른 일측에 따르면, 컴퓨터 판독 가능 기록매체에 저장되어, 컴퓨팅 장치가 구매자 생체 정보 및 금융 정보에 기초하여 금융 결제를 진행하는 프로그램에 있어서: 판매자의 제1 모바일 디바이스로부터 구매자의 생체 정보를 수신하는 명령어 세트; 상기 수신된 구매자의 생체 정보와 상기 컴퓨팅 장치에 미리 저장된 상기 구매자의 생체 정보가 일치하는지 확인하고, 상기 제1 모바일 디바이스에 확인 결과를 전송하는 명령어 세트; 및 상기 수신한 구매자의 생체 정보와 상기 컴퓨팅 장치에 저장된 구매자의 생체 정보가 일치하는 경우, 상기 제1 모바일 디바이스로부터 인증된 결제 내용을 수신하여, 상기 구매자의 하나 이상의 결제 방식 중 선택된 제1 결제 수단으로 상기 구매자로부터 입력 받은 상기 제1 결제 수단의 비밀번호에 대응하는 대체키를 이용하여 결제를 진행하는 명령어 세트를 포함하는 기록매체에 저장된 프로그램이 제공된다.

발명의 효과

- [17] 실시예들에 따르면, 높은 수준의 개인정보 보호가 요구되는 개인의 생체 정보를 이용하여 금융 결제를 하는 경우에도 생체 정보가 개인의 모바일 디바이스 외에 다른 기기에 노출되는 위험이 없다.
- [18] 현재 이미 보편화되어 있는 모바일 디바이스를 이용함으로써 별도의 인프라 구축 없이 소비자 측인 개인과 공급자 측인 사업자 모두 적은 비용으로 생체 정보를 이용한 금융 결제를 할 수 있다.
- [19] 사용자가 미리 설정한 다양한 결제 방식으로 금융 결제를 진행할 수 있으며,

금융 결제 수단의 비밀번호에 대응하는 대체키를 이용함으로써 가맹점 모바일 디바이스 측에 사용자의 비밀번호가 그대로 노출되는 것을 방지할 수 있다.

도면의 간단한 설명

- [20] 도 1은 일실시예에 따라 두 개의 모바일 디바이스를 이용하여 생체 정보를 확인하여 금융 결제를 진행하는 시스템의 블록도이다.
- [21] 도 2는 일실시예에 따른 소비자의 생체 정보를 확인하여 금융 결제를 진행하는 방법의 순서도이다.
- [22] 도 3은 일실시예에 따른 가맹점의 결제 정보를 확인하여 금융 결제를 진행하는 방법의 순서도이다.
- [23] 도 4는 일실시예에 따라 사용자 모바일 디바이스, 가맹점 모바일 디바이스 및 카드사 서버간의 상호작용을 나타낸 시퀀스 다이어그램이다.
- [24] 도 5a 및 도 5b는 일실시예에 따라 모바일 디바이스에서 표시하는 대체키 입력판의 예시이다.
- [25] 도 6은 일실시예에 따라 대체키의 각 자리를 입력할 때마다 도 5a의 입력판이 재배치되는 예시이다.

발명의 실시를 위한 최선의 형태

- [26] 이하에서, 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다. 그러나, 이러한 실시예들에 의해 권리범위가 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.
- [27] 아래 설명에서 사용되는 용어는, 연관되는 기술 분야에서 일반적이고 보편적인 것으로 선택되었으나, 기술의 발달 및/또는 변화, 관례, 기술자의 선호 등에 따라 다른 용어가 있을 수 있다. 따라서, 아래 설명에서 사용되는 용어는 기술적 사상을 한정하는 것으로 이해되어서는 안 되며, 실시예들을 설명하기 위한 예시적 용어로 이해되어야 한다.
- [28] 또한 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 설명 부분에서 상세한 그 의미를 기재할 것이다. 따라서 아래 설명에서 사용되는 용어는 단순한 용어의 명칭이 아닌 그 용어가 가지는 의미와 명세서 전반에 걸친 내용을 토대로 이해되어야 한다.
- [29]
- [30] 도 1은 일실시예에 따라 두 개의 모바일 디바이스를 이용하여 생체 정보를 확인하여 금융 결제를 진행하는 시스템의 블록도이다. 일실시예에서는 가맹점(판매자)의 모바일 디바이스(100)와 사용자(구매자)의 모바일 디바이스(200) 간의 생체 정보 및 금융 정보를 확인하는 등 상호작용을 통해 사용자(구매자, 소비자, 개인)와 가맹점(판매자, 공급자, 사업자)간의 금융 결제를 할 수 있다.
- [31] 가맹점의 모바일 디바이스(100)는 사용자(300)로부터 지문, 홍채 등과 같은 생체 정보를 센싱할 수 있는 센서부(110), 유선 또는 무선의 네트워크를 통해

다른 기기와 데이터를 전송 및 수신할 수 있는 통신부(130), 결제 내용을 생성하거나 결제를 요청, 승인할 수 있는 연산부(120), 및 데이터 베이스(DB, 140)을 포함한다.

- [32] 사용자의 모바일 디바이스(200)는 사용자(300)로부터 지문, 홍채 등과 같은 생체 정보를 센싱할 수 있는 센서부(230), 유선 또는 무선의 네트워크를 통해 다른 기기와 데이터를 전송 및 수신할 수 있는 통신부(210), 데이터의 일치 여부를 확인하거나, 이를 위해 암호화 또는 복호화를 하거나, 개인 정보, 생체 정보, 금융 정보 등을 미리 설정할 수 있는 연산부(220), 및 개인 정보, 생체 정보, 금융 정보 등의 개인 정보 보안이 필요한 데이터를 저장할 수 있는 데이터 베이스(DB, 240)을 포함한다.
- [33] 일실시에에 따라 사용자(300)가 금융 결제를 하기 위해서 가맹점의 모바일 디바이스(100)를 통해 자신(300)의 생체 정보를 센싱하고, 사용자의 모바일 디바이스(200)를 통해 센싱한 생체 정보를 인증한 후, 미리 설정된 사용자의 결제 방식에 따라 예를 들어 미리 등록된 신용카드로 해당 금융 결제를 진행하기 위해서 사용자는 가맹점의 모바일 디바이스(100)에서 대체키를 입력하고, 다시 사용자의 모바일 디바이스(200)를 통해 입력한 대체키를 인증한 후, 해당 신용카드로 사용자의 모바일 디바이스(200)에서 결제를 요청하면, 해당 신용카드사의 서버(미도시)를 통해 결제가 진행될 수 있다. 일실시에에 따른 금융 결제 방법은, 개인정보보호가 필요한 사용자의 개인정보, 생체정보, 금융정보를 모두 직접 사용자의 모바일 디바이스(200)를 통해 인증함으로써 높은 수준의 정보 보호가 이루어질 수 있으며, 사용자가 실물 카드 없이 자신의 생체 정보 및 미리 자신의 모바일 디바이스(200)에 설정해 둔 정보(개인정보, 생체정보, 금융정보 등)을 이용해 어디서든 가맹점의 모바일 디바이스(100)를 통해 직접 금융 결제를 진행할 수 있다.
- [34] 보다 구체적으로 가맹점의 모바일 디바이스(100)와 사용자의 모바일 디바이스(200) 간의 상호작용을 도 2 및 도 3을 통해 상세히 설명하고자 한다.
- [35]
- [36] 도 2는 일실시에에 따른 소비자의 생체 정보를 확인하여 금융 결제를 진행하는 방법의 순서도이다. 가맹점의 모바일 디바이스에서 소비자의 생체 정보를 확인하여 금융 결제를 진행할 때 다음의 단계들을 포함할 수 있다.
- [37] 201 단계에서는, 사용자의 하나 이상의 생체 정보를 센싱한다. 사용자는 결제를 하고자 하는 개인 즉 소비자를 의미한다. 생체 정보는 지문, 홍채, 특정 위치에 대한 정맥, 심전도, 또는 음성 등이 될 수 있다. 나아가 지문의 경우 사용자의 설정에 의한 특정 손가락에 대한 지문, 예를 들어 왼손의 약지 손가락 지문을 센싱할 수 있으며, 홍채의 경우도 오른쪽 눈동자, 왼쪽 눈동자, 또는 양쪽 눈동자 모두 중 어느 하나를 사용자가 미리 설정해두고, 이를 사용자가 센싱 대상으로 이용할 수 있다. 특정 위치에 대한 정맥 역시 오른쪽 손바닥에 위치한 정맥 정보, 또는 왼쪽 손목에 위치한 정맥 정보 등과 같이 위치를 사용자가 미리 설정해 둘

수 있다. 음성의 경우 육성 외에 개인의 휘파람 소리, 기침 소리 등 다양한 형태가 가능하고 육성의 경우 특정 단어, 문장, 이름 등을 말하는 것으로 미리 설정해 둘 수 있다. 이와 같이 생체 정보는 단순히 사용자의 신체 일부를 센싱하는 것을 의미하는 것 외에 사용자가 직접 미리 설정해 놓은 종류를 선택하여 이용하는 것으로써 금융 거래를 위한 높은 수준의 보안이 형성되는 것을 의미한다. 즉, 금융 거래를 위해 어떠한 생체 정보를 이용할 것인지 선택의 폭이 넓고 개인이 스스로(다른 어떠한 주체와 공유하지 않고) 설정한 것이기 때문이다.

[38] 예시적으로 사용자 A는 자신의 모바일 디바이스('제2 모바일 디바이스'라 함)에 왼손 약지 손가락의 지문을 사전에 등록해 놓고, 가맹점 모바일 디바이스('제1 모바일 디바이스'라 함)를 통해 왼손 약지 손가락의 지문을 인식시킴으로써 201 단계에서 사용자 A의 지문 정보를 생체 정보로써 센싱할 수 있다.

[39] 202 단계에서는 가맹점의 모바일 디바이스에서 미리 지정된 방법으로 센싱한 생체 정보를 사용자의 모바일 디바이스에 전송한다. 전송 대상이 되는 사용자의 모바일 디바이스는 사용자의 입력에 의해 식별되어 특정될 수 있다. 즉, 사용자 측에서는 자신의 생체 정보를 센싱시키고 자신의 모바일 디바이스 번호를 입력함으로써 자신의 정보를 인증하는 수단을 가맹점 측에 제시하게 되는 것이다.

[40] 생체 정보는 그 종류가 다양하기 때문에 각 정보의 종류에 따라 전송되는 파일의 형태가 다를 수 있다. 또한 생체 정보의 특성상 보안을 위해 다양한 방법으로 암호화 하거나 그 자체의 파일 형태 대신에 지정된 형태의 파일로 변환하여 전송할 수 있다. 예를 들어, 지문 정보는 이미지 파일로 생성되어 SHA 방식으로 암호화하여 전송할 수 있다. 이때 이미지 파일은 다양한 확장자 중에 선택된 한 종류로 변형될 수 있다. 또는 지문 정보가 동영상 파일로 생성될 수도 있다.

[41] 암호화 방법은 실시자가 적절히 선택하여 실시할 수 있으며, 양방향 암호화 방법으로 대칭키 방식의 RC4, OTPad, DES, TDES, AES, IDEA 등이 있고, 비대칭키 방식의 Diffie-Hellman, DSA, Elgamal, RSA, ECC 등이 있다.

[42] 무결성을 보장하는 일방향 암호화 방법으로는 SHA, MD5, HAVAL, HMAC, CBC-MAC 등이 있다. 다양한 실시예들에서는 다양한 방식의 암호화 방법을 선택하여 실시할 수 있다. 특히, 생체 정보의 종류에 따라서 최적의 암호화 방법을 선택함으로써 전송되는 생체 정보가 노출되는 위험을 1차 방지한다. 나아가 실시예들에서 만약 전송되는 생체 정보가 네트워크 상에서 권한이 없는 제3자에 노출되는 경우에도 해당 생체 정보의 개인에 대한 정보가 없기 때문에 노출된 센싱 생체 정보만으로는 개인 정보가 노출되었다고 볼 수 없다. 따라서 일실시예들에서 사용자가 자신의 생체 정보를 가맹점 모바일 디바이스에 노출시켰다고 할지라도 사용자의 개인정보 없이 생체 정보만 존재하기 때문에 진정한 의미의 개인 정보 노출이 되기 어렵다.

[43] 203 단계에서는 사용자의 모바일 디바이스로부터 전송한 생체 정보가

사용자의 모바일 디바이스에 미리 저장된 사용자의 생체 정보와 일치하는지 여부를 수신한다. 전송하는 생체 정보는 가맹점의 모바일 디바이스에서 센싱한 데이터이고, 사용자의 모바일 디바이스에 저장되어 있는 생체 정보는 사용자가 미리 저장해 둔 데이터로써, 두 데이터가 일치하는 경우 사용자의 생체 정보로써 사용자를 금융 거래의 주체로 사용자의 모바일 디바이스에 생체 정보와 함께 미리 저장된 개인 정보, 금융 정보를 이용하여 금융 거래를 할 수 있다. 예시적으로, 사용자 A가 자신의 지문 정보를 가맹점의 모바일 디바이스에 센싱시키고, 자신의 모바일 디바이스 번호를 입력하면, 가맹점의 모바일 디바이스는 센싱한 생체 정보가 사용자 A의 것이 맞는지 확인하기 위하여 사용자 A의 모바일 디바이스에 정보를 전송하고, 일치 여부 결과를 수신할 수 있다. 사용자 A의 모바일 디바이스는 사용자 A의 생체 정보를 수신한 경우, 일치한다(204단계-예)는 결과를 가맹점의 모바일 디바이스에 전송할 수 있고, 이것은 사용자 A의 모바일 디바이스에 미리 저장된 사용자 A의 개인 정보 및 금융 정보(예를 들어, 신용카드 정보 등)를 통해 금융 결제를 할 수 있도록 인증된 것을 의미한다.

[44] 만약, 사용자 A의 모바일 디바이스에 저장된 생체 정보와 가맹점의 모바일 디바이스에 센싱된 생체 정보가 일치하지 않는 경우, 금융 결제는 진행되지 않고 종료된다(204 단계-아니오). 다시 말해, 사용자 A의 모바일 디바이스에 저장된 사용자 A의 개인 정보 및 금융 정보로 금융 결제를 진행할 수 없는 것을 의미한다.

[45] 다시, 두 생체 정보가 일치하는 경우(204 단계-예) 205 단계로 진행하여, 결제 내용을 인증하게 된다. 결제 내용이란 인증된 사용자에게 대하여 가맹점에서 생성한 결제 상세 내역을 의미한다. 예시적으로, 사용자 A가 8000원짜리 점심 식사를 한 후 음식점(가맹점)의 모바일 디바이스에 자신의 지문을 센싱시키고 자신의 모바일 디바이스 번호를 입력하여 사용자 A임을 인증한 결과, 사용자 A는 자신의 모바일 디바이스에 미리 저장해 놓은 신용카드 정보를 이용하여 8000원의 음식 값을 지불하기 위한 결제 내용이 생성된다.

[46] 206 단계에서는 사용자 모바일 디바이스에 미리 지정된 결제 방식으로 결제 내용이 진행된다. 사용자는 금융 거래를 위해 자신의 모바일 디바이스에 하나 이상의 결제 수단을 미리 설정해 둘 수 있으며, 이들 중 선택된 하나를 이용하여 결제를 진행할 수 있다. 사용자는 기본 결제 수단을 지정해둘 수도 있고, 각 금융 거래 때마다 결제 수단 리스트를 확인한 후, 선택하여 지정할 수도 있다. 다양한 실시예에서는 사용자 편의성이 극대화될 수 있도록 다양한 조건으로 금융 결제 방식을 표시 및 선택하게 할 수 있으며, 사용자가 자신의 모바일 디바이스에 미리 결제 방식을 하나 이상 등록시켜 놓기만 하면, 본 명세서 상에 예시되지 않는 다양한 디스플레이 방식 및 선택을 위한 입력 방식이 활용되어 실제 구현될 수도 있다.

[47] 다양한 실시예들에서, 결제 방식은 다양하게 구현될 수 있다. 일반적인 카드

결제, 실시간 계좌이체, 비실시간 계좌이체, 핸드폰 결제, 선결제된 온라인 상품권 결제, 충전식 상품권 결제, 포인트 결제 등으로 구현될 수 있다. 실시자는 가맹점 모바일 디바이스 및 사용자 모바일 디바이스에 따라 적절한 결제 방식을 제공할 수 있도록 복수 개의 종류의 결제 방식을 미리 설정할 수 있다.

- [48] 일실시에에서, 미리 지정된 결제 방식은, 하나 이상의 결제 수단 중에서 사용자가 선택한 특정 결제 수단에 대해서 대체키를 이용하여 인증을 수행할 수 있다. 대체키란 특정 결제 수단에 대해서 결제 수단의 고유 비밀번호에 대응되는 것으로, 사용자가 미리 설정한 것으로 사용자의 모바일 디바이스에 저장된다. 구체적으로, 대체키는 가맹점 모바일 디바이스에 표시되는 입력키 조합 중에서 사용자의 비밀번호의 각 자리에 대응되도록 미리 설정된 것이다. 예시적으로, 사용자 A가 자신의 신용카드를 결제 수단으로 자신의 모바일 디바이스에 해당 신용카드로 결제할 때 필요한 정보(카드번호, 유효기간 등)를 모두 저장해 둘 수 있다. 이때 신용카드의 비밀번호가 1234인 경우, 이 비밀번호는 사용자 A와 신용카드사 간에 해당 신용카드를 사용하기 위해 미리 정한 것이다. 사용자 A는 카드 비밀번호의 각 자리마다 대체하는 키를 자신이 임의로 설정할 수 있다. 예를 들어서, 첫 번째 자리인 숫자 1의 대체 키는 특수 문자인 물음표(?)가 될 수 있고, 두 번째 자리인 숫자 2의 대체 키는 특수 문자인 콜뱅이(@)가 될 수 있고, 세 번째 자리인 숫자 3의 대체 키는 영문자 f(소문자)가 될 수 있다. 대체키가 될 수 있는 숫자, 영문자, 특수문자, 국어 모음 또는 자음은 일반적으로 사용되는 키보드 상에 노출되는 것으로 예를 들어 한글 두벌식 키보드(106키)를 구성하는 것으로 다양한 실시에에서 활용할 수 있다. 또 다른 예시로써, 휴대폰 결제를 할 수 있으며, 사용자는 비밀번호를 미리 설정한 후, 그에 대응되는 대체키를 이용할 수 있다. 나아가 휴대폰 결제를 위해 휴대폰 번호를 입력하는 것이 가능하고, 더 나아가 개인의 주민번호를 입력함으로써 휴대폰 번호가 변경되는 경우에도 바뀐 휴대폰 번호로 결제가 가능하도록 할 수도 있다. 이 경우 해당 주민번호로 등록된 모든 카드 등을 결제 수단으로 활용할 수 있다. 결제 수단이 다양해지는 경우, 새로운 결제 수단에 의해서도 다양한 실시에들에서 결제 내용을 결제할 수 있도록 구현할 수 있다. 이때도 해당 결제수단에 사용되는 비밀번호 등에 대체키를 설정하여 둘 수 있고, 가맹점 모바일 디바이스에서 비밀번호를 입력하고 해당 비밀번호가 맞는지 인증하는 것은 사용자 모바일 디바이스에 이루어질 수 있다.

- [49] 이와 같이 일실시에에서는 사용자가 대체키를 이용함으로써 금융 거래를 위해서 가맹점 모바일 디바이스에 자신의 신용카드 비밀번호를 그대로 노출시키는 것을 방지할 수 있다. 특정 암호화 방법이 아닌 사용자 스스로 만들어 놓은 보안체계가 될 수 있기 때문에 해커 또는 가맹점 측이 대체키를 알게 되는 경우에도 대체키에 실제 대응되는 숫자를 알기 위해서는 사용자의 모바일 디바이스에 저장된 카드 비밀번호와 매칭되는 대체키를 해킹해야만 하기 때문에 개인정보 보호를 위한 보안 수준이 매우 높은 효과를 가진다.

- [50] 일실시에에서, 사용자는 하나 이상의 결제 방식을 미리 저장해 둘 수 있고 복수 개의 결제 방식 중에서 선택된 하나로 각 금융 결제를 진행할 수 있다. 이때 하나 이상의 결제 방식은 결제금액에 대한 할인 여부, 할인 폭, 포인트 적립 여부, 포인트 적립금액, 카드 사용실적 포함여부, 카드 사용실적 누적금액 등을 기준으로 선택될 수 있다. 우선순위는 가맹점 모바일 디바이스 및 결제 수단의 특성에 따라 디폴트 값이 미리 설정될 수 있다. 예를 들어, 특정 가맹점 모바일 디바이스는 P라는 신용카드에 대해서 식사금액의 10%를 할인해주는 특징을 가질 수 있으며, 이러한 특징에 따라 가맹점 모바일 디바이스에 결제를 하고 하는 경우, 사용자의 결제수단 중에서 P 신용카드가 존재하는 경우 해당 카드에 대해서 할인된 내용을 적용하여 표시할 수 있다. 또는 캐시백 적립이나 포인트 적립, 포인트 사용 등 다양한 특징들에 대해서 각 결제 수단에 자동으로 할인 및 포인트 적립/사용 가능 내역이 표시될 수 있다. 이때 우선순위는 가장 할인 폭이 크거나 포인트 적립금이 큰 경우에 높은 값을 가지게 된다.
- [51] 나아가, 사용자는 각 기준조건들에 우선순위를 미리 설정해둘 수 있으며 우선순위에 따라 산출된 가장 최적의 결제 방식이 결제 수단으로 결정될 수 있다. 이 우선순위는 각각의 금융 결제에 대해서 결제 내용에 적응적으로 우선순위가 반영될 수 있다. 예를 들어, 특정 음식점에서 P라는 신용카드로 결제하는 경우 총 식사금액의 30%를 할인해주는 경우 사용자는 이 조건을 미리 우선순위로 설정해둘 수 있고, 해당 음식점에서 결제가 발생하는 경우 P가 선택되어 결제가 진행될 수 있다. 또는 P라는 카드가 결제금액 할인이 큰 경우에도 사용자가 사용실적 누적금액에 대해 우선순위를 높게 설정해 놓을 경우 Q라는 카드가 사용실적 누적금액에 매우 낮은 경우 Q 카드가 선택되어 결제가 진행될 수도 있다. 사용자는 다양한 조건에 대해 각 결제 방식마다 자유롭게 우선순위를 미리 설정해 둘 수 있다.
- [52] 일실시에에서는 가맹점의 모바일 디바이스에서 사용자의 결제 방식 리스트를 리스트업하여 디스플레이하고, 사용자가 직접 선택에 의해 결제 수단을 결정하게 할 수도 있다. 다양한 실시예에서 실시자는 사용자가 결제 방식을 금융 정보로써 자신의 모바일 디바이스에 미리 저장할 수 있도록 구현할 수 있다.
- [53]
- [54] 도 3은 일실시에에 따른 가맹점의 결제 정보를 확인하여 금융 결제를 진행하는 방법의 순서도이다. 사용자의 모바일 디바이스에서 가맹점의 결제 정보를 확인하여 금융 결제를 진행할 때 다음의 단계를 포함할 수 있다.
- [55] 301 단계에서, 가맹점의 모바일 디바이스('제1 모바일 디바이스'라 함)으로부터 사용자의 생체 정보를 수신한다. 사용자의 생체 정보는 가맹점의 모바일 디바이스에 부착된 센서에 의해 사용자가 센싱시킨 데이터를 의미한다. 생체 정보는 지문, 홍채, 특정 신체 부위의 정맥, 심전도, 음성 등이 될 수 있다. 다양한 생체 정보에 따라 생체 정보의 파일 형식도 다양해질 수 있다. 생체 정보의 종류에 따라 파일 종류가 한정되는 것은 아니고, 지문 정보의 경우 이미지 파일

또는 동영상 파일로 생성되어 수신될 수 있다. 생체 정보의 종류 및 전송되는 파일의 형태 또한 사용자의 모바일 디바이스에 사용자에게 의해 미리 지정되어 있을 수 있다. 이 단계는 도 2의 202 단계와 상호 대응되는 관계에 해당한다.

- [56] 302 단계에서는, 수신한 생체 정보와 사용자의 모바일 디바이스('제2 모바일 디바이스'라 함)에 미리 저장된 사용자의 생체 정보가 일치하는지 확인한다. 두 데이터의 일치 여부를 확인하기 위해서, 수신한 생체 정보가 암호화되어 있는 경우 복호화 과정을 거칠 수 있고, 특정 파일 형식으로 변환되어 수신한 경우 필요에 따라서 다른 형식으로 변환하는 과정을 거칠 수도 있다. 나아가 생체 정보의 종류(예를 들어, 지문 정보인지 홍채 정보인지), 수신한 생체 정보의 파일 형식(예를 들어, 이미지 파일인지 동영상 파일인지)이 미리 설정해 놓은 것과 동일한 것인지도 두 생체 정보가 일치하는지 확인하는 범위에 모두 포함될 수 있다. 예시적으로 사용자 A는 자신의 왼손 약지 손가락 지문을 생체 정보로 이용할 것을 자신의 모바일 디바이스에 지정해 둘 수 있고, 수신되는 생체 정보는 이미지 파일을 동영상 파일로 변환한 것으로 지정해 둘 수 있다. 만약 수신한 생체 정보가 음성 파일인 경우 두 생체 정보는 일치하지 않는 것으로 판단될 수 있고, 동영상 파일인 경우 이미지 파일로 변환한 다음 사용자의 모바일 디바이스에 저장된 왼손 약지 손가락 지문과 대조하여 일치하는지 확인할 수 있다. 상기 302 단계가 실시되기 이전에, 실시예들에서는 사용자 모바일 디바이스의 사용자로부터 하나 이상의 생체 정보를 입력 받는 단계를 포함할 수 있다. 입력 받은 생체 정보는 사용자 모바일 디바이스 내의 저장공간(DB)에 저장되고, 가맹점 모바일 디바이스로부터 생체정보를 수신하는 경우, 저장된 생체정보와 비교할 수 있다.

- [57] 생체 정보는 하나 이상의 조합으로 선택될 수 있고, 사용자는 선택된 생체 정보에 대해서 미리 자신의 모바일 디바이스에 생체 정보를 저장해두면 그 이후에 발생하는 금융 결제에 등록된 자신의 생체 정보를 이용할 수 있다. 자신의 모바일 디바이스에 자신의 생체 정보를 저장해둘 뿐, 가맹점의 모바일 디바이스에 데이터를 전송 또는 저장하지 않기 때문에 개인정보 보호가 필요한 생체 정보에 대한 보호가 충분히 이루어질 수 있다.

- [58] 303 단계에서, 가맹점의 모바일 디바이스에 302 단계에서 확인된 결과를 전송한다. 수신한 생체 정보와 사용자의 모바일 디바이스에 저장된 생체 정보가 일치하는 경우, 304 단계에서 305 단계(예)로 진행하여 금융 결제를 진행시키고, 두 생체 정보가 일치하지 않는 경우, 304 단계에서 그대로 종료(아니오)하게 된다.

- [59] 305 단계에서는 두 생체 정보가 일치하는 경우에 가맹점 모바일 디바이스로부터 인증된 결제 내용을 수신한다. 결제 내용은 사용자가 해당 가맹점에서 지불해야 하는 결제 금액에 대한 정보를 포함한다.

- [60] 306 단계에서, 사용자 모바일 디바이스에 미리 지정된 결제 방식으로 수신한 결제 내용을 진행한다. 구체적으로 하나 이상의 결제 방식 중에 선택된 결제

방식으로 결제가 진행되며, 결제 방식은 카드 결제, 휴대폰 결제, 계좌이체 등 다양한 온라인 결제 방법이 모두 적용될 수 있다. 상기 306 단계 실시 이전에, 사용자 모바일 디바이스의 사용자로부터 하나 이상의 결제 방식을 입력 받는 단계를 포함할 수 있다. 결제 방식은 다양하고, 각 결제 방식의 개체 역시 복수 개일 수 있다. 예를 들어, 다른 종류의 신용카드를 3장 등록하고, 서로 다른 은행계좌를 2개 등록하고, 휴대폰 결제를 위한 휴대폰 인증 절차를 미리 거칠 수 있다. 카드 결제의 경우 결제를 위한 정보(카드 번호, 카드 유효기간 등)를 사용자가 미리 입력해 두어야 하며, 이때 카드 비밀번호에 대응하여 사용자는 대체키를 설정할 수 있다.

- [61] 사용자는 가맹점의 모바일 디바이스를 통해 카드 비밀번호를 입력할 수 있으므로, 이때 가맹점 모바일 디바이스에 사용자의 비밀번호가 그대로 노출되는 것을 1차 방지하고, 비밀번호가 사용자 모바일 디바이스에 전송될 때 네트워크 상에 노출되는 것을 2차로 방지하기 위해서 카드 비밀번호를 대체할 대체키를 가맹점 모바일 디바이스에서 입력시키고, 가맹점 모바일 디바이스는 대체키를 사용자 모바일 디바이스에 전송함으로써 카드 비밀번호 확인은 사용자 모바일 디바이스와 카드사 서버 간에 이루어짐으로써 보안체계를 확장시키지 않을 수 있다.
- [62] 대체키는 가맹점의 모바일 디바이스(또는 사용자의 모바일 디바이스)에 표시되는 입력키 조합 중에서 사용자의 입력에 의해 비밀번호의 각 자리에 대응되도록 설정된 것이다. 사용자의 모바일 디바이스는 각 카드마다 비밀번호에 대응되는 대체키 정보를 저장해 둘 수 있다.
- [63] 따라서 대체키를 이용해 가맹점 모바일 디바이스와 사용자 모바일 디바이스 간에 카드 비밀번호 확인이 이루어지는 경우, 사용자 모바일 디바이스는 카드사 서버에 카드 결제를 요청할 수 있고, 카드사는 이를 승인하여 해당 가맹점의 매출로 카드 사용을 승인할 수 있다.
- [64]
- [65] 도 2에서 가맹점 모바일 디바이스(100)의 금융결제 방법에 대한 일실시예를 설명하였고, 도 3에서 사용자 모바일 디바이스(200) 측면에서 금융결제 방법에 대한 일실시예를 설명하였다. 두 모바일 디바이스 간의 상호작용을 상세히 설명하기 위해서 도 4는 일실시예에 따라 사용자 모바일 디바이스(200), 가맹점 모바일 디바이스(100) 및 카드사 서버(500)간의 상호작용을 나타낸 시퀀스 다이어그램이다.
- [66] S401 단계에서 사용자는 사용자 모바일 디바이스(200)에 자신의 생체 정보를 등록하고, 개인 정보(성명, 생년월일, 주민번호 등)를 저장하고, 금융 정보로써 하나 이상의 결제 방식을 설정할 수 있다. 이때 특정 결제수단에 대한 비밀번호에 대해서 사용자가 설정한 대체키를 저장할 수 있다. 사용자 모바일 디바이스(200)는 생체 정보를 인증하고, 저장된 결제 방식으로 결제를 진행할 수 있다.

- [67] S402 단계에서 가맹점 모바일 디바이스는 센싱한 생체정보를 사용자 모바일 디바이스에 전송하면, S403 단계에서 전송된 생체정보와 미리 저장된 생체정보가 일치하는지 여부를 확인하고, 그 결과는 S404 단계에서 가맹점 모바일 디바이스에 전송한다.
- [68] 전송한 생체 정보가 사용자 모바일 디바이스에 저장된 것과 일치하는 경우, S405 단계에서 가맹점 모바일 디바이스는 금융 결제를 위한 결제내용을 인증하고, 미리 지정된 결제 방식으로 결제를 진행하기 위해서 사용자로부터 결제 수단의 비밀번호에 대응되는 대체키를 입력 받아 S406 단계에서 대체키를 사용자 모바일 디바이스에 전송한다. S407 단계에서 생체 정보 인증과 마찬가지로 사용자 모바일 디바이스 내에서 카드 비밀번호에 대응하는 대체키가 일치하는지 확인하고, 그 결과를 S408 단계에서 가맹점 모바일 디바이스에 전송한다.
- [69] 대체키가 일치하는 경우, S409 단계에서 가맹점 모바일 디바이스는 사용자 모바일 디바이스에 결제를 요청하기 위해 결제내용을 전송한다.
- [70] 사용자 모바일 디바이스는 사용자가 미리 저장해 놓은 결제 방식으로 해당 카드사 서버(500)에 S410 단계에서 결제승인을 요청한다. 가맹점 모바일 디바이스 간에서는 대체키 정보를 전송 및 수신했으나, 카드사 서버 간에는 카드 비밀번호를 직접 전송 및 수신할 수 있다. 이 경우 카드사 서버가 제공하는 보안체계에 따라 신용카드 정보가 보호된다.
- [71] 카드사 서버(500)는 해당 결제내용에 대해서 S411 단계에서 사용자 모바일 디바이스에 결제를 승인해줄 수 있다.
- [72] 그러므로 가맹점 모바일 디바이스 측면에서는, 사용자인 개인의 신상 정보, 생체 정보, 금융 정보를 알 수 없으며 단편적으로 센싱한 생체 정보와 카드 비밀번호를 대체한 대체키 정보만을 공유하게 된다. 생체 정보는 개인의 정보와 결합되어야 진정한 의미가 있는 정보라고 볼 수 있으므로 가맹점 모바일 디바이스 상에 사용자가 자신의 지문을 노출시키는 경우에도 자신의 생체정보가 노출되었다고 보기 어렵다. 반대로 사용자 모바일 디바이스에서는 사용자 본인의 개인정보, 생체정보, 금융정보를 저장해 둘 수 있고, 각각 발생하는 금융 결제마다 본인 인증을 위한 확인, 카드 인증을 위한 확인을 자체적으로 하기 때문에 개인정보 보호가 높은 효과를 가진다. 카드사 서버 측에서는, 특정인의 카드 정보를 기초로 사용자 모바일 디바이스와 직접 결제를 진행하기 때문에 다수의 가맹점 기기가 결제를 요청하는 것보다 체계적으로 보안체계를 유지할 수 있다.
- [73]
- [74] 도 5a 및 도 5b는 일실시예에 따라 모바일 디바이스에서 표시하는 대체키 입력판의 예시이다. 도 5a는 숫자, 영문자, 국어 모음, 국어 자음으로 구성되어 있고, 도 5b는 특수문자로 구성되어 있다. 보안을 위해 실제 키보드 자판의 배치에서 구성되는 입력키 조합이 공백을 포함하여 배치되어 있다. 예시적으로

숫자 8과 숫자 9 사이에 공백이 있다. 가맹점 모바일 디바이스는 대체키 입력을 위해 도 5a와 같은 표시화면을 사용자에게 제공할 수 있다.

[75]

[76] 일실시에에서, 결제 수단의 비밀번호에 대응되는 대체키를 사용자는 가맹점 모바일 디바이스에 입력할 수 있는데, 대체키의 각 자리를 입력할 때마다 도 5a 또는 도 5b에 예시한 입력키 조합이 재배치될 수 있다. 보안을 한층 강화하기 위해서 대체키가 4자리인 경우 서로 다른 4종류의 입력판이 제공될 수 있다. 도 6은 일실시에 따라 대체키의 각 자리를 입력할 때마다 도 5a의 입력판이 재배치되는 예시이다. 도 5a에서 숫자 8과 숫자 9 사이에 공백이 있었던 것과 달리 도 6에서는 숫자 8과 숫자 9 사이에 공백이 없으며, 도 5a에서 숫자 4와 숫자 5 사이에 공백이 없었던 것과 달리 도 6에서는 숫자 4와 숫자 5 사이에 공백이 있도록 재배치된 것을 확인할 수 있다.

발명의 실시를 위한 형태

[77] 이상에서 설명된 실시예들은 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치, 방법 및 구성요소는, 예를 들어, 프로세서, 컨트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[78] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호

파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

- [79] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

- [80] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

산업상 이용가능성

- [81] 현재 이미 보편화되어 있는 모바일 디바이스를 이용함으로써 별도의 인프라 구축 없이 소비자 측인 개인과 공급자 측인 사업자 모두 적은 비용으로 생체 정보를 이용한 금융 결제를 할 수 있다.

청구범위

- [청구항 1] 판매자의 제1 모바일 디바이스가 금융 결제를 인증하는 방법에 있어서,
 상기 제1 모바일 디바이스에 구비된 센서를 이용하여 구매자의 하나 이상의 생체 정보를 센싱하는 단계;
 상기 제1 모바일 디바이스가 미리 지정된 방법으로 상기 구매자에 대응하여 식별되는 제2 모바일 디바이스에 상기 센싱한 생체 정보를 전송하는 단계;
 상기 제2 모바일 디바이스로부터 상기 전송한 생체 정보가 상기 구매자의 제2 모바일 디바이스에 미리 저장된 상기 구매자의 생체 정보와 일치하는지 여부를 수신하는 단계; 및
 상기 제1 모바일 디바이스가 전송한 생체 정보와 상기 제2 모바일 디바이스에 저장된 생체 정보가 일치하는 경우 상기 제1 모바일 디바이스가 결제 내용을 인증하는 단계를 포함하는 방법.
- [청구항 2] 제1항에 있어서,
 상기 생체 정보는 지문 정보, 홍채 정보, 정맥 정보, 심전도 정보 및 음성 정보 중 어느 하나 이상을 포함하는 방법.
- [청구항 3] 제1항에 있어서,
 상기 제2 모바일 디바이스에 미리 지정된 결제 방식으로 상기 제2 모바일 디바이스에 의해 상기 결제 내용을 진행하는 단계를 더 포함하는 방법.
- [청구항 4] 제3항에 있어서,
 상기 미리 지정된 결제 방식은,
 하나 이상의 결제 수단 중에서 상기 구매자가 선택한 제1 결제 수단에 대해서 상기 제1 결제 수단의 비밀번호에 대응하는 대체키로 상기 제1 결제 수단을 사용하기 위한 인증을 수행하는 방법.
- [청구항 5] 제4항에 있어서,
 상기 대체키는 상기 제1 모바일 디바이스에 표시되는 입력키 조합 중에서 상기 구매자가 상기 비밀번호의 각 자리에 대응되도록 미리 설정한 방법.
- [청구항 6] 제4항에 있어서,
 상기 제1 결제 수단은 상기 결제 내용에 적응적으로 상기 미리 지정된 하나 이상의 결제 방식 중에서 선택된 것인 방법.
- [청구항 7] 제1항에 있어서,
 상기 센싱한 생체 정보를 전송하는 단계는,
 상기 생체 정보를 미리 설정된 암호화 방법으로 암호화하거나, 상기 생체 정보를 미리 지정된 형태의 파일로 변환하여 전송하는 방법.
- [청구항 8] 제7항에 있어서,
 상기 미리 설정된 암호화 방법은 RC4, OTPad, DES, TDES, AES, IDEA,

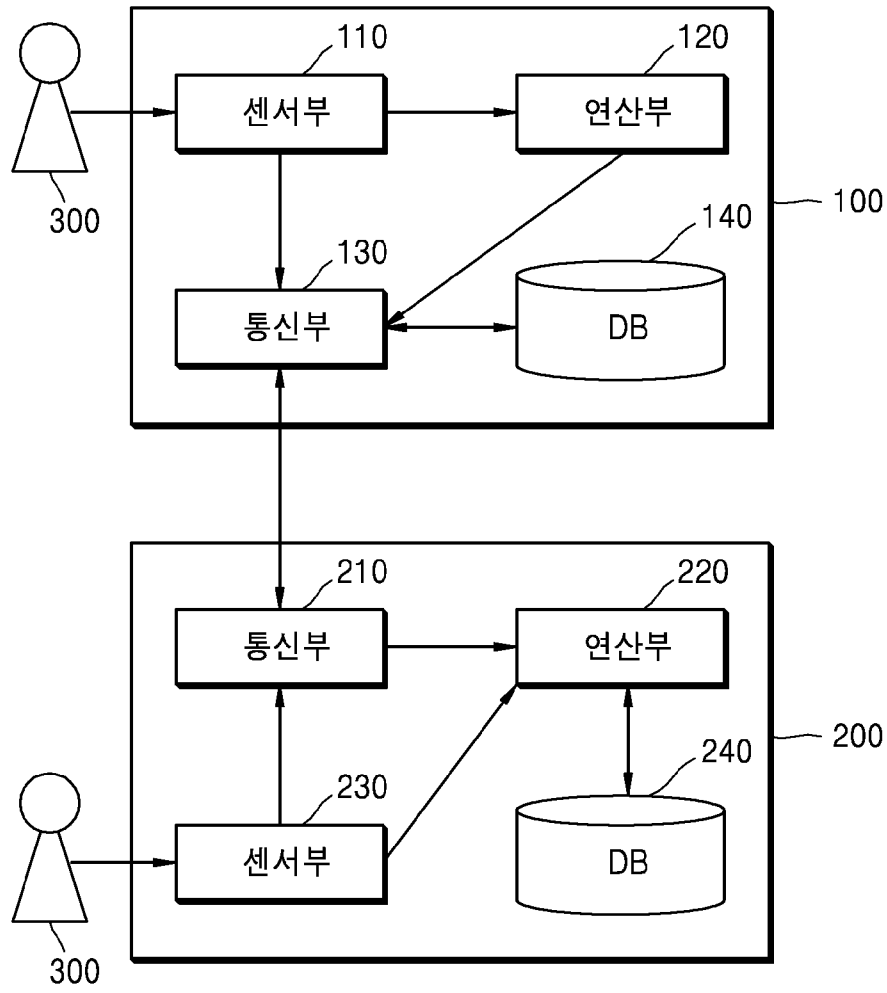
Diffie-Hellman, DSA, Elgamal, RSA, ECC, SHA, MD5, HAVAL, HMAC, CBC-MAC 중 어느 하나인 방법.

- [청구항 9] 제7항에 있어서,
상기 미리 지정된 형태의 파일은 이미지 파일, 동영상 파일, 음성 파일 중 어느 하나인 방법.
- [청구항 10] 제9항에 있어서,
상기 센싱한 생체 정보에 적응적으로 상기 파일의 형태를 결정하는 방법.
- [청구항 11] 구매자에 대응하여 식별되는 제2 모바일 디바이스가 금융 결제를 수행하는 방법에 있어서,
판매자의 제1 모바일 디바이스로부터 구매자의 생체 정보를 수신하는 단계;
상기 수신된 구매자의 생체 정보와 상기 제2 모바일 디바이스에 미리 저장된 상기 구매자의 생체 정보가 일치하는지 확인하는 단계;
상기 수신된 구매자의 생체 정보와 상기 제2 모바일 디바이스에 저장된 구매자의 생체 정보가 일치하는 경우, 상기 제1 모바일 디바이스로부터 인증된 결제 내용을 수신하는 단계; 및
상기 결제 내용에 대하여 미리 설정된 결제 방식으로 결제를 수행하는 단계
를 포함하는 방법.
- [청구항 12] 제11항에 있어서,
상기 구매자로부터 하나 이상의 생체 정보 및 하나 이상의 결제 방식을 입력 받는 단계를 더 포함하는 방법.
- [청구항 13] 제12항에 있어서,
상기 하나 이상의 결제 방식 중 선택된 제1 결제 수단에 대해서, 상기 구매자로부터 입력 받은 상기 제1 결제 수단의 비밀번호에 대응하는 대체키를 이용하여 상기 결제를 수행하는 방법.
- [청구항 14] 제13항에 있어서,
상기 대체키는 상기 제1 모바일 디바이스에 표시되는 입력키 조합 중에서 상기 사용자의 입력에 의해 상기 비밀번호의 각 자리에 대응되는 방법.
- [청구항 15] 제13항에 있어서,
상기 하나 이상의 결제 방식은 결제금액 할인, 포인트 적립, 또는 사용실적 누적금액 중 미리 설정된 우선순위에 의해 상기 제1 결제 수단으로 결정되는 방법.
- [청구항 16] 제15항에 있어서,
상기 결제 내용에 적응적으로 상기 우선순위를 반영하는 방법.
- [청구항 17] 적어도 하나의 프로세서를 포함하는 컴퓨팅 장치에 있어서, 상기 적어도 하나의 프로세서에 의해 적어도 일시적으로 구현되는:
구매자의 하나 이상의 생체 정보를 센싱하는 센서부;

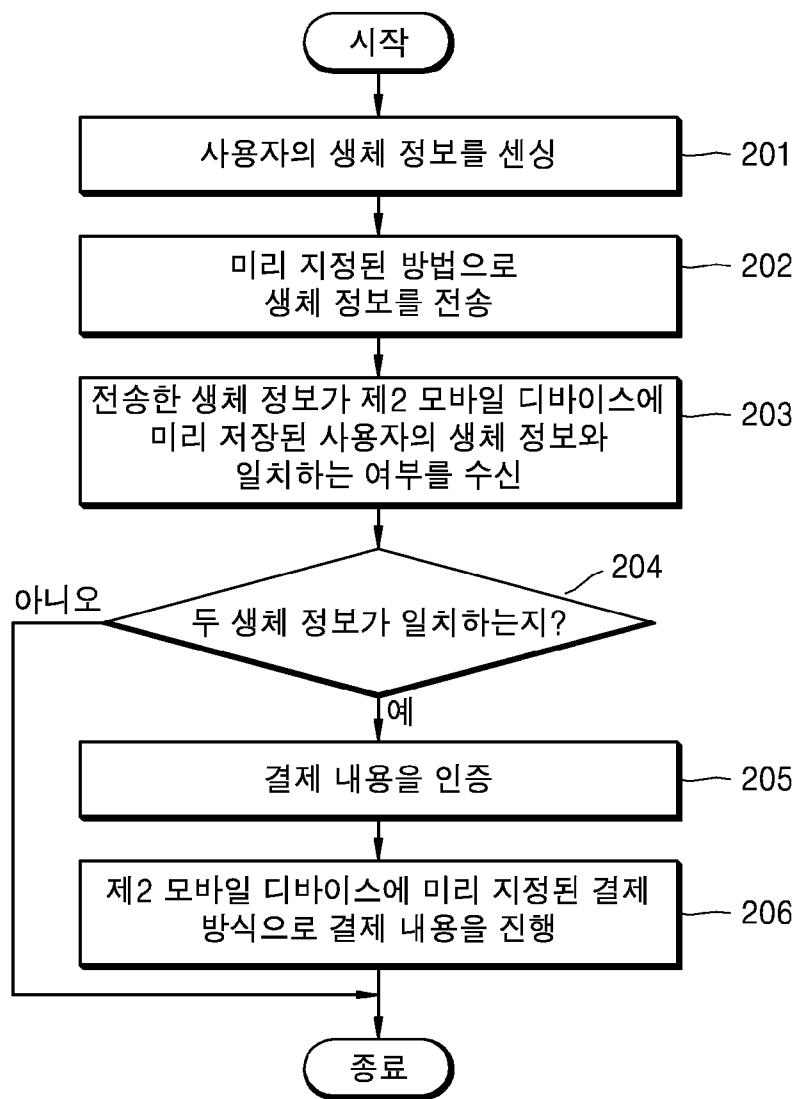
미리 지정된 방법으로 상기 구매자로 식별되는 제2 모바일 디바이스에 상기 센싱한 생체 정보를 전송하고, 상기 전송에 대한 응답으로 상기 제2 모바일 디바이스로부터 상기 전송한 생체 정보가 상기 구매자의 제2 모바일 디바이스에 미리 저장된 상기 구매자의 생체 정보와 일치하는지 여부를 수신하는 통신부; 및
 상기 전송한 생체 정보와 상기 제2 모바일 디바이스에 저장된 구매자의 생체 정보가 일치하는 경우 결제 내용을 인증하는 연산부를 포함하는 컴퓨팅 장치.

- [청구항 18] 컴퓨터 판독 가능 기록매체에 저장되어, 컴퓨팅 장치가 구매자 생체 정보 및 금융 정보에 기초하여 금융 결제를 진행하는 프로그램에 있어서:
 판매자의 제1 모바일 디바이스로부터 구매자의 생체 정보를 수신하는 명령어 세트;
 상기 수신된 구매자의 생체 정보와 상기 컴퓨팅 장치에 미리 저장된 상기 구매자의 생체 정보가 일치하는지 확인하고, 상기 제1 모바일 디바이스에 확인 결과를 전송하는 명령어 세트; 및
 상기 수신한 구매자의 생체 정보와 상기 컴퓨팅 장치에 저장된 구매자의 생체 정보가 일치하는 경우, 상기 제1 모바일 디바이스로부터 인증된 결제 내용을 수신하여, 상기 구매자의 하나 이상의 결제 방식 중 선택된 제1 결제 수단으로 상기 구매자로부터 입력 받은 상기 제1 결제 수단의 비밀번호에 대응하는 대체키를 이용하여 결제를 진행하는 명령어 세트를 포함하는 기록매체에 저장된 프로그램.

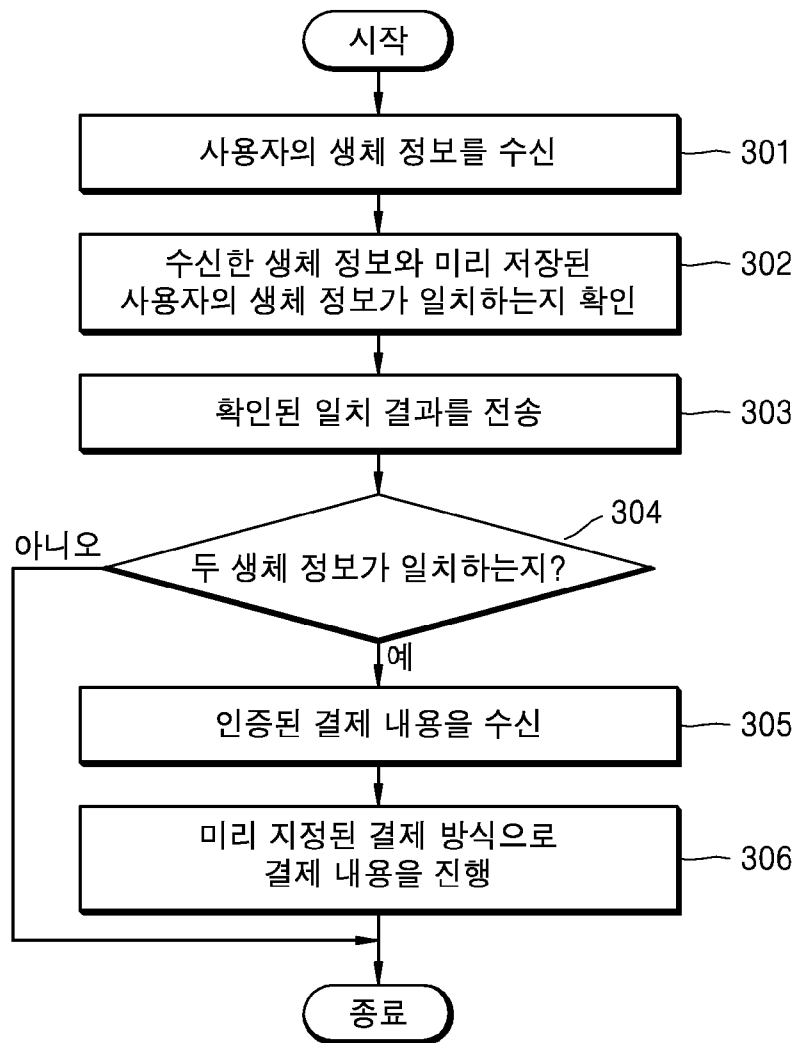
[도1]



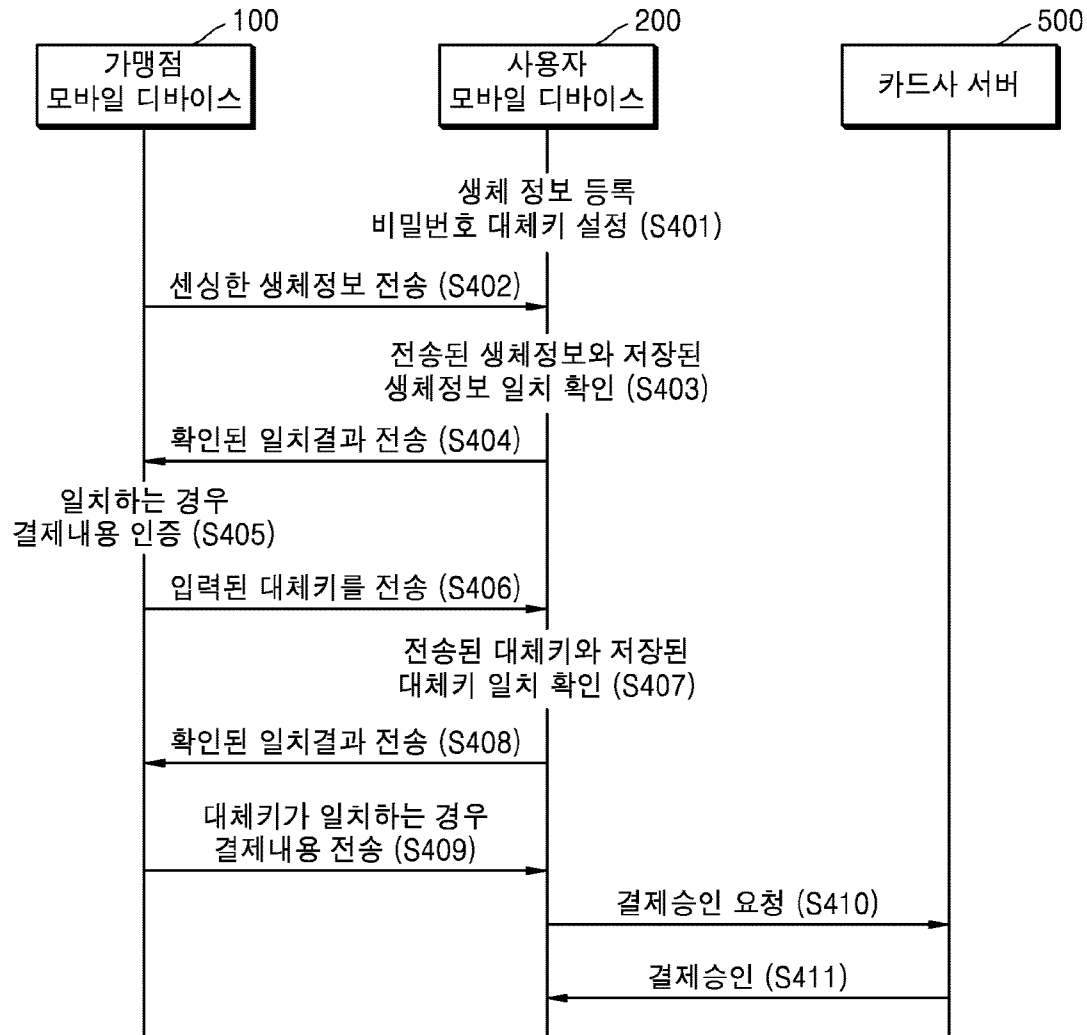
[도2]



[도3]



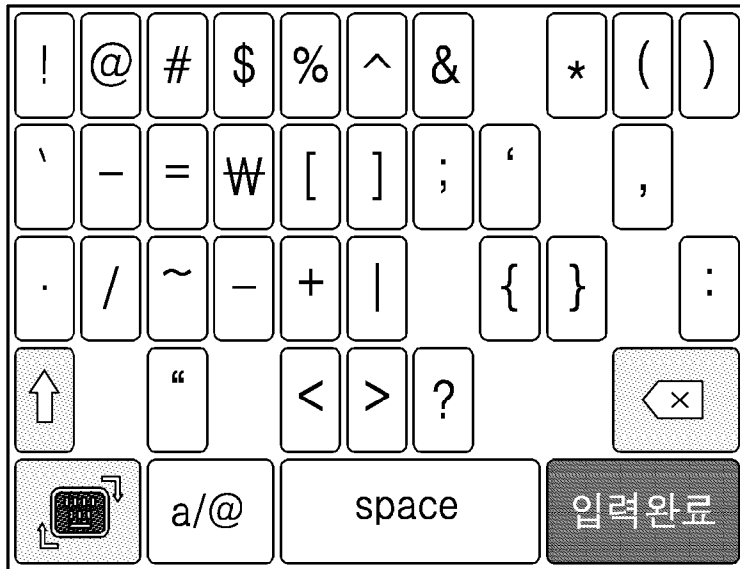
[도4]



[도5a]



[도5b]



[도6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2017/012829**A. CLASSIFICATION OF SUBJECT MATTER****G06Q 20/32(2012.01)i, G06Q 20/40(2012.01)i, G06Q 20/38(2012.01)i, G06F 21/32(2013.01)i, G06K 9/00(2006.01)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)

G06Q 20/32; G06Q 20/40; G06Q 20/10; G06Q 20/02; G06Q 20/34; G06K 9/00; G06Q 20/38; 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: biometric information, mobile, payment, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2015-0088768 A (LEE, Do Hun) 03 August 2015 See paragraph [0003], claims 1, 11 and figure 2.	1-18
A	KR 10-2011-0055112 A (CHOI, Un Ho) 25 May 2011 See paragraph [0014] and claims 1-2.	1-18
A	KR 10-2016-0013221 A (CRUCIALTEC CO., LTD. et al.) 03 February 2016 See paragraph [0119] and claim 1.	1-18
A	KR 10-2014-0141984 A (T-MONET. CO., LTD.) 11 December 2014 See claim 1 and figures 3-4.	1-18
A	KR 10-2016-0002623 A (KIM, Woo Jin et al.) 08 January 2016 See claims 1-2 and figure 3.	1-18



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

20 MARCH 2018 (20.03.2018)

Date of mailing of the international search report

21 MARCH 2018 (21.03.2018)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Sconsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2017/012829

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2015-0088768 A	03/08/2015	KR 10-1719065 B1	22/03/2017
KR 10-2011-0055112 A	25/05/2011	KR 10-1088029 B1	29/11/2011
		US 2012-0239567 A1	20/09/2012
		US 2017-0132623 A1	11/05/2017
		US 2017-0140369 A1	18/05/2017
		US 9589260 B2	07/03/2017
		WO 2011-062365 A2	26/05/2011
		WO 2011-062365 A3	01/09/2011
KR 10-2016-0013221 A	03/02/2016	NONE	
KR 10-2014-0141984 A	11/12/2014	KR 10-1607935 B1	01/04/2016
KR 10-2016-0002623 A	08/01/2016	NONE	

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06Q 20/32(2012.01)i, G06Q 20/40(2012.01)i, G06Q 20/38(2012.01)i, G06F 21/32(2013.01)i, G06K 9/00(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06Q 20/32; G06Q 20/40; G06Q 20/10; G06Q 20/02; G06Q 20/34; G06K 9/00; G06Q 20/38; 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: 생체 정보, 모바일, 결제, 보안

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2015-0088768 A (이도훈) 2015.08.03 단락 [0003], 청구항 1, 11 및 도면 2 참조.	1-18
A	KR 10-2011-0055112 A (최운호) 2011.05.25 단락 [0014] 및 청구항 1-2 참조.	1-18
A	KR 10-2016-0013221 A (크루셀텍 (주) 등) 2016.02.03 단락 [0119] 및 청구항 1 참조.	1-18
A	KR 10-2014-0141984 A (주식회사 티모넷) 2014.12.11 청구항 1 및 도면 3-4 참조.	1-18
A	KR 10-2016-0002623 A (김우진 등) 2016.01.08 청구항 1-2 및 도면 3 참조.	1-18

☐ 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

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

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

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

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

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

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

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2018년 03월 20일 (20.03.2018)

국제조사보고서 발송일

2018년 03월 21일 (21.03.2018)

ISA/KR의 명칭 및 우편주소



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

팩스 번호 +82-42-481-8578

심사관

김연정

전화번호 +82-42-481-3325



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2015-0088768 A	2015/08/03	KR 10-1719065 B1	2017/03/22
KR 10-2011-0055112 A	2011/05/25	KR 10-1088029 B1	2011/11/29
		US 2012-0239567 A1	2012/09/20
		US 2017-0132623 A1	2017/05/11
		US 2017-0140369 A1	2017/05/18
		US 9589260 B2	2017/03/07
		WO 2011-062365 A2	2011/05/26
		WO 2011-062365 A3	2011/09/01
KR 10-2016-0013221 A	2016/02/03	없음	
KR 10-2014-0141984 A	2014/12/11	KR 10-1607935 B1	2016/04/01
KR 10-2016-0002623 A	2016/01/08	없음	