(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2022 년 3 월 3 일 (03.03.2022)

WIPO | PCT

(10) 국제공개번호
WO 2022/045508 A1

(51) 국제특허분류:
G07C 9/00 (2006.01) *G07C 9/38* (2020.01)
G07C 9/37 (2020.01)

(21) 국제출원번호: PCT/KR2021/002773

(22) 국제출원일: 2021 년 3 월 5 일 (05.03.2021)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2020-0110271 2020 년 8 월 31 일 (31.08.2020) KR

(71) 출원인: (주)씨유박스 **(CUBOX CO, LTD.)** [KR/KR]; 08512 서울시 금천구 디지털로9길 68, 1701호, 1702호, 1703호, 1704호, 1705호, Seoul (KR).

(72) 발명자: **남운성 (NAM, Un Sung)**; 04196 서울시 마포구 백범로 212, 101동 1803호, Seoul (KR).

(74) 대리인: **특허법인 아이시스 (ISIS IP LAW LLC)**; 06160 서울시 강남구 테헤란로63길 14, 8층, Seoul (KR).

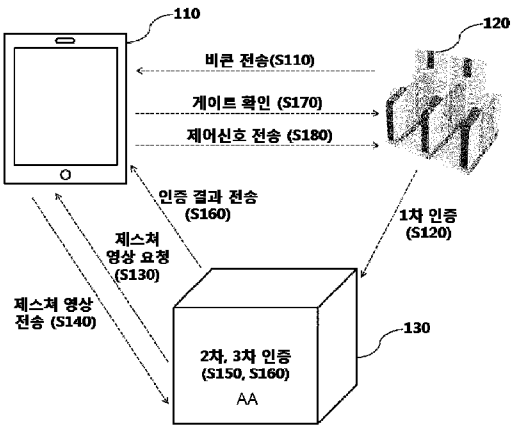
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, 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, 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, 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))

(54) Title: AUTHENTICATION METHOD AND SYSTEM FOR GATE ACCESS

(54) 발명의 명칭: 게이트 출입을 위한 인증 방법 및 시스템



S110 ... Transmit beacon
S120 ... Primary authentication
S130 ... Request gesture images
S140 ... Transmit gesture images
S160 ... Transmit authentication result
S170 ... Check gate
S180 ... Transmit control signal
AA ... Secondary, tertiary authentication

(57) Abstract: The present invention relates to an authentication method and system for gate access, the method comprising the steps in which: a gate device transmits a beacon to a user terminal that has entered a certain area; the gate device captures a face image of a user of the user terminal, performs primary authentication by comparing the face image with a plurality of pre-stored face images, and transmits the result of the primary authentication to an authentication server; if the authentication server determines that the user is a previously registered user according to the result of the primary authentication, the authentication server requests the user terminal for information for secondary authentication; the user terminal captures images of a gesture input by the user according to the request of the authenticati on server; the authentication server receives the images and performs secondary authentication by comparing the images with previously registered gesture images of the user; the authentication server performs tertiary authentication by looking up access restriction information about the user, and transmits the result of the tertiary authentication to the user terminal; the user terminal checks the location of a specific gate, to which access has been granted according to the result of the tertiary authentication, among a plurality of gates; and the user terminal transmits a control signal to a gate device provided in the specific gate.

WO 2022/045508 A1

[다음 쪽 계속]

(57) 요약서: 개시된 기술은 게이트 출입을 위한 인증 방법 및 시스템에 관한 것으로, 게이트 장치가 일 영역에 진입한 사용자 단말기에 비콘을 전송하는 단계; 상기 게이트 장치가 상기 사용자 단말기의 사용자에 대한 얼굴 이미지를 촬영하고 상기 얼굴 이미지 및 사전에 저장된 복수개의 얼굴 이미지를 비교하여 1차 인증을 수행하고 상기 1차 인증에 대한 결과를 인증서버에 전송하는 단계; 상기 인증서버가 상기 1차 인증에 대한 결과에 따라 상기 사용자가 기 등록된 사용자인 것으로 판단하면 상기 사용자 단말기에 2차 인증을 위한 정보를 요청하는 단계; 상기 사용자 단말기가 상기 인증서버의 요청에 따라 상기 사용자가 입력하는 제스쳐를 영상으로 촬영하는 단계; 상기 인증서버가 상기 영상을 수신하여 기 등록된 상기 사용자의 제스쳐 영상과 비교하여 상기 2차 인증을 수행하는 단계; 상기 인증서버가 상기 사용자에 대한 출입제한 정보를 조회하여 3차 인증을 수행하고 상기 3차 인증에 대한 결과를 상기 사용자 단말기에 전송하는 단계; 상기 사용자 단말기가 상기 3차 인증에 대한 결과에 따라 복수개의 게이트 중 출입권한이 부여된 특정 게이트의 위치를 확인하는 단계; 및 상기 사용자 단말기가 상기 특정 게이트에 구비된 게이트 장치에 제어신호를 전송하는 단계;를 포함한다.

명세서

발명의 명칭: 게이트 출입을 위한 인증 방법 및 시스템

기술분야

[1] 개시된 기술은 사용자 생체정보 기반 템플릿을 이용하여 게이트 출입을 위한 인증을 수행하는 방법 및 시스템에 관한 것이다.

배경기술

[2] 인간의 신체에는 지문, 음성, 얼굴, 홍채, 정맥 등의 다양한 생체정보가 존재하며 이러한 생체정보는 고유한 정보들이므로 이를 이용한 인증기술이 폭넓게 이용되고 있다. 특히, 안전관리를 위해서 출입을 엄격하게 제한해야하는 공항이나, 관공서, 사무소 등의 경우에는 이미 지문과 같은 생체정보를 이용하는 출입인증 기술이 다수 이용되고 있다.

[3] 이러한 생체정보를 이용하는 인증기술은 초기에는 지문이나 홍채와 같이 신체 일부를 감지장치에 접촉시켜서 얻어지는 정보를 이용하였으나 획득되는 생체정보의 부정확도가 높은 편이고 감지장치를 다수의 사용자가 이용하기 때문에 위생적으로 거부감이 드는 문제가 있었다. 이에 따라 최근에는 얼굴 이미지와 같이 비접촉 방식으로 획득되는 생체정보를 이용하는 인증기술이 늘어나고 있는 추세이다.

[4] 한편, 신체 특정 부위로부터 추출된 생체정보는 데이터화되어 이용된다. 이를 템플릿이라고 명명하고 있으며 사전에 등록된 템플릿과 현장에서 추출된 템플릿을 비교하는 방법으로 사용자를 인증하고 있다. 그러나 이러한 기술은 사용자의 의도와 상관없이 서버에 사용자의 생체정보가 보관되기 때문에 생체정보 보호 가이드라인에 위배되는 문제점이 있었다.

발명의 상세한 설명

기술적 과제

[5] 개시된 기술은 사용자 생체정보 기반 템플릿을 이용하여 게이트 출입을 위한 인증을 3단계로 수행하는 방법 및 시스템을 제공하는데 있다.

과제 해결 수단

[6] 상기의 기술적 과제를 이루기 위하여 개시된 기술의 제 1 측면은 게이트 장치가 일 영역에 진입한 사용자 단말기에 비콘을 전송하는 단계, 상기 게이트 장치가 상기 사용자 단말기의 사용자에 대한 얼굴 이미지를 촬영하고 상기 얼굴 이미지 및 사전에 저장된 복수개의 얼굴 이미지를 비교하여 1차 인증을 수행하고 상기 1차 인증에 대한 결과를 인증서버에 전송하는 단계, 상기 인증서버가 상기 1차 인증에 대한 결과에 따라 상기 사용자가 기 등록된 사용자인 것으로 판단하면 상기 사용자 단말기에 2차 인증을 위한 정보를 요청하는 단계, 상기 사용자 단말기가 상기 인증서버의 요청에 따라 상기 사용자가 입력하는 제스쳐를 영상으로 촬영하는 단계, 상기 인증서버가 상기 영상을 수신하여 기 등록된 상기

사용자의 제스쳐 영상과 비교하여 상기 2차 인증을 수행하는 단계, 상기 인증서버가 상기 사용자에 대한 출입제한 정보를 조회하여 3차 인증을 수행하고 상기 3차 인증에 대한 결과를 상기 사용자 단말기에 전송하는 단계, 상기 사용자 단말기가 상기 3차 인증에 대한 결과에 따라 복수개의 게이트 중 출입권한이 부여된 특정 게이트의 위치를 확인하는 단계 및 상기 사용자 단말기가 상기 특정 게이트에 구비된 게이트 장치에 제어신호를 전송하는 단계를 포함하는 게이트 출입을 위한 인증 방법을 제공하는데 있다.

[7] 상기의 기술적 과제를 이루기 위하여 개시된 기술의 제 2 측면은 사용자의 게이트 출입을 위한 어플리케이션을 탑재하고 상기 어플리케이션을 이용하여 상기 사용자의 얼굴 이미지를 토대로 생성된 인증템플릿 및 제스쳐 영상을 등록하는 사용자 단말기, 비콘을 이용하여 상기 사용자 단말기를 식별하면 상기 사용자 단말기의 사용자에 대한 얼굴 이미지를 촬영하여 임시 템플릿을 생성하고 상기 등록된 인증 템플릿과 상기 임시템플릿을 비교하여 1차 인증을 수행하는 게이트 장치, 상기 1차 인증에 대한 결과를 수신하여 상기 사용자가 기 등록된 사용자인 것으로 판단하고 상기 사용자 단말기에 제스쳐 영상을 요청하여 상기 등록된 제스쳐 영상과 비교함으로써 2차 인증을 수행하는 제 1 인증서버 및 상기 제 1 인증서버에서 상기 2차 인증에 대한 결과를 수신하면 상기 사용자에 대한 출입제한 정보를 조회하여 3차 인증을 수행하고 상기 3차 인증에 대한 결과를 상기 사용자 단말기에 전송하는 제 2 인증서버를 포함하는 게이트 출입을 위한 인증 시스템을 제공하는데 있다.

발명의 효과

[8] 개시된 기술의 실시 예들은 다음의 장점들을 포함하는 효과를 가질 수 있다. 다만, 개시된 기술의 실시 예들이 이를 전부 포함하여야 한다는 의미는 아니므로, 개시된 기술의 권리범위는 이에 의하여 제한되는 것으로 이해되어서는 아니 될 것이다.

[9] 개시된 기술의 일 실시예에 따르면 게이트 출입을 위한 인증 방법 및 시스템은 생체정보 기반의 3단계 인증을 통해 사용자의 게이트 출입을 신속하고 정확하게 처리하는 효과가 있다.

[10] 또한, 인증이 완료된 사용자의 생체정보를 저장하지 않아서 생체정보 보호 가이드라인을 준수하는 효과가 있다.

[11] 또한, 게이트 출입을 위한 별도의 입력이나 신체 일부를 접촉할 필요가 없어서 인증 과정에 따른 편의성이 증대되는 효과가 있다.

도면의 간단한 설명

[12] 도 1은 개시된 기술의 일 실시예에 따른 게이트 출입을 위한 인증 방법에 대한 도면이다.

[13] 도 2는 개시된 기술의 일 실시예에 따른 게이트 출입을 위한 인증 시스템에 대한 도면이다.

[14] 도 3은 게이트에 구비된 게이트 장치를 나타낸 도면이다.

발명의 실시를 위한 최선의 형태

[15] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[16] 제 1, 제 2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 해당 구성요소들은 상기 용어들에 의해 한정되지는 않으며, 단지 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제 1 구성요소는 제 2 구성요소로 명명될 수 있고, 유사하게 제 2 구성요소도 제 1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[17] 본 명세서에서 사용되는 용어에서 단수의 표현은 문맥상 명백하게 다르게 해석되지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 한다. 그리고 "포함한다" 등의 용어는 설시된 특징, 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 의미하는 것이지, 하나 또는 그 이상의 다른 특징들이나 개수, 단계 동작 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 배제하지 않는 것으로 이해되어야 한다.

[18] 도면에 대한 상세한 설명을 하기에 앞서, 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주기능 별로 구분한 것에 불과함을 명확히 하고자 한다. 즉, 이하에서 설명할 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다.

[19] 그리고 이하에서 설명할 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있음은 물론이다. 따라서, 본 명세서를 통해 설명되는 각 구성부들의 존재 여부는 기능적으로 해석되어야 할 것이다.

[20] 도 1은 개시된 기술의 일 실시예에 따른 게이트 출입을 위한 인증 방법에 대한 도면이다. 도 1을 참조하면 게이트 출입을 위한 인증 방법은 이하의 단계들(S110~S180)을 포함한다.

[21] S110 단계에서 게이트 장치가 사용자 단말기에 비콘을 전송한다. 게이트 장치는 일 영역에 진입한 사용자 단말기를 비콘을 이용하여 식별할 수 있다. 기본적으로는 게이트 장치가 사용자 단말기에 비콘을 수신하는 것일 수 있으나 필요에 따라 사용자 단말기가 게이트 장치로 비콘을 전송함으로써 상호

식별하도록 동작할 수도 있다. 사용자 단말기는 사용자가 소지하는 스마트 단말기일 수 있으며, 게이트 장치는 스마트 단말기와 비콘을 주고받을 수 있는 단말기 장치 내지는 이러한 모듈을 별도로 탑재한 장치일 수 있다.

[22] S120 단계에서 게이트 장치는 사용자 단말기의 사용자에 대한 얼굴 이미지를 촬영한다. 게이트 장치는 사용자의 얼굴을 촬영할 수 있는 카메라를 포함한다. 게이트 장치는 비콘을 통해 사용자 단말기가 식별되면 카메라를 초기화하거나 구동하여 사용자의 얼굴을 촬영하여 얼굴 이미지를 획득할수 있다.

[23] 한편, 게이트 장치는 촬영된 얼굴 이미지와 사전에 저장된 복수개의 얼굴 이미지를 비교하여 1차 인증을 수행한다. 일 실시예로, 게이트 장치는 얼굴 이미지를 토대로 템플릿을 생성하고 각각의 템플릿을 비교하는 것으로 1차 인증을 수행할 수 있다. 여기에서 게이트 장치가 직접 사용자를 촬영하여 획득된 얼굴 이미지를 토대로 생성되는 템플릿은 임시템플릿이고, 사전에 저장된 복수개의 얼굴 이미지를 토대로 생성하는 복수개의 템플릿은 인증템플릿이라 한다. 게이트 장치는 복수개의 인증템플릿들 중 임시 템플릿과 일치하거나 유사한 것이 존재하는지 비교함으로써 1차 인증을 수행한다.

[24] 한편, 게이트 장치는 복수개의 인증 템플릿을 사전에 미리 생성하여 데이터베이스에 저장할 수 있으며, 카메라가 사용자의 얼굴 이미지를 촬영하는 시점에 인증템플릿을 생성할 수도 있다. 다만 바람직하게는 1차 인증에 소요되는 시간을 단축시키기 위해서 복수개의 얼굴 이미지 각각에 대한 복수개의 인증템플릿을 미리 생성하고 이를 데이터베이스에 저장할 수 있다.

[25] 한편, 게이트 장치는 1차 인증에 대한 결과를 인증서버에 전송한다. 게이트 장치와 인증서버는 서로 유선 또는 무선으로 통신할 수 있다. 인증서버는게이트 장치가 설치된 현장에서 그리 멀지 않는 상황실과 같은 장소에 배치될 수도 있고 완전히 다른 장소에 배치될 수도 있다. 따라서, 게이트 장치와 인증서버 간의 데이터 전송에 따른 코스트를 고려하여 유선 또는 무선으로 자유롭게 통신환경을 설정할 수 있다.

[26] S130 단계에서 인증서버는 1차 인증에 대한 결과에 따라 사용자가 등록된 사용자인지 판단한다. 예컨대, 복수의 인증템플릿 중 하나가 사용자의 임시템플릿과 일치하거나 유사한 것이 존재하면 사용자가 사전에 등록절차를 마친 것으로 판단할 수 있다. 인증서버는 사용자가 기 등록된 사용자인 것으로 판단하면 사용자 단말기에 2차 인증을 위한 정보를 요청한다. 여기에서 2차 인증을 사용자에 대한 크리덴셜 스터핑(Credantial Stuffing) 방지 및 라이브니스 체크를 위하여 제스쳐를 입력하도록 요청하는 것을 의미한다. 일 실시예로, 사용자 단말기에 설치된 어플리케이션을 통해 사용자가 사전에 등록한 특정한 제스쳐를 입력하도록 하여 이를 영상으로 촬영하도록 제어할 수 있다.

[27] S140 단계에서 사용자 단말기는 인증서버의 요청에 따라 사용자의 제스쳐 영상을 촬영한다. 스마트폰과 같은 단말기이므로 제스쳐 영상을 촬영할 수 있는 카메라가 구비된다. 따라서 어플리케이션이 카메라를 이용하여 사용자의 2차

인증을 위한 제스쳐 영상을 촬영할 수 있다.

[28] S150 단계에서 인증서버는 사용자 단말기로부터 제스처 영상을 수신하여 기등록된 사용자의 제스쳐 영상과 비교한다. 인증서버는 제스쳐 영상을 비교하는 것으로 사용자에 대한 2차 인증을 수행한다. 제스쳐는 사전에 사용자가 등록한 특정한 몸짓이나 손동작 등일 수 있다. 사용자는 OK 사인과 같은 동작을 영상으로 촬영하여 사전에 등록하고 2차 인증을 위해 한번 더 동일한 동작을 입력할 수 있다. 인증서버는 사전에 등록된 제스처 영상과 2차 인증 과정에서 사용자 단말기로부터 수신한 제스쳐 영상을 비교하여 동일성 또는 유사성을 비교할 수 있다. 일 실시예로, 제스쳐 영상에 포함된 특징점이나 벡터값 등을 토대로 유사성을 비교할 수 있다. 2차 인증에서는 사용자의 얼굴 이미지나 지문, 홍채 등의 생체정보를 이용할 수도 있으나 바람직하게는 사용자를 식별할 수 있는 인증은 1차 인증을 통해 수행되고 2차 인증에서는 제스처의 유사도만 비교할 수 있다.

[29] 한편, 인증서버는 2차 인증을 성공하면 S160 단계에 따라 사용자에 대한 출입제한 정보를 조회하여 3차 인증을 수행한다. 3차 인증 과정에서는 사용자가 게이트를 출입하기에 적합한 사용자인지를 판단한다. 이를 위해서 인증서버는 사용자의 출입제한 정보를 조회하여 3차 인증을 수행할 수 있다. 출입제한 정보는 사용자에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나를 포함한다. 인증서버는 복수의 사용자들에 대한 출입제한 정보를 저장하는 데이터베이스를 포함한다. 데이터베이스에는 출입제한 정보 뿐만 아니라 각 사용자들에 대한 템플릿과 제스쳐 영상도 저장된다. 이러한 데이터베이스는 하나의 데이터베이스에 다수의 정보들이 서로 매칭관계를 이루면서 모두 저장될 수도 있고 복수의 데이터베이스에 분산저장될 수도 있다.

[30] 한편, S160 단계에서 인증서버는 3차 인증이 성공한 것으로 판단하면 사용자 단말기에 제어신호를 전송하기 위한 접근권한을 전송하고 3차 인증이 실패한 것으로 판단하면 사용자 단말기에 출입 제한에 따른 알림을 전송한다. 인증서버는 3차 인증에 따라 사용자에 대한 범죄기록이나 출입금지 기록, 입국금지 기록이 조회되면 해당 사용자가 1차 인증과 2차 인증에 성공하였더라도 게이트 출입을 막을 수 있다.

[31] 한편, 인증서버는 3차 인증에 대한 결과를 사용자 단말기에 전송한다. 이에 따라 사용자 단말기는 사용자의 게이트 출입에 따른 출입권한을 수신할 수 있다. 출입권한은 게이트에 접근하여 제어신호를 전송할 수 있는 권한을 포함하는 정보일 수 있다.

[32] S170 단계에서 사용자 단말기는 3차 인증에 대한 결과에 따라 복수개의 게이트 중 출입권한이 부여된 특정 게이트의 위치를 확인한다. 특정 게이트는 사전에 사용자가 통과하기로 결정된 게이트를 의미한다. 사용자 단말기에는 사전에 처리된 티케팅에 따라 발권정보가 저장되어 있다. 이를 이용하여 특정 게이트의 위치를 파악하는 것이 가능하다. 일 실시예로, 사용자 단말기에 설치된

어플리케이션이 3차 인증에 대한 결과를 수신하여 사용자 단말기에 기 저장된 발권정보를 로딩할 수 있다. 발권정보에는 게이트의 위치나 번호 등의 정보가 포함되어 있으며 이러한 정보는 스마트 단말기에서 읽을 수 있는 형태의 데이터일 수 있다. 사용자 단말기는 이러한 발권정보를 토대로 특정 게이트의 위치에 대한 정보를 확인하고 어플리케이션이 이를 화면에 출력할 수 있다.

[33] S180 단계에서 사용자 단말기는 특정 게이트에 구비된 게이트 장치에 제어신호를 전송한다. 사용자 단말기는 어플리케이션을 통해 특정 게이트 장치에 직접 제어신호를 전송한다. S180 단계에는 특정 게이트 장치가 제어신호를 수신함에 따라 인증서버에 응답을 전송하는 단계와 인증서버가 응답을 수신하여 사용자에 대한 인증 결과를 삭제하는 단계가 포함된다. 일 실시에로, 사용자 단말기에서 제어신호가 전송된 직후에 인증서버에 응답을 전송하거나 소정의 대기시간이 도과한 다음에 응답을 전송할 수 있다. 그리고 인증서버는 응답이 수신되면 사용자에 대한 인증 결과를 삭제할 수 있다.

[34] 여기에서 삭제하는 인증 결과는 게이트를 통과하는 사용자에 대한 임시템플릿과 인증템플릿, 그리고 제스쳐 영상을 포함한다. 출입제한 기록의 경우에는 사용자의 생체정보를 기반으로 생성되는 것이 아니므로 인증서버가 계속해서 저장하고 있어도 생체인증에 관련된 보안 가이드라인을 준수하는 것과는 무관하다. 다만 템플릿과 제스쳐 영상의 경우에는 사용자의 신체적 특징에 대한 정보를 포함하고 있는 고유한 정보들이므로 이를 계속해서 저장하고 있는 경우에는 사용자의 생체정보를 기반으로 하는 인증이나 절차에 있어서 정보의 위변조 내지는 유출로 인한 문제가 발생될 수 있으므로 인증서버와 게이트 장치는 이러한 문제를 방지하는 차원에서 게이트 통과에 따른 모든 절차를 성공한 사용자에 대해서는 템플릿과 제스쳐 정보를 삭제함으로써 문제 발생 가능성을 차단할 수 있다.

[35] 도 2는 개시된 기술의 일 실시예에 따른 게이트 출입을 위한 인증 시스템에 대한 도면이다. 도 2를 참조하면 게이트 출입을 위한 인증 시스템은 사용자 단말기, 게이트 장치, 제 1 인증서버 및 제 2 인증서버를 포함한다.

[36] 사용자 단말기는 사용자의 게이트 출입을 위한 어플리케이션을 탑재하고 어플리케이션을 이용하여 사용자의 얼굴 이미지를 토대로 생성된 인증템플릿 및 제스쳐 영상을 등록한다. 사용자 단말기는 게이트 장치 또는 인증서버와 통신할 수 있는 통신모듈(110a)이 구비된다. 그리고 어플리케이션을 저장하는 메모리(110b)와 어플리케이션을 이용한 발권, 제어신호 전송 등을 수행하기 위한 프로세서 또는 CPU가 구비된다. 사용자 단말기는 스마트폰일 수 있으며 이 경우 프로세서는 AP(110c)가 그 역할을 수행할 수 있다.

[37] 게이트 장치는 비콘을 이용하여 사용자 단말기를 식별한다. 예컨대, 게이트 장치가 전송한 비콘에 대하여 사용자 단말기로부터 응답을 회신하는 것으로 사용자 단말기를 식별할 수 있다. 또는 사용자 단말기로부터 비콘을 수신하고 이에 대한 응답을 사용자 단말기에 전송하는 것으로 식별할 수 있다. 게이트

장치는 비콘을 전송 또는 수신할 수 있는 BLE 모듈(120a)을 포함한다. BLE 모듈(120a)를 이용하여 블루투스 통신이 가능한 영역 이내로 진입한 사용자 단말기에 비콘을 전송함으로써 사용자 단말기를 식별할 수 있다.

[38] 한편, 게이트 장치는 비콘에 따라 사용자 단말기를 식별하면 사용자 단말기의 사용자에 대한 얼굴 이미지를 촬영하여 임시 템플릿을 생성한다. 게이트 장치는 사용자의 얼굴 이미지를 촬영하기 위한 카메라(120b)가 구비된다. 일 실시예로, 사용자 단말기를 식별함에 따라 카메라(120b)의 구동신호가 생성될 수 있다. 게이트 장치는 카메라(120b)를 이용하여 사용자의 얼굴 이미지를 촬영하고 이미지를 이용하여 임시템플릿을 생성한다.

[39] 한편, 게이트 장치는 사용자가 사전에 등록한 인증템플릿과 얼굴 이미지를 토대로 생성한 임시템플릿을 비교하여 1차 인증을 수행한다. 게이트 장치에는 다수의 인증템플릿을 저장하는 데이터베이스(120c)가 구비된다. 게이트 장치는 데이터베이스에 저장된 인증템플릿과 임시템플릿을 비교하여 일치하거나 유사한 템플릿이 존재하는지 확인할 수 있다.

[40] 한편, 도 2에 도시된 바와 같이 인증서버는 제 1 인증서버 및 제 2 인증서버로 구분될 수 있다. 각각의 인증서버는 서로 다른 인증을 수행할 수 있다. 먼저, 제 1 인증서버는 게이트 장치로부터 1차 인증에 대한 결과를 수신한다. 제 1 인증서버는 1차 인증에 대한 결과에 따라 사용자가 기 등록된 사용자인 것으로 판단하면 사용자 단말기에 제스쳐 영상을 요청할 수 있다. 제 1 인증서버는 사용자 단말기에 제스쳐 영상을 요청하기 위해서 통신모듈(130a)을 포함한다. 그리고 제스쳐 영상을 저장할 수 있는 데이터베이스(130b)와 통신모듈 및 데이터베이스를 제어하기 위한 프로세서(130c)가 구비된다.

[41] 한편, 제 1 인증서버는 복수의 사용자들에 대한 제스쳐 영상을 저장하는 데이터베이스가 구비된다. 제스쳐 영상이 저장되는 데이터베이스를 제 1 데이터베이스라 한다. 제 1 인증서버는 요청에 따라 사용자 단말기로부터 제스쳐 영상이 수신되면 데이터베이스(130b)를 검색하여 사용자 단말기에서 미리 등록한 제스쳐 영상을 검색하고 요청에 따른 제스쳐 영상과 비교할 수 있다. 이와 같이 제스쳐 영상을 비교하는 것으로 2차 인증을 수행할 수 있다.

[42] 제 2 인증서버는 제 1 인증서버와 통신하여 2차 인증에 대한 결과를 수신한다. 제 2 인증서버는 사용자가 2차 인증에 통과한 것으로 판단하면 해당 사용자에 대한 출입제한 정보를 조회한다. 출입제한 정보는 사용자에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나를 포함하며 제 2 인증서버의 데이터베이스에는 복수의 등록된 사용자들에 대한 출입제한 정보들이 저장된다. 제 2 인증서버는 2차 인증에 대한 결과를 수신하기 위한 통신모듈(140a), 출입제한 정보를 저장하는 데이터베이스(140b) 및 통신모듈(140a)과 데이터베이스(140b)를 제어하는 프로세서(140c)를 포함한다. 통신모듈(140a)은 2차 인증에 대한 결과 뿐 아니라 사용자 단말기와 통신하거나 게이트 장치와 통신하는 경우에도 이용된다. 이를 위해서 통신모듈(140a)은

블루투스를 포함한 여러가지 다른 종류의 통신 방식을 지원한다.

[43] 한편, 통신모듈(140a)dp 따라 2차 인증에 대한 결과를 수신하면 제 2 프로세서(140c)는 데이터베이스(140b)에 저장된 사용자에 대한 출입제한 정보를 조회하여 3차 인증을 수행한다. 제 2 인증서버는 3차 인증에 성공한 것으로 판단하면 사용자 단말기에 상기 게이트 출입을 위한 접근권한을 전송하고, 사용자 단말기는 접근권한에 따라 출입 가능한 특정 게이트에 구비된 게이트 장치에 제어신호를 전송할 수 있다. 물론 3차 인증이 실패한 것으로 판단하면 사용자 단말기에 출입 제한에 따른 알림을 전송할 수 있다.

[44] 한편, 제 2 인증서버는 3차 인증에 대한 결과를 사용자 단말기에 전송한다. 제 2 인증서버는 통신모듈(140a)을 이용하여 3차 인증에 대한 결과를 전송할 수 있다. 사용자 단말기는 3차 인증에 대한 결과를 수신하면 특정 게이트 장치에 제어신호를 전송할 수 있다.

[45] 한편, 제 2 인증서버는 사용자 단말기가 제어신호를 전송한 것을 확인하여 템플릿을 삭제할 수 있다. 일 실시예로, 제 2 인증서버가 특정 게이트에 구비된 게이트 장치와 통신하여 제어신호를 수신하였음을 알리는 응답을 수신할 수 있다. 이 경우 제 2 인증서버는 등록된 인증템플릿과 임시템플릿을 삭제할 수 있다. 즉, 인증에 이용된 사용자의 생체정보 기반의 데이터를 삭제함으로써 생체정보 보호 가이드라인을 준수할 수 있다.

[46] 한편, 제 2 인증서버는 특정 게이트에 구비된 게이트 장치가 제어신호를 수신한 것을 확인하면 제 1 인증서버와 통신하여 등록된 제스쳐 영상 과 요청한 제스쳐 영상을 삭제하도록 할 수 있다. 제 1 인증서버 또한 생체정보 보호 가이드라인을 준수하기 위해서 데이터베이스에 저장된 제스쳐 영상을 삭제할 수 있다. 일 실시예로, 제 1 인증서버가 서로 통신하여 특정 게이트 장치에서 제어신호를 수신하였음을 알리는 응답을 제 2 인증서버를 통해 전달받을 수 있다. 물론 제 1 인증서버가 특정 게이트 장치와 직접 통신하여 제어신호에 대한 응답을 수신할 수도 있다. 제 2 인증서버가 템플릿을 삭제하는 것과 마찬가지로 제 1 인증서버 또한 미리 등록한 제스쳐 영상과 사용자 단말기에 요청한 제스쳐 영상을 삭제할 수 있다.

[47] 도 3은 게이트에 구비된 게이트 장치를 나타낸 도면이다. 도 3을 참조하면 하나의 게이트마다 게이트 장치가 구비될 수 있다. 각 게이트에 구비된 게이트 장치는 주변으로 접근하는 사용자의 얼굴을 촬영하기 위한 카메라가 구비된다. 사용자의 얼굴에 포함된 생체정보를 보다 정확하게 식별하기 위해서 카메라는 게이트의 중앙에 배치될 수 있다. 도 3과 같이 게이트는 좌우로 슬라이딩되어 열리는 구조일 수 있으며 게이트가 마주보는 일 영역에 게이트 장치가 배치될 수 있는 공간을 형성하여 게이트 장치를 정면으로 배치할 수 있다. 게이트 장치는 카메라가 탑재된 단말기 형태의 장치일 수 있으며 필요에 따라 카메라만 게이트의 정면에 배치되고 카메라를 제외한 나머지 장치는 게이트의 주변이나 게이트가 고정되는 구조물의 내부에 삽입될 수도 있다.

[48] 한편, 게이트 장치는 비콘을 이용하여 사용자가 소지한 사용자 단말기를 식별할 수 있고 카메라를 이용하여 사용자의 얼굴 이미지를 촬영할 수 있다. 게이트 장치는 사용자 단말기에 비콘을 전송하거나 사용자 단말기로부터 비콘을 수신할 수 있으며 비콘을 통해 무선으로 통신할 수 있는 밤위가 설정된다. 예컨대, 블루투스로 통신할 수 있는 통신범위이 설정될 수 있다. 일반적으로 BLE 기반 통신의 경우 50미터 정도의 통신범위가 형성되며 게이트 장치 또한 이와 유사하거나 동일하게 통신범위가 설정될 수 있다.

[49] 한편, 게이트 장치는 사용자의 얼굴 이미지를 촬영할 수 있는 범위도 설정될 수 있다. 예컨대, 사용자의 얼굴에 포함된 특징정보를 정확하게 식별할 수 있는 거리에 사용자가 위치할 수 있도록 소정의 촬영범위가 설정될 수 있다. 일반적으로는 통신범위가 촬영범위보다 넓은 범위로 형성되기 때문에 도 6에 도시한 바와 같이 촬영범위와 통신범위는 서로 다를 수 있다. 다만 블루투스 모듈의 통신감도나 범위 등을 제한하거나 고성능의 카메라를 구비하는 것으로 촬영범위와 통신범위를 동일하게 설정하는 것도 가능하다. 이와 같이 설정하면 사용자가 게이트에 일정 이상 접근하면 위치를 이동하지 않고 그 자리에서 인증을 수행할 수도 있다. 이때, 게이트 장치를 손으로 터치하거나 자신의 단말기에 별도의 입력을 하지 않아도 자동으로 어플리케이션이 활성화되어 인증과정이 수행되기 때문에 인증 과정에 별다른 불편한 없이 게이트를 출입할 수 있다.

[50] 개시된 기술의 일 실시예에 따른 게이트 출입을 위한 인증 방법 및 시스템은 이해를 돕기 위하여 도면에 도시된 실시 예를 참고로 설명되었으나, 이는 예시적인 것에 불과하며, 당해 분야에서 통상적 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 개시된 기술의 진정한 기술적 보호범위는 첨부된 특허청구범위에 의해 정해져야 할 것이다.

청구범위

[청구항 1] 게이트 장치가 일 영역에 진입한 사용자 단말기에 비콘을 전송하는 단계;
상기 게이트 장치가 상기 사용자 단말기의 사용자에 대한 얼굴 이미지를 촬영하고 상기 얼굴 이미지 및 사전에 저장된 복수개의 얼굴 이미지를 비교하여 1차 인증을 수행하고 상기 1차 인증에 대한 결과를 인증서버에 전송하는 단계;
상기 인증서버가 상기 1차 인증에 대한 결과에 따라 상기 사용자가 기 등록된 사용자인 것으로 판단하면 상기 사용자 단말기에 2차 인증을 위한 정보를 요청하는 단계;
상기 사용자 단말기가 상기 인증서버의 요청에 따라 상기 사용자가 입력하는 제스쳐를 영상으로 촬영하는 단계;
상기 인증서버가 상기 영상을 수신하여 기 등록된 상기 사용자의 제스쳐 영상과 비교하여 상기 2차 인증을 수행하는 단계;
상기 인증서버가 상기 사용자에 대한 출입제한 정보를 조회하여 3차 인증을 수행하고 상기 3차 인증에 대한 결과를 상기 사용자 단말기에 전송하는 단계;
상기 사용자 단말기가 상기 3차 인증에 대한 결과에 따라 복수개의 게이트 중 출입권한이 부여된 특정 게이트의 위치를 확인하는 단계; 및
상기 사용자 단말기가 상기 특정 게이트에 구비된 게이트 장치에 제어신호를 전송하는 단계;를 포함하는 게이트 출입을 위한 인증 방법.

[청구항 2] 제 1 항에 있어서, 상기 인증서버에 전송하는 단계는,
상기 게이트 장치가 상기 얼굴 이미지를 이용하여 임시템플릿을 생성하고 복수개의 얼굴 이미지를 토대로 생성된 복수개의 인증템플릿과 상기 임시템플릿을 비교하여 상기 1차 인증을 수행하는 게이트 출입을 위한 인증 방법.

[청구항 3] 제 1 항에 있어서,
상기 인증서버는 복수의 사용자들에 대한 템플릿, 제스쳐 영상 및 출입제한 정보를 저장하는 데이터베이스를 포함하고 사전에 상기 게이트 장치에 템플릿을 전송하는 게이트 출입을 위한 인증 방법.

[청구항 4] 제 1 항에 있어서, 상기 제어신호를 전송하는 단계는,
상기 특정 게이트 장치가 상기 제어신호를 수신함에 따라 상기 인증서버에 응답을 전송하는 단계; 및
상기 인증서버가 상기 응답을 수신하여 상기 사용자에 대한 인증 결과를 삭제하는 단계를 포함하는 게이트 출입을 위한 인증 방법.

[청구항 5] 제 1 항에 있어서, 상기 제어신호를 전송하는 단계는,
상기 특정 게이트 장치가 상기 제어신호를 수신함에 따라 상기 인증서버에 응답을 전송하는 단계; 및

상기 인증서버가 상기 응답을 수신하여 상기 사용자에 대한 임시 템플릿, 인증 템플릿 및 제스쳐 영상을 삭제하는 게이트 출입을 위한 인증 방법.

[청구항 6] 제 1 항에 있어서, 특정 게이트의 위치를 확인하는 단계는,
상기 사용자 단말기에 설치된 어플리케이션이 상기 3차 인증에 대한 결과를 수신하여 상기 사용자 단말기에 기 저장된 발권정보를 로딩하고 상기 특정 게이트의 위치에 대한 정보를 화면에 출력하는 게이트 출입을 위한 인증 방법.

[청구항 7] 제 1 항에 있어서,
상기 인증서버는 상기 3차 인증이 성공한 것으로 판단하면 상기 사용자 단말기에 상기 제어신호를 전송하기 위한 접근권한을 전송하고 상기 3차 인증이 실패한 것으로 판단하면 상기 사용자 단말기에 출입 제한에 따른 알림을 전송하는 게이트 출입을 위한 인증 방법.

[청구항 8] 제 1 항에 있어서,
상기 출입제한 정보는 상기 사용자에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나를 포함하는 게이트 출입을 위한 인증 방법.

[청구항 9] 사용자의 게이트 출입을 위한 어플리케이션을 탑재하고 상기 어플리케이션을 이용하여 상기 사용자의 얼굴 이미지를 토대로 생성된 인증템플릿 및 제스쳐 영상을 등록하는 사용자 단말기;
비콘을 이용하여 상기 사용자 단말기를 식별하면 상기 사용자 단말기의 사용자에 대한 얼굴 이미지를 촬영하여 임시 템플릿을 생성하고 상기 등록된 인증 템플릿과 상기 임시템플릿을 비교하여 1차 인증을 수행하는 게이트 장치; 및
상기 1차 인증에 대한 결과를 수신하여 상기 사용자가 기 등록된 사용자인 것으로 판단하고 상기 사용자 단말기에 제스쳐 영상을 요청하여 상기 등록된 제스쳐 영상과 비교함으로써 2차 인증을 수행하는 제 1 인증서버; 및
상기 제 1 인증서버에서 상기 2차 인증에 대한 결과를 수신하면 상기 사용자에 대한 출입제한 정보를 조회하여 3차 인증을 수행하고 상기 3차 인증에 대한 결과를 상기 사용자 단말기에 전송하는 제 2 인증서버;를 포함하는 게이트 출입을 위한 인증 시스템.

[청구항 10] 제 9 항에 있어서,
상기 제 1 인증서버는 복수의 사용자들에 대한 제스쳐 영상을 저장하는 제 1 데이터베이스를 포함하고 상기 데이터베이스에서 상기 사용자 단말기에서 등록한 제스쳐 영상을 검색하고 상기 요청한 제스쳐 영상과 비교하는 게이트 출입을 위한 인증 시스템.

[청구항 11] 제 9 항에 있어서,
상기 제 2 인증서버는 상기 3차 인증에 성공한 것으로 판단하면 상기 사용자 단말기에 상기 게이트 출입을 위한 접근권한을 전송하고,

상기 사용자 단말기는 상기 접근권한에 따라 출입 가능한 특정 게이트에 구비된 게이트 장치에 제어신호를 전송하는 게이트 출입을 위한 인증 시스템.

[청구항 12] 제 11 항에 있어서,
상기 제 2 인증서버는 상기 특정 게이트에 구비된 게이트 장치가 상기 제어신호를 수신하면 상기 게이트 장치와 통신하여 상기 등록된 인증템플릿 및 상기 임시템플릿을 삭제하는 게이트 출입을 위한 인증 시스템.

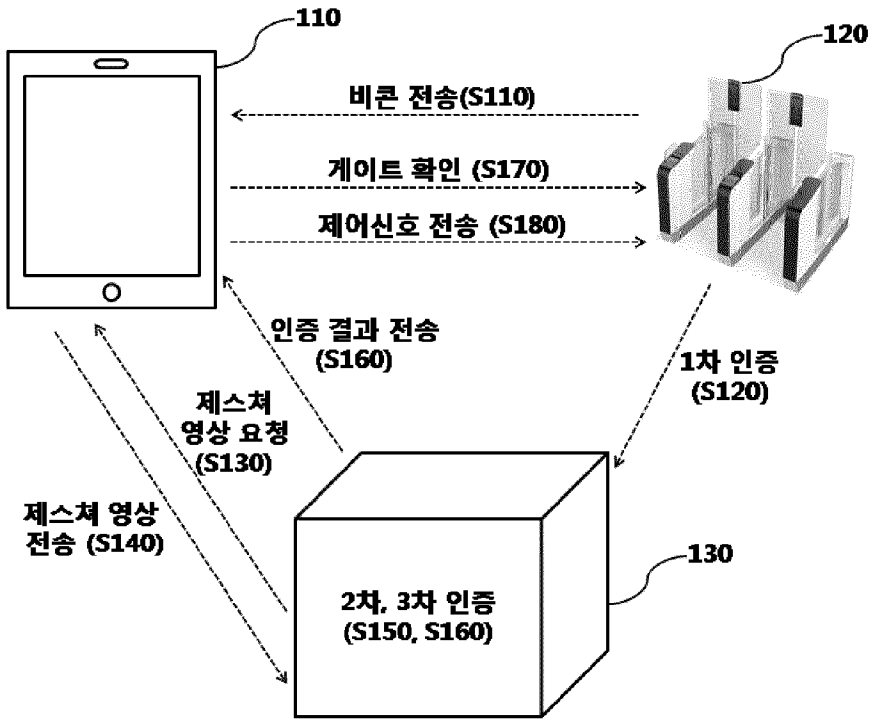
[청구항 13] 제 11 항에 있어서,
상기 제 2 인증서버는 상기 특정 게이트에 구비된 게이트 장치가 상기 제어신호를 수신하면 상기 제 1 인증서버와 통신하여 상기 등록된 제스쳐 영상 및 상기 요청한 제스쳐 영상을 삭제하는 게이트 출입을 위한 인증 시스템.

[청구항 14] 제 9 항에 있어서,
상기 제 2 인증서버는 상기 3차 인증이 실패한 것으로 판단하면 상기 사용자 단말기에 출입 제한에 따른 알림을 전송하는 게이트 출입을 위한 인증 시스템.

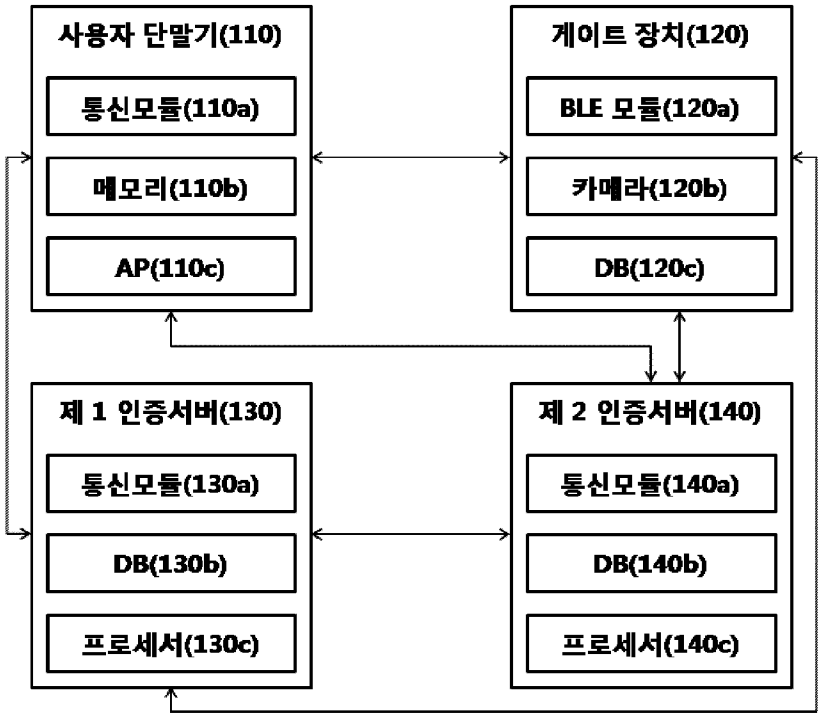
[청구항 15] 제 9 항에 있어서,
상기 출입제한 정보는 상기 사용자에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나를 포함하는 게이트 출입을 위한 인증 시스템.

WO 2022/045508 PCT/KR2021/002773

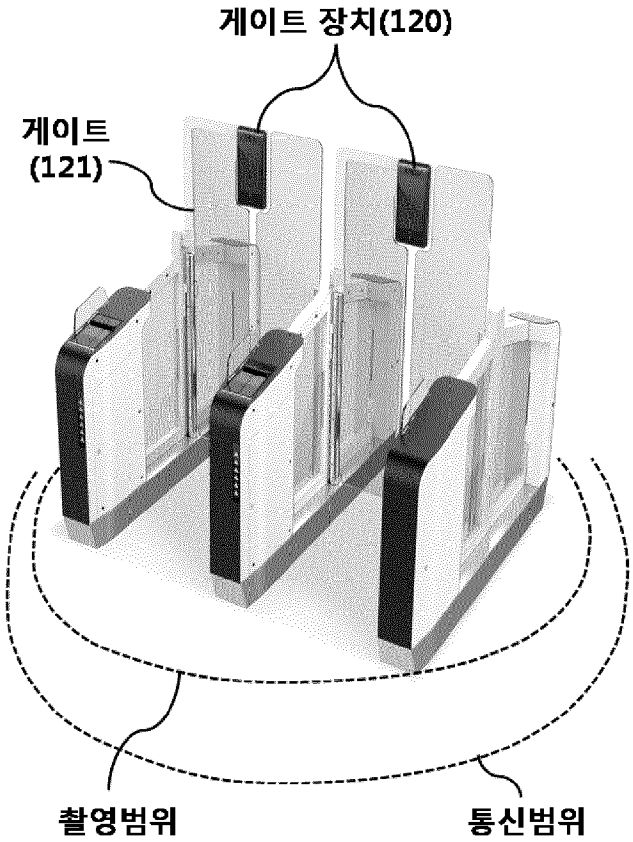
[도1]



[도2]



[도3]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2021/002773

A. CLASSIFICATION OF SUBJECT MATTER

G07C 9/00(2006.01)i; **G07C 9/37**(2020.01)i; **G07C 9/38**(2020.01)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)

G07C 9/00(2006.01); G06Q 50/10(2012.01); H04W 84/18(2009.01)

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: 게이트 출입(gate access), 얼굴 인식(face recognition), 비콘(beacon), 위치(location)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-1907958 B1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 16 October 2018 (2018-10-16) See paragraphs [0040]-[0088] and figures 1-6.	1-15
Y	KR 10-2019-0051751 A (SUPREMA HQ INC) 15 May 2019 (2019-05-15) See paragraphs [0036]-[0081], [0103]-[0180] and [0269]-[0271] and figures 2, 5 and 14-15.	1-15
Y	KR 10-2020-0092608 A (JEONG, Seong Hyun) 04 August 2020 (2020-08-04) See paragraph [0052].	1-15
Y	KR 10-0789370 B1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 28 December 2007 (2007-12-28) See paragraphs [0044]-[0048] and figures 1-2.	1-8
Y	KR 10-1939696 B1 (EVER INFORMATION TECHNOLOGY CO., INC.) 17 January 2019 (2019-01-17) See paragraphs [0036]-[0038] and figure 1.	3

☐ 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
14 December 2021	**14 December 2021**

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
Information on patent family members

International application No.
PCT/KR2021/002773

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
KR 10-1907958 B1	16 October 2018	KR 10-2017-0079857 A	10 July 2017
		US 2017-0195322 A1	06 July 2017
KR 10-2019-0051751 A	15 May 2019	KR 10-2020-0107896 A	16 September 2020
		KR 10-2151843 B1	04 September 2020
		US 10755500 B2	25 August 2020
		US 2019-0139342 A1	09 May 2019
		US 2020-0349782 A1	05 November 2020
KR 10-2020-0092608 A	04 August 2020	None	
KR 10-0789370 B1	28 December 2007	EP 2074539 A1	01 July 2009
		US 2010-0321150 A1	23 December 2010
		WO 2008-048020 A1	24 April 2008
KR 10-1939696 B1	17 January 2019	None	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2021/002773

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G07C 9/00(2006.01)i; **G07C 9/37**(2020.01)i; **G07C 9/38**(2020.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G07C 9/00(2006.01); G06Q 50/10(2012.01); H04W 84/18(2009.01)

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: 게이트 출입(gate access), 얼굴 인식(face recognition), 비콘(beacon), 위치(location)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-1907958 B1 (한국전자통신연구원) 2018.10.16 단락 [0040]-[0088] 및 도면 1-6	1-15
Y	KR 10-2019-0051751 A (주식회사 슈프리마에이치큐) 2019.05.15 단락 [0036]-[0081], [0103]-[0180], [0269]-[0271] 및 도면 2, 5, 14-15	1-15
Y	KR 10-2020-0092608 A (정성현) 2020.08.04 단락 [0052]	1-15
Y	KR 10-0789370 B1 (한국전자통신연구원) 2007.12.28 단락 [0044]-[0048] 및 도면 1-2	1-8
Y	KR 10-1939696 B1 (주식회사 에버정보기술) 2019.01.17 단락 [0036]-[0038] 및 도면 1	3

☐ 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
2021년12월14일(14.12.2021)	**2021년12월14일(14.12.2021)**

ISA/KR의 명칭 및 우편주소

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

팩스 번호 **+82-42-481-8578**

심사관

박혜련

전화번호 **+82-42-481-3463**

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2021/002773

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-1907958 B1	2018/10/16	KR 10-2017-0079857 A	2017/07/10
		US 2017-0195322 A1	2017/07/06
KR 10-2019-0051751 A	2019/05/15	KR 10-2020-0107896 A	2020/09/16
		KR 10-2151843 B1	2020/09/04
		US 10755500 B2	2020/08/25
		US 2019-0139342 A1	2019/05/09
		US 2020-0349782 A1	2020/11/05
KR 10-2020-0092608 A	2020/08/04	없음	
KR 10-0789370 B1	2007/12/28	EP 2074539 A1	2009/07/01
		US 2010-0321150 A1	2010/12/23
		WO 2008-048020 A1	2008/04/24
KR 10-1939696 B1	2019/01/17	없음	