

명세서

발명의 명칭: 게이트 출입을 위한 인증 방법 및 장치

기술분야

- [1] 개시된 기술은 사용자 생체정보 기반 템플릿을 이용하여 게이트 출입을 위한 인증을 수행하는 방법 및 단말기에 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 이중으로 수행하는 방법 및 단말기를 제공하는데 있다.

과제 해결 수단

- [6] 상기의 기술적 과제를 이루기 위하여 개시된 기술의 제 1 측면은 사용자 단말기가 비콘을 이용하여 복수개의 게이트 각각에 구비된 게이트 장치들을 식별하는 단계, 상기 사용자 단말기가 사전에 저장된 생체정보를 이용하여 인증을 수행하고 상기 인증에 대한 결과를 인증서버에 전송하는 단계, 상기 사용자 단말기가 상기 복수개의 게이트 중 출입권한이 부여된 특정 게이트의 위치를 확인하는 단계, 상기 인증서버가 상기 인증에 대한 결과를 수신하고 상기 사용자 단말기의 사용자에 대한 출입 가능 여부를 확인하는 단계 및 상기 사용자 단말기가 상기 출입 가능 여부에 따라 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 사용자 단말기가 복수개의 게이트 각각에 구비된 게이트 장치들 중 적어도 하나에서 비콘을 수신하는 단계, 상기 사용자 단말기가 상기 비콘을 수신함에 따라 어플리케이션을 활성화하여 사용자의 얼굴 이미지를 촬영하는 단계, 상기 사용자 단말기가 상기 얼굴 이미지를 토대로 임시템플릿을 생성하고 사전에 저장된 인증템플릿과 비교하여 인증을 수행하는 단계, 상기 사용자 단말기가 상기 인증에 대한 결과에 따라 상기 복수개의 게이트 중 출입권한이 부여된 특정 게이트의 위치를 확인하는 단계, 상기 사용자 단말기가 상기 인증에 대한 결과 및 상기 출입권한에 대한 정보를 인증서버에 전송하는 단계, 상기 인증서버가 상기 인증에 대한 결과를 토대로 상기 사용자 단말기의 사용자에 대한 출입 가능 여부를 확인하는 단계 및 상기 인증서버가 상기 출입 가능 여부를 확인한 결과 및 상기 출입권한에 대한 정보에 따라 상기 특정 게이트에 제어신호를 전송하는 단계를 포함하는 게이트 출입을 위한 인증 방법을 제공하는데 있다.
- [8] 상기의 기술적 과제를 이루기 위하여 개시된 기술의 제 3 측면은 사용자 단말기가 복수개의 게이트 각각에 구비된 게이트 장치들 중 근거리 무선 통신이 가능한 영역 이내에 위치한 일부의 게이트 장치에 비콘을 전송하는 단계, 상기 일부의 게이트 장치 중 상기 사용자 단말기와 가장 인접한 위치의 특정 게이트 장치가 상기 비콘에 따라 카메라를 구동하여 사용자의 얼굴 이미지를 촬영하는 단계, 인증서버가 상기 특정 게이트 장치로부터 상기 얼굴 이미지를 수신하고 데이터베이스에 등록된 복수 사용자들의 생체정보들과 비교하여 인증을 수행하는 단계, 상기 인증서버가 상기 인증 결과에 따라 상기 사용자에 대한 출입 가능 여부를 확인하는 단계, 상기 사용자 단말기가 상기 인증서버로부터 상기 인증 결과 및 상기 출입 가능 여부를 회신하고 상기 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.
- [9] 상기의 기술적 과제를 이루기 위하여 개시된 기술의 제 4 측면은 사용자 단말기가 복수개의 게이트 각각에 구비된 게이트 장치들 중 근거리 무선 통신이 가능한 영역 이내에 위치한 일부의 게이트 장치에 비콘을 전송하는 단계, 상기 일부의 게이트 장치 중 상기 사용자 단말기와 가장 인접한 위치의 특정 게이트 장치가 상기 비콘에 따라 카메라를 구동하여 사용자의 얼굴 이미지를 촬영하는 단계, 상기 특정 게이트 장치가 상기 사용자의 얼굴 이미지를 이용하여 임시템플릿을 생성하고 기 저장된 복수개의 생체정보를 토대로 생성된 복수개의 인증템플릿들과 비교하여 인증을 수행하는 단계, 인증서버가 상기 특정 게이트 장치로부터 상기 인증에 대한 결과를 수신하여 상기 사용자에 대한 출입 가능 여부를 확인하는 단계, 상기 사용자 단말기가 상기 인증서버로부터 상기 인증에 대한 결과 및 상기 출입 가능 여부를 회신하고 상기 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.

- [10] 상기의 기술적 과제를 이루기 위하여 개시된 기술의 제 5 측면은 일정 주기마다 비콘을 전송하여 통신이 가능한 영역에 접근하는 사용자 단말기를 감지하는 블루투스 모듈, 상기 사용자 단말기의 사용자가 촬영이 가능한 영역에 접근하면 상기 사용자의 얼굴 이미지를 촬영하는 카메라, 상기 얼굴 이미지를 토대로 템플릿을 생성하고 상기 템플릿과 기 저장된 복수의 사용자들에 대한 복수개의 템플릿을 비교하여 상기 사용자에 대한 인증을 수행하는 인증모듈 및 상기 인증모듈에서 수신된 인증 결과에 따라 게이트를 개방하는 게이트 제어모듈을 포함하는 게이트 출입을 위한 인증 장치를 제공하는데 있다.

발명의 효과

- [11] 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.
- [12] 개시된 기술의 일 실시예에 따르면 게이트 출입을 위한 인증 방법 및 장치는 생체정보 기반 이중 인증을 통해 사용자의 게이트 출입을 신속하고 정확하게 처리하는 효과가 있다.
- [13] 또한, 인증이 완료된 사용자의 생체정보를 저장하지 않아서 생체정보 보호 가이드라인을 준수하는 효과가 있다.
- [14] 또한, 게이트 출입을 위한 별도의 입력이나 신체 일부를 접촉할 필요가 없어서 인증 과정에 따른 편의성이 증대되는 효과가 있다.

도면의 간단한 설명

- [15] 도 1은 개시된 기술의 일 실시예에 따른 사용자 단말기 중심의 게이트 출입을 위한 인증 방법에 대한 도면이다.
- [16] 도 2는 개시된 기술의 일 실시예에 따른 인증서버 중심의 게이트 출입을 위한 인증 방법에 대한 도면이다.
- [17] 도 3은 개시된 기술의 일 실시예에 따른 게이트 장치와 인증서버 중심의 게이트 출입을 위한 인증 방법에 대한 도면이다.
- [18] 도 4는 개시된 기술의 일 실시예에 따른 게이트 장치 중심의 게이트 출입을 위한 인증 방법에 대한 도면이다.
- [19] 도 5는 개시된 기술의 일 실시예에 따른 게이트 출입을 위한 인증 장치를 나타낸 도면이다.
- [20] 도 6은 게이트에 구비된 게이트 장치를 나타낸 도면이다.

발명의 실시를 위한 최선의 형태

- [21] 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.

- [22] 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.
- [23] 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.
- [24] 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.
- [25] 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.
- [26] 도 1은 개시된 기술의 일 실시예에 따른 사용자 단말기 중심의 게이트 출입을 위한 인증 방법에 대한 도면이다. 도 1을 참조하면 게이트 출입을 위한 인증 방법은 이하의 단계들(S110~S150)을 포함한다.
- [27] S110 단계에서 사용자 단말기는 비콘을 이용하여 복수개의 게이트 각각에 구비된 게이트 장치들을 식별한다. 사용자 단말기는 일정 주기마다 주변에 비콘을 전송하여 이를 게이트 장치가 수신하게 하거나 게이트 장치에서 전송되는 비콘을 수신하여 게이트 장치를 식별할 수 있다. 여기에서 사용자 단말기는 사용자가 소지하는 스마트 단말기일 수 있다. 그리고 게이트 장치는 스마트 단말기와 비콘을 주고받을 수 있는 단말기 장치 내지는 이러한 모듈을 별도로 탑재한 장치일 수 있다.
- [28] 사용자 단말기는 복수개의 게이트 장치들 중 근거리 무선 통신이 가능한 영역

이내에 위치한 적어도 하나의 게이트 장치가 식별되면 생체정보를 이용한 인증을 수행하는 어플리케이션을 활성화한다. 어플리케이션은 게이트 장치와 통신하기 위해서 사용자가 사전에 설치하거나 현장에서 즉석으로 설치할 수 있다. 게이트 장치는 사용자 단말기에 어플리케이션이 미설치되어 있으면 어플리케이션을 다운로드할 수 있는 URL을 전송하거나 근거리 무선 통신을 통해 직접 어플리케이션을 전송할 수 있다.

- [29] S120 단계에서 사용자 단말기는 기 저장된 생체정보를 이용하여 인증을 수행하고 인증에 대한 결과를 인증서버에 전송한다. 사용자 단말기에는 사용자가 게이트 출입을 수행하기 이전에 생체정보가 저장된다. 여기에서 생체정보는 사용자의 얼굴 이미지일 수 있으며 홍채 또는 지문과 같이 사용자를 식별할 수 있는 고유한 정보를 생체정보로 이용할 수 있다. 이러한 생체정보는 사용자 단말기에 포함된 카메라 또는 센서를 이용하여 획득할 수 있다. 예컨대, 카메라를 이용하여 사용자의 얼굴 이미지를 촬영하는 것으로 얼굴 이미지에 포함된 생체정보를 획득할 수 있다.
- [30] 한편, 사용자 단말기는 이하의 세부적인 단계들을 S120 단계에서 수행한다. 먼저 생체정보를 사전에 저장하는 단계를 수행한다. 그리고 생체정보를 이용하여 인증템플릿을 생성하는 단계를 수행한다. 그리고 어플리케이션을 이용하여 현장에서 사용자의 생체정보를 촬영하는 단계를 수행한다. 그리고 촬영된 생체정보를 이용하여 임시템플릿을 생성하는 단계를 수행한다. 그리고 인증템플릿과 임시템플릿을 비교하여 인증을 수행하는 단계를 수행한다. 이와 같은 과정들이들이 S120 단계에서 하나의 프로세스처럼 수행될 수 있으며 사용자 단말기가 직접 사용자의 생체정보를 기반으로 하는 인증을 수행하게 된다.
- [31] 여기에서 인증은 두 개의 생체정보를 토대로 생성된 템플릿을 비교하는 것으로 수행될 수 있다. 예컨대, 기 저장된 사용자의 생체정보와 즉석에서 획득된 동일한 종류의 생체정보를 이용하여 각각 템플릿을 생성하고 두 템플릿을 비교하는 것으로 인증을 수행할 수 있다. 여기에서 사용자 단말기는 생체정보를 토대로 추출된 템플릿의 유사도를 비교하는 것으로 인증을 수행할 수 있다. 템플릿은 생체정보의 특징을 추출하고 분석해서 저장되는 일종의 데이터를 의미한다. 이러한 데이터는 소정의 방식으로 부호화(encoding)되어 사용자 단말기에 저장된다.
- [32] 사용자 단말기는 기 저장된 생체정보를 토대로 템플릿을 생성할 수 있으며 즉석에서 획득된 생체정보를 이용하여 동일한 과정에 따라 템플릿을 생성할 수 있다. 당연히 같은 동일한 사용자의 얼굴 이미지를 토대로 생성된 템플릿은 생성 시기만 다를 뿐 동일하거나 높은 유사도를 갖는 것이 바람직하다. 다만, 실제 얼굴을 촬영하는데 있어서 촬영각도나 방향 등에 따라 얼굴에 포함된 특징점이 정확하게 촬영되지 않을 수도 있다. 따라서 완벽하게 일치하지 않더라도 동일 사용자를 판단할 수 있는 기준에 따라 일정 이상의 유사도를 만족하면 동일한

사용자로 판단하는 근거가 될 수 있다. 사용자 단말기는 이와 같이 두 템플릿의 유사도를 비교하여 기준값을 초과하면 동일한 사용자로 판단하고, 기준값 미만이면 다른 사용자로 판단할 수 있다. 이와 같이 생체정보를 기반으로 하는 인증방식은 다수의 기술들이 공지되어 있으며 이러한 기술을 응용하거나 결합하여 사용자를 인증하는 것이 가능하다. 이하부터는 기 저장된 생체정보를 토대로 생성되는 템플릿을 인증템플릿이라 하고, 즉석에서 획득된 생체정보를 이용하여 생성되는 템플릿을 임시템플릿이라 한다.

- [33] 한편, 사용자 단말기는 인증에 대한 결과를 인증서버에 전송한다. 즉, 인증을 수행하는 주체가 사용자 단말기이며 인증서버는 사용자 단말기에서 처리된 결과를 수신하게 된다. 여기에서 인증서버는 사용자 단말기로부터 인증에 대한 결과만을 수신할 수도 있고, 생체정보 및 인증에 대한 결과를 모두 수신할 수 있다. 인증서버는 생체정보와 인증에 대한 결과를 데이터로 저장하는 데이터베이스를 포함한다.
- [34] S130 단계에서 사용자 단말기는 복수개의 게이트 중 출입권한이 부여된 특정 게이트의 위치를 확인한다. 상술한 바와 같이 복수의 게이트 각각에 게이트 장치들이 구비되어 있는데 사용자는 이 중 특정 게이트를 통과할 수 있는 권한이 부여된다. 사전에 발권한 정보를 토대로 특정 루트나 플랫폼으로 이동하기 위해 통과해야 하는 게이트가 정해져 있기 때문에 사용자 단말기는 출입권한이 부여된 특정 게이트의 위치를 확인한다. 일 실시예로, 사용자 단말기에 설치된 어플리케이션이 발권정보를 이용하여 출입권한이 부여된 게이트의 위치에 대한 정보나 특정 게이트의 번호를 사용자 단말기의 화면에 출력할 수 있다. 따라서, 사용자는 화면에 출력된 정보를 토대로 본인이 통과할 수 있는 게이트의 위치로 이동하게 된다.
- [35] 한편, 개시된 기술의 일 실시예에 따르면 생체정보 기반의 인증은 단말기에 저장된 생체정보와 현장에서 획득된 정보를 비교하여 이루어지는 것이므로 사용자의 게이트 출입 가능 여부와 상관없이 인증 자체는 성공될 수 있다. 따라서 S140 단계에 따라 인증서버가 사용자의 출입 가능 여부를 확인한다. 여기에서 출입 가능 여부는 사용자가 게이트를 통과하여 출국 또는 입국해도 별다른 문제가 없는지 확인하는 것으로, 예컨대 사용자의 출입제한 정보를 검색하여 게이트 출입을 허용하거나 제한함으로써 게이트 출입을 엄격하게 처리하는 것일 수 있다. 인증서버는 복수의 사용자들에 대한 출입제한 정보를 저장하는 데이터베이스를 포함한다. 앞서 사용자의 생체정보와 인증에 대한 결과를 저장하는 데이터베이스를 활용할 수 있으며 별도의 데이터베이스에 출입제한 정보를 저장하는 것도 얼마든지 가능하다. 인증서버는 데이터베이스에서 사용자의 출입제한 정보가 검색되면 사용자 단말기에 출입 제한에 따른 알림을 전송할 수 있다.
- [36] 한편 출입제한 정보는 복수의 사용자들 각각에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나를 포함한다. 인증서버는 데이터베이스를

이용하여 인증을 수행한 사용자의 출입제한 정보를 검색한다. 만약, 출입제한 정보가 하나라도 검색된다면 인증에 성공한 사용자라 하더라도 게이트 출입을 막을 수 있다. 즉, 이러한 과정에 따라 이중으로 인증을 수행함으로써 사용자의 게이트 출입 절차를 강화하는 것이다. 종래의 경우 다수의 절차를 통해 사용자가 직접 자신의 정보를 제공하거나 입력함으로써 게이트 통과를 위한 인증을 단계별로 수행하였다. 이는 보안성을 강화하는 효과는 제공할 수 있으나 보안성이 강화되는 만큼 사용자의 불편함이 증가되기 때문에 개시된 기술에서는 이러한 단점을 해소하기 위해서 사용자가 별도의 입력이나 절차를 수행하지 않고도 이중으로 인증을 처리한다.

- [37] S150 단계에서 사용자 단말기는 인증서버로부터 출입 가능 여부를 회신한다. 그리고 출입 가능 여부에 따라 특정 게이트에 구비된 게이트 장치에 제어신호를 전송한다. 사용자 단말기는 게이트 장치와 근거리 무선 통신을 수행할 수 있는 어플리케이션을 탑재하고 있으며, 이를 이용하여 제어신호를 직접 전송할 수 있다. 따라서, 사용자 단말기가 인증의 수행주체가 되어 게이트 개폐를 위한 제어신호를 전송할 수 있다.
- [38] 한편, 인증서버는 게이트 장치로부터 제어신호가 수신되었음을 알리는 응답을 수신할 수 있다. 예컨대, 게이트 장치가 사용자 단말기로부터 제어신호를 수신하면 자동으로 인증서버에 ACK와 같은 신호를 전달할 수 있다. 이와 같이 제어신호에 따른 응답이 수신되면 인증서버는 데이터베이스에 저장된 데이터를 삭제할 수 있다. 또는 사전에 타이머를 이용하여 설정된 시간이 도과하면 사용자 단말기로부터 수신한 인증에 대한 결과를 자동으로 삭제할 수도 있다. 이와 같이 사용자의 생체정보와 인증에 관한 기록을 남겨두지 않고 폐기함으로써 생체정보 보호 가이드라인을 위배하지 않고 사용자에게 대한 인증을 처리할 수 있다.
- [39] 도 2는 개시된 기술의 일 실시예에 따른 인증서버 중심의 게이트 출입을 위한 인증 방법에 대한 도면이다. 도 2를 참조하면 인증을 수행하는 실질적인 수행주체가 인증서버이고 사용자 단말기와 게이트 장치는 인증서버의 인증 결과에 따라 동작할 수 있다.
- [40] S210 단계에서 사용자 단말기는 복수개의 게이트 각각에 구비된 게이트 장치들 중 적어도 하나에서 비콘을 수신한다. 이와 같이 비콘을 수신함으로써 게이트 장치를 확인하면 사용자 단말기는 S220 단계에 따라 어플리케이션을 활성화한다. 사용자 단말기에 설치된 어플리케이션은 비콘을 통해 게이트 장치가 주변에 있다는 것을 확인하면 자동으로 실행될 수 있다. 사용자 단말기에는 사전에 게이트 장치와 통신하기 위한 어플리케이션이 설치된다. 이러한 어플리케이션은 비콘을 트리거로 하여 자동으로 실행될 수 있다. 사용자 단말기는 복수개의 게이트 장치들 중 근거리 무선 통신이 가능한 영역 이내에 위치한 적어도 하나의 게이트 장치가 식별되면 생체정보를 이용한 인증을 수행하는 어플리케이션을 활성화할 수 있다.

- [41] 한편, S220 단계에서 사용자 단말기는 실행된 어플리케이션에 따라 사용자의 얼굴 이미지를 촬영한다. 그리고 얼굴 이미지를 토대로 임시템플릿을 생성한다. 그리고 사전에 저장된 인증템플릿과 비교하여 인증을 수행한다. 두 템플릿을 생성하는 방법과 과정은 앞서 도 1을 통해 설명한 바와 동일하게 수행될 수 있다.
- [42] 한편, 사용자 단말기는 S230 단계에서 인증에 대한 결과에 따라 복수개의 게이트 중 출입권한이 부여된 특정 게이트의 위치를 확인한다. 예컨대, 인증에 성공하면 어플리케이션이 사용자의 발권정보를 로딩하여 출입권한이 부여된 특정 게이트의 위치를 확인할 수 있다. 이러한 어플리케이션은 단순히 게이트 장치와 통신하기 위한 것 외에도 사전에 사용자의 발권을 처리할 수 있는 어플리케이션과 통합될 수 있다. 따라서, 어플리케이션을 통해 처리된 사용자의 발권정보를 저장하고 있으며, 인증에 성공하면 발권정보에 접근할 수 있는 권한을 획득하여 특정 게이트의 위치를 확인하도록 동작할 수 있다.
- [43] 한편, 게이트의 위치까지 확인이 완료되면 사용자 단말기는 S240 단계에 따라 인증에 대한 결과 및 상기 출입권한에 대한 정보를 인증서버에 전송한다. 사용자 단말기가 전송하는 인증에 대한 결과는 당연히게도 인증을 성공하였음을 나타내는 정보이며 출입권한에 대한 정보는 사용자가 어떤 게이트를 통과할 수 있는지를 나타내는 정보를 의미한다. 사용자 단말기는 인증에 성공한 후 게이트의 위치까지 확인하면 인증에 대한 결과와 기 저장된 출입권한에 대한 정보를 인증서버로 전송한다.
- [44] 한편, 인증서버는 인증에 대한 결과 및 출입권한에 대한 정보를 데이터로 저장하는 데이터베이스를 포함한다. 인증서버는 S250 단계에 따라 데이터베이스에 저장된 인증에 대한 결과를 토대로 사용자 단말기의 사용자에 대한 출입 가능 여부를 확인한다. 예컨대, 사용자에 대한 출입제한 정보를 검색하여 출입 가능 여부를 확인할 수 있다. 출입제한 정보는 복수의 사용자들 각각에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나를 포함하며, 인증서버는 복수의 사용자들에 대한 출입제한 정보를 저장하는 데이터베이스를 포함한다. 그리고 데이터베이스를 이용하여 사용자의 출입제한 정보를 검색하는 것으로 사용자가 출입이 가능한 인물인지 판단하게 된다.
- [45] 한편, 사용자가 출입이 가능한 인물로 확인되면 인증서버는 S260 단계에 따라 특정 게이트에 제어신호를 전송한다. 앞서 도 1을 통해 설명한 경우에는 사용자 단말기가 어플리케이션을 통해 직접 제어신호를 전송하였으나 여기에서는 인증서버가 사용자 단말기로부터 인증 관련 정보를 수신하고 출입이 가능한 사용자인지 판단하여 게이트에 제어신호를 전송하게 된다.
- [46] 도 3은 개시된 기술의 일 실시예에 따른 게이트 장치와 인증서버 중심의 게이트 출입을 위한 인증 방법에 대한 도면이다. 도 3을 참조하면 임시템플릿을 생성하는 수행주체를 게이트 장치로 하고 인증의 수행주체를 서버로 하여 게이트 출입을 위한 인증 방법을 수행할 수 있다.
- [47] 먼저, S310 단계에 따라 사용자 단말기가 복수개의 게이트 각각에 구비된

게이트 장치들 중 근거리 무선 통신이 가능한 영역 이내에 위치한 일부의 게이트 장치에 비콘을 전송한다. 그리고 S320 단계에 따라 일부의 게이트 장치 중 사용자 단말기와 가장 인접한 위치의 특정 게이트 장치와 통신할 수 있는 환경을 조성할 수 있다. 예컨대, 사용자 단말기와 특정 게이트 장치 간에 신호를 송수신할 수 있는 블루투스 페어링이 수행될 수 있다.

[48] 한편, S320 단계에서 사용자 단말기와 페어링된 게이트 장치는 비콘에 따라 카메라를 구동하여 사용자의 얼굴 이미지를 촬영한다. 게이트 장치 또한 사용자 단말기와 동일하게 비콘을 트리거로 하여 구동되는 어플리케이션이 설치될 수 있다. 게이트 장치는 카메라를 이용하여 사용자의 얼굴 이미지를 촬영하는데 정확한 얼굴 이미지를 촬영하기 위해서 사용자의 위치를 정위치로 이동시키기 위한 추가적인 단계가 수행될 수도 있다. 예컨대, 음성을 통해 사용자가 좀 더 가까이 오도록 유도하거나 게이트 정면의 바닥에 표시된 촬영위치를 안내할 수 있다.

[49] 한편, S330 단계에서 인증서버는 특정 게이트 장치로부터 사용자의 얼굴 이미지를 수신한다. 인증서버와 게이트 장치는 유선 또는 무선으로 사전에 연결되어 있으며 연결된 통신방법에 따라 게이트 장치가 인증서버에 얼굴 이미지를 전송할 수 있다. 인증서버는 데이터베이스에 등록된 복수 사용자들의 생체정보들과 비교하여 인증을 수행하고 인증 결과에 따라 사용자에 대한 출입 가능 여부를 확인한다. S330 단계에서 수행되는 인증 또한 사용자의 얼굴 이미지를 토대로 생성된 템플릿을 비교하는 것으로 수행될 수 있다. 즉, 인증서버는 게이트 장치가 촬영한 얼굴 이미지를 이용하여 임시템플릿을 생성하고 사전에 데이터베이스에 저장된 복수의 생체정보들을 토대로 생성된 복수개의 인증템플릿과 비교하여 인증을 수행할 수 있다. 동일한 사용자가 정상적으로 얼굴 이미지를 촬영하였다면 인증에 성공할 가능성이 높아진다. 그러나 부정확한 얼굴 이미지가 촬영되거나 타 사용자인 경우에는 인증에 실패할 수 있다. 이 경우 인증서버는 게이트 장치에 제어신호를 전송하여 사용자의 얼굴 이미지를 재촬영할 수 있다. 물론 재촬영에 따른 횟수를 제한하여 보안성을 유지할 수 있다.

[50] 한편, 인증서버는 사용자에 대한 출입 가능 여부를 사용자의 출입제한 정보를 검색하는 것으로 확인할 수 있다. 앞서 설명한 바와 마찬가지로 인증서버는 출입제한 정보를 저장하는 데이터베이스를 검색하여 사용자의 출입 가능 여부를 판단할 수 있다.

[51] 한편, S340 단계에서 사용자 단말기는 인증서버로부터 인증 결과 및 출입 가능 여부를 회신한다. 앞서 도 1 및 도 2를 통해 설명한 것과는 달리 여기에서는 인증서버가 인증의 수행주체가 되며 사용자 단말기가 인증서버로부터 인증 결과를 수신하게 된다. 정당한 사용자인 경우라면 인증서버를 통해 정상적으로 인증이 수행될 수 있다. 사용자 단말기는 인증서버를 통해 인증에 성공하였음이 확인되면 S340 단계에 따라 복수개의 게이트 중 출입권한이 부여된 특정

게이트의 위치를 확인한다. 여기에서 사용자의 얼굴 이미지를 촬영한 게이트 장치와 출입권한이 부여된 특정 게이트에 구비된 게이트 장치는 동일한 것일 수도 있고 서로 다른 것일 수도 있다. 즉, 사용자가 게이트 주변에 위치하면 사용자의 편의를 위해 가장 가까운 게이트를 통해 얼굴을 촬영하도록 동작하는 것이며, 사전에 발권한 정보에 따라 실제 사용자가 통과할 수 있도록 출입권한이 부여된 게이트는 다른 게이트일 수 있다. 따라서 사용자 단말기는 S340 단계에 따라 출입권한이 부여된 특정 게이트의 위치를 확인한다. 그리고 S350 단계에서 특정 게이트에 구비된 게이트 장치에 제어신호를 전송하게 된다.

- [52] 도 4는 개시된 기술의 일 실시예에 따른 게이트 장치 중심의 게이트 출입을 위한 인증 방법에 대한 도면이다. 도 4를 참조하면 게이트 장치가 사용자의 얼굴 이미지를 이용하여 1차 인증을 수행하고 인증서버가 2차 인증을 수행할 수 있다.
- [53] S410 단계에서 사용자 단말기는 복수개의 게이트 각각에 구비된 게이트 장치들 중 근거리 무선 통신이 가능한 영역 이내에 위치한 일부의 게이트 장치에 비콘을 전송한다. 일 실시예로, 블루투스 통신이 가능한 영역 이내에 위치하는 게이트 장치에 비콘을 전송할 수 있다.
- [54] S420 단계에서 사용자 단말기의 비콘을 수신한 일부의 게이트 장치들 중 사용자 단말기와 가장 인접한 위치의 특정 게이트 장치가 카메라를 구동한다. 앞서 도 1 내지 도 3을 통해 설명한 바와 같이 게이트 장치에 설치된 어플리케이션이 비콘에 따라 구동되어 카메라를 제어하는 것으로 사용자의 얼굴 이미지를 촬영할 수 있다. 여기에서 가장 인접한 위치의 게이트 장치는 복수의 게이트 장치들 중에서 사용자 단말기와 가장 안정적으로 통신하기 위해서 단순히 거리가 가장 가까운 순서에 따라 결정되는 것으로, 블루투스와 같은 근거리 무선 통신은 단말기 간의 거리가 가까울수록 신호강도가 강하기 때문에 별도의 우선순위 보다는 사용자 단말기와의 거리를 기준으로 특정 게이트 장치가 선정될 수 있다. 이와 같이 선정된 게이트 장치가 사용자의 얼굴 이미지를 촬영하게 된다.
- [55] S430 단계에서 사용자의 얼굴 이미지를 촬영한 특정 게이트 장치가 사용자의 얼굴 이미지를 이용하여 임시템플릿을 생성한다. 그리고 기 저장된 복수개의 생체정보를 토대로 생성된 복수개의 인증템플릿들과 비교하여 인증을 수행한다. 임시템플릿은 게이트 출입을 위해 즉석에서 촬영된 얼굴 이미지를 토대로 생성된다. 그리고 인증템플릿은 사전에 소정의 등록 절차를 거쳐 게이트 장치가 저장한다. 게이트 장치는 두 템플릿의 유사도를 비교하여 인증을 수행할 수 있다.
- [56] 한편, S440 단계에서 인증서버는 특정 게이트 장치로부터 인증에 대한 결과를 수신한다. 인증에 대한 결과는 인증 성공 또는 실패일 수 있으며, 바람직하게는 인증 성공에 대한 결과를 수신하여 사용자에게 대한 출입 가능 여부를 확인한다. 사용자에게 대한 출입 가능 여부는 데이터베이스에 저장된 복수의 사용자들에 대한 출입제한 정보를 조회하여 확인할 수 있다. 인증서버는 별다른 출입제한

정보가 조회되지 않은 사용자인 경우에는 출입이 가능한 것으로 판단할 수 있다. 출입제한 정보는 복수의 사용자들 각각에 대한 범죄기록, 출국금지 기록 및 입국금지 기록을 포함한다. 물론 출입국금지 기록이나 범죄기록이 존재하는 사용자는 출입이 불가능한 것으로 판단할 수 있다. 이 경우에는 사용자 단말기에 출입 제한에 따른 알림을 전송한다.

- [57] 한편, 인증서버는 인증에 대한 결과 및 출입 가능 여부를 사용자 단말기에 전송한 이후에 또는 전송 후 일정시간이 도과한 다음에 사용자의 인증에 대한 결과 및 출입 가능 여부를 삭제한다. 즉, 사용자의 생체정보 기반 인증에 대한 데이터를 저장하지 않고 폐기한다.
- [58] S450 단계에서 사용자 단말기는 인증서버로부터 인증에 대한 결과 및 출입 가능 여부를 회신하고 복수개의 게이트 중 출입권한이 부여된 특정 게이트의 위치를 확인한다. 게이트의 위치는 발권정보를 토대로 확인할 수 있다. 사용자 단말기는 인증서버를 통해서 게이트 장치의 인증에 대한 결과와 인증서버가 확인한 출입 가능 여부에 대한 결과를 회신할 수 있다. 두 가지 인증에 성공하면 사용자 단말기는 S450 단계에 따라 특정 게이트에 구비된 게이트 장치에 제어신호를 전송한다.
- [59] 도 5는 개시된 기술의 일 실시예에 따른 게이트 출입을 위한 인증 장치를 나타낸 도면이다. 도 5를 참조하면 게이트 출입을 위한 인증 장치는 블루투스 모듈, 카메라, 인증모듈 및 제어모듈을 포함한다. 인증 장치는 게이트에 구비된 게이트 장치일 수 있으며 필요에 따라 사용자 단말기나 인증서버가 인증 장치의 역할을 수행할 수도 있다.
- [60] 블루투스 모듈은 일정 주기마다 비콘을 전송하여 통신이 가능한 영역에 접근하는 사용자 단말기를 감지한다. 비콘을 이용하여 사용자 단말기의 위치를 파악할 수 있다. 인증 장치는 블루투스 모듈이 사용자 단말기를 감지한 것을 확인하면 사용자를 촬영하기 위하여 카메라를 초기화할 수 있다.
- [61] 카메라는 사용자 단말기의 사용자가 촬영이 가능한 영역에 접근하면 촬영을 수행한다. 카메라는 사용자의 얼굴 이미지를 촬영한다. 얼굴 이미지에 포함된 생체적 특징을 나타내는 정보를 정확하게 획득하기 위해서 카메라는 사용자의 얼굴 정면을 촬영하여 이미지를 획득할 수 있다. 이를 위해서 카메라 촬영이 원활하게 이루어질 수 있는 위치나 지점이 사전에 정해질 수 있다.
- [62] 인증모듈은 카메라에서 촬영된 사용자의 얼굴 이미지를 수신한다. 그리고 얼굴 이미지를 토대로 템플릿을 생성한다. 사용자의 얼굴 이미지는 게이트가 구비된 현장에서 즉석으로 촬영된 것으로 이를 이용하여 생성하는 템플릿이 임시템플릿이 된다.
- [63] 한편, 인증모듈은 복수의 사용자들에 대한 복수개의 템플릿을 미리 저장하는 데이터베이스를 포함하고 있으며, 이와 같이 사전에 미리 저장된 템플릿은 임시템플릿과 비교하여 인증을 수행하기 위한 정보로 활용된다. 앞서 도 1 내지 도 4를 통해 설명한 바와 같이 현장에서 즉석으로 획득된 템플릿은 임시템플릿

이고, 사전에 저장된 복수의 사용자들에 대한 복수개의 템플릿은 인증템플릿이라 한다. 인증모듈은 두 템플릿을 비교하여 복수개의 인증템플릿들 중에서 임시템플릿과 매칭되는 것을 찾을 수 있다. 인증모듈은 이러한 과정에 따라 사용자를 인증하게 된다.

- [64] 한편, 인증모듈은 복수의 사용자들에 대한 출입제한 정보 또한 데이터베이스에 저장하고 있다. 그리고 데이터베이스에서 사용자의 출입제한 정보가 검색되면 사용자 단말기에 출입 제한에 따른 알림을 전송할 수 있다. 예컨대, 사용자에 대한 인증에 성공하면 출입제한 정보를 검색하는 과정이 수행될 수 있고 사용자에 대한 인증이 실패하면 출입제한 정보를 검색하는 대신 재인증을 수행할 수 있다. 인증모듈의 데이터베이스에는 복수의 사용자들 각각에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나가 기록되어 있다. 인증모듈은 사용자에 대한 1차 인증을 수행한 다음 출입제한 정보들을 검색하여 2차 인증을 수행할 수 있다.
- [65] 한편, 인증모듈은 상술한 과정에 따라 2단계로 사용자에 대한 인증을 수행하면 게이트 제어모듈의 인증 결과를 전송한다. 그리고 사용자의 얼굴 이미지, 사용자의 템플릿 및 인증 결과를 데이터베이스에서 삭제한다.
- [66] 게이트 제어모듈은 인증모듈에서 수신된 인증 결과에 따라 게이트를 개방한다. 인증모듈이 인증에 성공했다면 게이트 제어모듈은 게이트에 제어신호를 전송하여 게이트를 개방할 수 있다. 만약 인증모듈이 인증에 실패했다면 게이트를 개방하는 대신 카메라가 사용자의 얼굴 이미지를 재촬영할 수 있다.
- [67] 도 6은 게이트에 구비된 게이트 장치를 나타낸 도면이다. 도 6을 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 6과 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.
- [68] 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 범위가 설정된다. 예컨대, 블루투스로 통신할 수 있는 통신범위가 설정될 수 있다. 일반적으로 BLE 기반 통신의 경우 50미터 정도의 통신범위가 형성되며 게이트 장치 또한 이와 유사하거나 동일하게 통신범위가 설정될 수 있다.
- [69] 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.

- [70] 개시된 기술의 일 실시예에 따른 게이트 출입을 위한 인증 방법 및 장치는 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] 사용자 단말기가 비콘을 이용하여 복수개의 게이트 각각에 구비된 게이트 장치들을 식별하는 단계;
상기 사용자 단말기가 사전에 저장된 생체정보를 이용하여 인증을 수행하고 상기 인증에 대한 결과를 인증서버에 전송하는 단계;
상기 사용자 단말기가 상기 복수개의 게이트 중 출입권한이 부여된 특정 게이트의 위치를 확인하는 단계;
상기 인증서버가 상기 인증에 대한 결과를 수신하고 상기 사용자 단말기의 사용자에게 대한 출입 가능 여부를 확인하는 단계; 및
상기 사용자 단말기가 상기 출입 가능 여부에 따라 상기 특정 게이트에 구비된 게이트 장치에 제어신호를 전송하는 단계;를 포함하는 게이트 출입을 위한 인증 방법.
- [청구항 2] 제 1 항에 있어서,
상기 사용자 단말기는 상기 복수개의 게이트 장치들 중 근거리 무선 통신이 가능한 영역 이내에 위치한 적어도 하나의 게이트 장치가 식별되면 상기 생체정보를 이용한 인증을 수행하는 어플리케이션을 활성화하는 게이트 출입을 위한 인증 방법.
- [청구항 3] 제 1 항에 있어서, 상기 인증서버에 전송하는 단계는,
상기 사용자 단말기가 상기 생체정보를 사전에 저장하는 단계;
상기 사용자 단말기가 상기 생체정보를 이용하여 인증템플릿을 생성하는 단계;
상기 사용자 단말기가 어플리케이션을 이용하여 현장에서 상기 사용자의 생체정보를 촬영하는 단계;
상기 촬영된 생체정보를 이용하여 임시템플릿을 생성하는 단계; 및
상기 인증템플릿과 상기 임시템플릿을 비교하여 상기 인증을 수행하는 단계;를 포함하는 게이트 출입을 위한 인증 방법.
- [청구항 4] 제 1 항에 있어서,
상기 인증서버는 상기 생체정보 및 상기 인증에 대한 결과를 데이터로 저장하는 데이터베이스를 포함하고 상기 게이트 장치로부터 상기 제어신호가 수신되었음을 알리는 응답을 수신하면 상기 데이터베이스에 저장된 데이터를 삭제하는 게이트 출입을 위한 인증 방법.
- [청구항 5] 제 1 항에 있어서,
상기 인증서버는 기 설정된 시간이 도과하면 상기 사용자 단말기로부터 수신한 상기 인증에 대한 결과를 자동으로 삭제하는 게이트 출입을 위한 인증 방법.
- [청구항 6] 제 1 항에 있어서,
상기 생체정보는 상기 사용자의 얼굴 이미지에서 추출된 특징정보를

- 포함하는 게이트 출입을 위한 인증 방법.
- [청구항 7] 제 1 항에 있어서, 특정 게이트의 위치를 확인하는 단계는,
상기 사용자 단말기가 기 저장된 발권정보를 토대로 상기 특정 게이트의 위치에 대한 정보를 화면에 출력하는 게이트 출입을 위한 인증 방법.
- [청구항 8] 제 1 항에 있어서,
상기 인증서버는 복수의 사용자들에 대한 출입제한 정보를 저장하는 데이터베이스를 포함하고, 상기 데이터베이스에서 상기 사용자의 출입제한 정보가 검색되면 상기 사용자 단말기에 출입 제한에 따른 알림을 전송하는 게이트 출입을 위한 인증 방법.
- [청구항 9] 제 8 항에 있어서,
상기 출입제한 정보는 상기 복수의 사용자들 각각에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나를 포함하는 게이트 출입을 위한 인증 방법.
- [청구항 10] 사용자 단말기가 복수개의 게이트 각각에 구비된 게이트 장치들 중 적어도 하나에서 비콘을 수신하는 단계;
상기 사용자 단말기가 상기 비콘을 수신함에 따라 어플리케이션을 활성화하여 사용자의 얼굴 이미지를 촬영하고 상기 얼굴 이미지를 토대로 임시템플릿을 생성하고 사전에 저장된 인증템플릿과 비교하여 인증을 수행하는 단계;
상기 사용자 단말기가 상기 인증에 대한 결과에 따라 상기 복수개의 게이트 중 출입권한이 부여된 특정 게이트의 위치를 확인하는 단계;
상기 사용자 단말기가 상기 인증에 대한 결과 및 상기 출입권한에 대한 정보를 인증서버에 전송하는 단계;
상기 인증서버가 상기 인증에 대한 결과를 토대로 상기 사용자 단말기의 사용자에게 대한 출입 가능 여부를 확인하는 단계; 및
상기 인증서버가 상기 출입 가능 여부를 확인한 결과 및 상기 출입권한에 대한 정보에 따라 상기 특정 게이트에 제어신호를 전송하는 단계;를 포함하는 게이트 출입을 위한 인증 방법.
- [청구항 11] 제 10 항에 있어서,
상기 사용자 단말기는 상기 복수개의 게이트 장치들 중 근거리 무선 통신이 가능한 영역 이내에 위치한 적어도 하나의 게이트 장치가 식별되면 상기 생체정보를 이용한 인증을 수행하는 어플리케이션을 활성화하는 게이트 출입을 위한 인증 방법.
- [청구항 12] 제 10 항에 있어서,
상기 인증서버는 상기 인증에 대한 결과 및 상기 출입권한에 대한 정보를 데이터로 저장하는 데이터베이스를 포함하고 상기 제어신호를 전송한 이후에 상기 데이터를 삭제하는 게이트 출입을 위한 인증 방법.
- [청구항 13] 제 10 항에 있어서, 특정 게이트의 위치를 확인하는 단계는,

- 상기 사용자 단말기가 기 저장된 발권정보를 토대로 상기 특정 게이트의 위치에 대한 정보를 화면에 출력하는 게이트 출입을 위한 인증 방법.
- [청구항 14] 제 10 항에 있어서, 상기 출입 가능 여부를 확인하는 단계는, 상기 인증서버가 복수의 사용자들에 대한 출입제한 정보를 저장하는 데이터베이스를 이용하여 상기 사용자의 출입제한 정보를 검색하고 상기 출입제한 정보가 검색되지 않으면 상기 제어신호를 전송하고 상기 출입제한 정보가 검색되면 상기 사용자 단말기에 출입 제한에 따른 알림을 전송하는 게이트 출입을 위한 인증 방법.
- [청구항 15] 제 14 항에 있어서, 상기 데이터베이스는 상기 복수의 사용자들 각각에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나를 포함하는 게이트 출입을 위한 인증 방법.
- [청구항 16] 사용자 단말기가 복수개의 게이트 각각에 구비된 게이트 장치들 중 근거리 무선 통신이 가능한 영역 이내에 위치한 일부의 게이트 장치에 비콘을 전송하는 단계; 상기 일부의 게이트 장치 중 상기 사용자 단말기와 가장 인접한 위치의 특정 게이트 장치가 상기 비콘에 따라 카메라를 구동하여 사용자의 얼굴 이미지를 촬영하는 단계; 인증서버가 상기 특정 게이트 장치로부터 상기 얼굴 이미지를 수신하고 데이터베이스에 등록된 복수 사용자들의 생체정보들과 비교하여 인증을 수행하고 상기 인증 결과에 따라 상기 사용자에 대한 출입 가능 여부를 확인하는 단계; 상기 사용자 단말기가 상기 인증서버로부터 상기 인증 결과 및 상기 출입 가능 여부를 회신하고 상기 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 17] 제 16 항에 있어서, 상기 인증을 수행하는 단계는, 상기 인증서버가 상기 얼굴 이미지를 이용하여 임시템플릿을 생성하는 단계; 및 상기 데이터베이스에 저장된 복수의 생체정보들을 토대로 생성된 복수개의 인증템플릿과 상기 임시템플릿을 비교하는 단계;를 포함하는 게이트 출입을 위한 인증 방법.
- [청구항 18] 제 16 항에 있어서, 특정 게이트의 위치를 확인하는 단계는, 상기 사용자 단말기가 기 저장된 발권정보를 토대로 상기 특정 게이트의 위치에 대한 정보를 화면에 출력하는 게이트 출입을 위한 인증 방법.
- [청구항 19] 제 16 항에 있어서, 상기 출입 가능 여부를 확인하는 단계는, 상기 인증서버가 상기 인증에 성공하면 상기 데이터베이스에 저장된

상기 사용자에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나를 조회하여 상기 출입 가능 여부를 판단하는 게이트 출입을 위한 인증 방법.

- [청구항 20] 제 16 항에 있어서, 상기 출입 가능 여부를 확인하는 단계는, 상기 인증서버가 상기 인증에 실패하면 상기 특정 게이트 장치에 제어신호를 전송하여 상기 사용자의 얼굴 이미지를 재촬영하는 게이트 출입을 위한 인증 방법.
- [청구항 21] 사용자 단말기가 복수개의 게이트 각각에 구비된 게이트 장치들 중 근거리 무선 통신이 가능한 영역 이내에 위치한 일부의 게이트 장치에 비콘을 전송하는 단계;
상기 일부의 게이트 장치 중 상기 사용자 단말기와 가장 인접한 위치의 특정 게이트 장치가 상기 비콘에 따라 카메라를 구동하여 사용자의 얼굴 이미지를 촬영하는 단계;
상기 특정 게이트 장치가 상기 사용자의 얼굴 이미지를 이용하여 임시템플릿을 생성하고 기 저장된 복수개의 생체정보를 토대로 생성된 복수개의 인증템플릿들과 비교하여 인증을 수행하는 단계;
인증서버가 상기 특정 게이트 장치로부터 상기 인증에 대한 결과를 수신하여 상기 사용자에 대한 출입 가능 여부를 확인하는 단계;
상기 사용자 단말기가 상기 인증서버로부터 상기 인증에 대한 결과 및 상기 출입 가능 여부를 회신하고 상기 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 22] 제 21 항에 있어서,
상기 인증서버는 상기 인증에 대한 결과 및 상기 출입 가능 여부를 저장하는 데이터베이스를 포함하고, 상기 사용자 단말기에 상기 인증에 대한 결과 및 상기 출입 가능 여부를 전송하면 상기 사용자의 인증에 대한 결과 및 상기 출입 가능 여부를 삭제하는 게이트 출입을 위한 인증 방법.
- [청구항 23] 제 21 항에 있어서,
상기 인증서버는 상기 사용자 단말기에 상기 인증에 대한 결과 및 상기 출입 가능 여부를 전송하고 일정 시간이 도과하면 상기 사용자 단말기에 전송한 인증 결과 및 출입 가능 여부를 자동으로 삭제하는 게이트 출입을 위한 인증 방법.
- [청구항 24] 제 21 항에 있어서, 특정 게이트의 위치를 확인하는 단계는,
상기 사용자 단말기가 기 저장된 발권정보를 토대로 상기 특정 게이트의 위치에 대한 정보를 화면에 출력하는 게이트 출입을 위한 인증 방법.
- [청구항 25] 제 21 항에 있어서, 상기 출입 가능 여부를 확인하는 단계는,
상기 인증서버가 데이터베이스에 저장된 복수의 사용자들에 대한

출입제한 정보를 이용하여 상기 사용자의 출입 가능 여부를 판단하는 게이트 출입을 위한 인증 방법.

- [청구항 26] 제 25 항에 있어서,
상기 인증서버는 상기 사용자에 대한 출입제한 정보가 검색되면 상기 사용자 단말기에 출입 제한에 따른 알림을 전송하는 게이트 출입을 위한 인증 방법.
- [청구항 27] 제 26 항에 있어서,
상기 출입제한 정보는 상기 복수의 사용자들 각각에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나를 포함하는 게이트 출입을 위한 인증 방법.
- [청구항 28] 일정 주기마다 비콘을 전송하여 통신이 가능한 영역에 접근하는 사용자 단말기를 감지하는 블루투스 모듈;
상기 사용자 단말기의 사용자가 촬영이 가능한 영역에 접근하면 상기 사용자의 얼굴 이미지를 촬영하는 카메라;
상기 얼굴 이미지를 토대로 템플릿을 생성하고 상기 템플릿과 기 저장된 복수의 사용자들에 대한 복수개의 템플릿을 비교하여 상기 사용자에 대한 인증을 수행하는 인증모듈; 및
상기 인증모듈에서 수신된 인증 결과에 따라 게이트를 개방하는 게이트 제어모듈;을 포함하는 게이트 출입을 위한 인증 장치.
- [청구항 29] 제 28 항에 있어서,
상기 인증모듈은 상기 복수개의 템플릿을 저장하는 데이터베이스를 포함하고, 상기 사용자의 템플릿이 상기 복수개의 템플릿 중 하나에 매칭되는지 비교하여 상기 인증을 수행하는 게이트 출입을 위한 인증 장치.
- [청구항 30] 제 28 항에 있어서,
상기 인증모듈은 복수의 사용자들에 대한 출입제한 정보를 상기 데이터베이스에 저장하고, 상기 데이터베이스에서 상기 사용자의 출입제한 정보가 검색되면 상기 사용자 단말기에 출입 제한에 따른 알림을 전송하는 게이트 출입을 위한 인증 장치.
- [청구항 31] 제 30 항에 있어서,
상기 출입제한 정보는 상기 복수의 사용자들 각각에 대한 범죄기록, 출국금지 기록 및 입국금지 기록 중 적어도 하나를 포함하는 게이트 출입을 위한 인증 장치.
- [청구항 32] 제 28 항에 있어서,
상기 인증모듈은 상기 게이트 제어모듈에 상기 인증 결과를 전송하면 상기 사용자의 얼굴 이미지, 상기 사용자의 템플릿 및 상기 인증 결과를 삭제하는 게이트 출입을 위한 인증 장치.