[CLAIMS]

[Claim 1]

A method of authenticating gate access, the method comprising:

identifying, by a user terminal, gate devices provided in a plurality of gates using a beacon;

performing, by the user terminal, authentication using biometric information stored in advance and transmitting a result of the authentication to an authentication server;

checking, by the user terminal, a location of a specific gate for which access authorization is given among the plurality of gates;

receiving, by the authentication server, the result of the authentication and checking whether access of a user of the user terminal is allowed; and

transmitting, by the user terminal, a control signal to a gate device provided in the specific gate according to whether the access is allowed,

wherein the user terminal activates an application for performing the authentication using the biometric information in response to identifying at least one gate device located within an area in which short-range wireless communication is available among the plurality of gate devices,

wherein the authentication server includes a database for storing the biometric information and the result of the authentication as data, and in response to receiving, from the gate device, a response indicating that the control signal has been received by the gate device, deletes the data stored in the database, and

wherein the database stores access restriction information for a plurality of users, and in response to the access restriction information of the user being retrieved

in the database, the authentication server transmits a notification according to the access restriction to the user terminal.

[Claim 2]

The method of claim 1, wherein the transmitting of the result of the authentication to the authentication server includes:

storing, by the user terminal, the biometric information in advance;

generating, by the user terminal, an authentication template using the biometric information;

capturing, by the user terminal, biometric information of the user in a field using the application;

generating a temporary template using the captured biometric information; and

comparing the authentication template with the temporary template to perform the authentication.

[Claim 3]

The method of claim 1, wherein the authentication server automatically deletes the result of the authentication received from the user terminal when a preset time has elapsed.

[Claim 4]

The method of claim 1, wherein the biometric information includes feature information extracted from a face image of the user.

[Claim 5]

The method of claim 1, wherein the checking, by the user terminal, of the location of the specific gate includes outputting, by the user terminal, information

about the location of the specific gate on a screen on the basis of pre-stored ticketing information.

[Claim 6]

The method of claim 1, wherein the access restriction information includes at least one of a criminal record, a departure prohibition record, and an entry prohibition record for each of the plurality of users.

[Claim 7]

A method of authenticating gate access, the method comprising:

receiving, by a user terminal, a beacon from at least one of a plurality of gate devices provided in a plurality of gates;

in response to the beacon being received, activating, by the user terminal, an application to capture a face image of a user, generating a temporary template on the basis of the face image, and comparing the temporary template with an authentication template stored in advance to perform authentication;

checking, by the user terminal, a location of a specific gate, for which access authorization is given among the plurality of gates, according to a result of the authentication;

transmitting, by the user terminal, the result of the authentication and information about the access authorization to the authentication server;

checking, by the authentication server, whether access of a user of the user terminal is allowed on the basis of the result of the authentication; and

transmitting, by the authentication server, a control signal to the specific gate according to a result of the checking of whether access is allowed and the information about the access authorization,

wherein the user terminal activates the application for performing the authentication using biometric information in response to identifying at least one gate device located within an area in which short-range wireless communication is available among the plurality of gate devices,

wherein the authentication server includes a database for storing the result of the authentication and the information about the access authorization as data, and after transmitting the control signal, deletes the data stored in the database, and

wherein the checking, by the authentication server, of whether access is allowed includes: retrieving access restriction information of the user using the database for storing the access restriction information for a plurality of users, in response to the access restriction information being not retrieved, transmitting the control signal, and in response to the access restriction information being retrieved, transmitting a notification according to the access restriction to the user terminal.

[Claim 8]

The method of claim 7, wherein the checking, by the user terminal, of the location of the specific gate includes outputting, by the user terminal, information about the location of the specific gate on a screen on the basis of pre-stored ticketing information.

[Claim 9]

The method of claim 7, wherein the database includes at least one of a criminal record, a departure prohibition record, and an entry prohibition record for each of the plurality of users.