

DESCRIPTION

Title Of Invention: GATE DEVICE, AUTHENTICATION SYSTEM, GATE
DEVICE CONTROL METHOD, AND STORAGE MEDIUM

5

[Technical Field]

[0001]

The present disclosure relates to a gate device, an authentication
system, a gate device control method, and a storage medium.

10

[Background Art]

[0002]

Services using face authentication have started to spread (see PTLs
1 to 3). For example, face authentication has started to be applied to
various procedures (for example, check-in, baggage check, security check,
15 and the like) at airports. A service using face authentication is often
provided using a gate device.

[Citation List]

[Patent Literature]

[0003]

20

[PTL 1] JP 2006-236244 A

[PTL 2] JP 2018-128970 A

[PTL 3] JP 2018-109935 A

[Summary]

[Technical Problem]

25

[0004]

As described above, services using face authentication have started
to be provided at airports and the like. For example, a security check
using face authentication is performed at a security check site at an
airport. Here, the device installation space of the existing airport is

limited, and the gate device for face authentication is often installed in a narrow space.

[0005]

Therefore, when the gate device acquires the image (the image
5 including the face area), the image may include not only the face image of the user in the foremost row (the user of the authentication target) but also the face image of the user behind. That is, since the gate device supporting the face authentication is installed in a narrow space, the distance between the users aligned in the gate device is short, and a
10 plurality of persons may appear in the same image.

[0006]

In this case, the gate device needs to select one face image from the plurality of face images and set the selected face image as the authentication target. For example, it is conceivable that the gate device
15 calculates an area (size) for each of a plurality of face images and sets a face image having the largest area as an authentication target. The handling is based on the premise that the face image of the user aligned in the foremost row of the gate device is larger than the face image of the user aligned behind. However, the size of the face has a large individual
20 difference, and in the above correspondence (determination of the authentication target based on the area of the face image), the user aligned behind the user aligned in the foremost row may be set as the authentication target.

[0007]

25 A main object of the present disclosure is to provide a gate device, an authentication system, a gate device control method, and a storage medium that contribute to accurately determining a user of the authentication target.

[Solution to Problem]

[0008]

According to a first aspect of the present disclosure, there is provided a gate device including: an acquisition unit configured to acquire an image from a camera; a setting unit configured, in a case where a plurality of users appears in the acquired image, to specify a user in a foremost row among the plurality of users according to positions of the plurality of users in the image, and set the specified user as an authentication target person; and a gate control unit configured to control a gate based on an authentication result of the authentication target person.

[0009]

According to a second aspect of the present disclosure, there is provided an authentication system including: a server device configured to store biometric information of each of a plurality of system users and execute authentication processing using the plurality of pieces of biometric information; and a gate device connected to the server device. The gate device includes: an acquisition unit configured to acquire an image from a camera; a setting unit that configured, in a case where a plurality of users appears in the acquired image, to specify a user in a foremost row among the plurality of users according to positions of the plurality of users in the image, and set the specified user as an authentication target person; an authentication request unit configured to request a server device to authenticate the authentication target person; and a gate control unit configured to control a gate based on an authentication result of the authentication target person.

[0010]

According to a third aspect of the present disclosure, there is provided a gate device control method including: in a gate device, acquiring an image from a camera; in a case where a plurality of users

appears in the acquired image, specifying a user in a foremost row among the plurality of users according to positions of the plurality of users in the image, and setting the specified user as an authentication target person; and controlling a gate based on an authentication result of the authentication target person.

[0011]

According to a fourth aspect of the present disclosure, there is provided a computer-readable storage medium storing a program for causing a computer mounted in a gate device to execute: acquiring an image from a camera; in a case where a plurality of users appears in the acquired image, specifying a user in a foremost row among the plurality of users according to positions of the plurality of users in the image, and setting the specified user as an authentication target person; and controlling a gate based on an authentication result of the authentication target person.

[Advantageous Effects]

[0012]

According to each aspect of the present disclosure, a gate device, an authentication system, a gate device control method, and a storage medium that contribute to accurately determining a user of the authentication target are provided. Note that the effect of the present disclosure is not limited to the above. According to the present disclosure, other effects may be exhibited instead of or in addition to the effects.

[Brief Description of Drawings]

[0013]

Fig. 1 is a diagram for explaining an outline of an example embodiment.

Fig. 2 is a diagram illustrating an example of a schematic

configuration of an authentication system according to a first example embodiment.

Fig. 3 is a diagram illustrating an example of an appearance of a gate device according to the first example embodiment.

5 Fig. 4 is a diagram illustrating an example of a plan view of the gate device according to the first example embodiment.

Fig. 5 is a diagram illustrating an example of a processing configuration of the gate device according to the first example embodiment.

10 Fig. 6 is a diagram for explaining the operation of a biometric information acquisition unit according to the first example embodiment.

Fig. 7 is a flowchart illustrating an example of an operation of an authentication target setting unit according to the first example embodiment.

15 Fig. 8 is a diagram for explaining an operation of the authentication target setting unit according to the first example embodiment.

Fig. 9 is a diagram for explaining an operation of the authentication target setting unit according to the first example
20 embodiment.

Fig. 10 is a diagram for explaining the operation of the authentication target setting unit according to the first example embodiment.

Fig. 11 is a flowchart illustrating an example of anteroposterior
25 relationship specifying processing of the authentication target setting unit according to the first example embodiment.

Fig. 12 is a diagram for explaining the operation of the authentication target setting unit according to the first example embodiment.

Fig. 13 is a diagram for explaining the operation of the authentication target setting unit according to the first example embodiment.

Fig. 14 is a diagram illustrating an example of a graph illustrating
5 a correspondence relationship between a distance between a camera installation surface and an object and a position of the object in a common region.

Fig. 15 is a diagram illustrating an example of an authentication request.

10 Fig. 16 is a flowchart illustrating an example of an operation of the gate device according to the first example embodiment.

Fig. 17 is a diagram illustrating an example of a processing configuration of a server device according to the first example embodiment.

15 Fig. 18 is a diagram illustrating an example of a user database.

Fig. 19 is a sequence diagram illustrating an example of an operation of the authentication system according to the first example embodiment.

20 Fig. 20 is a diagram for explaining the relationship between the actual position of a user and the position of the user appearing in the image.

Fig. 21 is a flowchart illustrating an example of an operation of an authentication target setting unit according to a second example embodiment.

25 Fig. 22 is a diagram illustrating an example of a hardware configuration of the gate device.

[Example Embodiment]

[0014]

First, an outline of an example embodiment will be described.

Note that the reference numerals in the drawings attached to this outline are attached to each element for convenience as an example for assisting understanding, and the description of this outline is not intended to be any limitation. In addition, in a case where there is no particular

5 explanation, the block described in each drawing represents not a configuration of a hardware unit but a configuration of a functional unit. Connection lines between blocks in each drawing include both bidirectional and unidirectional lines. The unidirectional arrow schematically indicates a flow of a main signal (data), and does not
10 exclude bidirectionality. Note that, in the present specification and the drawings, elements that can be similarly described are denoted by the same reference numerals, and redundant description can be omitted.

[0015]

The gate device 100 according to one example embodiment
15 includes an acquisition unit 101, a setting unit 102, and a gate control unit 103 (see Fig. 1). The acquisition unit 101 acquires an image from a camera. When a plurality of users is included in the acquired image, the setting unit 102 specifies a user on the foremost row among the plurality of users in accordance with the positions of the plurality of users in the
20 image, and sets the specified user as an authentication target person. The gate control unit 103 controls a gate on the basis of an authentication result of the authentication target person.

[0016]

The gate device 100 acquires an image from the camera. In a
25 case where a plurality of users appears in the image, the gate device 100 specifies an authentication target person. For example, the gate device 100 specifies the user in the foremost row based on the position of the user appearing in the image. For example, the gate device 100 specifies the user appearing at the right end or the left end of the image among the

plurality of users as the user in the foremost row. Whether the user at the right end is determined as the foremost row or the user at the left end is determined as the foremost row is based on the relationship between the traveling direction of the user and the installation position of the camera.

5 Details of the relationship between the traveling direction of the user and the installation position of the camera will be described later. The gate device 100 specifies the user in the foremost row regardless of the size of the face area having a large individual difference, so that the user to be authenticated can be accurately determined.

10 [0017]

Hereinafter, specific example embodiments will be described in more detail with reference to the drawings.

[0018]

[First example embodiment]

15 A first example embodiment will be described in more detail with reference to the drawings.

[0019]

Fig. 2 is a diagram illustrating an example of a schematic configuration of the authentication system according to the first example embodiment. Referring to Fig. 2, the authentication system includes a plurality of gate devices 10-1 to 10-3 and a server device 20.

20 [0020]

In the following description, in a case where there is no particular reason to distinguish the gate devices 10-1 to 10-3, they are simply referred to as “gate device 10”. Similarly, for other components, reference numerals on the left side separated by hyphens are used to represent the components.

25 [0021]

The configuration illustrated in Fig. 2 is an example and is not

intended to limit the number of gate devices 10 or the like. The authentication system may include at least one or more gate devices 10.
[0022]

The gate device 10 and the server device 20 are configured to be
5 able to communicate with each other by wired or wireless communication means. The server device 20 may be installed in the same building as the gate device 10, or may be installed on a network (cloud).
[0023]

The gate device 10 is, for example, a device installed in an airport
10 or a station. The gate device 10 controls passage of a user. The gate device 10 permits passage of a user (hereinafter, described as an authentication successful person) who has been successfully authenticated by the server device 20. The gate device 10 does not permit passage of a user who has not been authenticated by the server device 20 or a user who
15 has failed in authentication.
[0024]

The server device 20 is a device that performs authentication processing. Specifically, server device 20 stores biometric information of a user (system user) who can pass through the gate device 10. The
20 server device 20 executes authentication processing using the biometric information acquired from the gate device 10 and the biometric information stored in advance, and notifies the gate device 10 of an authentication result (authentication success, authentication failure).
[0025]

25 The gate device 10 opens the gate to allow the passing of the authentication successful person when the authentication successful person enters the internal area of the own device (the area surrounded by the main body of the gate device 10).
[0026]

Examples of the biometric information of the user include data (feature amount) calculated from physical features unique to an individual such as a face and an iris pattern. Alternatively, the biometric information of the user may be image data such as a face image and an iris image. The biometric information of the user may include the physical feature of the user as information.

[0027]

Next, details of each device included in the authentication system according to the first example embodiment will be described. In the following description, a “face image” of the user will be described as an example of the biometric information.

[0028]

[Gate device]

Fig. 3 is a diagram illustrating an example of an appearance of the gate device 10 according to the first example embodiment.

[0029]

Referring to Fig. 3, the gate device 10 includes a face authentication module 11. The face authentication module 11 is attached to the main body of the gate device 10. The face authentication module 11 includes two cameras (upper camera 12-1 and lower camera 12-2).

Note that the “main body” of the gate device 10 is a structure forming the center of the gate device 10, and is a member that is in contact with the floor and to which a face authentication module and the like are attached.

[0030]

The face authentication module 11 is installed to be inclined at a predetermined angle with respect to the direction in which the user walks toward the gate device 10. Fig. 4 is a diagram (plan view) illustrating a case where the gate device 10 is viewed from above.

[0031]

As illustrated in Fig. 4, the face authentication module 11 is installed to be inclined at an angle θ with respect to the traveling direction of the user (the direction perpendicular to a gate 17). Note that the angle θ is selected (adjusted) so that the upper camera 12-1 and the lower camera 12-2 can image a user U in the authentication area.

[0032]

When the angle θ is reduced, only the vicinity of the gate device 10 can be imaged, and there is a possibility that the user enters the inside (internal area) of the gate device 10 before the authentication processing using the face image is ended. In this case, the user needs to stop and stand by until the authentication processing is completed, and it cannot be said that comfortable walk-through can be achieved. On the other hand, when the angle θ is increased, it is possible to capture an image far away from the gate device 10. In this case, although it is advantageous for achieving a comfortable walk-through, there is a possibility that even a user who is not walking toward the own device may be authenticated. For example, in the example of Fig. 2, the gate device 10-1 captures an image of a user who is not walking toward the gate device 10-1, and requests the server device 20 for authentication. As described above, when the angle θ is too large, there is a possibility that useless authentication processing occurs. It is desirable that the administrator and the operator of the system determine the optimum angle in consideration of the advantages and disadvantages caused by the setting angle θ of the face authentication module 11 as described above. As a result of intensive studies by the inventors, it has been found that the angle θ is desirably selected from a range of 30 to 60 degrees.

[0033]

Although Figs. 3 and 4 illustrate an example in which the face authentication module 11 is installed on the right side with respect to the

traveling direction of the user, it is a matter of course that the installation position of the face authentication module 11 is not limited to the right side. The face authentication module 11 may be installed on the left side with respect to the traveling direction of the user. Although Figs. 3 and 4 illustrate an example in which the face authentication module 11 is directly installed in the main body of the gate device 10, the face authentication module 11 may be installed away from the main body of the gate device 10. Alternatively, the gate device 10 may be mounted on the ceiling portion (roof; not illustrated), the face authentication module 11 may be installed on the ceiling. The face authentication module 11 may be installed at a predetermined angle with respect to the traveling direction of the user.

[0034]

The upper camera 12-1 is attached to the vertically upper side of the face authentication module 11. The lower camera 12-2 is attached to the vertically lower side of the face authentication module 11. That is, as illustrated in Fig. 3, the lower camera 12-2 is installed on the vertically lower side of the upper camera 12-1.

[0035]

On the surface (camera installation surface) of the face authentication module, the positions of the two cameras in the perpendicular direction (vertical direction) are different as described above, but are attached at the same position in the horizontal direction (horizontal position). Similarly, in the depth direction of the two cameras, the two cameras are mounted on the same surface (camera installation surface). Note that the meaning of "the positions of the two cameras in the horizontal direction are the same" does not mean that the positions of the two cameras in the horizontal direction strictly coincide with each other, but allows some deviation. That is, the positions of the

two cameras in the horizontal direction may be substantially the same.

[0036]

The upper camera 12-1 and the lower camera 12-2 are cameras having substantially the same performance, and parameters such as an angle of view and a focal length are substantially the same. According to the method of installing the two cameras or the like as described above, the images obtained from the two cameras have different photographing ranges in the height direction, but have substantially the same photographing ranges in the horizontal direction.

10 [0037]

Two cameras (upper camera 12-1 and lower camera 12-2) included in the gate device 10 are provided to authenticate every person (subject) from a short height to a high height. The upper camera 12-1 is installed to acquire a face image of a tall authentication target person. The lower camera 12-2 is installed to acquire a face image of a short authentication target person.

[0038]

With these cameras, the face image of the tall authentication target person is acquired by the upper camera 12-1, and the face image of the short authentication target person is acquired by the lower camera 12-2. The face image of a medium-height authentication target person is acquired from both the upper camera 12-1 and the lower camera 12-2. Most of the users are classified as medium height, and it is rare that a face image is acquired from one of the upper camera 12-1 and the lower camera 12-2.

25 [0039]

The upper camera 12-1 and the lower camera 12-2 operate in conjunction with each other. Specifically, the two cameras image the user at substantially the same timing.

[0040]

As illustrated in Fig. 3, the face authentication module 11 includes a light emitting diode (LED) (not illustrated) for dimming and a display 13. The gate device 10 controls an environment (light irradiated to the user) at the time of acquiring the user's face image using the LED for dimming. The gate device 10 notifies the user of a necessary message or the like by using display 13. For example, the gate device 10 displays an authentication result (authentication success, authentication failure) by the server device 20.

10 [0041]

The gate device 10 includes a display 14. The gate device 10 notifies the user of a necessary message or the like by using the display 14. For example, the gate device 10 displays an authentication result (authentication success, authentication failure) by the server device 20. Alternatively, the gate device 10 may notify the user of a necessary message by using a speaker (not illustrated).

[0042]

The gate device 10 includes an area sensor 15. The area sensor 15 is a sensor that detects whether a person is present in a predetermined area (an area surrounded by a dotted line in Fig. 3) set in front of the gate device 10. The area sensor 15 can be configured using a sensor (so-called human sensor) using infrared rays.

[0043]

When confirming that a person is present in the predetermined area based on the detection signal from the area sensor 15, the gate device 10 controls two cameras (upper camera 12-1 and lower camera 12-2) to acquire two images (image data). In the following description, an area where the area sensor 15 detects the presence of a person is referred to as an "authentication area". When detecting that the user is present in the

authentication area, the gate device 10 captures an image of the user located in the authentication area.

[0044]

The gate device 10 includes an in-gate sensor 16. The in-gate
5 sensor 16 is a sensor for detecting that a person enters the inside of the own device (gate device 10). As the in-gate sensor 16, for example, a sensor (so-called passage sensor using light) including a light transmitting device and a light receiving device can be used. For example, the light
10 transmitting device and the light receiving device are installed to face each other (two devices are installed on an inner wall of the main body). The transmitting device constantly transmits light, and the receiving device receives the transmitted light. The gate device 10 determines that a person enters the gate device 10 when the receiving device cannot receive the light. Note that Fig. 3 illustrates one of the two devices
15 constituting the in-gate sensor 16. A plurality of pairs of in-gate sensors 16 may be provided at substantially equal intervals in the traveling direction of the person.

[0045]

The gate device 10 includes the gate 17. When confirming that
20 the user is present in the authentication area, the gate device 10 acquires a face image of the user. The gate device 10 generates a feature amount (biometric information) from the acquired image, and transmits an authentication request including the generated feature amount to the server device 20. The gate device 10 opens the gate 17 when the
25 authentication successful person enters the internal area of the own device. The gate device 10 closes the gate 17 after the authentication successful person passes through the gate 17.

[0046]

The type of the gate 17 is not particularly limited, and is, for

example, a flapper gate in which a flapper provided from one side or both sides of the passage opens and closes, a turnstile gate in which three bars rotate, or the like.

[0047]

5 Fig. 5 is a diagram illustrating an example of a processing configuration (processing module) of the gate device 10 according to the first example embodiment. Referring to Fig. 5, the gate device 10 includes a communication control unit 201, a user detection unit 202, a biometric information acquisition unit 203, an authentication target
10 setting unit 204, an authentication request unit 205, an entrant determination unit 206, a gate control unit 207, a message output unit 208, and a storage unit 209.

[0048]

 The communication control unit 201 is a unit that controls
15 communication with other devices. Specifically, the communication control unit 201 receives data (packet) from the server device 20. In addition, the communication control unit 201 transmits data to the server device 20. The communication control unit 201 delivers data received from another device to another processing module. The communication
20 control unit 201 transmits data acquired from another processing module to another device. In this manner, the other processing modules transmit and receive data to and from other devices via the communication control unit 201.

[0049]

25 The user detection unit 202 is a unit that detects a user located in the authentication area. The user detection unit 202 detects a user present in the authentication area on the basis of a detection signal from the area sensor 15. In a case where the output of the area sensor 15 indicates that "there is a user in the authentication area", the user

detection unit 202 notifies the biometric information acquisition unit 203 of the fact.

[0050]

The biometric information acquisition unit 203 is a unit that
5 acquires the biometric information of the user present in the authentication area. Upon acquiring the notification related to “there is a user in the authentication area” from the user detection unit 202, the biometric information acquisition unit 203 controls the two cameras (upper camera 12-1 and lower camera 12-2) and captures an image of the
10 user located in the authentication area.

[0051]

The biometric information acquisition unit 203 acquires images from each of the two cameras. As described above, the upper camera 12-1 is attached to the upper side of the face authentication module 11.
15 Therefore, the image (hereinafter, referred to as an upper image) obtained from the upper camera 12-1 includes the upper side of the authentication area. For example, when a medium-height user is located in the authentication area, an upper image surrounded by a broken line in Fig. 6(a) is obtained.

20 [0052]

In contrast, the lower camera 12-2 is attached to the lower side of the face authentication module 11. Therefore, the image (hereinafter, referred to as a lower image) obtained from the lower camera 12-2 includes the lower side of the authentication area. For example, when a
25 medium-height user is located in the authentication area, a lower image surrounded by a broken line in Fig. 6(b) is obtained.

[0053]

The upper image and the lower image include a common region. In the example of Fig. 6, a region indicated by a one-dot chain line in Fig.

6(c) is a region common to the upper image and the lower image. In the following description, a region common to the upper image and the lower image is referred to as a "common region".

[0054]

5 The biometric information acquisition unit 203 delivers two images (upper image, lower image) captured by the upper camera 12-1 and the lower camera 12-2 to the authentication target setting unit 204.

[0055]

 The authentication target setting unit 204 is a unit that sets
10 (determines) a user (authentication target person) to be authenticated from users appearing in an image. When there are a plurality of users in the authentication area, the authentication target setting unit 204 selects one user from the plurality of users and sets the selected user as the
"authentication target person". The operation of the authentication
15 target setting unit 204 will be described with reference to the flowchart illustrated in Fig. 7.

[0056]

 The authentication target setting unit 204 extracts a face image (Step S101). The authentication target setting unit 204 extracts a face
20 image from the upper image. The authentication target setting unit 204 extracts a face image from the lower image. The authentication target setting unit 204 extracts a face image from the image using various methods. For example, the authentication target setting unit 204 extracts a face image (face area) from the image data using a learning model
25 learned by a convolutional neural network (CNN). Alternatively, the authentication target setting unit 204 may extract the face image using a method such as template matching.

[0057]

 The authentication target setting unit 204 determines the

distribution status of the face images in the two images (Step S102).

The authentication target setting unit 204 determines whether the face image is included only in the upper image or the lower image or whether the face image is included in both the upper image and the lower image.

- 5 In the former case, the processing in and after Step S103 is executed. In the latter case, the processing from Step S110 is executed.

[0058]

When Step S102 is executed and it is determined that the face image is distributed in the upper image or the lower image, the

- 10 authentication target setting unit 204 determines whether there is one face image included only in the upper image or the lower image (Step S103).

[0059]

When one face image is included in the upper image or the lower image (Step S103: Yes branch), the authentication target setting unit 204

15 sets the face image as the authentication target (Step S104).

[0060]

For example, as illustrated in Fig. 8(a), the face image of the tall authentication target person is included only in the upper image. In addition, as illustrated in Fig. 8(b), the face image of the short

- 20 authentication target person is included only in the lower image. In the case illustrated in Fig. 8, the authentication target setting unit 204 sets the face image included in the upper image and the face image included in the lower image as the authentication target (the face image of the authentication target person). Note that, in the drawings including Fig.
- 25 8, the range of each image is moved in the horizontal direction in order to facilitate distinction between the upper image and the lower image.

[0061]

When two or more face images are included in the upper image or the lower image (Step S103: No branch), the authentication target setting

unit 204 sets an error (Step S105).

[0062]

For example, as illustrated in Figs. 9(a) and 9(b), an error is set when a plurality of face images is included only in the upper image or the lower image. In the case illustrated in Fig. 9, it is difficult to determine which one of the plurality of face images is set as the authentication target. However, the situation illustrated in Fig. 9 rarely occurs. When such a situation occurs, the gate device 10 takes a measure such as instructing the user to leave the authentication area.

10 [0063]

As described above, in a case where the face image is distributed in each of the upper image and the lower image, the processing after Step S110 illustrated in Fig. 7 is executed.

[0064]

15 The authentication target setting unit 204 determines whether one face image is included in each of the upper image and the lower image (Step S110).

[0065]

Specifically, the authentication target setting unit 204 determines whether a situation as illustrated in Fig. 10(a) has occurred or a situation as illustrated in Fig. 10(b) has occurred.

[0066]

When one face image is included in each of the upper image and the lower image (Step S110: Yes branch), the authentication target setting unit 204 sets the face image included in either the upper image or the lower image as the authentication target (Step S111). In the example of Fig. 10(a), a face image extracted from either the upper image or the lower image is set as the authentication target.

[0067]

When two or more face images are included in each of the upper image and the lower image (Step S110: No branch), the authentication target setting unit 204 specifies the anteroposterior relationship of each user (Step S112). In the example of Fig. 10(b), which of a user U1 and a user U2 is walking in front is identified (determined). Details regarding the identification processing of the anteroposterior relationship will be described later.

[0068]

The authentication target setting unit 204 sets a user in the foremost row (forefront) among a plurality of users (a plurality of users present in the authentication area) as the authentication target (Step S113). In the example of Fig. 10(b), in a case where the user U1 is walking in front of the user U2 (in a case where the user U1 is closer to the gate device 10 than the user U2), the face image of the user U1 is set as the authentication target.

[0069]

As described above, when one user appears in both the upper image and the lower image, the authentication target setting unit 204 sets the one user as the authentication target person. In addition, when one user appears in one of the upper image and the lower image, the authentication target setting unit 204 sets the one user as the authentication target person.

[0070]

Note that the authentication target setting unit 204 desirably confirms whether the users appearing in the upper image and the lower image are the same person before setting the authentication target in Step S111. Specifically, the authentication target setting unit 204 calculates the feature amount from each of the two face images. The authentication target setting unit 204 determines whether the two feature amounts

substantially match. The authentication target setting unit 204 calculates similarity between two feature amounts (feature vectors). If the calculated similarity is equal to or more than a predetermined value, the authentication target setting unit 204 determines that the two feature amounts substantially match. That is, the authentication target setting unit 204 determines whether the two face images are face images of the same person by one-to-one collation using the feature amounts generated from the upper face image and the lower face image. When the two feature amounts do not match, the authentication target setting unit 204 may set an error. That is, a situation in which one face image is included in each of the upper image and the lower image and each face image is not a face image of the same person does not usually occur. Therefore, it is appropriate to set the situation as an error.

[0071]

In addition, in a case where there are one tall authentication target person and one short authentication target person in the authentication area, the processing related to Step S112 is executed. However, in this case, since there is no common region between the upper image and the lower image, the anteroposterior relationship in Step S112 cannot be specified. Therefore, when the above situation occurs, the authentication target setting unit 204 sets an error.

[0072]

Next, the processing (the identification processing of the anteroposterior relationship) according to Step S112 in Fig. 7 will be described. Fig. 11 is a flowchart illustrating an example of the anteroposterior relationship specifying processing of the authentication target setting unit 204.

[0073]

The authentication target setting unit 204 sets the “distance

measurement band” in the common region of the two images (upper image, lower image) (Step S201). For example, in a case where the upper image and the lower image illustrated in Fig. 12 are obtained, the region colored in gray is set as the “distance measurement band”. As
 5 illustrated in Fig. 12, the distance measurement band is desirably set on the lower side of the upper image. The distance measurement band is set to a region in which two or more users simultaneously appear in the common region. In an extreme example, the distance measurement band may be set at the lowermost side of the upper image, or the entire common
 10 region may be set as the distance measurement band. The authentication target setting unit 204 sets all or a part of the upper image and the lower image in the distance measurement band.

[0074]

The authentication target setting unit 204 calculates the distance to
 15 the camera installation surface for the object appearing in the distance measurement band (all or part of the common region common to the upper image and the lower image) (Step S202). Specifically, the authentication target setting unit 204 calculates the distance to the camera (upper camera 12-1 and lower camera 12-2) installation surface for each small area
 20 included in the distance measurement band. The authentication target setting unit 204 calculates the distance between each small area (object) and the camera installation surface using the parallax (deviation between upper image and lower image) of the two images.

[0075]

25 The authentication target setting unit 204 calculates a deviation amount (parallax) between the upper image and the lower image regarding the object included in the distance measurement band. The authentication target setting unit 204 calculates the distance between the object and the camera installation surface using the calculated parallax.

That is, the authentication target setting unit 204 calculates the distance between the camera installation surface and the object (small region of the distance measurement band) using a so-called stereo method. Although the calculation of the distance using the stereo method is obvious to those skilled in the art and detailed description is omitted, the authentication target setting unit 204 calculates the distance between the camera installation surface and the object by the following method.

[0076]

The authentication target setting unit 204 divides the distance measurement band into a plurality of small areas. For example, the authentication target setting unit 204 divides the distance measurement band such that the size of one area is $A1 \times A2$ pixels. The authentication target setting unit 204 calculates a distance D between the small area (object) and the camera installation surface by the following Expression

(1).

[0077]

[Math. 1]

$$D = B \times f/Z$$

... (1)

[0078]

In Expression (1), B is a distance (camera interval) between the upper camera 12-1 and the lower camera 12-2. f is the focal length of the two cameras. Z is parallax (deviation amount). Fig. 13 illustrates the relationship between the parameters expressed by Expression (1).

[0079]

In Expression (1), the camera interval B and the focal length f are values determined in advance according to the installation and selection of the two cameras. Therefore, the authentication target setting unit 204 can calculate the distance D by obtaining the parallax Z .

[0080]

The authentication target setting unit 204 searches for a region having a matching pattern in a small region forming a common region band of the reference camera (the upper camera 12-1) with respect to one
5 small region in the image (distance measurement band) of the camera (the lower camera 12-2 in Fig. 13) as a base. For example, the authentication target setting unit 204 calculates a city block distance for each small region, and selects a region having the shortest distance as a region with the same pattern. The authentication target setting unit 204 calculates a
10 deviation between the small region on the base camera side and the small region on the reference camera side selected as described above as the parallax Z.

[0081]

For example, when the distance D between the object included in
15 the distance measurement band illustrated in Fig. 12 and the camera installation surface is calculated, and the position (position in the horizontal direction) of the object is set to the X axis and the calculated distance D is set to the Y axis, a graph as illustrated in Fig. 14 is obtained.

20 [0082]

In order to obtain a waveform as illustrated in Fig. 14, the authentication target setting unit 204 desirably performs predetermined data processing or the like on the calculated distance D. For example, in order to remove a high frequency component (a high frequency component
25 of the distance D) caused by noise included in the image, the authentication target setting unit 204 may apply a low pass filter (LPF) to the calculated distance D. Alternatively, in a case where the variation of the distance D falls within a predetermined range, the authentication target setting unit 204 may execute processing of converging each value

of the distance D to a predetermined value (for example, the average value of the variation values).

[0083]

As illustrated in Fig. 14, when a plurality of users is imaged by the upper camera 12-1 and the lower camera 12-2, peaks depending on the number of people appearing in the two images appear. In the examples of Figs. 12 and 14, two peaks appear.

[0084]

The authentication target setting unit 204 specifies a position (X coordinate) where each peak appears (Step S203). In the example of Fig. 14, coordinates $X1$ and $X2$ are specified. That is, the authentication target setting unit 204 specifies (searches) peaks depending on the number of the plurality of users in the position of the object (the position of the object in the image) and the distance (for example, a graph of Fig. 14 illustrating the relationship between the position and the distance.) to the camera installation surface of the object.

[0085]

The authentication target setting unit 204 specifies the peak of the distance D using an arbitrary method. For example, the authentication target setting unit 204 calculates a difference between data regarding the distance D , and sets a point at which the calculated difference changes from positive to negative as a peak. It is desirable that the authentication target setting unit 204 specify the peak from the data to which the filtering processing and the convergence processing are applied.

[0086]

The authentication target setting unit 204 selects the X coordinate related to the minimum peak value (Step S204). The user (face image) located on the vertically upper side of the selected X coordinate is specified as a person in the foremost row of the authentication area. In

the examples of Figs. 12 and 14, the user U1 located above the coordinate X1 is specified as the user in the foremost row. That is, the authentication target setting unit 204 treats the user at the position related to the minimum peak value among the plurality of specified peaks as the user in the foremost row.

[0087]

The authentication target setting unit 204 sets the face image of the user in the foremost row as the authentication target (Step S113 in Fig. 7). As described above, in a case where a plurality of users appears in both the upper image and the lower image, the authentication target setting unit 204 specifies the user in the foremost row from among the plurality of users by calculating the distance between each of the plurality of users and the camera installation surface. The authentication target setting unit 204 sets the specified user as an authentication target person.

[0088]

The authentication target setting unit 204 delivers the face image (biometric information) of the authentication target person to the authentication request unit 205.

[0089]

The authentication request unit 205 is a unit that requests the server device 20 to authenticate the authentication target person. The authentication request unit 205 generates a feature amount (a feature vector including a plurality of feature amounts) from the face image acquired from the biometric information acquisition unit 203. The authentication request unit 205 transmits an authentication request including the generated feature amount (biometric information) to the server device 20.

[0090]

Note that an existing technique can be used for the feature amount

generation processing by the authentication request unit 205, and thus, a detailed description thereof will be omitted. For example, the authentication request unit 205 extracts eyes, a nose, a mouth, and the like as feature points from the face image. Thereafter, the authentication request unit 205 calculates the position of each feature point and the distance between the feature points as feature amounts, and generates a feature vector (vector information characterizing the face image) including a plurality of feature amounts.

[0091]

The authentication request unit 205 generates an authentication request including an identifier (hereinafter, referred to as a gate identifier) of the own device, a feature amount, and the like (see Fig. 15). As the gate identifier, a media access control (MAC) address or an Internet protocol (IP) address of the gate device 10 can be used.

[0092]

When transmitting the authentication request to the server device 20, the authentication request unit 205 delivers the feature amount included in the request to the entrant determination unit 206.

[0093]

The authentication request unit 205 receives a response to the authentication request from the server device 20. The authentication request unit 205 delivers a response (authentication success, authentication failure) from the server device 20 to the gate control unit 207.

[0094]

The entrant determination unit 206 is a unit that detects an entrant using the in-gate sensor 16 for detecting an entrant into the own device (gate device 10) and determines whether the entrant and the authentication target person are the same person. The entrant determination unit 206

monitors (polls) the output of the in-gate sensor 16. When the output of the in-gate sensor 16 indicates “there is an entrant inside”, the entrant determination unit 206 determines whether the entrant and the authentication target person match. Specifically, similarly to the biometric information acquisition unit 203, the entrant determination unit 206 controls at least one camera to acquire a face image. The entrant determination unit 206 calculates a feature amount (a feature amount of an entrant) from the obtained face image.

[0095]

The entrant determination unit 206 determines whether the calculated feature amount (the feature amount of the entrant) and the feature amount (the feature amount of the authentication target person) acquired from the authentication request unit 205 substantially match. Specifically, the entrant determination unit 206 calculates the similarity between the two feature amounts. A chi-square distance, a Euclidean distance, or the like can be used for the similarity. Note that the similarity is lower as the distance is longer, and the similarity is higher as the distance is shorter. When the similarity is equal to or greater than a predetermined value, the entrant determination unit 206 determines that the two feature amounts substantially match (the entrant and the authentication target person are the same person).

[0096]

In this manner, the entrant determination unit 206 detects an entrant based on the detection signal from a passage sensor (the in-gate sensor 16) using light. Thereafter, the entrant determination unit 206 performs one-to-one collation using two feature amounts (feature amount of entry person, feature amount of authentication target person). Whether the entrant and the authentication target person are the same person is determined by the one-to-one collation (one-to-one collation

using the biometric information of the entrant and the biometric information of the authentication target person).

[0097]

When determining that the entrant and the authentication target person are the same person, the entrant determination unit 206 notifies the gate control unit 207 of the fact.

[0098]

The gate control unit 207 is a unit that controls the gate 17 included in the gate device 10. The gate control unit 207 controls the gate 17 based on the authentication result of the authentication target person. The gate control unit 207 opens the gate 17 when the authentication result of the server device 20 is “authentication success” and the entrant and the authentication target person are the same person. In other words, in principle, the gate control unit 207 does not open the gate 17 unless the above condition (authentication success, the entrant and the authentication target person are the same person) is satisfied. The gate control unit 207 closes the gate 17 after a user permitted to pass by using a distance sensor or the like passes through the gate 17.

[0099]

The message output unit 208 is a unit that outputs a message to be notified to the user (authentication target person, authentication successful person, etc.). The message output unit 208 notifies the user of a necessary message using the displays 13 and 14, a speaker, or the like.

[0100]

The storage unit 209 is a unit that stores information necessary for the operation of the gate device 10.

[0101]

Fig. 16 is a flowchart illustrating an example of the operation of

the gate device 10 according to the first example embodiment.

[0102]

The gate device 10 detects whether the user is present in the authentication area (Step S301). When the user is not detected in the

5 authentication area (Step S301: No branch), the gate device 10 repeats the process in Step S301.

[0103]

When the user is detected (Step S301: Yes branch), the gate device 10 images the user located in the authentication area and acquires the face
10 image (Step S302).

[0104]

The gate device 10 calculates a feature amount from the face image (Step S303).

[0105]

15 The gate device 10 transmits an authentication request including the calculated feature amount to the server device 20, and receives a response (authentication result) to the authentication request (Step S304).

[0106]

The gate device 10 determines whether an entrant is present in the
20 internal area of the own device (Step S305). When the entrant cannot be detected even after the lapse of a predetermined time from the start of the process of detecting the entrant (Step S305: No branch), the gate device 10 executes the processing related to Step S309.

[0107]

25 When the entrant is detected during the predetermined period (Step S305: Yes branch), the gate device 10 determines whether the entrant and the authentication target person are the same person (Step S306). When the entrant and the authentication target person are not the same person (Step S306: No branch), the gate device 10 executes the processing

related to Step S309.

[0108]

If the entrant and the authentication target person are the same person (Step S306: Yes branch), the gate device 10 determines whether the authentication result acquired from the server device 20 is “authentication success” (Step S307). When the authentication result is "authentication failure", the gate device 10 executes the processing related to Step S309. Note that it is a matter of course that the processing related to Step S307 may be executed before the processing related to Step S305.

10 [0109]

If the authentication result is "authentication success", the gate device 10 opens the gate 17 (Step S308). When a gate opening condition (the authentication success, and the entrant and the authentication target person are the same person) is satisfied, the gate device 10 controls the gate 17 so that the authentication target person can pass through. At that time, the gate device 10 may display on displays 13 and 14 that the authentication of the authentication target person has succeeded.

[0110]

When the above condition is not satisfied (No branch in any of Steps S305, S306, and S307), the gate device 10 performs error processing (Step S309). Specifically, when the entrant cannot be detected during the predetermined period (Step S305: No branch), the gate device 10 discards the authentication result acquired from the server device 20. When the entrant and the authentication target person are different (Step S306: No branch), the gate device 10 displays the fact on the displays 13 and 14. When the authentication by the server device 20 fails (Step S307: No branch), the gate device 10 displays the fact on the displays 13 and 14.

[0111]

In this way, the gate device 10 acquires the biometric information (face image) on the users from the short height to the high height using the two cameras (upper camera 12-1 and lower camera 12-2) installed vertically. In addition, the gate device 10 uses the parallax of the object commonly appearing in the images obtained from the two cameras, determines the anteroposterior relationship in a case where a plurality of users is imaged, and specifies the correct authentication target person.

That is, the gate device 10 uses the two cameras to acquire biometric information from users having greatly different heights without omission, and prevents erroneous determination of the authentication target person.

[0112]

[Server Device]

Fig. 17 is a diagram illustrating an example of a processing configuration (processing module) of the server device 20 according to the first example embodiment. Referring to Fig. 17, the server device 20 includes a communication control unit 301, a user registration unit 302, an authentication unit 303, and a storage unit 304.

[0113]

The communication control unit 301 is a unit that controls communication with other devices. Specifically, the communication control unit 301 receives data (packet) from the gate device 10. Further, the communication control unit 301 transmits data to the gate device 10. The communication control unit 301 delivers data received from another device to another processing module. The communication control unit 301 transmits data acquired from another processing module to another device. In this manner, the other processing modules transmit and receive data to and from other devices via the communication control unit 301.

[0114]

The user registration unit 302 is a unit that performs system registration of a user (system user) who can pass through the gate device 10. The user registration unit 302 acquires biometric information (for example, a face image) and personal information (for example, the name) of a user who can pass through the gate device 10 using an arbitrary means.

[0115]

For example, in a case where the gate device 10 is a device installed at an airport, the system user inputs biometric information and personal information (name, passport number, etc.) to the server device 20 using a web page of an airline company or a kiosk terminal installed at the airport. Alternatively, in a case where the gate device 10 is a device installed at a ticket gate of a station, the system user inputs biometric information, personal information, and the like to the server device 20 from a web page of a railway company or the like or a terminal installed at a station.

[0116]

When acquiring a face image, the user registration unit 302 calculates a feature amount from the face image. The user registration unit 302 registers the biometric information (for example, the feature amount calculated from the face image) of the system user in the “user database”. The user registration unit 302 registers a user identifier (ID) for identifying the system user, personal information (for example, name, nationality, gender, and the like), and biometric information in the user database in association with each other as necessary (see Fig. 18). The user database illustrated in Fig. 18 is an example, and other items may be stored in association with the biometric information (feature amount). For example, a “face image” may be registered in the user database.

[0117]

The authentication unit 303 is a unit that processes the authentication request received from the gate device 10. Specifically, the authentication unit 303 sets the biometric information (feature amount) included in the authentication request as the collation target, and
5 performs the collation processing with the biometric information registered in the user database.

[0118]

More specifically, the authentication unit 303 sets the feature amount extracted from the authentication request as the collation target,
10 and executes one-to-N (N is a positive integer, and the same applies hereinafter) collation with the plurality of feature amounts registered in the user database.

[0119]

The authentication unit 303 calculates similarity between the
15 feature amount (feature vector) of the collation target and each of the plurality of feature amounts on the registration side. The authentication unit 303 sets “authentication success” if the feature amount of which the similarity is equal to or greater than the predetermined value is registered in the user database. The authentication unit 303 sets “authentication
20 failure” if the feature amount of which the similarity is equal to or greater than the predetermined value is not registered in the user database.

[0120]

In addition, the authentication unit 303 specifies a feature amount of which the similarity with the feature amount of the collation target is
25 equal to or greater than a predetermined value and of which the similarity is the highest among the plurality of feature amounts registered in the user database. The authentication unit 303 transmits the user ID and the personal information related to the specified feature amount to another module and the gate device 10 as necessary. For example, in a case

where the gate device 10 is a device installed in an airport, the progress (check passage, security check passage, etc.) of the procedure is managed using the information (name, passport number, etc.) specified by the authentication unit 303. For example, in a case where gate device 10 is
5 a device installed at a ticket gate of a station, fare adjustment processing or the like is performed using the specified information.

[0121]

The storage unit 304 stores various types of information necessary for the operation of the server device 20. In the storage unit 304, a user
10 database is constructed.

[0122]

Fig. 19 is a sequence diagram illustrating an example of the operation of the authentication system according to the first example embodiment. It is assumed that the system user is registered in advance
15 prior to the operation of Fig. 19.

[0123]

The gate device 10 detects the user located in the authentication area (Step S01). Note that the gate device 10 may take a measure such that the user can recognize that the authentication processing is being
20 executed when the authentication target person is detected. For example, the gate device 10 may display the face image of the authentication target person on the displays 13 and 14. Alternatively, the gate device 10 may display, on displays 13 and 14, a message or a symbol (for example, an arrow or the like) prompting the user to enter the
25 internal area of the gate device 10 from the authentication area.

[0124]

The gate device 10 acquires the biometric information of the authentication target person (the user located in the authentication area), and transmits an authentication request including the biometric

information to the server device 20 (Step S02).

[0125]

The server device 20 executes authentication processing using the biometric information included in the authentication request and the

5 biometric information registered in the user database (Step S11).

[0126]

The server device 20 transmits the authentication result (authentication success, authentication failure) to the gate device 10 (Step S12).

10 [0127]

The gate device 10 determines whether the authentication target person enters in parallel with the authentication processing of the server device 20 (detection of the entrant; Step S03).

[0128]

15 The gate device 10 checks whether a condition for opening the gate 17 (gate opening condition) is satisfied (Step S04). Specifically, the gate device 10 confirms whether the authentication succeeds and whether the entrant and the authentication target person are the same person.

[0129]

20 When the gate opening condition is satisfied, the gate device 10 opens the gate 17 (Step S05).

[0130]

As described above, the authentication system according to the first example embodiment specifies the authentication target person in a
25 case where a plurality of persons (candidates of system user and authentication target person) is captured in images obtained from two cameras (upper camera 12-1 and lower camera 12-2). At that time, the gate device 10 calculates the distance between each user and the camera installation surface using the parallax of the object (the user commonly

appearing in the two images) in the two images. The gate device 10 specifies a user closest to the own device based on the calculated distance, and sets the specified user as an authentication target person.

As described above, in the first example embodiment, the user in the
5 foremost row is specified regardless of the size of the face area having a large individual difference, so that the user to be authenticated can be accurately determined.

[0131]

[Second Example Embodiment]

10 Next, a second example embodiment will be described in detail with reference to the drawings.

[0132]

In the first example embodiment, the distance between the common region of the upper image and the lower image and the camera installation
15 surface is calculated, and the anteroposterior relationship of the user is determined based on the calculated distance. In the second example embodiment, a case where the anteroposterior relationship is determined on the basis of the positional relationship of the user appearing in the image will be described.

20 [0133]

Since the configuration of the authentication system according to the second example embodiment can be the same as that of the first example embodiment, the description related to Fig. 2 is omitted. In addition, since the processing configurations of the gate device 10 and the
25 server device 20 according to the second example embodiment can be the same as those of the first example embodiment, the description thereof will be omitted.

[0134]

In the first example embodiment, the case where the user is imaged

using the two cameras has been described. However, in the second example embodiment, it is sufficient that the image of the user can be capture using at least one or more cameras. For example, in a case where a user with a high height and a short height can be imaged by one
5 camera, two cameras are unnecessary. Alternatively, the two cameras are unnecessary even in a case where authentication regarding a user with a high height and a short height is unnecessary or an error is allowed at the time of authentication. It is a matter of course that the gate device
10 according to the second example embodiment may include two cameras. In the following description, a case where the gate device 10 according to the second example embodiment includes two cameras will be described.

[0135]

Hereinafter, differences between the first and second example
15 embodiments will be mainly described.

[0136]

As described above, the face authentication module 11 is installed to be inclined at a predetermined angle with respect to the traveling direction of the user. For example, the face authentication module 11 is
20 installed at 45 degrees (θ illustrated in Fig. 4 is 45 degrees).

[0137]

Since the face authentication module 11 is installed to be inclined with respect to the traveling direction of the user, the position where the user appears in the image changes according to the position of the user
25 (distance between the user and the gate device 10). Specifically, in a case where the user is present far away, the user appears on the side where the face authentication module 11 of the gate device 10 is installed (the left direction in the example of Fig. 4). Thereafter, when the user approaches the gate device 10, the position of the user (the position of the

user shown in the image) moves on the right side (in the rightward direction; the X coordinate in a case where the lower left of the image is set as the origin moves in the positive direction).

[0138]

5 For example, as illustrated in Fig. 20(a), a case where the user moves to positions P1, P2, and P3 is considered. In this case, the position of the user in the captured image moves from left to right as illustrated in Fig. 20(b). This fact indicates that the user appeared on the right side of the image is close to the gate device 10. In other words, in a case where a plurality of users appears in the same image, it indicates that the user located on the right side of the image is closer to the gate device 10 than the user located on the left side. The gate device 10 according to the second example embodiment specifies the anteroposterior relationship among the plurality of users using the fact.

15 [0139]

 The authentication target setting unit 204 of the gate device 10 according to the second example embodiment is different from that of the first example embodiment in the processing of Step S112 illustrated in Fig. 7. In a case where a plurality of users appears in the image, the authentication target setting unit 204 specifies the user in the foremost row among the plurality of users according to the position of each of the plurality of users in the image. The authentication target setting unit 204 sets the specified user as an authentication target person.

[0140]

25 Fig. 21 is a flowchart illustrating an example of the operation of the authentication target setting unit 204 according to the second example embodiment. With reference to Fig. 21, the anteroposterior relationship specifying processing of the authentication target setting unit will be described.

[0141]

The authentication target setting unit 204 calculates X coordinates (coordinates in the horizontal direction) of each face image included in the image (Step S401). Note that the calculation of the X coordinates
 5 may be performed using any one of the upper image and the lower image.

[0142]

The authentication target setting unit 204 selects the X coordinate of the right end (Step S402). The face image related to the selected X coordinate is to be authenticated.

10 [0143]

The authentication target setting unit 204 may apply a predetermined condition to a target for specifying the anteroposterior relationship to a plurality of users (face images) included in the image. The authentication target setting unit 204 may set a face image satisfying
 15 a predetermined condition as the identification target of the anteroposterior relationship. Specifically, the authentication target setting unit 204 may exclude a user whose interocular distance is smaller than a predetermined value (for example, 60 pixels) from the determination related to the user in the foremost row among the plurality
 20 of users. By setting such a condition, it is possible to exclude a user who appears at the right end of the image while being located far from the gate device 10.

[0144]

Note that, in the gate device 10 illustrated in Figs. 3 and 4, since
 25 the face authentication module 11 is installed on the right side with respect to the traveling direction of the user, the user appearing at the right end of the image is set as the authentication target person. In a case where the face authentication module 11 is installed on the left side with respect to the traveling direction of the user, the user appearing at

the left end of the image is set as the authentication target person.

[0145]

As described above, the gate device 10 according to the second example embodiment specifies the user located at the end on the side determined according to the traveling direction of the user and the installation position of the camera as the user in the foremost row. As a result, similarly to the first example embodiment, the gate device 10 can accurately determine the user of the authentication target.

[0146]

Next, hardware of each device constituting the authentication system will be described. Fig. 22 is a diagram illustrating an example of a hardware configuration of the gate device 10. Note that, since the face authentication module 11, the camera 12, and the like have already been described, these elements are not illustrated in Fig. 22.

[0147]

The gate device 10 includes a processor 311, a memory 312, an input/output interface 313, a communication interface 314, and the like. The components such as the processor 311 are connected by an internal bus or the like and are configured to be able to communicate with each other.

[0148]

However, the configuration illustrated in Fig. 22 is not intended to limit the hardware configuration of the gate device 10. The gate device 10 may include hardware (not illustrated) or may not include the input/output interface 313 as necessary. In addition, the number of processors 311 and the like included in the gate device 10 is not limited to the example of Fig. 22, and for example, a plurality of processors 311 may be included in the gate device 10.

[0149]

The processor 311 is a programmable device such as a central processing unit (CPU), a micro processing unit (MPU), or a digital signal processor (DSP). Alternatively, the processor 311 may be a device such as a field programmable gate array (FPGA) or an application specific integrated circuit (ASIC). The processor 311 is configured to execute various programs including an operating system (OS).

[0150]

The memory 312 is a random access memory (RAM), a read only memory (ROM), a hard disk drive (HDD), a solid state drive (SSD), or the like. The memory 312 stores an OS program, an application program, and various data.

[0151]

The input/output interface 313 is an interface of a display device or an input device (not illustrated). The display device may be the display 14. The input device may be a touch panel integrated with the display 14.

[0152]

The communication interface 314 is a circuit, a module, or the like that communicates with another device. For example, the communication interface 314 includes a network interface card (NIC) or the like.

[0153]

The functions of the gate device 10 are implemented by various processing modules. The processing module is implemented, for example, by the processor 311 executing a program stored in the memory 312. In addition, the program can be recorded in a computer-readable storage medium. The storage medium may be a non-transient (non-transitory) medium such as a semiconductor memory, a hard disk, a magnetic recording medium, or an optical recording medium. That is,

the present disclosure can also be embodied as a computer program product. In addition, the program can be downloaded via a network or updated using a storage medium storing the program. Further, the processing module may be achieved by a semiconductor chip.

5 [0154]

The server device 20 can be configured similarly to the gate device 10, and a basic hardware configuration of the server device is not different from that of the gate device 10. Therefore, the description is omitted.

10 [0155]

The gate device 10 is equipped with a computer, and can achieve the function of the gate device 10 by causing the computer to execute a program. The gate device 10 executes the "gate device control method" by the program.

15 [0156]

[Modified Example]

Note that the configuration, operation, and the like of the authentication system described in the above example embodiments are merely examples, and are not intended to limit the configuration and the
20 like of the system.

[0157]

The application destination of the gate device 10 of the present disclosure is not particularly limited. For example, "airport" is exemplified as an application destination (installation place) of the gate
25 device 10 of the present disclosure. Specifically, the gate device 10 may be used as a part of an apparatus responsible for an examination system using biometric authentication performed at an airport. In the examination system, identity confirmation (confirmation as to whether the photographed face image matches the face image described in the

passport) is performed at the time of check-in, and face data (face image or feature amount), flight information, and passport information are stored in association with each other. When the identity confirmation is completed, a token for performing examination in biometric

5 authentication is generated. The gate device 10 of the present disclosure is installed in various examination areas (for example, the security inspection site) in an airport, and the gate device 10 authenticates a user by collating a face image registered at the time of check-in with a face image captured by the own device.

10 [0158]

In the above example embodiments, the case of detecting an entrant using the in-gate sensor 16 has been described. However, when it is difficult for a user different from the authentication target person to enter the gate device 10, the detection of the entrant is unnecessary. For
15 example, by configuring the length of the main body of the gate device 10 in the traveling direction of the person passing through the gate to be long and setting the authentication area inside gate device 10, it is difficult for a user different from the authentication target person to enter the inside of the gate device 10.

20 [0159]

In the above example embodiments, the gate device 10 including the two cameras (upper camera 12-1 and lower camera 12-2) has been described. However, the gate device 10 may include one camera. In this case, one camera may be configured to be movable up and down, and
25 the gate device 10 may acquire two images (upper image, lower image) by changing a position of the camera.

[0160]

In the above example embodiments, the case where the user is imaged by the two cameras (upper camera 12-1 and lower camera 12-2),

and the authentication target person (the user in the foremost row) is specified using the parallax obtained from the two images has been described. However, the number of cameras is not limited to two, and the authentication target person may be specified using three or more
5 cameras. For example, a middle camera is installed between the upper camera 12-1 and the lower camera 12-2. The gate device 10 can determine the anteroposterior relationship between the users appearing in the upper camera 12-1 and the middle camera and the anteroposterior relationship between the users appearing in the middle camera and the
10 lower camera 12-2.

[0161]

In the above example embodiments, the description has been made on the assumption that the performance of the upper camera 12-1 and the lower camera 12-2 is substantially the same. However, the performance
15 of these cameras may be different. In this case, the gate device 10 may take measures to fill the performance difference between the two cameras. For example, the gate device 10 may convert the size or the like of one of the obtained two images. That is, the gate device of the disclosure of the present application can be achieved even in a case where the selection
20 of the camera that can be used is widened by the measures such as the conversion processing, and the installation place and the like of the camera in the face authentication module 11 are limited.

[0162]

In the above example embodiments, the case where the biometric
25 information related to the feature amount generated from the face image is transmitted from the gate device 10 to the server device 20 has been described. However, the "face image" itself may be transmitted as the biometric information from the gate device 10 to the server device 20. The server device 20 may generate a feature amount from the acquired

face image and execute authentication processing (one-to-N collation).
Even when the face image itself is transmitted to the server device 20, the
gate device 10 determines the identity between the authentication target
person and the entrant using the feature amount generated from the face
5 image.

[0163]

In the above example embodiments, the determination on the
identity between the authentication target person and the entrant is
executed by the gate device 10, but the determination may be executed by
10 the server device 20. In this case, the gate device 10 acquires biometric
information of an entrant into the internal area, and transmits the
biometric information to the server device 20. The server device 20 may
collate the biometric information included in the authentication request
with the biometric information of the entrant to determine the identity
15 between the authentication target person and the entrant.

[0164]

In the above example embodiments, a so-called client server
system has been described in which the gate device 10 transmits the
authentication request to the server device 20, and the server device 20
20 processes the request. However, the authentication processing executed
by the server device 20 may be executed by the gate device 10. That is,
some or all of the functions of server device 20 may be implemented by
the gate device 10.

[0165]

25 In the above example embodiments, it has been described that an
error is set in a case where the face image is distributed in either the
upper image or the lower image and the image includes a plurality of face
images (Step S105 in Fig. 7). In this case, when the upper image
includes a plurality of face images, the gate device 10 may determine the

anteroposterior relationship using the parallax between the two images and the position of the user. For example, in the case of Fig. 9(a), the anteroposterior relationship may be determined using an object (torso, legs, or the like of the user) that appears in common in the upper image and the lower image. Alternatively, as described in the second example embodiment, the gate device 10 may determine the anteroposterior relationship according to the position of the face image included in the upper image.

[0166]

In addition, in the case illustrated in Fig. 9(b), since there is no object (user) that appears in common in the upper image and the lower image, it is not possible to determine the anteroposterior relationship using parallax. Therefore, when the face image is present only in the lower image, the gate device 10 may determine the anteroposterior relationship of the user according to the position of the user in the image (lower image).

[0167]

Alternatively, by combining the first and second example embodiments, an authentication target person may be selected using parallax in the case illustrated in Figs. 8(a) and 9(a), and an authentication target person may be selected according to the position of the image in the case illustrated in Fig. 9(b).

[0168]

The gate device 10 may change the control of the LED for dimming according to the purpose of the image (face image; biometric information) to be acquired. For example, the gate device 10 may change the light intensity between the case of imaging the user located in the authentication area and the case of imaging the entrant into the own device.

[0169]

A plurality of gate devices 10 may operate in conjunction with each other or in cooperation with each other. Specifically, the server device 20 may transmit a response to the authentication request acquired from one gate device 10 to another gate device 10. For example, in the example of Fig. 2, the authentication result for the authentication request acquired from the gate device 10-1 may be transmitted to each of the gate devices 10-1 to 10-3. In this case, even if the authentication target person detected by the gate device 10-1 moves toward the gate device 10-2 (even if the authentication target person enters the gate device 10-2), the authentication target person can pass through the gate device 10-2. In this case, the biometric information of the authentication target person generated by the gate device 10-1 is transmitted from the gate device 10-1 to the other gate devices 10-2 and 10-3. Alternatively, the biometric information of the authentication target person may be transmitted from the server device 20 to the other gate devices 10-2 and 10-3.

[0170]

The gate device 10 may be installed in a limited space of an existing facility, for example. In this case, the length of the main body of the gate device 10 in the traveling direction of the person who passes through the gate device 10 can be about 1.5 meters, which is shorter than 2 to 3 meters, which is the length of a general face authentication gate, and the distance to the gate 17 can be, for example, 96 centimeters (corresponding to one and a half steps of the stride of an adult male). When the length of the main body of the gate device 10 is about 1.5 meters, the length of the authentication area in the traveling direction is preferably about 30 cm to 60 cm.

[0171]

A form of data transmission and reception between the gate device

10 and the server device 20 is not particularly limited, but data transmitted and received between these devices may be encrypted. The face image and the feature amount calculated from the face image are personal information, and in order to appropriately protect the personal information, it is desirable that encrypted data be transmitted and received.

[0172]

In the flowchart (Sequence Diagram) used in the above description, a plurality of steps (processes) is described in order, but the execution order of the steps executed in the example embodiments is not limited to the described order. In the example embodiments, for example, the order of the illustrated steps can be changed within a range in which there is no problem in terms of content, such as executing each process in parallel.

[0173]

The above example embodiments have been described in detail in order to facilitate understanding of the present disclosure, and it is not intended that all the configurations described above are necessary. In addition, in a case where a plurality of example embodiments has been described, the example embodiments may be used alone or in combination. For example, a part of the configuration of the example embodiment can be replaced with the configuration of another example embodiment, or the configuration of another example embodiment can be added to the configuration of the example embodiment. Further, it is possible to add, delete, and replace other configurations for a part of the configuration of the example embodiment.

[0174]

Although the industrial applicability of the present disclosure is apparent from the above description, the present disclosure can be

suitably applied to an authentication system installed in an airport, a station, or the like.

[0175]

Some or all of the above example embodiments may be described
5 as the following supplementary notes, but are not limited to the following.

[Supplementary Note 1]

A gate device including:

an acquisition unit configured to acquire an image from a camera;

a setting unit configured, in a case where a plurality of users

10 appears in the acquired image, to specify a user in a foremost row among the plurality of users according to a position of each of the plurality of users in the image, and set the specified user as an authentication target person; and

a gate control unit configured to control a gate based on an

15 authentication result of the authentication target person.

[Supplementary Note 2]

The gate device according to Supplementary Note 1, in which the camera is installed at a predetermined angle with respect to a traveling direction of the user.

20 [Supplementary Note 3]

The gate device according to Supplementary Note 1 or 2, in which the setting unit specifies a user located at an end on a side determined according to the traveling direction of the user and an installation position of the camera as the user in the foremost row.

25 [Supplementary Note 4]

The gate device according to any one of Supplementary Notes 1 to 3, in which the setting unit excludes a user whose interocular distance is smaller than a predetermined value from the determination related to the user in the foremost row among the plurality of users.

[Supplementary Note 5]

The gate device according to any one of Supplementary Notes 1 to 4, in which in a case where the camera is installed on a right side with respect to the traveling direction of the user, the setting unit specifies a user appearing at a right end of the image as the user in the foremost row.

[Supplementary Note 6]

The gate device according to any one of Supplementary Notes 1 to 4, in which in a case where the camera is installed on a left side with respect to the traveling direction of the user, the setting unit specifies a user appearing at a left end of the image as the user in the foremost row.

[Supplementary Note 7]

The gate device according to any one of Supplementary Notes 1 to 6, further including an authentication request unit configured to transmit an authentication request including biometric information of the authentication target person to a server device.

[Supplementary Note 8]

The gate device according to Supplementary Note 7, in which the authentication request unit transmits the authentication request including a feature amount generated from a face image of the authentication target person to the server device.

[Supplementary Note 9]

An authentication system including:

a server device configured to store biometric information of each of a plurality of system users and execute authentication processing using the plurality of pieces of biometric information; and

a gate device connected to the server device, in which the gate device includes:

an acquisition unit configured to acquire an image from a camera;

a setting unit that configured, in a case where a plurality of users

appears in the acquired image, to specify a user in a foremost row among the plurality of users according to a position of each of the plurality of users in the image, and set the specified user as an authentication target person;

- 5 an authentication request unit configured to request a server device to authenticate the authentication target person; and
- a gate control unit configured to control a gate based on an authentication result of the authentication target person.

[Supplementary Note 10]

- 10 The authentication system according to Supplementary Note 9, in which

 the authentication request unit transmits an authentication request including biometric information of the authentication target person to the server device, and

- 15 the server device authenticates the authentication target person using the biometric information acquired from the authentication request and the biometric information of the plurality of system users.

[Supplementary Note 11]

 A gate device control method including:

- 20 in a gate device,
- acquiring an image from a camera;

 in a case where a plurality of users appears in the acquired image, specifying a user in a foremost row among the plurality of users according to a position of each of the plurality of users in the image, and setting the specified user as an authentication target person; and

- 25 controlling a gate based on an authentication result of the authentication target person.

[Supplementary Note 12]

 A computer-readable storage medium storing a program for causing

a computer mounted in a gate device to execute:

acquiring an image from a camera;

in a case where a plurality of users appears in the acquired image,
specifying a user in a foremost row among the plurality of users according
5 to a position of each of the plurality of users in the image, and setting the
specified user as an authentication target person; and

controlling a gate based on an authentication result of the
authentication target person.

[0176]

10 The disclosures of the cited prior art documents are incorporated
herein by reference. While the example embodiments of the present
disclosure have been particularly shown and described above, the present
disclosure is not limited to these example embodiments. It will be
understood by those skilled in the art that these example embodiments are
15 exemplary only and that various modifications may be made without
departing from the scope and spirit of the present disclosure as defined by
the claims. That is, it goes without saying that the present disclosure
includes various modifications and corrections that can be made by those
skilled in the art in accordance with the entire disclosure including the
20 claims and the technical idea.

[Reference signs List]

[0177]

10, 10-1 to 10-3, 100 gate device

11 face authentication module

25 12-1 upper camera

12-2 lower camera

13 display

14 display

15 area sensor

	16	in-gate sensor
	17	gate
	20	server device
	101	acquisition unit
5	102	setting unit
	103, 207	gate control unit
	201, 301	communication control unit
	202	user detection unit
	203	biometric information acquisition unit
10	204	authentication target setting unit
	205	authentication request unit
	206	entrant determination unit
	208	message output unit
	209, 304	storage unit
15	302	user registration unit
	303	authentication unit
	311	processor
	312	memory
	313	input/output interface
20	314	communication interface

[Document Name] CLAIMS

[Claim 1]

A gate device comprising:

an acquisition unit configured to acquire an image from a camera;

5 a setting unit configured, in a case where a plurality of users appears in the acquired image, to specify a user in a foremost row among the plurality of users according to a position of each of the plurality of users in the image, and set the specified user as an authentication target person; and

10 a gate control unit configured to control a gate based on an authentication result of the authentication target person.

[Claim 2]

The gate device according to claim 1, wherein the camera is installed at a predetermined angle with respect to a traveling direction of
15 the user.

[Claim 3]

The gate device according to claim 1 or 2, wherein the setting unit specifies a user located at an end on a side determined according to the traveling direction of the user and an installation position of the camera
20 as the user in the foremost row.

[Claim 4]

The gate device according to any one of claims 1 to 3, wherein the setting unit excludes a user whose interocular distance is smaller than a predetermined value from the determination related to the user in the
25 foremost row among the plurality of users.

[Claim 5]

The gate device according to any one of claims 1 to 4, wherein in a case where the camera is installed on a right side with respect to the traveling direction of the user, the setting unit specifies a user appearing

at a right end of the image as the user in the foremost row.

[Claim 6]

The gate device according to any one of claims 1 to 4, wherein in a case where the camera is installed on a left side with respect to the

5 traveling direction of the user, the setting unit specifies a user appearing at a left end of the image as the user in the foremost row.

[Claim 7]

The gate device according to any one of claims 1 to 6, further comprising an authentication request unit configured to transmit an

10 authentication request including biometric information of the authentication target person to a server device.

[Claim 8]

The gate device according to claim 7, wherein the authentication request unit transmits the authentication request including a feature

15 amount generated from a face image of the authentication target person to the server device.

[Claim 9]

An authentication system comprising:

20 a server device configured to store biometric information of each of a plurality of system users and execute authentication processing using the plurality of pieces of biometric information; and

a gate device connected to the server device, wherein

the gate device includes:

an acquisition unit configured to acquire an image from a camera;

25 a setting unit that configured, in a case where a plurality of users appears in the acquired image, to specify a user in a foremost row among the plurality of users according to a position of each of the plurality of users in the image, and set the specified user as an authentication target person;

an authentication request unit configured to request a server device to authenticate the authentication target person; and

a gate control unit configured to control a gate based on an authentication result of the authentication target person.

5 [Claim 10]

The authentication system according to claim 9, wherein

the authentication request unit transmits an authentication request including biometric information of the authentication target person to the server device, and

10 the server device authenticates the authentication target person using the biometric information acquired from the authentication request and the biometric information of the plurality of system users.

[Claim 11]

A gate device control method comprising:

15 in a gate device,

acquiring an image from a camera;

in a case where a plurality of users appears in the acquired image, specifying a user in a foremost row among the plurality of users according to a position of each of the plurality of users in the image, and setting the

20 specified user as an authentication target person; and

controlling a gate based on an authentication result of the authentication target person.

[Claim 12]

A computer-readable storage medium storing a program for causing

25 a computer mounted in a gate device to execute:

acquiring an image from a camera;

in a case where a plurality of users appears in the acquired image, specifying a user in a foremost row among the plurality of users according to a position of each of the plurality of users in the image, and setting the

specified user as an authentication target person; and

controlling a gate based on an authentication result of the authentication target person.