(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 116 499 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
20.08.2014 Bulletin 2014/34

(21) Application number: **07713926.9**

(22) Date of filing: **08.02.2007**

(51) Int Cl.:
B66B 5/00 *(2006.01)* ***G08B 13/196*** *(2006.01)*
B66B 1/46 *(2006.01)*

(86) International application number:
PCT/JP2007/052210

(87) International publication number:
WO 2008/096433 (14.08.2008 Gazette 2008/33)

(54) **ELEVATOR SECURITY SYSTEM**

AUFZUGSSICHERHEITSSYSTEM

SYSTÈME DE SÉCURITÉ D'ASCENSEUR

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

(43) Date of publication of application:
11.11.2009 Bulletin 2009/46

(73) Proprietor: **Mitsubishi Electric Corporation**
Chiyoda-ku
Tokyo 100-8310 (JP)

(72) Inventor: **KURODA, Shinichi**
Tokyo 100-8310 (JP)

(74) Representative: **HOFFMANN EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(56) References cited:
JP-A- 2003 109 129
JP-A- 2003 109 129
JP-A- 2005 132 549
JP-A- 2006 103 854
JP-A- 2006 109 014
JP-A- 2006 109 014
JP-A- 2007 022 776
JP-A- 2007 022 776

EP 2 116 499 B1

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD

[0001] The present invention relates to an elevator security system that includes an authenticating apparatus that authenticates permission to use an elevator.

BACKGROUND ART

[0002] Conventionally, as described in JP 2006-103854 A, elevator security systems have been proposed in which an area around an authenticating apparatus that authenticates permission to use an elevator is photographed by a security camera when a predetermined operation is performed on the authenticating apparatus. In these conventional elevator security systems, a date and time that the operation was performed on the authenticating apparatus, and an authentication result, etc., are displayed on a display portion

[0003] JP 2007/22776 A discloses a security system for an elevator comprising a camera inside an elevator car. A face image of a passenger is processed to be compared against image data of wanted criminals stored in a wanted criminals database, which is supplied and updated by an external source. When it is determined that a passenger is a wanted criminal, an information part sends the face image to a remote monitoring center.

[0004] Also according to JP 2003/109129 A, previously registered face images are used to identify suspicious persons by determining that the suspicious person is not among the previously registered face images, in order to inform a manager or watchman to take countermeasures.

[0005] JP 2006/109014 A discloses a suspicious person determining device which takes into account a face direction determined from an photographed image of a person's face over some time. If the face direction coincides over a prescribed period of time, the person is determined as a suspicious.

[0006] JP 2006/103854 A discloses a security system for an elevator in which a data address of image data from a crime prevention camera recorded in a recoding means is linked to a certification operation of an elevator user so that image date and user operation can be retrieved in common for display.

DISCLOSURE OF THE INVENTION

PROBLEM TO BE SOLVED BY THE INVENTION

[0007] However, in conventional elevator security systems, because the date and time and the authentication result are only displayed on the display portion, it is not possible to decide if an elevator user is a suspicious person or if the person has simply pressed a wrong button.

[0008] The present invention aims to solve the above problems and an object of the present invention is to provide an elevator security system that enables improvements in security by determining whether or not an elevator user is a suspicious person.

MEANS FOR SOLVING THE PROBLEM

[0009] The above object is solved by an elevator security system comprising an authenticating apparatus that authenticates permission to use an elevator in response to a predetermined authorizing operation being performed; a security camera for photographing a user who performs the authorizing operation; a processor comprising a sampling portion that samples facial portion image data of the user from image data from the security camera as sampled image data only if authentication by the authenticating apparatus results in a denial of permission; a recording medium in which stored information is stored that includes suspicious person image data consisting of sampled image data that have been sampled in the past for identifying a suspicious person; and a determining portion that determines whether or not the user is a suspicious person by searching whether or not identifying image data that can be recognized as identical to the sampled image data are present in the stored information as the suspicious person image data, and that records the sampled image data in the recording medium as the suspicious person image data if presence of the identifying image data is negated; and an alarm device that issues a warning that indicates that the user is a suspicious person if a determination is made by the determining portion that the user is a suspicious person.

EFFECTS OF THE INVENTION

[0010] In an elevator security system according to the present invention, because facial portion image data of a user are sampled as sampled image data by the sampling portion only if the authentication result is "failed", and sampled image data that have been sampled in the past are stored in the recording medium as suspicious person image data, and whether a user is a suspicious person or not can be determined by searching whether or not identifying image data that can be recognized as identical to the sampled image data from the sampling portion are present as suspicious person image data, a user who has had an authentication result "failed" in the past can be designated a suspicious person, enabling determination as to whether or not an elevator user is a suspicious person to be performed easily. Thus, use of an elevator by suspicious persons can be prevented, enabling elevator security to be improved.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011]

Figure 1 is a block diagram that shows an elevator security system according to Embodiment 1 of the present invention;

Figure 2 is a flowchart that shows actions of a determining portion from Figure 1;

Figure 3 is a block diagram that shows an elevator security system according to Embodiment 2 of the present invention; and

Figure 4 is a flowchart for explaining processing actions of a determining portion from Figure 3.

BEST MODE FOR CARRYING OUT THE INVENTION

[0012] Preferred embodiments of the present invention will now be explained with reference to the drawings.

Embodiment 1

[0013] Figure 1 is a block diagram that shows an elevator security system according to Embodiment 1 of the present invention. An elevator that moves a car inside a hoistway elevator is disposed in a building. The car can be stopped at a plurality of floors by control from an elevator control board 1. An elevator authenticating apparatus 2 is disposed on a predetermined floor (in this example, a first floor (1 F) which is a lobby floor) .

[0014] The authenticating apparatus 2 authenticates permission to use the elevator in response to a predetermined authorizing operation being performed. Examples of a predetermined authorizing operation include operations such as holding a card on which personal information is registered, or a key, etc., over the authenticating apparatus 2, for example.

[0015] When the permission to use the elevator is authenticated, the authenticating apparatus 2 generates authenticating information 21 that includes an authentication result that is either "passed" or "failed". The authenticating apparatus 2 has a clock function, and generates date and time information 22 that corresponds to the date and time that the authorizing operation was performed when the authorizing operation is performed.

[0016] The authenticating information 21 is sent from the authenticating apparatus 2 to the elevator control board 1. If the authentication result from the authenticating apparatus 2 is "failed", the elevator control board 1 disables call registration by the operation of landing buttons (not shown), and releases the disabling of call registration only if the authentication result from the authenticating apparatus 2 is "passed".

[0017] A security camera 3 for photographing users that perform the authorizing operation on the authenticating apparatus 2 is disposed on the floor on which the authenticating apparatus 2 is disposed (the lobby floor). The security camera 3 photographs a predetermined range in the vicinity of the authenticating apparatus 2. The security camera 3 is also capable of serial photography. In addition, the security camera 3 constantly outputs image data 23 that are obtained by that photography.

[0018] The authenticating information 21, the date and time information 22, and the image data 23 are sent to a processor 4. The processor 4 performs processes related to the determination of whether or not the user is a suspicious person based on the authenticating information 21, the date and time information 22, and the image data 23. The processor 4 has a recording medium 5, a sampling portion 6, and a determining portion 7.

[0019] Stored information that includes suspicious person image data for identifying suspicious persons is stored in the recording medium 5. The suspicious person image data that are stored in the recording medium 5 are also associated with the date and time information and saved.

[0020] The sampling portion 6 determines the ability to process the image data 23 from the security camera 3 based on the authenticating information 21. Specifically, the sampling portion 6 performs processing of the image data 23 if the authentication result from the authenticating apparatus 2 is "failed", and stops the processing of the image data 23 if the authentication result from the authenticating apparatus 2 is "passed". In other words, processing of the image data 23 by the sampling portion 6 is performed by sampling image data from a facial portion of the user in the image data 23 as sampled image data 24 only if the authentication that is performed by the authenticating apparatus 2 results in a denial of permission. The sampled image data 24 that have been sampled by the processing of the sampling portion 6 are sent to the determining portion 7 from the sampling portion 6.

[0021] The determining portion 7 receives the sampled image data 24 from the sampling portion 6 and the date and time information 22 from the authenticating apparatus 2. The determining portion 7 has a searching portion 8. The searching portion 8 searches whether or not identifying image data that can be recognized as identical to the sampled image data 24 (i.e., image data that identify a facial portion that is identical to the facial portion of the user identified by the sampled image data 24) are present as suspicious person image data in the stored information. Moreover, the method for searching the stored information is not dependent on any specific method, provided that the algorithm outputs presence or absence of identifying image data as a search result.

[0022] If identifying image data are not present as suspicious person image data in the stored information, the searching portion 8 records the sampled image data 24 as suspicious person image data in the recording medium 5, and also records the date and time information 22 from the authenticating apparatus 2 in the recording medium 5 so as to be associated with the sampled image data 24. If the identifying image data are present as suspicious person image data in the stored information, the searching portion 8 adds the date and time information 22 from the authenticating apparatus 2 to past date and time information that has been associated with the identifying image data.

[0023] In this manner, among users who have operated the authenticating apparatus 2 in the past, sampled image data (facial portion image data) of users whose authentication result in the authenticating apparatus 2

was "failed" are accumulated as suspicious person image data in the recording medium 5, and the date and time information when the authentication result was "failed" is accumulated so as to be associated with the suspicious person image data.

[0024] The determining portion 7 determines whether or not the user who performed the authorizing operation is a suspicious person based on the search results from the searching portion 8. Specifically, the determining portion 7 determines that the user is a legitimate user if the presence of identifying image data is negated by the searching portion 8 (i.e., if identifying image data are not present as suspicious person image data in the stored information). The determining portion 7 determines that the user is a suspicious person if the presence of identifying image data is found by the searching portion 8 (i.e., if identifying image data are present as suspicious person image data in the stored information).

[0025] The determining portion 7 outputs the sampled image data 24 to an alarm device 9 as warning image data 25 only when it has determined that the user is a suspicious person.

[0026] Moreover, the processor 4 is constituted by a computer that has: an arithmetic processing portion (a CPU), a storage portion (ROM, RAM, etc.), and a signal input/output portion. The functions of the sampling portion 6 and the determining portion 7 are implemented by the computer of the processor 4. That is, programs for implementing the functions of the sampling portion 6 and the determining portion 7 are stored in the storage portion of the computer. The data processing portion executes arithmetic processing that relates to the functions of the processor 4 based on the programs that are stored in the storage portion.

[0027] The alarm device 9 is disposed at a predetermined position in a vicinity of the authenticating apparatus 2. The alarm device 9 generates an alarm that indicates that the user is a suspicious person in response to receiving warning image data 25 from the determining portion 7. In addition, the alarm device 9 has a display portion 10 that displays an image that is obtained from the warning image data 25 (i.e., the sampled image data) as a warning. The alarm device 9 issues a warning sound together with the display of the image on the display portion 10.

[0028] Next, operation will be explained. Photography by a security camera 3 is performed continuously on the floor on which the authenticating apparatus 2 is disposed (the lobby floor). Thus, image data 23 from the security camera 3 is sent to the sampling portion 6 continuously. Processing of the image data 23 is not performed by the sampling portion 6 and output of sampled image data 24 from the sampling portion 6 is stopped if an authorizing operation has not been performed on the authenticating apparatus 2.

[0029] When an authorizing operation is performed on the authenticating apparatus 2 by a user, permission to use the elevator is authenticated by the authenticating apparatus 2. If the authentication result is "failed" (i.e., the authentication returns that use of the elevator is not permitted), then call registration by operation of the landing buttons is disabled by control from the elevator control board 1. Consequently, call registration cannot be performed even if the landing buttons are operated.

[0030] In that case, processing of the image data 23 is performed by the sampling portion 6. Facial portion image data of the user from the image data 23 of the security camera 3 is thereby sampled as sampled image data 24.

[0031] The sampled image data 24 that has been sampled by the sampling portion 6 is sent to the determining portion 7. Next, whether the user is a suspicious person or not is determined by the determining portion 7 based on the sampled image data 24. If it is determined that the user is a suspicious person, the sampled image data 24 are sent from the determining portion 7 to the alarm device 9 as warning image data 25. Thus, the image that is obtained from the warning image data 25 is displayed on the display portion 10 as a warning. At that point, the warning sound issues from the warning device 9.

[0032] If it is determined that the user is a legitimate user, transmission of the warning image data 25 from the determining portion 7 to the alarm device 9 is not performed, nor is warning performed by the alarm device 9.

[0033] On the other hand, if the authentication result is "passed" (i.e., if the authentication returns that use of the elevator is permitted), then disabling of call registration by operation of the landing buttons is released by control from the elevator control board 1. In that case, call registration can be performed by operating the landing buttons, and a car that responds to the call registration is moved to the lobby floor (the floor on which the authenticating apparatus 2 is disposed). Here, processing of the image data 23 is not performed by the sampling portion 6, and output of the sampled image data 24 from the sampling portion 6 remains stopped.

[0034] Next, processing actions of the determining portion 7 will be explained. Figure 2 is a flowchart that shows actions of the determining portion 7 from Figure 1. In the figure, when the determining portion 7 receives sampled image data 24 from the sampling portion 6 (S1), the searching portion 8 searches whether or not image data that can be recognized as identical to the sampled image data 24 (identifying image data) are stored in the recording medium 5 as suspicious person image data (S2).

[0035] If the identifying image data are not present as suspicious person image data, the searching portion 8 records the sampled image data 24 in the recording medium 5 as suspicious person image data, and also records the date and time information 22 from the authenticating apparatus 2 in the recording medium 5 so as to be associated with the sampled image data 24 (S3). In that case, the determining portion 7 determines that the user is not a suspicious person (S4).

[0036] On the other hand, if the identifying image data are present as suspicious person image data, the search-

ing portion 8 adds the date and time information 22 from the authenticating apparatus 2 to past date and time information that has been stored in the recording medium 5 so as to be associated with the identifying image data (S5). In that case, the determining portion 7 determines that the user is a suspicious person (S6), and also outputs the sampled image data 24 to the alarm device 9 as warning image data 25 (S7). Processing by the determining portion 7 is performed in this manner.

[0037] In an elevator security system of this kind, because facial portion image data of a user are sampled as sampled image data 24 by the sampling portion 6 only if the authentication result is "flailed", and sampled image data 24 that have been sampled in the past are stored in the recording medium 5 as suspicious person image data, and whether a user is a suspicious person or not can be determined by searching whether or not identifying image data that can be recognized as identical to the sampled image data 24 from the sampling portion 6 are present as suspicious person image data, a user who has had an authentication result "failed" in the past can be designated a suspicious person, enabling determination as to whether or not an elevator user is a suspicious person to be performed easily. Thus, use of an elevator by suspicious persons can be prevented, enabling elevator security to be improved.

[0038] Because the alarm device 9 has a display portion 10 that displays an image that is obtained from the warning image data 25 (the sampled image data) as a warning, the warning that indicates that the person is suspicious can be presented visually, facilitating identification of the suspicious person to whom the warning refers.

[0039] Moreover, in the above example, the alarm device 9 is installed in the vicinity of the authenticating apparatus 2, but the alarm device 9 may also be installed in a control room of the building. The warning from the alarm device 9 can thereby be transmitted to a controller who is stationed inside the control room, enabling elevator security to be improved further.

Embodiment 2

[0040] Figure 3 is a block diagram that shows an elevator security system according to Embodiment 2 of the present invention. In the figure, a processor 4 has a recording medium 5, a sampling portion 6, and a determining portion 31. Configuration of the recording medium 5 and the sampling portion 6 is similar to that of the recording medium 5 and the sampling portion 6 according to Embodiment 1. The determining portion 31 has a searching portion 32 and a condition comparing portion 33.

[0041] In response to the determining portion 7 receiving sampled image data 24, the searching portion 32 searches whether or not identifying image data (i.e., image data that can be recognized as identical to the sampled image data 24) are present as suspicious person image data in the stored information in the recording medium 5. As a result of the search, if identifying image data are not present as suspicious person image data in the stored information, the searching portion 32 records the sampled image data 24 as suspicious person image data in the recording medium 5, and also records the date and time information 22 from the authenticating apparatus 2 in the recording medium 5 so as to be associated with the sampled image data 24. In addition, as a result of the search, if the identifying image data are present as suspicious person image data in the stored information, the searching portion 32 adds the date and time information 22 from the authenticating apparatus 2 to past date and time information that has been associated with the identifying image data, and outputs the sampled image data 24, the past date and time information that has been linked to the identifying image data, and the date and time information 22 from the authenticating apparatus 2 to the condition comparing portion 33 as suspicious person candidate information 26.

[0042] The condition comparing portion 33 determines whether or not the suspicious person candidate information 26 satisfies preset suspicious person qualifying conditions.

[0043] Specifically, the condition comparing portion 33 obtains the count of past date and time information that has been linked to the identifying image data in the suspicious person candidate information 26 (Count), and compares the obtained count of past date and time information (Count) and a set count value (a predetermined threshold value) (TH1) that has been preset. The condition comparing portion 33 also obtains the past date and time information that has been linked to the identifying image data in the suspicious person candidate information 26 (the newest past date and time information item if more than one past date and time information item exists) and the date and time information 22 from the authenticating apparatus 2, and compares a time difference between the obtained past date and time information and the date and time information 22 from the authenticating apparatus 2 (Time) and a set time value (a predetermined threshold value) (TH2) that has been preset. The set time value can be set to one minute, for example.

[0044] The condition comparing portion 33 determines that the user does not satisfy the suspicious person qualifying conditions only if a relationship between the past date and time information count (Count) and the set count value (TH1) satisfies Expression (1) and a relationship between the date and time information time difference (Time) and the set time value (TH2) satisfies Expression (3). The condition comparing portion 33 determines that the user satisfies the suspicious person qualifying conditions if a relationship between the past date and time information count (Count) and the set count value (TH1) satisfies Expression (2), or a relationship between the date and time information time difference (Time) and the set time value (TH2) satisfies Expression (4).

$$(\text{Count}) \leq (\text{TH1}) \quad \ldots \quad (1)$$

$$(\text{Count}) > (\text{TH1}) \quad \ldots \quad (2)$$

$$(\text{Time}) > (\text{TH2}) \quad \ldots \quad (3)$$

$$(\text{Time}) \leq (\text{TH2}) \quad \ldots \quad (4)$$

[0045] The determining portion 31 determines that the user is a suspicious person only if the condition comparing portion 33 has made a determination that the user satisfies the suspicious person qualifying conditions. The determining portion 31 also outputs the sampled image data 24 that is included in the suspicious person candidate information 26 to the alarm device 9 as warning image data 25 only if it has been determined that the user is a suspicious person. The rest of the configuration is similar to that of Embodiment 1.

[0046] Next, operation will be explained. Because operation according to the present embodiment is similar to operation according to Embodiment 1 except for processing actions of the determining portion 31, only the processing actions of the determining portion 31 will be explained.

[0047] Figure 4 is a flowchart that shows actions of the determining portion 31 from Figure 3. In the figure, when the determining portion 31 receives sampled image data 24 from the sampling portion 6 (S11), the searching portion 32 searches whether or not image data that can be recognized as identical to the sampled image data 24 (identifying image data) are stored in the recording medium 5 as suspicious person image data (S12).

[0048] If the identifying image data are not present as suspicious person image data, the searching portion 32 records the sampled image data 24 in the recording medium 5 as suspicious person image data, and also records the date and time information 22 from the authenticating apparatus 2 in the recording medium 5 so as to be associated with the sampled image data 24 (S13). In that case, the determining portion 31 determines that the user is not a suspicious person (S14).

[0049] On the other hand, if the identifying image data are present as suspicious person image data, the searching portion 32 adds the date and time information 22 from the authenticating apparatus 2 to past date and time information that has been stored in stored in the recording medium 5 so as to be associated with the identifying image data (S15). In that case, suspicious person candidate information 26 is sent from the searching portion 32 to the condition comparing portion 33.

[0050] Next, the condition comparing portion 33 determines whether or not the suspicious person candidate information 26 satisfies the suspicious person qualifying conditions (S16). If the suspicious person qualifying conditions are not satisfied, the determining portion 31 determines that the user is not a suspicious person (S14).

[0051] If the suspicious person qualifying conditions are satisfied, the determining portion 31 determines that the user is a suspicious person (S17), and also outputs the sampled image data 24 to the alarm device 9 as warning image data 25 (S18). Processing by the determining portion 31 is performed in this manner.

[0052] In an elevator security system of this kind, because the determining portion 31 determines whether or not a user is a suspicious person by comparing a count of past date and time information that has been associated with the identifying image data and a predetermined threshold value, it is possible to designate as a suspicious person only a user for whom the authentication result has been "failed" frequently. Consequently, legitimate users who have accidentally had an authentication result "failed" in the past can be excluded from being treated as suspicious persons, enabling erroneous determinations to be prevented.

[0053] Because the determining portion 31 determines whether or not a user is a suspicious person by comparing a time difference between past date and time information that has been associated with the identifying image data and date and time information 22 from the authenticating apparatus 2 with a predetermined threshold value, it can be determined that a user is a suspicious person when an authentication result is repeatedly "failed" a number of times in a short time, enabling accuracy in determining whether or not someone is a suspicious person to be improved.

[0054] Moreover, the configuration may also be such that elevator running information is transmitted to the display portion 10 from the elevator control board 1, and the display portion 10 displays the elevator running information during normal operation, and display images that are obtained from the suspicious person image data instead of the elevator running information or together with the elevator running information when warning image data 25 is input.

Claims

1. An elevator security system comprising:

an authenticating apparatus (2) that authenticates permission to use an elevator in response to a predetermined authorizing operation being performed;
a security camera (3) for photographing a user who performs the authorizing operation;
a processor (4) comprising:

a sampling portion (6) that samples facial portion image data (24) of the user from image data from the security camera (3) as

sampled image data (23) only if authentication by the authenticating apparatus results in a denial of permission;
a recording medium (5) in which stored information is stored that includes suspicious person image data consisting of sampled image data that have been sampled in the past for identifying a suspicious person; and
a determining portion (7) that determines whether or not the user is a suspicious person by searching whether or not identifying image data that can be recognized as identical to the sampled image data (24) are present in the stored information as the suspicious person image data, and that records the sampled image data (24) in the recording medium (5) as the suspicious person image data if presence of the identifying image data is negated; and

an alarm device (9) that issues a warning that indicates that the user is a suspicious person if a determination is made by the determining portion (7) that the user is a suspicious person.

2. An elevator security system according to Claim 1, **characterized in that**:

the authenticating apparatus (2) generates date and time information (22) that corresponds to a date and time that the authorizing operation was performed;
the determining portion (7) associates and records the date and time information (22) and the sampled image data (24) in the recording medium (5) if presence of the identifying image data is negated, and adds the date and time information (22) from the authenticating apparatus (2) to past date and time information (22) that has been associated with the identifying image data if the identifying image data are present in the stored information; and
the determination by the determining portion (7) as to whether or not the user is a suspicious person is made by comparing:

a count of the past date and time information (22) that has been associated with the identifying image data; and
a predetermined threshold value.

3. An elevator security system according to Claim 1, **characterized in that**:

the authenticating apparatus (2) generates date and time information (22) that corresponds to a date and time that the authorizing operation was performed;
the determining portion (7) associates and records the date and time information (22) and the sampled image data (24) in the recording medium (5) if presence of the identifying image data is negated, and adds the date and time information (22) from the authenticating apparatus (2) to past date and time information (22) that has been associated with the identifying image data if the identifying image data are present in the stored information; and
the determination by the determining portion (7) as to whether or not the user is a suspicious person is made by comparing:

a time difference between the date and time information (22) that has been associated with the identifying image data and the date and time information (22) from the authenticating apparatus (2); and
a predetermined threshold value.

4. An elevator security system according to any of Claims 1 through 3, **characterized in that** the alarm device (9) has a display portion (1 0) that displays an image that is obtained from the sampled image data (24) as the warning.

Patentansprüche

1. Aufzugssicherheitssystem, Folgendes umfassend:

eine Authentisierungsvorrichtung (2), die eine Erlaubnis zur Verwendung eines Aufzugs in Reaktion auf das Ausführen eines festgelegten Autorisierungsvorganges authentisiert,
eine Sicherheitskamera (3) zum Fotografieren eines Benutzers, der den Autorisierungsvorgang ausführt,
einen Prozessor (4), Folgendes umfassend:

einen Abtastabschnitt (6), der Gesichtsabschnitt-Bilddaten (24) des Benutzers aus Bilddaten der Sicherheitskamera (3) als abgetastete Bilddaten (23) abtastet, nur wenn die Authentifizierung durch die Authentifizierungsvorrichtung zu einer Verweigerung der Erlaubnis führt,
ein Aufzeichnungsmedium (5), in dem gespeicherte Informationen gespeichert sind, welche die Bilddaten verdächtiger Personen beinhalten, die aus abgetasteten Bilddaten bestehen, die in der Vergangenheit für die Identifizierung einer verdächtigen Person abgetastet wurden, und
einen Bestimmungsabschnitt (7), der be-

stimmt, ob der Benutzer eine verdächtige Person ist oder nicht, indem er fahndet, ob in den gespeicherten Informationen identifizierende Bilddaten, die als identisch mit den abgetasteten Bilddaten (24) erkannt werden können, als Bilddaten verdächtiger Personen vorhanden sind, und der die abgetasteten Bilddaten (24) als Bilddaten verdächtiger Personen im Aufzeichnungsmedium (5) aufzeichnet, wenn das Vorhandensein der identifizierenden Bilddaten verneint wird, und
eine Alarmeinrichtung (9), die eine Warnung ausgibt, die anzeigt, dass der Benutzer eine verdächtige Person ist, wenn vom Bestimmungsabschnitt (7) eine Bestimmung vorgenommen wird, dass der Benutzer eine verdächtige Person ist.

2. Aufzugssicherheitssystem nach Anspruch 1, **dadurch gekennzeichnet, dass**:

die Authentisierungsvorrichtung (2) Datums- und Zeitinformationen (22) erzeugt, die einem Datum und einem Zeitpunkt entsprechen, zu dem der Autorisierungsvorgang ausgeführt wurde,
der Bestimmungsabschnitt (7) die Datums- und Zeitinformationen (22) und die abgetasteten Bilddaten (24) zuordnet und im Aufzeichnungsmedium (5) aufzeichnet, wenn das Vorhandensein der identifizierenden Bilddaten verneint wird, und der die Datums- und Zeitinformationen (22) von der Authentisierungsvorrichtung (2) zu Datums- und Zeitinformationen (22) aus der Vergangenheit hinzufügt, die den identifizierenden Bilddaten zugeordnet wurden, wenn die identifizierenden Bilddaten in den gespeicherten Informationen vorhanden sind, und
die Bestimmung durch den Bestimmungsabschnitt (7), ob der Benutzer eine verdächtige Person ist oder nicht, ausgeführt wird durch Vergleichen:

einer Anzahl der Datums- und Zeitinformationen (22) aus der Vergangenheit, die den identifizierenden Bilddaten zugeordnet wurden, mit
einem festgelegten Grenzwert.

3. Aufzugssicherheitssystem nach Anspruch 1, **dadurch gekennzeichnet, dass**:

die Authentisierungsvorrichtung (2) Datums- und Zeitinformationen (22) erzeugt, die einem Datum und einem Zeitpunkt entsprechen, zu dem der Autorisierungsvorgang ausgeführt wurde,
der Bestimmungsabschnitt (7) die Datums- und Zeitinformationen (22) und die abgetasteten Bilddaten (24) zuordnet und im Aufzeichnungsmedium (5) aufzeichnet, wenn das Vorhandensein der identifizierenden Bilddaten verneint wird, und die Datums- und Zeitinformationen (22) von der Authentisierungsvorrichtung (2) zu Datums- und Zeitinformationen (22) aus der Vergangenheit hinzufügt, die den identifizierenden Bilddaten zugeordnet wurden, wenn die identifizierenden Bilddaten in den gespeicherten Informationen vorhanden sind, und
die Bestimmung durch den Bestimmungsabschnitt (7), ob der Benutzer eine verdächtige Person ist oder nicht, ausgeführt wird durch Vergleichen:

einer Zeitabweichung zwischen den Datums- und zeitinformationen (22), die den identifizierenden Bilddaten zugeordnet wurden, und den Datums- und Zeitinformationen (22) aus der Authentisierungsvorrichtung (2) mit
einem festgelegten Grenzwert.

4. Aufzugssicherheitssystem nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** die Alarmeinrichtung (9) einen Anzeigeabschnitt (10) aufweist, der als Warnung ein Bild anzeigt, das aus den abgetasteten Bilddaten (24) gewonnen wird.

Revendications

1. Système de sécurité pour ascenseur comprenant :

un appareil d'authentification (2) qui authentifie une permission d'utilisation d'un ascenseur en réponse à une opération d'autorisation prédéterminée étant effectuée ;
une caméra de sécurité (3) pour photographier un utilisateur qui effectue l'opération d'autorisation ;
un processeur (4) comprenant :

une partie d'échantillonnage (6) qui échantillonne des données d'image de partie faciale (24) de l'utilisateur à partir de données d'image provenant de la caméra de sécurité (3) en tant que données d'image échantillonnées (23) uniquement si l'authentification par l'appareil d'authentification conduit à un refus de permission ;
un support d'enregistrement (5) dans lequel sont stockées des informations stockées qui comportent des données d'image de personne suspecte constituées de données d'image échantillonnées qui ont été échan-

tillonnées dans le passé pour identifier une personne suspecte ;
et
une partie de détermination (7) qui détermine si l'utilisateur est une personne suspecte ou non en recherchant si des données d'image d'identification qui peuvent être reconnues comme étant identiques aux données d'image échantillonnées (24) sont présentes dans les informations stockées comme étant les données d'image de personne suspecte ou non, et qui enregistre les données d'image échantillonnées (24) dans le support d'enregistrement (5) comme étant les données d'image de personne suspecte si la présence des données d'image d'identification est niée ; et
un dispositif d'alarme (9) qui émet un avertissement qui indique que l'utilisateur est une personne suspecte si la partie de détermination (7) détermine que l'utilisateur est une personne suspecte.

2. Système de sécurité pour ascenseur selon la revendication 1, **caractérisé en ce que** :

l'appareil d'authentification (2) génère des informations de date et d'heure (22) qui correspondent à une date et à une heure auxquelles l'opération d'autorisation a été effectuée ;
la partie de détermination (7) associe et enregistre les informations de date et d'heure (22) et les données d'image échantillonnées (24) dans le support d'enregistrement (5) si la présence des données d'image d'identification est niée, et ajoute les informations de date et d'heure (22) provenant de l'appareil d'authentification (2) à des informations de date et d'heure passées (22) qui ont été associées aux données d'image d'identification si les données d'image d'identification sont présentes dans les informations stockées ; et
la détermination par la partie de détermination (7) selon laquelle l'utilisateur est une personne suspecte ou non est faite en comparant :

un comptage des informations de date et d'heure passées (22) qui ont été associées aux données d'image d'identification ; et
une valeur seuil prédéterminée.

3. Système de sécurité pour ascenseur selon la revendication 1, **caractérisé en ce que** :

l'appareil d'authentification (2) génère des informations de date et d'heure (22) qui correspondent à une date et une heure auxquelles l'opération d'autorisation a été effectuée ;
la partie de détermination (7) associe et enregistre les informations de date et d'heure (22) et les données d'image échantillonnées (24) dans le support d'enregistrement (5) si la présence des données d'image d'identification est niée, et ajoute les informations de date et d'heure (22) provenant de l'appareil d'authentification (2) à des informations de date et d'heure passées (22) qui ont été associées aux données d'image d'identification si les données d'image d'identification sont présentes dans les informations stockées ; et
la détermination par la partie de détermination (7) selon laquelle l'utilisateur est une personne suspecte ou non est faite en comparant :

une différence temporelle entre les informations de date et d'heure (22) qui ont été associées aux données d'image d'identification et les informations de date et d'heure (22) provenant de l'appareil d'authentification (2) ; et
une valeur seuil prédéterminée.

4. Système de sécurité pour ascenseur selon l'une des revendications 1 à 3, **caractérisé en ce que** le dispositif d'alarme (9) a une partie d'affichage (10) qui affiche une image qui est obtenue à partir des données d'image échantillonnées (24) en tant qu'avertissement.

FIG. 1

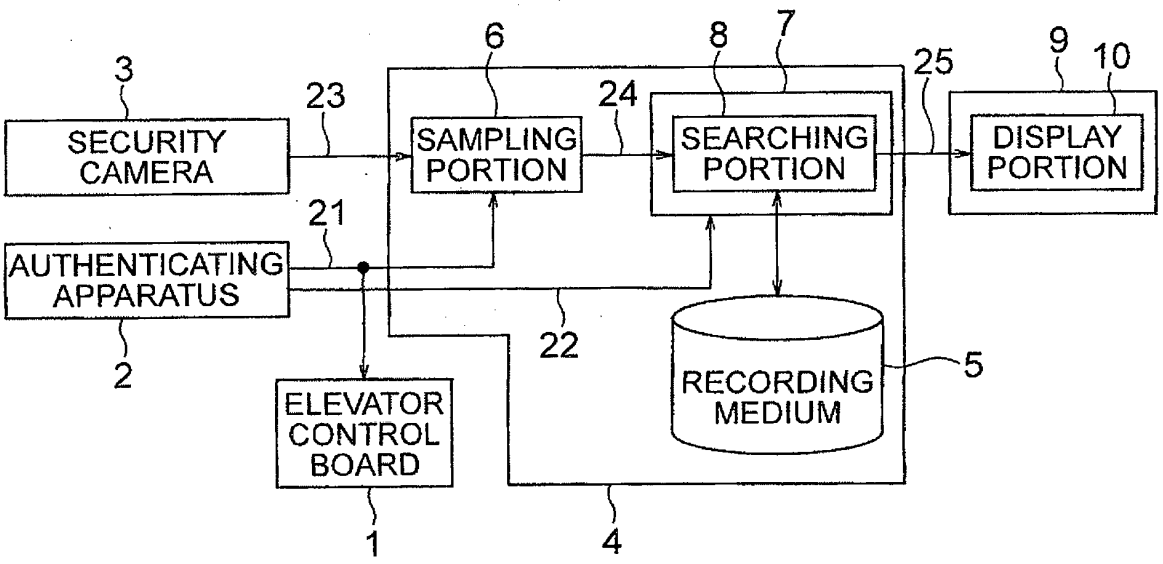

3
SECURITY CAMERA
23
6
SAMPLING PORTION
24
8
7
SEARCHING PORTION
25
9
10
DISPLAY PORTION
21
AUTHENTICATING APPARATUS
2
22
RECORDING MEDIUM
5
ELEVATOR CONTROL BOARD
1
4

FIG. 2

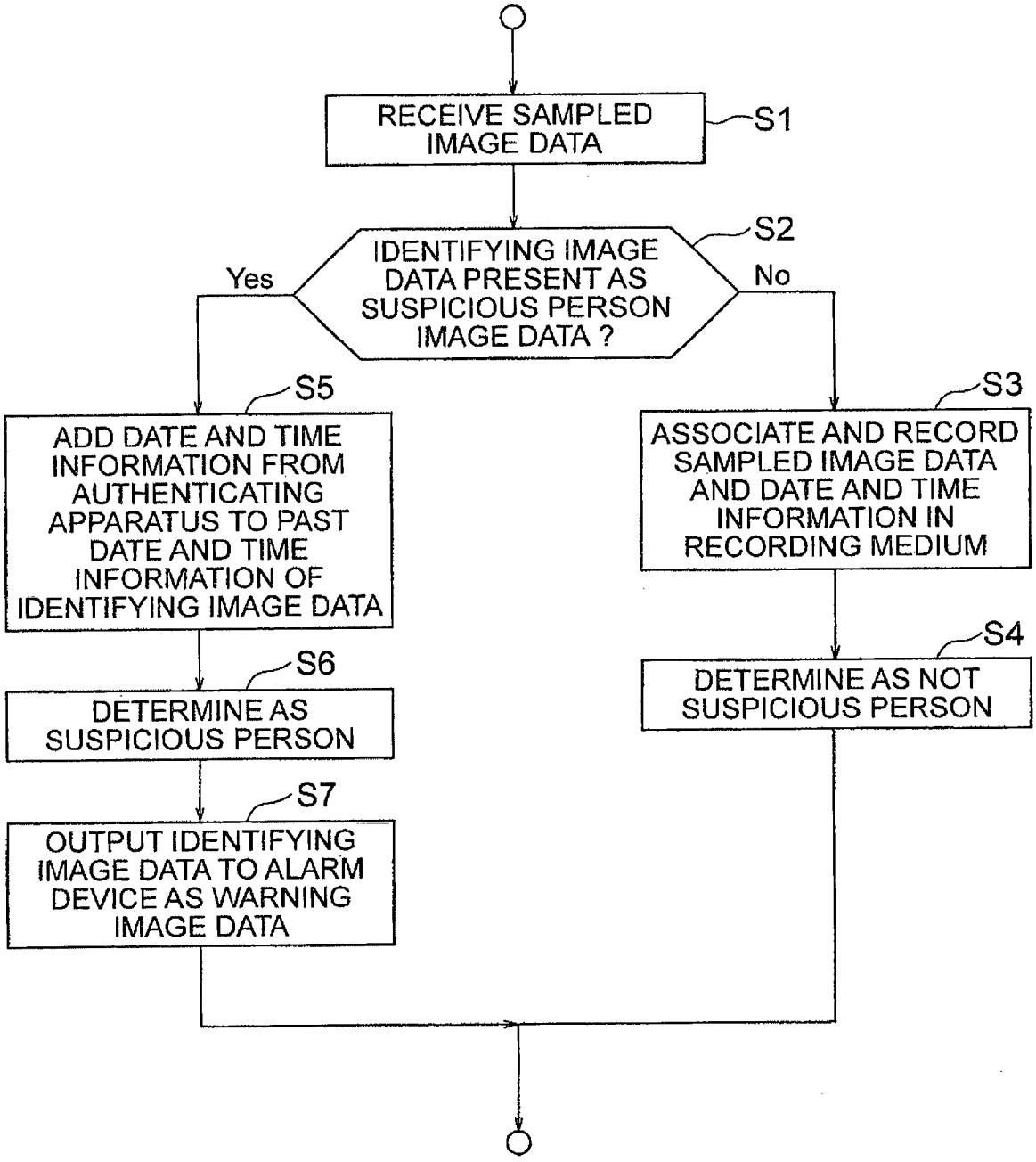

RECEIVE SAMPLED IMAGE DATA
S1
IDENTIFYING IMAGE DATA PRESENT AS SUSPICIOUS PERSON IMAGE DATA ?
S2
Yes
No
S5
ADD DATE AND TIME INFORMATION FROM AUTHENTICATING APPARATUS TO PAST DATE AND TIME INFORMATION OF IDENTIFYING IMAGE DATA
S3
ASSOCIATE AND RECORD SAMPLED IMAGE DATA AND DATE AND TIME INFORMATION IN RECORDING MEDIUM
S6
DETERMINE AS SUSPICIOUS PERSON
S4
DETERMINE AS NOT SUSPICIOUS PERSON
S7
OUTPUT IDENTIFYING IMAGE DATA TO ALARM DEVICE AS WARNING IMAGE DATA

FIG. 3

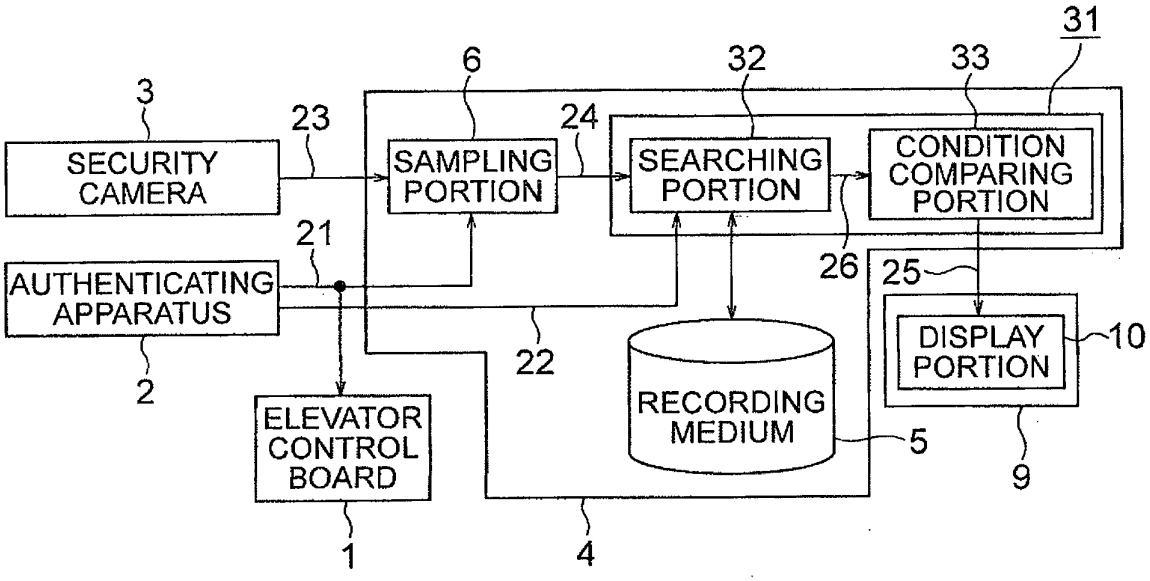
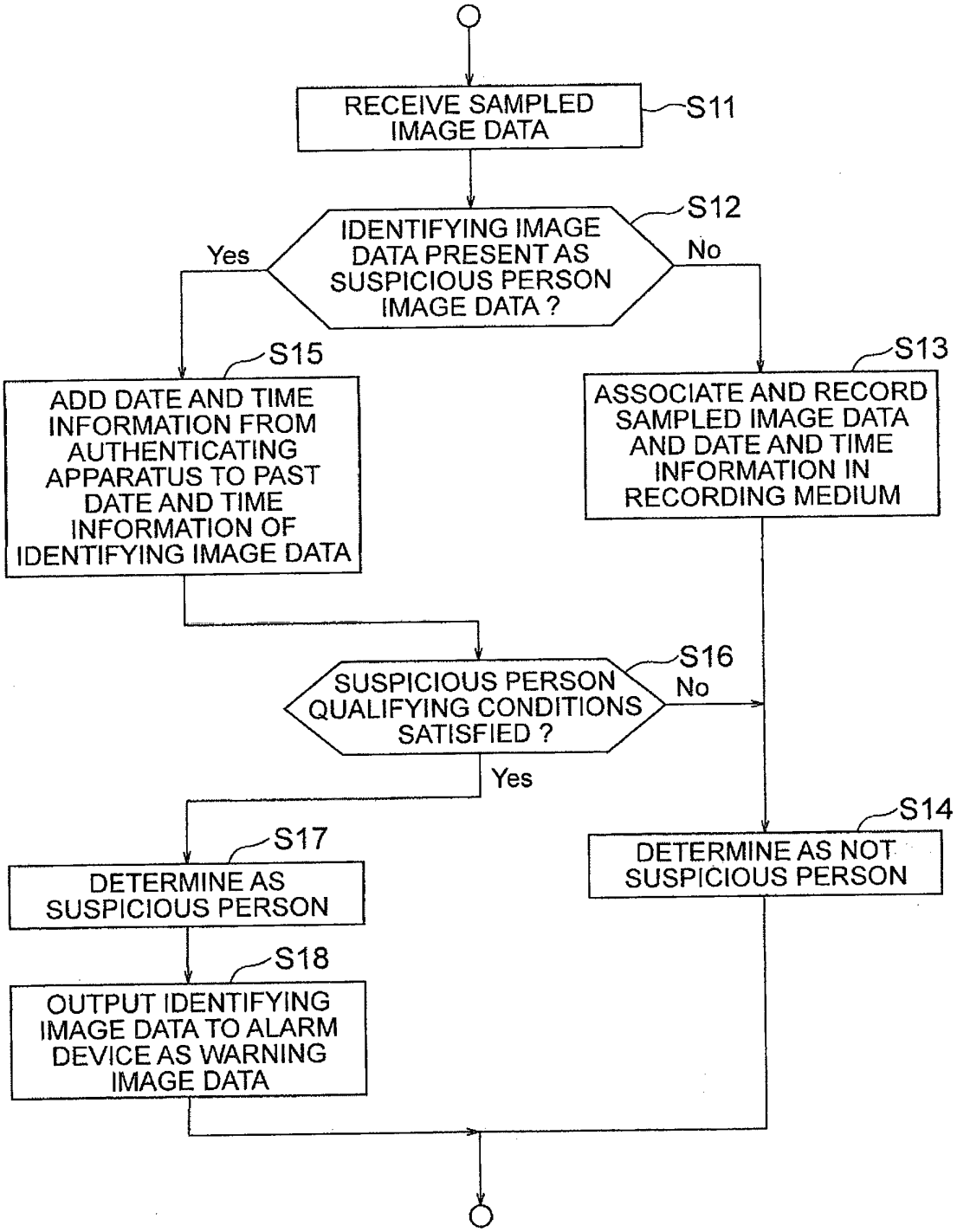

31
6
32
33
3
23
24
SECURITY CAMERA
SAMPLING PORTION
SEARCHING PORTION
CONDITION COMPARING PORTION
21
AUTHENTICATING APPARATUS
26
25
DISPLAY PORTION
10
22
RECORDING MEDIUM
5
2
ELEVATOR CONTROL BOARD
9
1
4

FIG. 4


RECEIVE SAMPLED IMAGE DATA
S11
IDENTIFYING IMAGE DATA PRESENT AS SUSPICIOUS PERSON IMAGE DATA ?
S12
Yes
No
S15
ADD DATE AND TIME INFORMATION FROM AUTHENTICATING APPARATUS TO PAST DATE AND TIME INFORMATION OF IDENTIFYING IMAGE DATA
S13
ASSOCIATE AND RECORD SAMPLED IMAGE DATA AND DATE AND TIME INFORMATION IN RECORDING MEDIUM
SUSPICIOUS PERSON QUALIFYING CONDITIONS SATISFIED ?
S16
No
Yes
S17
DETERMINE AS SUSPICIOUS PERSON
S14
DETERMINE AS NOT SUSPICIOUS PERSON
S18
OUTPUT IDENTIFYING IMAGE DATA TO ALARM DEVICE AS WARNING IMAGE DATA

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- JP 2006103854 A **[0002] [0006]**
- JP 2007022776 A **[0003]**
- JP 2003109129 A **[0004]**
- JP 2006109014 A **[0005]**