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

(11) EP 3 852 076 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.07.2021 Bulletin 2021/29

(51) Int Cl.:
G08B 25/00 *(2006.01)*

(21) Application number: **20151921.2**

(22) Date of filing: **15.01.2020**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
KH MA MD TN

(71) Applicant: **Climax Technology Co., Ltd.**
Taipei 114 (TW)

(72) Inventors:
- **CHEN, Yi-Kai**
  10850 Taipei City (TW)
- **Liu, Tang Hui**
  11469 Taipei City (TW)

(74) Representative: **Karakatsanis, Georgios**
Haft Karakatsanis Patentanwaltskanzlei
Dietlindenstrasse 18
80802 München (DE)

(54) SMART HOME SECURITY SYSTEM AND METHOD OF DISARMING A SECURITY SETTING

(57) A method of disarming a smart home security setting includes displaying a prompt page for instructing a user to proceed with facial image capture; capturing at least one face image of the user; allowing the user to enter a password only when an area ratio of captured face on the face image to a whole face is greater than a predetermined first threshold and an image quality of the face image is greater than a predetermined second threshold; and issuing a warning notification if identification according to the password fails.

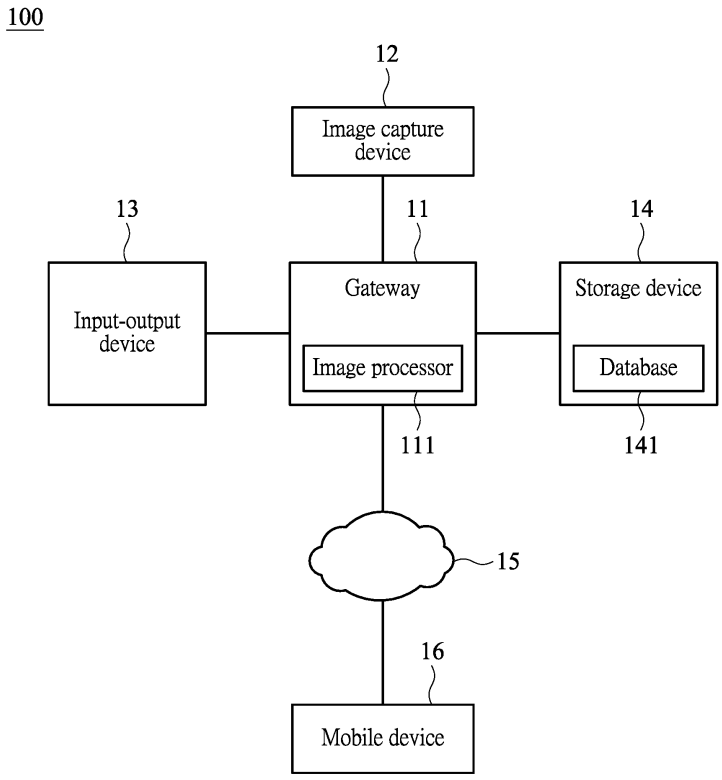

FIG. 1

EP 3 852 076 A1

Description

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

[0001] The present invention generally relates to a security system, and more particularly to a method of disarming a security setting.

2. DESCRIPTION OF RELATED ART

[0002] A smart home network is a computer network that connects electronic devices in a house via wired or wireless communication to interact with each other or create more functions. The smart home network, for example, may construct a smart home security system, the security setting of which may be armed via a gateway when the user leaves home, and may be disarmed when the user returns home. During the period between arm and disarm, the user may be notified by message, email or phone when any security device is triggered.

[0003] In a conventional security system, a user may disarm the security setting by entering a password, which however is liable to theft or break. Moreover, there is no way of being aware of the intruder when the security setting is unlawfully disarmed.

[0004] A need has thus arisen to propose a novel security scheme to overcome the drawbacks of the conventional security system.

SUMMARY OF THE INVENTION

[0005] In view of the foregoing, it is an object of the embodiment of the present invention to provide a method of disarming a smart home security setting according to facial detection in addition to password identification, thereby enhancing security and recognizing intruder's appearance.

[0006] According to a method of disarming a smart home security setting in one embodiment, a prompt page for instructing a user to proceed with facial image capture is displayed, and at least one face image of the user is captured. The user is allowed to enter a password only when an area ratio of captured face on the face image to a whole face is greater than a predetermined first threshold and an image quality of the face image is greater than a predetermined second threshold. A warning notification is issued if identification according to the password fails.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007]

FIG. 1 shows a block diagram illustrating a smart home security system according to one embodiment of the present invention;

FIG. 2 shows a flow diagram illustrating a method of disarming a smart home security setting according to one embodiment of the present invention;

FIG. 3A shows an exemplary prompt page of the input-output device; and

FIG. 3B shows an exemplary unlock page of the input-output device.

DETAILED DESCRIPTION OF THE INVENTION

[0008] FIG. 1 shows a block diagram illustrating a smart home security system 100 according to one embodiment of the present invention. The smart home security system (security system hereinafter) 100 of the embodiment may include a gateway 11, an image capture device 12, an input-output device 13 and a storage device 14. In the embodiment, the gateway 11 is used as a server in a smart home network to control the image capture device 12, the input-output device 13 and the storage device 14. Further, the gateway 11 may include an image processor 111 configured to perform image processing. In one embodiment, the image capture device 12 may include a camera; the input-output device 13 may include a touch screen; and the storage device 14 may include a memory device configured to store a database 141 and temporary data. The image capture device 12 may, for example, be disposed in the input-output device 13.

[0009] FIG. 2 shows a flow diagram illustrating a method 200 of disarming a smart home security setting according to one embodiment of the present invention, adaptable to a smart home network such as the security system 100 as shown in FIG. 1. In step 21, the gateway 11 may determine whether a disarm request is received. In one embodiment, a user may activate the input-output device 13 (e.g., touch the touch screen of the input-output device 13) when disarming the security setting. When the input-output device 13 receives the disarm request, a signal may be sent to notify the gateway 11. Accordingly, the gateway 11 may control the input-output device 13 to display a prompt page (step 22) for instructing the user to proceed with facial image capture by facing the image capture device 12 (or the input-output device 13). FIG. 3A shows an exemplary prompt page 31 of the input-output device 13. Specifically, in the embodiment, the prompt page 31 may include a current image area 311 that displays a current image captured by the image capture device 12. The prompt page 31 may also include a password entering area 312 through which the user may enter a predetermined password for identification.

[0010] In step 23, the gateway 11 may control the image capture device 12 to capture at least one face image of the user. If no image that substantially includes whole face and is clear has been captured, the image capture device 12 may continuously perform image capture until a predetermined first period (e.g., 30 seconds) lapses. In the specification, the term "whole" face means that a substantial portion (e.g., 90%) of face lies inside the image captured by the image capture device 12, or alter-

native speaking, an area ratio of captured face on the face image to a whole face is greater than a predetermined (first) threshold; and the term "clear" image refers to a captured image that can be sufficiently processed by the image processor 111, or alternatively speaking, an image quality of the face image is greater than a predetermined (second) threshold. According to one aspect of the embodiment, before an image that substantially includes whole face and is clear has been captured, the password entering area 312 of the input-output device 13 may be locked by the gateway 11 to prevent the user from entering a password.

[0011] In step 24, it determines whether the captured face image substantially includes whole face and is clear, that is, it determines whether facial detection succeeds. If the determination of step 24 is negative and a predetermined first period (e.g., 30 seconds) lapses, the gateway 11 may lock the (entire prompt) page on the touch screen of the input-output device 13 (step 25) to render it inactive. After a predetermined second period (e.g., 3 minutes) lapses, the flow goes back to step 21. If the determination of step 24 is positive, the gateway 11 may release the password entering area 312 of the input-output device 13 (step 26) to allow the user to enter a password through the password entering area 312, and the captured face image substantially including whole face and being clear may be stored in the storage device 14. Accordingly, the touch screen of the input-output device 13 may display an unlock page 32. FIG. 3B shows an exemplary unlock page 32 of the input-output device 13, on which the current image area 311 is replaced with an unlock notification 313.

[0012] In step 27, the gateway 11 may determine whether identification of the password entered by the user is correct, for example, by comparing it with a password stored beforehand in the storage device 14. If the password identification in step 27 fails (indicating that the current user has no qualification to disarm the security setting), the gateway 11 may issue a warning notification to a mobile device 16 of an associated person (e.g., administrator of the smart home network) via the network 15 such as Internet (step 29). At the same time, the captured face image of the user may be sent or stored in the storage device 14.

[0013] If the password identification in step 27 succeeds, indicating that the current user passes the facial detection and password identification, the gateway 11 may disarm the security setting (step 28) of the smart home network. In one embodiment, the gateway 11 may store the captured face image of the user in the storage device 14 or send the captured face image to the associated person after disarming the security setting.

[0014] In one embodiment, in step 30, the image processor 111 of the gateway 11 may further perform facial recognition according to the captured face image and a database 141 stored beforehand in the storage device 14. Specifically, the database 141 may store beforehand facial image data (e.g., facial image features) of at least one admissible user. The image processor 111 of the embodiment may perform facial recognition by using conventional facial recognition techniques, details of which are omitted for brevity.

[0015] If the facial recognition in step 30 fails (indicating that the current user has no qualification to disarm the security setting), in step 29, the gateway 11 may issue a warning notification to the mobile device 16 of the associated person (e.g., administrator of the smart home network) via the network 15 (e.g., Internet). At the same time, the captured face image of the user may be sent or stored in the storage device 14.

Claims

1. A method of disarming a smart home security setting, comprising:

   displaying a prompt page for instructing a user to proceed with facial image capture;
   capturing at least one face image of the user;
   allowing the user to enter a password only when an area ratio of captured face on the face image to a whole face is greater than a predetermined first threshold and an image quality of the face image is greater than a predetermined second threshold; and
   issuing a warning notification if identification according to the password fails.

2. The method of claim 1, further comprising:

   sending or storing the face image when issuing the warning notification.

3. The method of claim 1, wherein the prompt page comprises:

   a current image area that display a current image of the user; and
   a password entering area through which the user enters the password.

4. The method of claim 3, wherein the password entering area is locked until the area ratio is greater than the first threshold and the image quality is greater than the second threshold.

5. The method of claim 1, further comprising:
   locking the prompt page when the area ratio is not greater than the first threshold or the image quality is not greater than the second threshold, and a predetermined period lapses.

6. The method of claim 1, wherein the smart home security setting is disarmed when the identification succeeds.

7. The method of claim 6, further comprising:
sending or storing the face image when disarming the smart home security setting.

8. The method of claim 6, further comprising:
performing facial recognition on the face image after disarming the smart home security setting.

9. A smart home security system, comprising:

a gateway;
an input-output device that displays a prompt page for instructing a user to proceed with facial image capture; and
an image capture device that captures at least one face image of the user;
wherein the user is allowed to enter a password only when an area ratio of captured face on the face image to a whole face is greater than a predetermined first threshold and an image quality of the face image is greater than a predetermined second threshold; and a warning notification is issued if identification according to the password fails.

10. The system of claim 9, further comprising:

a storage device that stores the face image;
wherein the gateway sends or stores the face image when issuing the warning notification.

11. The system of claim 9, wherein the prompt page comprises:

a current image area that display a current image of the user; and
a password entering area through which the user enters the password.

12. The system of claim 11, wherein the password entering area is locked until the area ratio is greater than the first threshold and the image quality is greater than the second threshold.

13. The system of claim 9, wherein a smart home security setting is disarmed by the gateway when the identification succeed.

14. The system of claim 13, wherein the face image is sent or stored when disarming the security setting.

15. The system of claim 13, wherein the gateway performs facial recognition on the face image after disarming the smart home security setting.

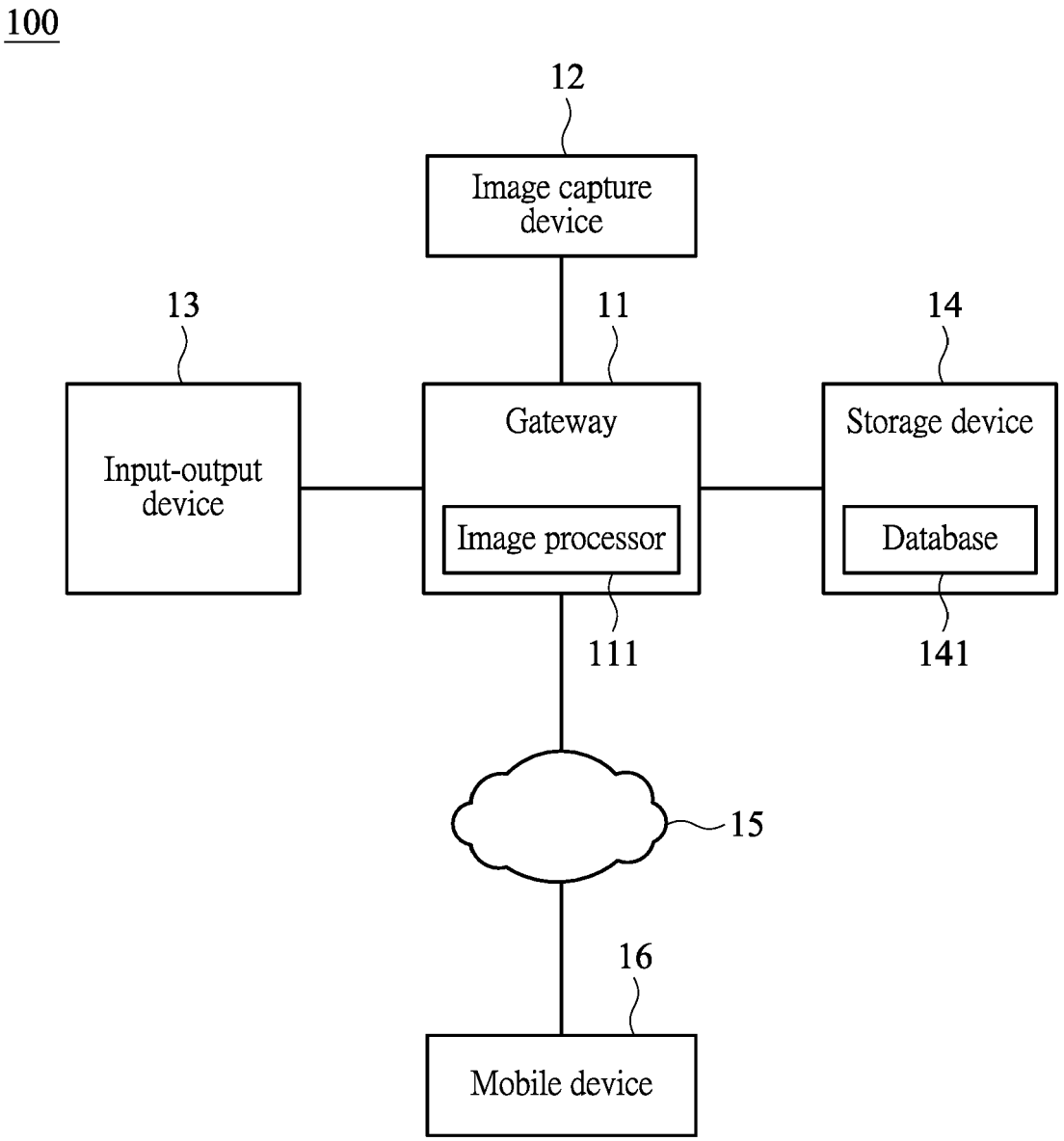
100
12
Image capture device
13
11
14
Input-output device
Gateway
Image processor
Storage device
Database
111
141
15
16
Mobile device

FIG. 1

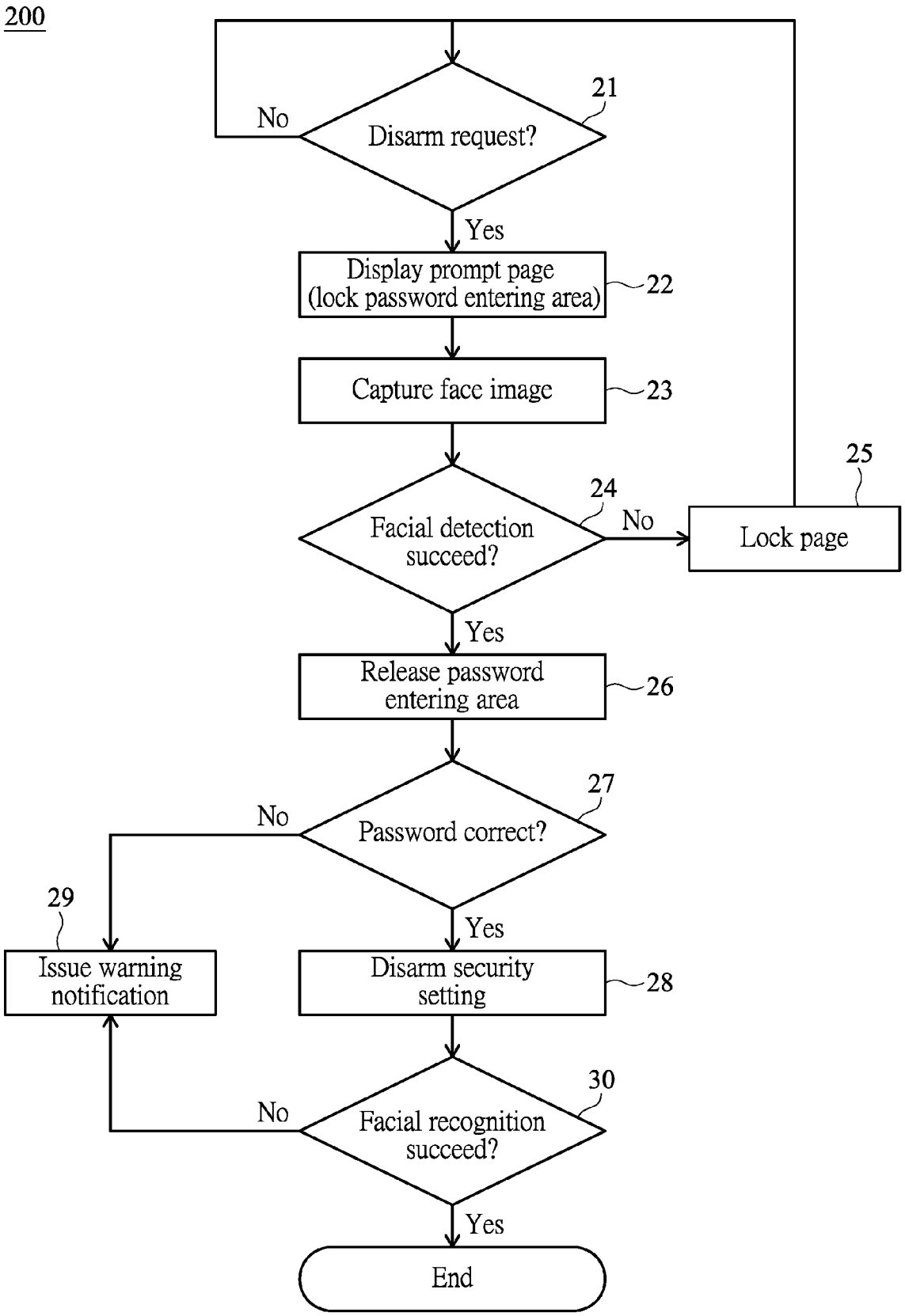
200
Disarm request?
21
No
Yes
Display prompt page (lock password entering area)
22
Capture face image
23
Facial detection succeed?
24
No
Lock page
25
Yes
Release password entering area
26
Password correct?
27
No
Yes
Issue warning notification
29
Disarm security setting
28
Facial recognition succeed?
30
No
Yes
End

FIG. 2

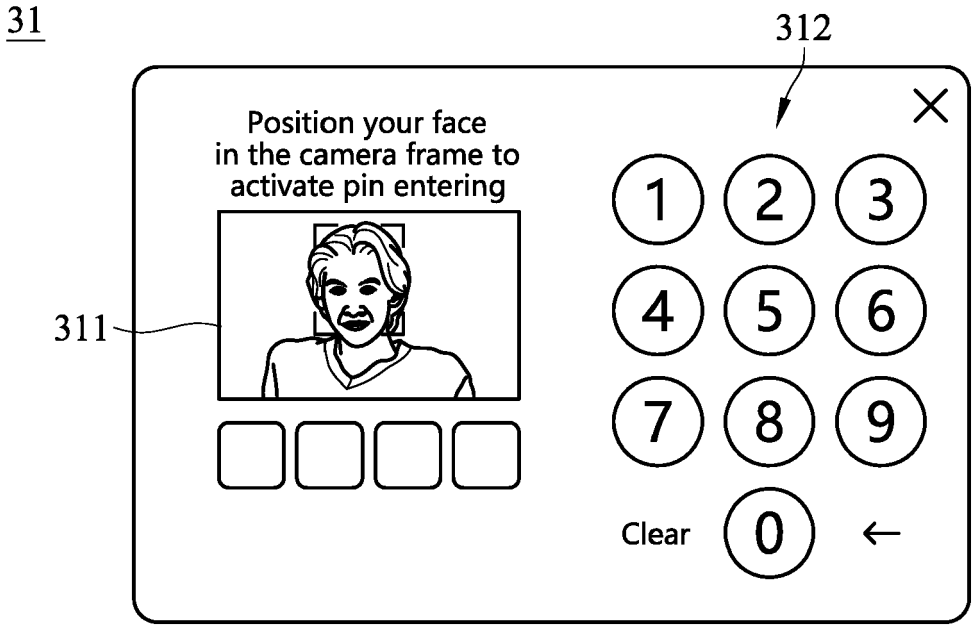
31
312
Position your face
in the camera frame to
activate pin entering
311
1
2
3
4
5
6
7
8
9
Clear
0

FIG. 3A

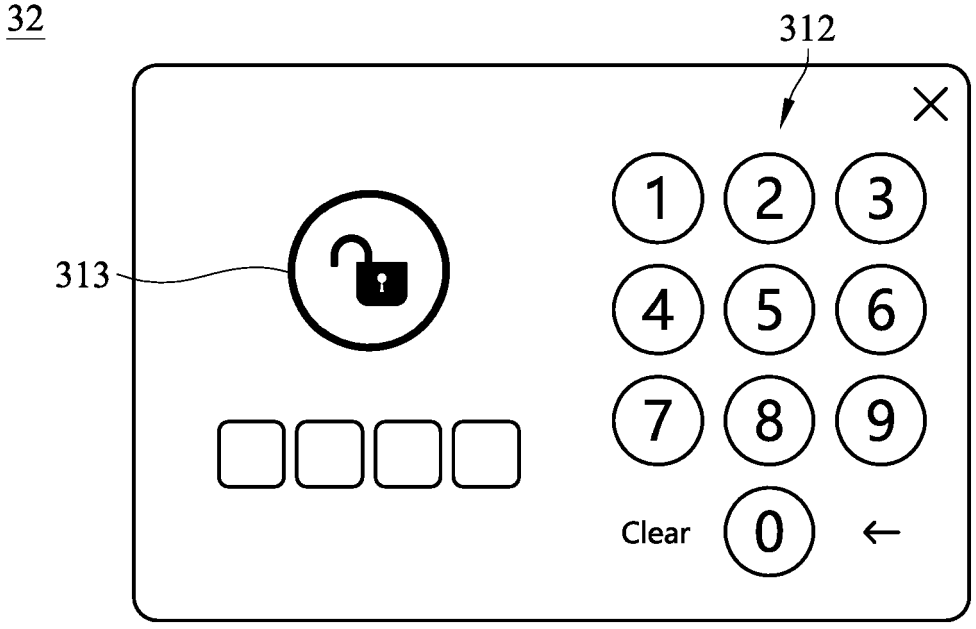
32
312
313
1
2
3
4
5
6
7
8
9
Clear
0

FIG. 3B

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 20 15 1921

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	EP 3 048 594 A2 (HONEYWELL INT INC [US]) 27 July 2016 (2016-07-27) * paragraph [0010] * * paragraph [0021] * * paragraphs [0026] - [0029] * * paragraphs [0031], [0032] * * paragraph [0034] * * figures 1-3 *	1-15	INV. G08B25/00
A	CN 109 145 801 A (ZHEJIANG UNIVIEW TECH CO LTD) 4 January 2019 (2019-01-04) * figure 1 *	1-15	
L	WO 2020/034645 A1 (ZHEJIANG UNIVIEW TECH CO LTD [CN]) 20 February 2020 (2020-02-20) * paragraph [0024] * * paragraph [0072] * * paragraph [0074] * * figure 1 *	1-15	

TECHNICAL FIELDS SEARCHED (IPC)

G08B
G07C

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	2 July 2020	Meister, Mark

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 20 15 1921

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

02-07-2020

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 3048594 A2	27-07-2016	CA 2918075 A1	26-07-2016
		CN 105828025 A	03-08-2016
		EP 3048594 A2	27-07-2016
		ES 2661301 T3	28-03-2018
		US 2016217677 A1	28-07-2016
CN 109145801 A	04-01-2019	CN 109145801 A	04-01-2019
		WO 2020034645 A1	20-02-2020
WO 2020034645 A1	20-02-2020	CN 109145801 A	04-01-2019
		WO 2020034645 A1	20-02-2020