(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 December 2010 (29.12.2010)

PCT

(10) International Publication Number
WO 2010/151246 A1

(51) International Patent Classification:
A61B 5/00 (2006.01) *G06F 19/00* (2006.01)
G06F 21/00 (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/US2009/048166

(22) International Filing Date:
22 June 2009 (22.06.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **ANALOGIC CORPORATION** [US/US]; 8 Centennial Drive, Peabody, MA 01960 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TVERSKOY, Mark** [US/US]; 12 Whispering Pines Drive, Andover, MA 01810 (US). **DICIACCIO, Anthony, Ralph** [US/US]; 5 Manomet Road, Peabody, MA 01960 (US).

(74) Agent: **DEL ZOPPO, Anthony, M. III**; Driggs, Hogg, Daugherty And Del Zoppo Co., LPA, 38500 Chardon Road, Willoughby Hills, OH 44094 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: TWO-WAY AUTHENTICATION

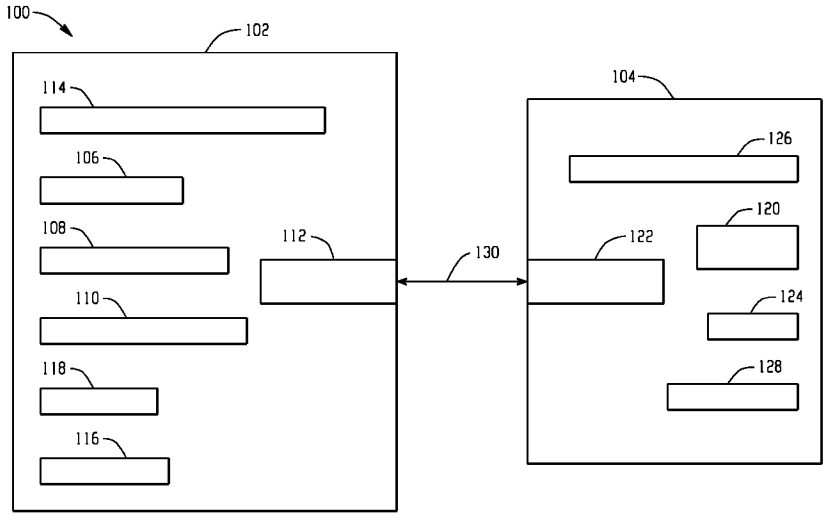

Fig. 1

(57) **Abstract**: A method for activating a physiologic sensor (124) of a peripheral device (104) of a monitoring apparatus (100) includes receiving, at the peripheral device (104), a signal indicating a host device (102) authenticated the peripheral device (104), receiving, at the peripheral device (104), a host device authentication response signal, authenticating, at the peripheral device (104), the host device (102) based on the host device authentication response signal, and activating the physiologic sensor (124) of the peripheral device (104) in response to authentication of both the host and peripheral devices (102, 104).

WO 2010/151246 A1

TWO-WAY AUTHENTICATION

TECHNICAL FIELD

The following generally relates to two-way authentication and is described with particular application to physiologic parameter monitoring. However, it is also amenable to other medical and non-medical applications.

BACKGROUND

Physiological parameter monitors have included a combination of a host monitoring device (host device) and a single or multiple peripheral sensing devices (peripheral device) which are connected to the host device. The peripheral device(s) usually includes a connector that attaches to the complimentary connector on the host device side. Once the peripheral device connector is coupled to the host device, the peripheral device function is activated by the host monitoring device. Unfortunately, with such a connection configuration, the host monitor may not be able to tell whether a proper peripheral device is attached. As a consequence, an improper peripheral device can be plugged into the host monitoring device (assuming the physical shapes of the respective connectors allow for such mating) and the host monitor may be programmed by the user as if the intended peripheral device was connected. Likewise, the peripheral device may not be able to distinguish whether the host monitor attached to it is intended for proper coupling. As a consequence, the peripheral sensing device can be connected with the incorrect host monitoring device and the incorrect host device may be programmed by the user as if the proper peripheral device was connected thereto.

SUMMARY

Aspects of the application address the above matters, and others.

In one aspect, a method for activating a physiologic sensor of a peripheral device of a monitoring apparatus is discussed. The method includes receiving, at the peripheral device, a signal indicating a host device authenticated the peripheral device. The method further includes receiving, at the peripheral device, a host device authentication response signal. The

method further includes authenticating, at the peripheral device, the host device based on the host device authentication response signal. The method further includes activating the physiologic sensor of the peripheral device in response to authentication of both the host and peripheral devices.

In another aspect, a physiologic parameter monitoring apparatus includes a host device with a peripheral device authenticator and a peripheral device with a host device authenticator and a sensor that senses a physiologic state of a patient. The peripheral device authenticator authenticates the peripheral device and the host device authenticator authenticates the host device, and the sensor is activated in response to two-way authentication of the host and peripheral devices.

In another aspect, a method includes activating a physiologic sensor of a peripheral device based on two-way authentication between the peripheral device and the host device.

In another aspect, a method for activating a physiologic sensor of a peripheral device of a monitoring apparatus is discussed. The method includes receiving, at a host device, a signal indicating the peripheral device authenticated the host device. The method further includes receiving, at the host device, a peripheral device authentication response signal. The method further includes authenticating, at the host device, the peripheral device based on the peripheral device authentication response signal. The method further includes activating the physiologic sensor of the peripheral device in response to authentication of both the host and peripheral devices.

BRIEF DESCRIPTION OF THE DRAWINGS

The application is illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like references indicate similar elements and in which:

FIGURE 1 illustrates an example physiologic parameter monitoring system;

FIGURE 2 illustrates an example host authenticator;

FIGURE 3 illustrates an example peripheral authenticator;

FIGURE 4 illustrates an example method.

DETAILED DESCRIPTION

FIGURE 1 illustrates an apparatus 100 that includes a host device 102 and at least one peripheral device 104. An example of such an apparatus includes a patient temperature monitoring apparatus with a temperature-sensing probe (peripheral device) that removably attaches via a cable or the like to a monitor unit (host device) that displays the sensed temperature. Other suitable apparatuses include, but are not limited to, blood pressure, heart rate and/or other physiologic parameter monitors, and/or non-physiologic parameter monitors.

The host device 102 includes a microprocessor or host controller 106 that controls overall operation of the host device 102. The host controller 106 also transmits and/or receives signals to and from the peripheral device 104. A processing component 108 processes data such as sensed data obtained from the peripheral device 104 and/or input by a user. A presentation component 110 presents processed data, messages, warning, alarms, and/or other information in a human readable format.

A communications interface 112, with input and output ports, is configured for communicating signals with the peripheral device 104. A user interface 116 accepts input provided by a user to the host device 102. A power supply 118 provides power for powering the host and/or peripheral devices 102 and 104. The power supply 118 provides power from a power source such as a battery, wall outlet alternating current, and/or other power source. The host device 102 also includes a peripheral device authenticator 114. As described in greater detail below, the peripheral device authenticator 114 facilitates host device authentication of the peripheral device 104.

The peripheral device 104 includes a microprocessor or peripheral controller 120 that controls overall operation of the peripheral device 104. The peripheral controller 120 transmits and/or receives signals to and from the host device 102. At least one physiologic sensor 124 senses a signal indicative of a physiologic state (e.g., temperature, blood pressure, heart rate, etc.) of a patient. The illustrated physiologic sensor 124 is configured to be in an inactive initial state when the peripheral device 104 is powered up. As described in greater detail below, the illustrated sensor 124 transitions to an active state based on two-way authentication between the host and peripheral devices 102 and 104.

A communications interface 122, with input and output ports, is configured for communicating signals. A user interface 128 accepts input provided by a host device to the peripheral device 104. The illustrated peripheral device 104 is powered with power supplied by the host device 102 through the communications interface 122. The peripheral device 104 further includes a host device authenticator 126. As described in greater detail below, the host device authenticator 126 facilitates peripheral device authentication of the host device 102.

The host and peripheral devices 102 and 104 communicate with each other through their respective communications interfaces 112 and 122 over a suitable communications link 130, which may be a cable or the like, or a wireless communications medium. In the illustrated embodiment, the host and peripheral devices 102 and 104 are configured to authenticate each other (two-way authentication), and at least one sensor 124 is selectively activated based on two-way authentication. In one instance, this allows for determining whether the host and peripheral devices 102 and 104 are permitted to operate with each other before allowing the sensor 124 to be activated.

FIGURES 2 and 3 respectively illustrate examples of the authenticators 114 and 126.

Initially referring to FIGURES 1 and 2, the peripheral device authenticator 114 of the host device 102 includes a storage component 202 with at least one key 204 and a random signal generator 206 that generates random signals. The key(s) stored in the storage component 202 correspond to one or more peripheral devices 104 pre-validated for use with the host device 102.

An authentication signal generator 208 generates authentication signals, including an authentication request signal based on a random signal from the random signal generator 206, an authentication compare signal based on the random signal and the key 204, and an authentication response signal based on a random signal from the peripheral device 104.

The peripheral device authenticator 114 also includes a comparator 210 that compares the authentication compare signal with an authentication response signal generated by the peripheral device 104, and generates a signal indicative of the comparison.

Turning to FIGURES 1 and 3, the host device authenticator 126 of the peripheral device 104 includes a storage component 302 with at least one key 304 (which, in the illustrated embodiment, is indicative of a same value as the key 204) and a random signal

generator 306. The key(s) stored in the storage component 302 correspond to one or more host devices 102 pre-validated for use with the peripheral device 104.

An authentication signal generator 308 generates authentication signals, including an authentication request signal based on a random signal from the random signal generator 306, an authentication compare signal based on the random signal and the key 304, and an authentication response signal based on a random signal from the host device 102.

The host device authenticator 126 also includes a comparator 310 that compares the authentication compare signal with an authentication response signal generated by the host device 102, and generates a signal indicative of the comparison.

With respect to FIGURES 1, 2 and 3, the host device 102 authenticates the peripheral device 104, and vice versa. For host device authentication of the peripheral device 104, the authentication signal generator 208 of the host device 102 generates an authentication request signal and an authentication compare signal. The authentication request signal is transmitted to the peripheral device 104. The peripheral device 104, in response to receiving the authentication request signal, generates an authentication response signal. In the illustrated embodiment, the peripheral device 104 generates the authentication response signal based on a secure algorithm such as a secure cryptographic, hash or other secure algorithm. The authentication response signal is transmitted to the host device 102.

The comparator 210 of the host device 102 compares the received authentication response signal and the generated authentication compare signal. The output of the comparator 210 is indicative of whether the signals match. If the signals match, the host device 102 authenticates the peripheral device 104, and the host controller 106 may send a signal to the peripheral device 104, notifying the peripheral device 104 that the peripheral device 104 is authenticated by the host device 102. If the two signals do not match, the host device 102 does not authenticate the peripheral device 104. In this case, a message indicating unsuccessful authentication may be displayed via the presentation component 110.

Still referring to FIGURES 1, 2 and 3, for peripheral device authentication of the host device 102, the authentication signal generator 308 of the peripheral device 104 generates an authentication request signal and an authentication compare signal. The authentication request signal is transmitted to the host device 102. The host device 102, in response to

receiving the authentication request signal, generates an authentication response signal. In the illustrated embodiment, the host device 102 also generates the authentication response signal based on a secure algorithm such as a secure cryptographic, hash or other secure algorithm. The authentication response signal is transmitted to the peripheral device 104.

The comparator 310 of the peripheral device 104 compares the received authentication response signal and the generated authentication compare signal. The output of the comparator 310 is indicative of whether the signals match. If the signals match, the peripheral device 104 authenticates the host device 102, and the peripheral device controller 120 may send a signal to the host device 102, notifying the host device 102 that the host device 102 is authenticated by the peripheral device 104. If the two signals do not match, the peripheral device 104 likewise does not authenticate the host device 102. Again, message or other indicia indicating unsuccessful authentication may be displayed via the presentation component 110.

When both the host and the peripheral devices 102 and 104 have authenticate each other (2-way authentication), the sensor 124 is activated by the peripheral device 104. If the authentication signals do not match, the peripheral device 104 does not activate the sensor 124.

Various embodiments are discussed.

In another embodiment, an unsecure authentication approach is employed. In such an embodiment, the authentication signals are not generated based on random signals and/or secure authentication algorithms.

In another embodiment, the order of authentication is reversed. That is, the host device 102 is first authenticated and then the peripheral device 104 is authenticated.

In yet another embodiment, the host and peripheral devices 102 and 104 concurrently authenticate each other.

In another embodiment, a user of the apparatus 100 can override successful and/or unsuccessful authentication.

In another embodiment, the peripheral device 104 includes its own power supply.

In another embodiment, the host device 102 activates the sensor 124.

In another embodiment, a one-way authentication approach, either authentication of the peripheral device 104 or the host device 102, is utilized.

In another embodiment, matching authentication signals may results in actively preventing activation of the sensor 124.

FIGURE 4 illustrates a non-limiting example method of suitable two-way secure authentication using a secure hashing algorithm. It is to be appreciated that the ordering of the acts is for explanatory purposes and not limiting. In addition, other embodiments may include more or less, including different, acts.

At 400, the host and peripheral devices 102 and 104 are coupled via respective communication interfaces 112 and 122.

At 402, the host device 102 supplies power for the peripheral device 104.

At 404, the host device 102 transmits an authentication request to the peripheral device 104. As noted herein, in one embodiment the authentication request includes a random signal generated by the host device 102.

At 406, the peripheral device 104 generates a peripheral device authentication response signal in response to the received authentication request. In the illustrated embodiment, the peripheral device authentication response signal is based on the received authentication request and a key 304.

At 408, the peripheral device 104 transmits the peripheral device authentication response signal to the host device 102.

At 410, the host device 102 determines an authentication compare signal based on the random signal and a key 204 of the host device 102. The keys 204 and 304 may represent the same known value common to both the host and peripheral devices 102 and 104.

At 412, the host device 102 compares the response and compare signals.

At 414, if the response and compare signals do not match, then at 416 the host device 102 does not authenticate the peripheral device 104.

If at 414 the response and compare signals match, then at 418 the host device 102 authenticates the peripheral device 104. Authentication may include transmitting an authentication confirmation signal to the peripheral device 104.

At 420, in response to authenticating the peripheral device, the peripheral device 104 transmits an authentication request signal to the to the host device 102. In one embodiment, the authentication request includes a random signal generated by the peripheral device 104.

At 422, the host device 102 generates a host device authentication response signal in response to the received authentication request. In the illustrated embodiment, the host device authentication signal is based on the request and the key 204.

At 424, the host device 102 transmits the host device authentication response signal to the peripheral device 104.

At 426, the peripheral device 104 determines an authentication compare signal based on the random signal and the key 304.

At 428, the peripheral device 104 compares the response and compare signals.

At 430, if the response and compare signals do not match, then at 432 the peripheral device 104 does not authenticate the host device 102.

If at 430 the response and compare signals match, then at 434 the peripheral device 104 authenticates the host device 102.

At 436, the sensor 124 is activated based on the two-way authentication. As described herein, the sensor 124 may be activated by the host device 102 in one embodiment and by the peripheral device 104 in another embodiment.

As described herein, in another embodiment the peripheral device 104 authenticates the host device 102 and then the host device 102 authenticates the peripheral device 104, and in another embodiment, the host and peripheral devices 102 and 104 concurrently authenticate each other.

Another method includes authenticating the peripheral device 104 by the host device 102, authenticating the host device 102 by the peripheral device 104, and activating the physiologic sensor 124 of the peripheral device 104 in response to authentication of the host and peripheral devices 102, 104.

The above may be implemented by way of computer readable instructions, which when executed by a computer processor(s), cause the processor(s) to carry out the acts. The instructions can be stored in a computer readable storage medium associated with or otherwise accessible to the relevant computer.

The application has been described with reference to various embodiments. Modifications and alterations will occur to others upon reading the application. It is intended that the invention be construed as including all such modifications and alterations, including insofar as they come within the scope of the appended claims and the equivalents thereof.

5

CLAIMS

What is claimed is:

1. A method for activating a physiologic sensor (124) of a peripheral device (104) of a monitoring apparatus (100), comprising:

receiving, at the peripheral device (104), a signal indicating a host device (102) authenticated the peripheral device (104);

receiving, at the peripheral device (104), a host device authentication response signal;

authenticating, at the peripheral device (104), the host device (102) based on the host device authentication response signal; and

activating the physiologic sensor (124) of the peripheral device (104) in response to authentication of both the host and peripheral devices (102, 104).

2. The method of claim 1, further comprising: authenticating at least one of the host or peripheral devices (102, 104) using a secure authentication algorithm.

3. The method of claim 2, wherein the secure authentication algorithm is a secure hashing algorithm.

4. The method of claim 1, further comprising: authenticating the host and peripheral devices (102, 104) using an unsecure authentication algorithm.

5. The method of claim 1, further comprising: activating the sensor (124) in response to two-way authentication of both the host and peripheral devices (102, 104).

6. The method of claim 5, wherein the sensor (124) remains in an inactive state in response to unsuccessful authentication of at least one of the host and peripheral devices (102, 104).

7. The method of claim 1, wherein the peripheral device (104) activates the physiologic sensor (124).

8. The method of claim 1, wherein the host device (102) activates the physiologic sensor (124).

9. The method of claim 1, further comprising:

generating, at the peripheral device (104), an authentication compare signal; and

authenticating the host device (102) in response to successfully matching the received host device authentication response signal and the authentication compare signal.

10. The method of claim 9, further comprising:

generating, at the peripheral device (104), a random number, wherein the authentication compare signal is based on the random number and a key (304) of the peripheral device (104).

11. The method of claim 10, wherein the host device authentication response signal is based on the random number and a key (204) of the host device (102).

12. The method of claim 11, further comprising:

generating, at the peripheral device (104), a host device authentication request signal based on the random number, wherein the host device (102) generates and transmits the host device authentication response signal in response to receiving the host device authentication request signal.

13. A physiologic parameter monitoring apparatus (100), comprising:

a host device (102) with a peripheral device authenticator (114); and

a peripheral device (104) with a host device authenticator (126) and a sensor (124) that senses a physiologic state of a patient,

wherein the peripheral device authenticator (114) authenticates the peripheral device (104) and the host device authenticator (126) authenticates the host device (102), and the sensor (124) is activated in response to two-way authentication of the host and peripheral devices (102, 104).

14. The apparatus of claim 13, wherein at least one of the peripheral or host device authenticators (114, 126) respectively authenticates the peripheral or host devices (104, 102) based on an unsecure authentication algorithm.

15. The apparatus of claim 13, wherein at least one of the peripheral or host device authenticators (114, 126) respectively authenticates the peripheral or host devices (104, 102) based on a secure authentication algorithm.

16. The apparatus of claim 15, wherein the secure authentication algorithm is a secure hashing algorithm.

17. The apparatus of claim 13, wherein activating the sensor (124) includes transitioning the sensor (124) from an inactive state to an active state.

18. The apparatus of claim 13, the peripheral device authenticator (126), including:

a first random signal generator (306) that generates a first random signal;

first storage (302) including a first key (304);

a first authentication signal generator (308) that generates an authentication compare signal based on the first random signal and the first key (304); and

a comparator (310) that compares the generated authentication compare signal with an authentication response signal provided by the host device authenticator (126), wherein the peripheral device (104) authenticates the host device (102) in response to the compare and response signals matching.

19. The apparatus of claim 18, the host device authenticator (126), including:

second storage (202) including a second key (204); and

a second authentication signal generator (208) that generates the authentication response signal based on the first random signal and the second key (204).

20. The apparatus of claim 13, the host device authenticator (126), including:

a first random signal generator (206) that generates a first random signal;

first storage (202) including a first key (204);

a first authentication signal generator (208) that generates an authentication compare based on the random signal and the first key (204); and

a comparator (210) that compares the generated authentication signal with an authentication response signal generated by the peripheral device authenticator (114), wherein the host device (102) authenticates the peripheral device (104) in response to the first and second authentication signals matching.

21. The apparatus of claim 20, the peripheral device authenticator (114), including:

second storage (302) including a second key (304);

a second authentication signal generator (308) that generates the authentication response signal based on the first random signal and the second key (304).

22. The apparatus of claim 13, the host device (102), further comprising: a power supply (118) that supplies power to the host device (102) and the peripheral device (104).

23. The apparatus of claim 13, the host device (102), further comprising: a presentation component (110) that present information indicative of a state of the two-way authentication.

24. The apparatus of claim 13, wherein the sensor (124) senses at least one of a body temperature, a heart rate and a blood pressure of a patient.

25. The apparatus of claim 13, wherein the peripheral device (104) activates the physiologic sensor (124).

26. The apparatus of claim 13, wherein the host device (102) activates the physiologic sensor (124).

27. A method, comprising:

activating a physiologic sensor (124) of a peripheral device (104) based on two-way authentication between the peripheral device (104) and the host device (102).

28. A method for activating a physiologic sensor (124) of a peripheral device (104) of a monitoring apparatus (100), comprising:

receiving, at the host device (102), a signal indicating a peripheral device (104) authenticated the host device (102);

receiving, at the host device (102), a peripheral device authentication response signal;

authenticating, at the host device (102), the peripheral device (104) based on the peripheral device authentication response signal; and

activating the physiologic sensor (124) of the peripheral device (104) in response to authentication of both the host and peripheral devices (102, 104).

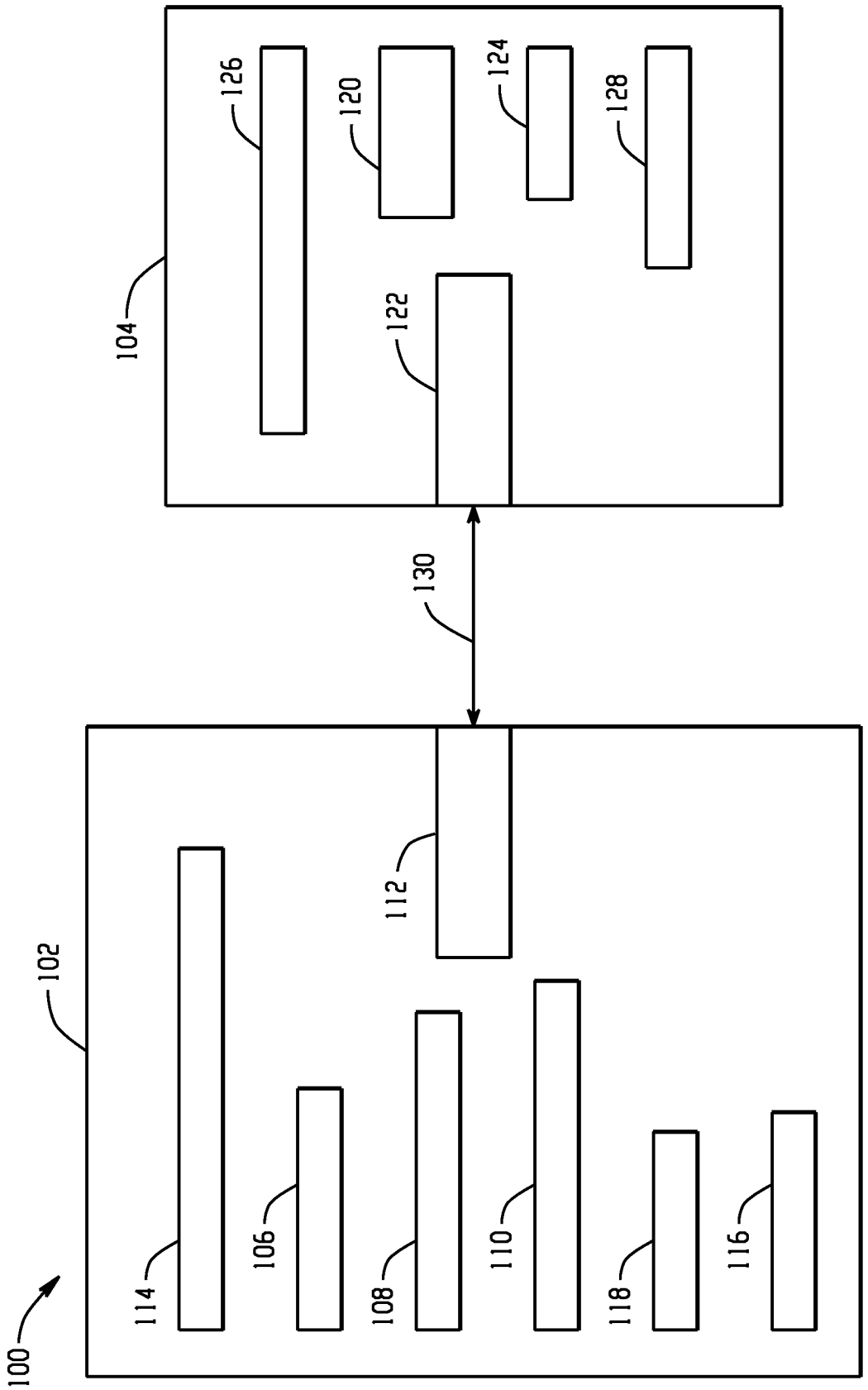

Fig. 1

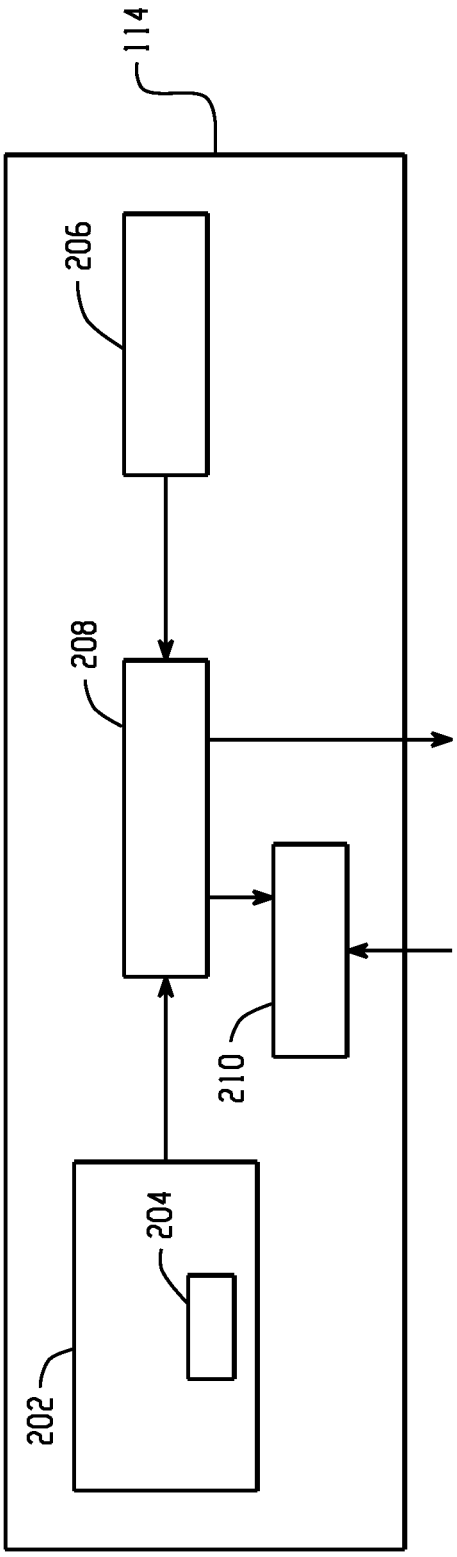

Fig. 2

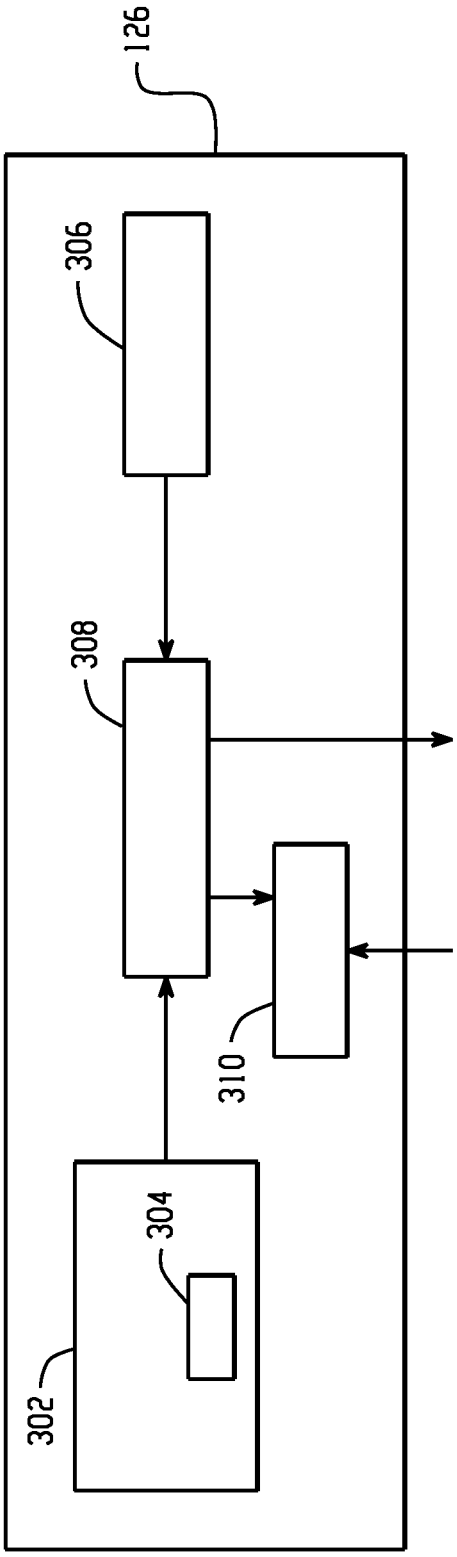

Fig. 3

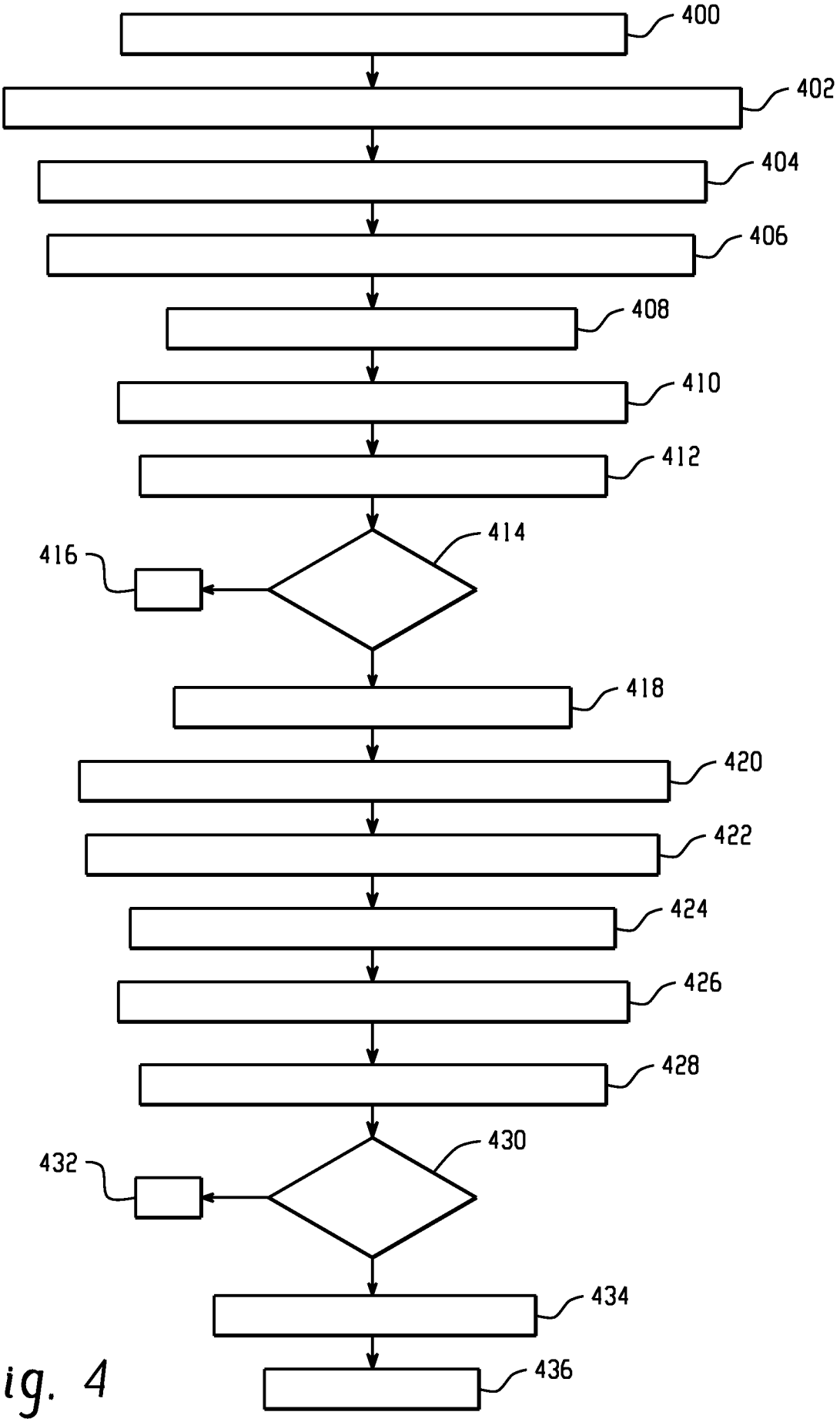
400
402
404
406
408
410
412
414
416
418
420
422
424
426
428
430
432
434
436

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/048166

A. CLASSIFICATION OF SUBJECT MATTER
INV. A61B5/00 G06F21/00 G06F19/00 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
A61B G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/209545 A1 (ASANO TOMOYUKI [JP]) 28 August 2008 (2008-08-28)	1-3,5,7, 9-11,13, 15-20, 23,25, 27-28
Y	abstract figures 1,2,4,7,8 paragraph [0044] paragraph [0059] paragraph [0063] - paragraph [0064] paragraph [0084] paragraph [0087] paragraph [0104] - paragraph [0105] paragraph [0110] - paragraph [0115] paragraph [0119] - paragraph [0120] paragraph [0148]	4,6,8, 12,14, 21-22, 24,26

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 March 2010	17/03/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Möhrs, Sascha

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/048166

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2005/119486 A2 (TELESTREAM INC [US]; CARNAHAN SHAWN [US]) 15 December 2005 (2005-12-15) abstract page 9, line 18 - page 9, line 21	4,14
Y	US 2006/031378 A1 (VALLAPUREDDY VINEEL [US] ET AL) 9 February 2006 (2006-02-09) abstract claims 1,12	6,8,26
Y	US 2007/135866 A1 (BAKER STEVEN D [US] ET AL) 14 June 2007 (2007-06-14) abstract paragraph [0098]	12
Y	EP 0 867 843 A2 (SONY CORP [JP]) 30 September 1998 (1998-09-30) abstract figure 1 claims 13,15	21
Y	WO 2007/101141 A2 (HMICRO INC [US]; MAGAR SURENDAR [US]; SATTIRAJU VENKATESWARA RAO [US]) 7 September 2007 (2007-09-07) abstract claims 33,38	22
Y	US 2009/112769 A1 (DICKS KENT [US] ET AL) 30 April 2009 (2009-04-30) abstract claims 14,21,25	24
A	US 2007/214357 A1 (BALDUS HERIBERT [DE] ET AL) 13 September 2007 (2007-09-13) abstract figures 1,3,6,8	1-28
A	WO 2007/126360 A1 (GAMBRO LUNDIA AB [SE]; GAGNER JOHAN [SE]; MATTSSON FREDRIK [SE]; HOBRO) 8 November 2007 (2007-11-08) abstract figures 1,2	1-28

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2009/048166

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008209545 A1	28-08-2008	JP 2008181295 A	07-08-2008
WO 2005119486 A2	15-12-2005	US 2006010245 A1	12-01-2006
US 2006031378 A1	09-02-2006	EP 1784123 A1	16-05-2007
		JP 2008508081 T	21-03-2008
		WO 2006017615 A1	16-02-2006
US 2007135866 A1	14-06-2007	AU 2006325783 A1	21-06-2007
		CA 2632648 A1	21-06-2007
		EP 1968691 A2	17-09-2008
		WO 2007070855 A2	21-06-2007
EP 0867843 A2	30-09-1998	DE 69821159 D1	26-02-2004
		DE 69821159 T2	09-09-2004
		JP 4268690 B2	27-05-2009
		JP 10327142 A	08-12-1998
		TW 423242 B	21-02-2001
		US 6058477 A	02-05-2000
WO 2007101141 A2	07-09-2007	EP 1993437 A2	26-11-2008
		US 2010049006 A1	25-02-2010
US 2009112769 A1	30-04-2009	NONE	
US 2007214357 A1	13-09-2007	NONE	
WO 2007126360 A1	08-11-2007	AU 2007244000 A1	08-11-2007
		CA 2647361 A1	08-11-2007
		EP 2012848 A1	14-01-2009
		US 2009306573 A1	10-12-2009

专利名称(译)	双向认证		
公开(公告)号	EP2445390A1	公开(公告)日	2012-05-02
申请号	EP2009789876	申请日	2009-06-22
申请(专利权)人(译)	ANALOGIC CORPORATION		
当前申请(专利权)人(译)	ANALOGIC CORPORATION		
[标]发明人	TVERSKOY MARK DICIACCIO ANTHONY RALPH		
发明人	TVERSKOY, MARK DICIACCIO, ANTHONY, RALPH		
IPC分类号	A61B5/00 G06F21/00 G06F19/00 H04L29/06		
CPC分类号	A61B5/0002 G06F19/3418 G06F21/445 H04L63/0869 H04L67/12		
其他公开文献	EP2445390B1		
外部链接	Espacenet		

摘要(译)

一种用于激活监视装置（100）的外围设备（104）的生理传感器（124）的方法，包括：在外围设备（104）处接收指示主机设备（102）对外围设备（104）进行认证的信号。 ），在外围设备（104）处接收主机设备认证响应信号，在外围设备（104）处基于主机设备认证响应信号认证主机设备（102），并激活生理传感器（ 124）外围设备（104）响应主机和外围设备（102,104）的认证。