



- (51) **International Patent Classification:**
H04B 13/00 (2006.01) *H04L 29/06* (2006.01)
- (21) **International Application Number:**
PCT/US2016/033901
- (22) **International Filing Date:**
24 May 2016 (24.05.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
14/751,233 26 June 2015 (26.06.2015) US
- (71) **Applicant: INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95054 (US).
- (72) **Inventors; and**
- (71) **Applicants (for US only): SYDIR, Jaroslaw J.** [US/US]; 1270 Chateau Drive, San Jose, California 95120 (US). **KONANUR, Anand S.** [IN/US]; 1063 Morse Ave, Apt 8-102, Sunnyvale, California 94089 (US). **KARACAOGLU, Ulun** [US/US]; 2215 Linwood Street, Apt. # C4, San Diego, California 92110 (US). **LAMARCA, Anthony G.** [US/US]; 10016 Ravenna Avenue, NE, Seattle, Washington 98125 (US). **WOOD, Stephen R.** [US/US]; 765 SW Murray Blvd, Beaverton, Oregon 97005 (US). **BURR, Jeremy** [GB/US]; 2816 NW Xavier Street, Portland, Oregon 97210 (US).
- (74) **Agent: JORDAN, B. Delano;** Jordan IP Law LLC, c/o CPA Global, 900 Second Avenue South, Suite 600, Minneapolis, Minnesota 55402 (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, BN, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).
- Published:**
— with international search report (Art. 21(3))

(54) **Title:** HUMAN BODY COMMUNICATION DEVICE WITH SECURE ACCESS

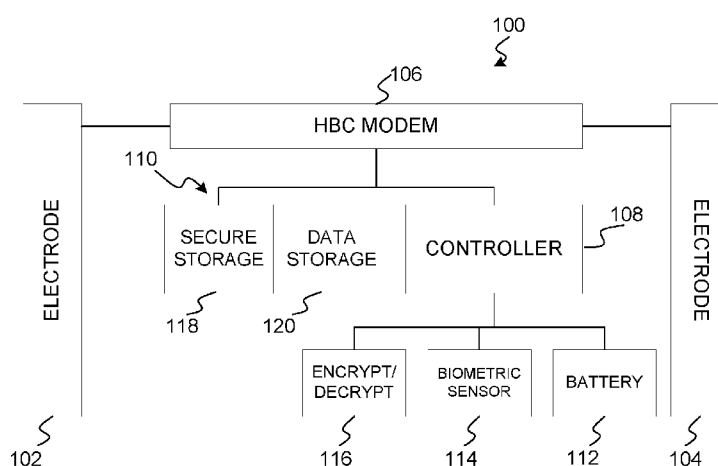


FIG. 1

(57) **Abstract:** Systems, apparatuses, and methods may include a human body communication data storage device having at least first and second electrodes and a human body communication modem. A storage component communicating with the human body communication modem includes a first secure storage location provided with a user-specific authentication record and a second data storage location.

HUMAN BODY COMMUNICATION DEVICE WITH SECURE ACCESS

CROSS-REFERENCE TO RELATED APPLICATIONS

5 The present application claims the benefit of priority to U.S. Non-Provisional Patent Application No. 14/751,233 filed on June 26, 2015.

TECHNICAL FIELD

10 Embodiments generally relate to human body communication. More particularly, embodiments relate to human body communication storage devices with secure access.

BACKGROUND

Human body communication is a communication technology in which a signal is
15 coupled directly onto a human body through a transmission electrode; it is transmitted over the body to its destination. The signal may be delivered to an external device via a body member contacting a receiving pad on the device. Human body communication transmission electrodes and receiving electrodes typically touch the skin or are in close proximity to the skin. There may be no interference between human body communication transmissions on one person's
20 body and those on another person's body, even if the bodies are located in close proximity. Thus, applications for human body communication include use as a general purpose body area network communications technology or as an extension of near field communication technology.

 Data may be transferred to and from human body communication devices as users
25 share documents or files. In some cases, an unauthorized user may have access to data stored on the human body communication device.

BRIEF DESCRIPTION OF THE DRAWINGS

 The various advantages of the embodiments will become apparent to one skilled in the art by reading the following specification and appended claims, and by referencing the
30 following drawings, in which:

 FIG. 1 is a schematic diagram of an example of a human body communication storage device;

FIGs. 2 and 3 are flowcharts of examples of methods of ensuring that a human body communication storage device has secure access by an authorized user according to an embodiment;

FIG. 3 is a flowchart of an example of a method according to an embodiment; and

5 FIG. 4 is an illustration of an example of a use of multiple user-specific authentication records according to an embodiment.

DESCRIPTION OF EMBODIMENTS

Turning to the drawings in detail, FIG. 1 depicts an example of a human body communication (HBC) storage device 100 according to an embodiment. A first electrode 102 typically faces towards a user's body while a second electrode 104 typically faces away from the user's body. The first electrode 102 and the second electrode 104 may electrically communicate with a modem 106 either directly or through intermediate components. The modem 106 may include, among other components, a transmission buffer, transmitter, receiver, and receiving buffer. The modem 106 may be connected to a controller 108 and to storage 110. The controller 108 and storage 110 may also be connected to each other and optionally included in the modem 106. Optionally, the human body communication storage device 100 may include a power source such as battery 112, a biometric sensor 114, and a security module 116 that includes encryption and decryption capabilities.

20 Illustrated storage 110 includes a secure storage component 118 and a data storage component 120. In operation, the secure storage component 118 is typically provided with a user-specific authorization record while data to be transferred to external devices is stored in the data storage component 120. As will be discussed below, the inclusion of a user-specific authorization record may ensure that an unauthorized third party cannot gain access to the human body communication storage device 100, put it on, and touch an external device to read the data stored in the data storage component 120.

FIGs. 2 and 3 show exemplary authentication methods 200 and 300, respectively, of ensuring that the human body communication storage device 100 has secure access by an authorized user. The methods 200 and 300 may be implemented as a set of logic instructions stored in a machine- or computer-readable storage medium such as random access memory (RAM), read only memory (ROM), programmable ROM (PROM), firmware, flash memory, etc., in configurable logic such as, for example, programmable logic arrays (PLAs), field programmable gate arrays (FPGAs), complex programmable logic devices (CPLDs), in fixed-functionality logic hardware using circuit technology such as, for example, application specific

integrated circuit (ASIC), complementary metal oxide semiconductor (CMOS) or transistor-transistor logic (TTL) technology, or any combination thereof. For example, computer program code to carry out operations shown in methods 200 and 300 may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages.

With continued reference to FIGs. 1-3, in block 210 of the method 200, a user-specific authorization record that identifies the user is provided in the secure storage component 118. The record may be one or more biometric markers that uniquely identify the user or a password or passphrase known only to the user. Exemplary biometric markers include fingerprints, palmprints, bioimpedances, voice data, facial recognition patterns, blood vessel patterns, retinal scans, iris scans, heart rhythm records (e.g., electrocardiogram/EKG) or any unique user attribute that may be sensed and recorded. Alternatively, a marker may be implanted into or ingested by the user and the implanted/ingested marker may be sensed to identify the user. Examples include RFIDs and microchips but are not limited thereto.

In block 220, a user of the human body communication storage device 100 may initiate communication with an external device by, for example, touching an external device capable of receiving human body communications. In illustrated block 230, the human body communication storage device 100 obtains information from the user. This information may be biometric information sensed by biometric sensor 114 or may be biometric information sensed by the external device and communicated to the human body communication storage device 100. Alternatively, the user may input a password or passphrase to the external device that is communicated to the human body communication storage device 100.

The human body storage communication device 100 may compare the information obtained from the user with the stored user-specific authorization record in block 240. At block 250 it is determined whether the obtained information matches the stored user-specific authorization record. If a match is determined, the human body communication storage device 100 may permit access to the data stored in data storage component 120 in block 260. If no match is determined, data access is denied in illustrated block 270.

In use, the authentication method 200 may be performed each time the user encounters a different external device or each time data access is desired. Alternatively, the method 300 of FIG. 3 may be used. In FIG. 3, at processing block 310, the human body communication storage device 100 may be provided with the user-specific authentication

record. In processing block 320, the authentication method 200 may be performed and communication may be established between the human body communication storage device 100 and an external device when there is an information match to the user-specific authentication record.

5 In illustrated block 340, the human body communication storage device 100 determines whether it has been worn by the user continuously since the last authentication method 200 was performed. This determination may be made through sensors, such as the biometric sensor 114 or other optional sensors provided on the human body communication storage device 100. In an exemplary technique, a loss of EKG or heart rhythm reading or a
10 significant change in bioimpedance reading would indicate that the device 100 has been removed by a user. If it is determined that the device has been worn continuously since the last authentication method 200 was performed, the human body communication storage device 100 may permit data access to the data storage component 120 in process block 350 without performing additional authentication. If it is determined that the storage device 100 has not
15 been worn continuously since the last authentication method was performed, the storage device 100 goes through a complete authentication method 200 before allowing access to data in illustrated block 330.

 A variety of data may be stored on the human body communication storage device 100. Data stored on the human body communication storage device 100 may be classified
20 based on who owns and/or access the data. For example, data stored in the data storage component 120 may be owned by and accessible to the user directly. This might include personal data, data files, or personal credentials such as an encryption key used to encrypt files sent to a secure print service. This data is written to and read from the human body communication storage device 100 by the user.

25 In contrast, data stored in the secure storage component 118 may be data placed there by a third party for use of the user. An example of such data is information including the user's account numbers and biometrics written to the secure storage component 118 by a bank. This information is owned by the user but is not directly accessed by the user. Typically, the information is encrypted by the third party (such as a bank) so that access to it cannot be gained
30 directly. It may be accessed by point of sale terminals and other payment devices on behalf of the user.

 Note that different user-specific authentication records may be used to authenticate the user depending upon the particular external device with which communication is to be established. That is, each third-party may provide its own user authentication record for that

user, to control access to that third-party's data on storage device 100. The user authentication record may be provided at secure storage component 118 while the data may be provided at data storage component 120. For example, the human body communication storage device 100 may be configured so that data owned by the user is secured using a heart rhythm monitor with the biometric sensor 114 being a heart rhythm monitor used in the authentication process 200. Data owned by the user's bank might be secured using fingerprint data provided to device 100 via an external device such as a payment terminal. Thus multiple user-specific authentication records may be provided to the secure storage component 118 to permit access to different data items in data storage component 120.

FIG. 4 depicts the use of multiple user-specific authentication records. A security monitor 400 partitions the secure storage component 118 into plural user-specific authentication records, each of which permits access to a corresponding set of data in the data storage component 120. For example, for access to a first set of data, authentication process 410 is performed (selected from authentication method 200 or 300 in FIGs. 2 or 3, respectively) using a first set of user-obtained information 420 that is compared to the stored user-specific authentication record. If there is a match, data access to the first set of data is granted at illustrated block 430. Similarly, for access to a second set of data, authentication process 440 is performed (selected from authentication method 200 or 300 in FIGs. 2 or 3, respectively) using a second set of user-obtained information 450 that is compared to a further stored user-specific authentication record. If there is a match, data access to the second set of data is granted at illustrated block 460. Note that there may be any number of different data sets using different combinations of user-specific authentication records and information obtained from the user.

Further, the authentication procedures may be nested. For example, the human body communication storage device 100 may be configured to use heart rhythm data sensed by sensor 114 for authentication to all data sets and a bank could also require fingerprint information from the user at a pay terminal.

Advantageously, human body communication described in the embodiments may have a variety of applications depending upon the specific data that is transmitted. Transmitted data may be information such as text from a document that is temporarily stored on the human body communication storage device (after being copied) and then transferred to another touch device such as a computer, smart phone, or tablet. Similarly it may be a URL (Uniform Resource Locator) that is later copied to another device or geo-coordinates that are later copied to a GPS (Global Positioning System) navigation unit. Data may be a prescription written to

the device by a doctor and retrieved by a pharmacy, or bank account information written to the device by a bank and retrieved and modified at a point of sale terminal. Similarly, it may be an encryption key that was used to encrypt a file sent to a public printer that is retrieved by the printer to decrypt the file. Numerous other encryption key scenarios are possible.

5 Embodiments are applicable for use with all types of semiconductor integrated circuit (“IC”) chips. Examples of these IC chips include but are not limited to processors, controllers, chipset components, programmable logic arrays (PLAs), memory chips, network chips, systems on chip (SoCs), SSD/NAND controller ASICs, and the like. In addition, in some of the drawings, signal conductor lines are represented with lines. Some may be different, 10 to indicate more constituent signal paths, have a number label, to indicate a number of constituent signal paths, and/or have arrows at one or more ends, to indicate primary information flow direction. This, however, should not be construed in a limiting manner. Rather, such added detail may be used in connection with one or more exemplary embodiments to facilitate easier understanding of a circuit. Any represented signal lines, whether or not 15 having additional information, may actually comprise one or more signals that may travel in multiple directions and may be implemented with any suitable type of signal scheme, e.g., digital or analog lines implemented with differential pairs, optical fiber lines, and/or single-ended lines.

Example sizes/models/values/ranges may have been given, although embodiments 20 are not limited to the same. As manufacturing techniques (e.g., photolithography) mature over time, it is expected that devices of smaller size could be manufactured. In addition, well known power/ground connections to IC chips and other components may or may not be shown within the figures, for simplicity of illustration and discussion, and so as not to obscure certain aspects of the embodiments. Further, arrangements may be shown in block diagram form in order to 25 avoid obscuring embodiments, and also in view of the fact that specifics with respect to implementation of such block diagram arrangements are highly dependent upon the platform within which the embodiment is to be implemented, i.e., such specifics should be well within purview of one skilled in the art. Where specific details (e.g., circuits) are set forth in order to describe example embodiments, it should be apparent to one skilled in the art that embodiments 30 can be practiced without, or with variation of, these specific details. The description is thus to be regarded as illustrative instead of limiting.

The term “coupled” may be used herein to refer to any type of relationship, direct or indirect, between the components in question, and may apply to electrical, mechanical, fluid, optical, electromagnetic, electromechanical or other connections. In addition, the terms “first”,

“second”, etc. may be used herein only to facilitate discussion, and carry no particular temporal or chronological significance unless otherwise indicated.

As used in this application and in the claims, a list of items joined by the term “one or more of” may mean any combination of the listed terms. For example, the phrases “one or
5 more of A, B or C” may mean A, B, C; A and B; A and C; B and C; or A, B and C.

Additional Notes and Examples:

Example 1 may include a human body communication data storage device having least first and second electrodes, a human body communication modem communicating with the at least first and second electrodes, and a storage component communicating with the
10 human body communication modem, the storage component including a first secure storage location and a second data storage location.

Example 2 may include the device of example 1 where the human body communication modem further comprises a transmitter and a receiver.

Example 3 may include the device of examples 1 or 2 further comprising a
15 controller coupled to the human body communication modem, wherein the storage component is coupled to the controller and the modem.

Example 4 may include the device of example 1 further comprising one or more biometric sensors.

Example 5 may include a human body communication method comprising
20 establishing communication from a human body communication storage device to an external device, the human body communication storage device being formatted with a user-specific authorization record in a secure storage location and data in a separate storage location, obtaining information from a user of the human body communication storage device, comparing the information obtained from the user with the user-specific authorization record,
25 and permitting access to the data if the information obtained from the user matches the user-specific authorization record.

Example 6 may include the method of example 5, wherein the human body communication storage device senses the information from the user.

Example 7 may include the method of example 6, wherein the sensed information
30 is biometric sensed information.

Example 8 may include the method of example 7, wherein the biometric sensed information is selected from a bioimpedance, a heart rhythm, or a fingerprint.

Example 9 may include the method of example 5, wherein the user provides the information to the external device.

Example 10 may include the method of example 9, wherein the information is biometric information sensed by the external device.

Example 11 may include the method of example 10, wherein the biometric information is a fingerprint, a heart rhythm, a retina pattern, a blood vessel pattern, an iris
5 pattern, a facial recognition, or a voice pattern.

Example 12 may include the method of example 9, wherein the user enters the information into the external device.

Example 13 may include the method of examples 5 or 9, further comprising sensing whether the human body communication storage device has been continually worn by the user.

10 Example 14 may include the method of example 13, wherein if the human body communication storage device has been continually worn by the user, permitting access by a further external device without authentication.

Example 15 may include a non-transitory computer readable medium comprising a set of instructions which, when executed by a device, cause the device to establish
15 communication from a human body communication storage device to an external device, the human body communication storage device being provided with a user-specific authorization record in a secure storage location and data in a separate storage location, obtain information from a user of the human body communication storage device, compare information from the user with the user-specific authorization record, and permit access to the data if the information
20 from the user matches the user-specific authorization record.

Example 16 may include the computer readable medium of example 15 wherein the human body communication storage device senses the information from the user.

Example 17 may include the computer readable medium of example 16 wherein the sensed information is biometric information.

25 Example 18 may include the computer readable medium of example 17 wherein the biometric sensed information is selected from a bioimpedance, a heart rhythm, or a fingerprint.

Example 19 may include the computer readable medium of example 15 comprising further instructions, which, when executed, cause the device to sense whether the human body communication storage device has been continually worn by the user.

30 Example 20 may include the computer readable medium of example 15 wherein if the human body communication storage device has been continually worn by the user, permitting access by a further external device without authentication.

Example 21 may include an apparatus for human body communication comprising means for establishing communication from a human body communication storage device to

an external device, the human body communication storage device being provided with a user-specific authorization record in a secure storage location and data in a separate storage location, means for obtaining information from a user of the human body communication storage device, means for comparing obtained information from the user with the user-specific authorization record, and means for permitting access to the data if the information obtained from the user
5 matches the user-specific authorization record.

Example 22 may include the apparatus of example 21 further comprising means for sensing the information from the user.

Example 23 the apparatus of example 22 wherein the sensed information is
10 biometric information.

Example 24 may include the apparatus of example 23 wherein the biometric sensed information is selected from a bioimpedance, a heart rhythm, or a fingerprint.

Example 25 may include the apparatus of example 21 further comprising means for sensing whether the human body communication storage device has been continually worn by
15 the user.

Those skilled in the art will appreciate from the foregoing description that the broad techniques of the embodiments can be implemented in a variety of forms. Therefore, while the embodiments have been described in connection with particular examples thereof, the true scope of the embodiments should not be so limited since other modifications will become
20 apparent to the skilled practitioner upon a study of the drawings, specification, and following claims.

CLAIMS

We claim:

1. A human body communication data storage device comprising:
5 at least first and second electrodes;
a human body communication modem communicating with the at least first and second electrodes; and
a storage component communicating with the human body communication modem, the storage component including a first secure storage location provided with a user-specific
10 authorization record and a second data storage location.
2. The device of claim 1, where the human body communication modem further comprises a transmitter and a receiver.
- 15 3. The device of claims 1 or 2, further comprising:
a controller coupled to the human body communication modem, wherein the storage component is coupled to the controller and the modem.
- 20 4. The device of claim 3, further comprising:
one or more biometric sensors coupled to the controller.
5. A human body communication method comprising:
establishing communication from a human body communication storage device to an external device, the human body communication storage device being provided with a user-
25 specific authorization record in a secure storage location and data in a separate storage location;
obtaining information from a user of the human body communication storage device;
comparing the information obtained from the user with the user-specific authorization record; and
permitting access to the data if the information obtained from the user matches the user-
30 specific authorization record.
6. The method of claim 5, wherein the human body communication storage device senses the information from the user.

7. The method of claim 6, wherein the sensed information is biometric sensed information.

8. The method of claim 7, wherein the biometric sensed information is selected
5 from a bioimpedance, a heart rhythm, or a fingerprint.

9. The method of claim 5, wherein the user provides the information to the external device.

10 10. The method of claim 9, wherein the information is biometric information sensed by the external device.

11. The method of claim 10, wherein the biometric information is a fingerprint, a heart rhythm, a retina pattern, a blood vessel pattern, an iris pattern, a facial recognition, or a
15 voice pattern.

12. The method of claim 9, wherein the user enters the information into the external device.

20 13. The method of claim 5 or 9, further comprising sensing whether the human body communication storage device has been continually worn by the user.

14. The method of claim 13, wherein if the human body communication storage device has been continually worn by the user, permitting access by a further external device
25 without authentication.

15. A non-transitory computer readable medium comprising a set of instructions which, when executed by a device, cause the device to:

establish communication from a human body communication storage device to an
30 external device, the human body communication storage device being provided with a user-specific authorization record in a secure storage location and data in a separate storage location;
obtain information from a user of the human body communication storage device;
compare information from the user with the user-specific authorization record; and

permit access to the data if the information from the user matches the user-specific authorization record.

16. The computer readable medium of claim 15, wherein the human body
5 communication storage device senses the information from the user.

17. The computer readable medium of claim 16, wherein the sensed information is biometric information.

10 18. The computer readable medium of claim 17, wherein the biometric sensed information is selected from a bioimpedance, a heart rhythm, or a fingerprint.

19. The computer readable medium of claim 15, comprising further instructions, which, when executed, cause the device to sense whether the human body communication
15 storage device has been continually worn by the user.

20. The computer readable medium of claim 15, wherein if the human body communication storage device has been continually worn by the user, permitting access by a further external device without authentication.

20

21. An apparatus for human body communication comprising:

means for establishing communication from a human body communication storage device to an external device, the human body communication storage device being provided with a user-specific authorization record in a secure storage location and data in a separate
25 storage location;

means for obtaining information from a user of the human body communication storage device;

means for comparing obtained information from the user with the user-specific authorization record; and

30 means for permitting access to the data if the information obtained from the user matches the user-specific authorization record.

22. The apparatus of claim 21, further comprising means for sensing the information from the user.

23. The apparatus of claim 22, wherein the sensed information is biometric information.

5 24. The apparatus of claim 23, wherein the biometric sensed information is selected from a bioimpedance, a heart rhythm, or a fingerprint.

25. The apparatus of claims 21, further comprising means for sensing whether the human body communication storage device has been continually worn by the user.

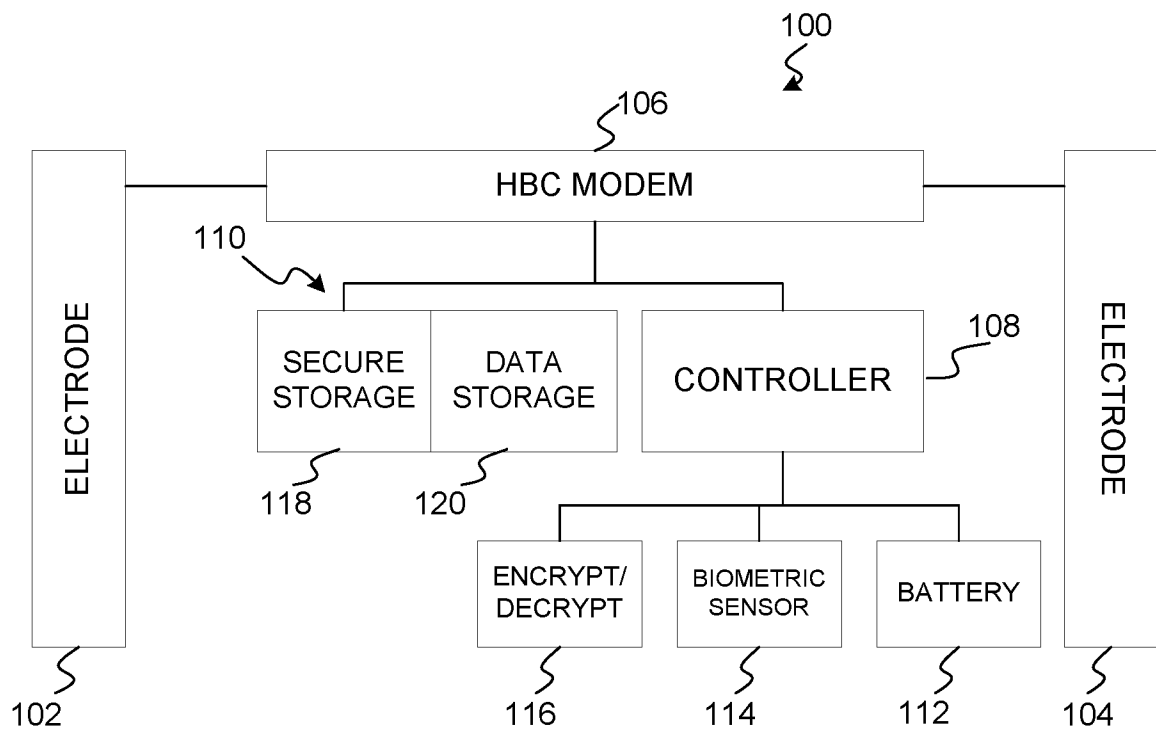


FIG. 1

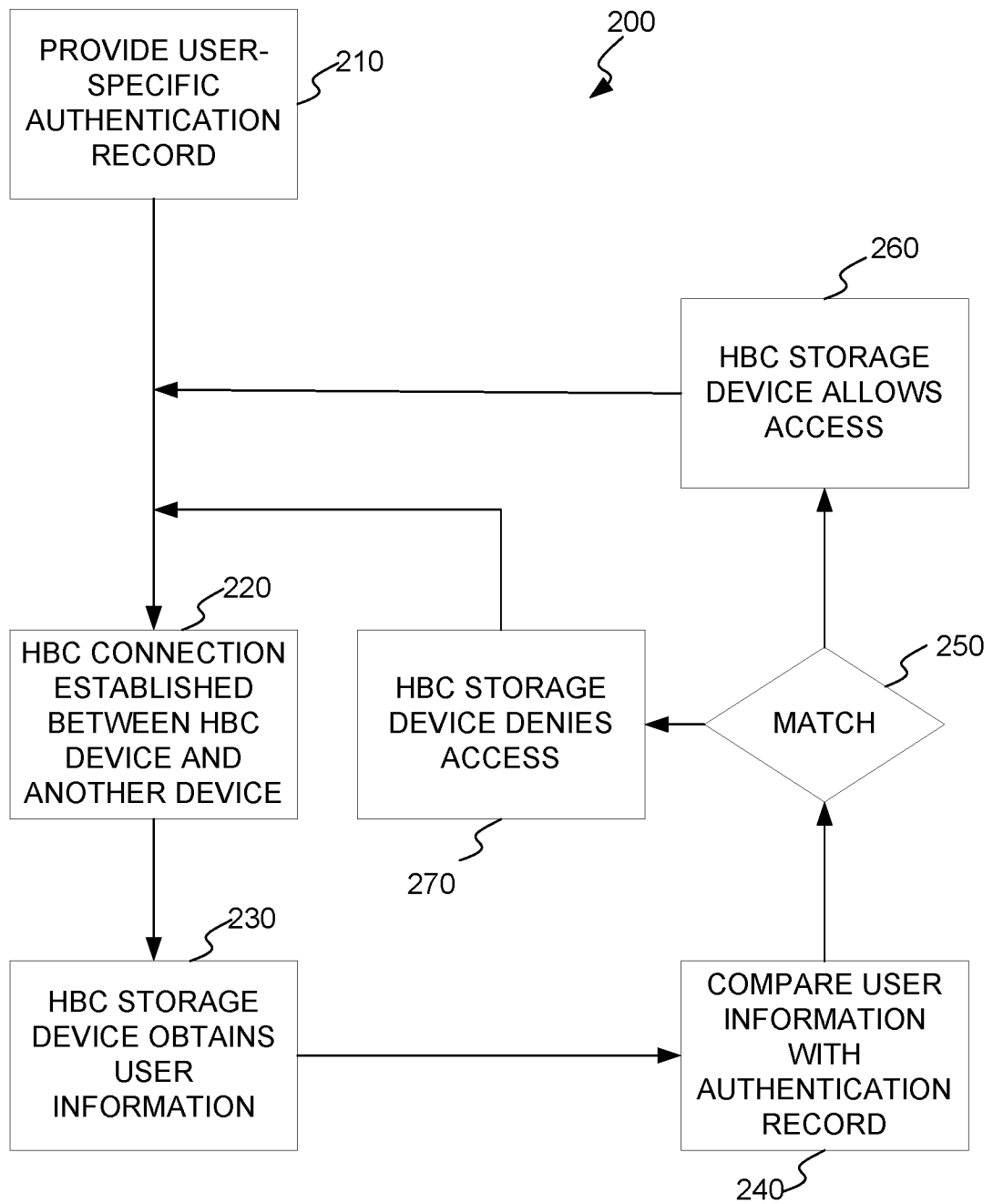


FIG. 2

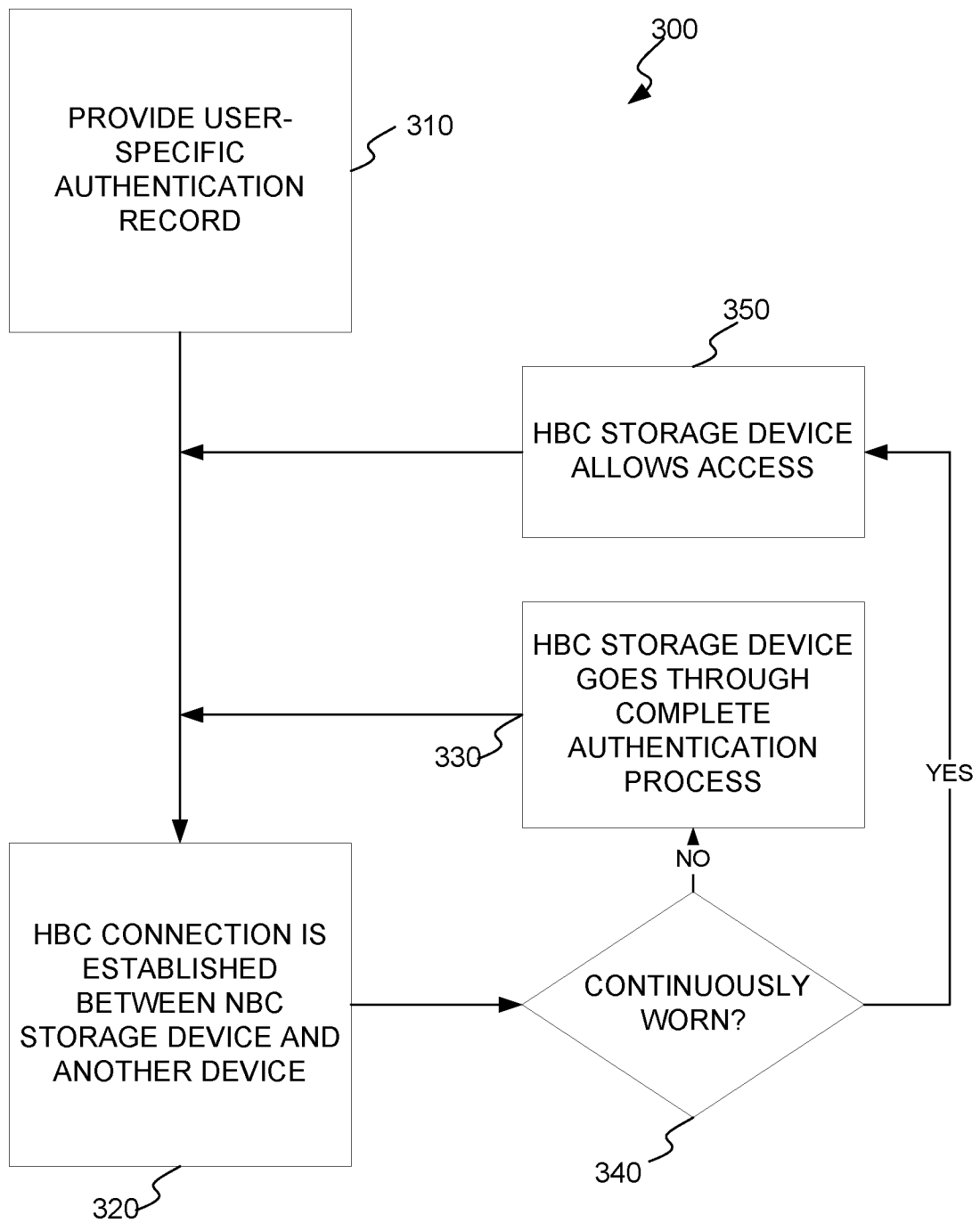


FIG. 3

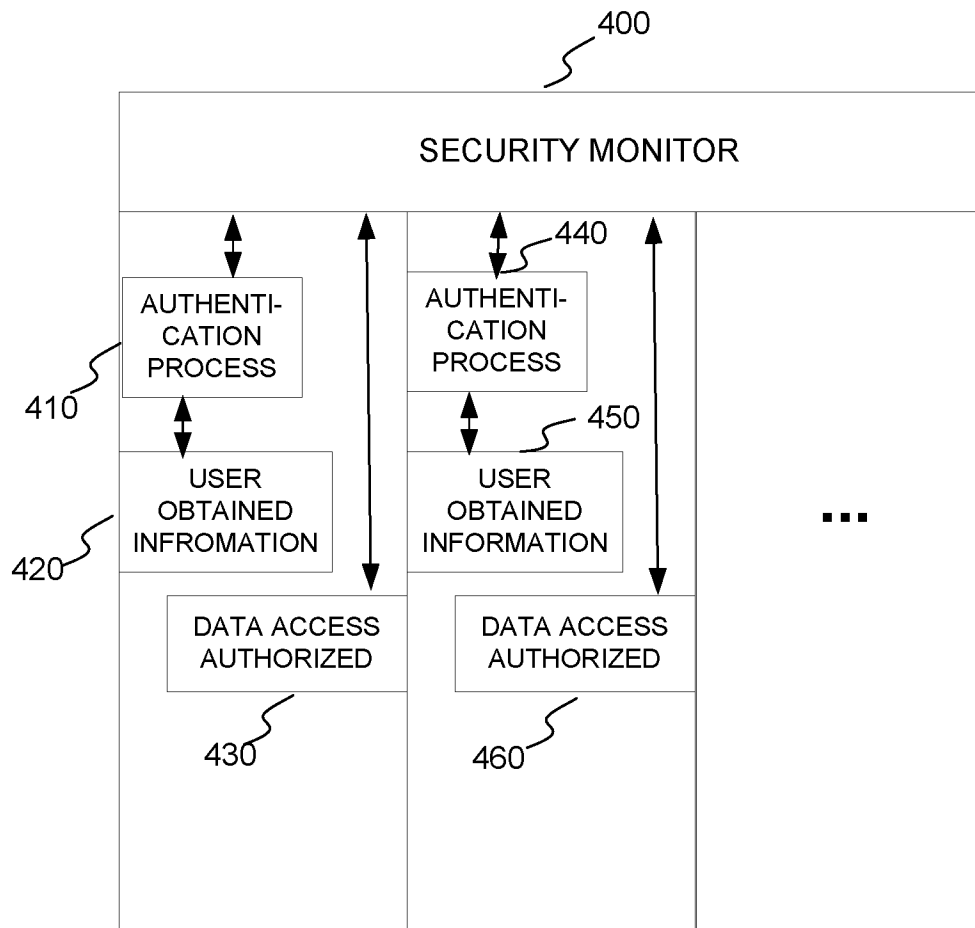


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/033901**A. CLASSIFICATION OF SUBJECT MATTER****H04B 13/00(2006.01)I, H04L 29/06(2006.01)I**

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)

H04B 13/00; H04R 25/00; G06F 15/16; G06Q 20/38; G06Q 20/32; H04L 9/32; H04Q 5/22; G06F 3/041; G06F 7/04; H04L 29/06

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: human body communication, electrodes, user-specific authorization record, data storage, separate storage location

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2011-0227856 A1 (STEVEN CORROY et al.) 22 September 2011 See paragraphs [0002], [0010]-[0016], [0033]-[0056], [0076]; and figures 4-5.	1-25
Y	US 2014-0279566 A1 (SAMSUNG ELECTRONICS CO., LTD.) 18 September 2014 See paragraphs [0019], [0027]-[0039], [0066]; and figures 2-5.	1-25
A	US 2013-0142363 A1 (BRIAN AMENTO et al.) 06 June 2013 See paragraphs [0017]-[0050]; and figures 1-3.	1-25
A	US 2009-0094681 A1 (DANIEL J. SADLER et al.) 09 April 2009 See paragraphs [0017], [0043]-[0044]; and figures 3A-3B.	1-25
A	US 2013-0019292 A1 (ALEXANDER VARSHAVSKY et al.) 17 January 2013 See paragraphs [0062]-[0064]; and figures 7-8.	1-25



Further documents are listed in the continuation of Box C.



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 application or patent 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

10 August 2016 (10.08.2016)

Date of mailing of the international search report

16 August 2016 (16.08.2016)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

LEE, EUN KYU

Telephone No. +82-42-481-3580



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2016/033901

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0227856 A1	22/09/2011	CN 102239655 A EP 2374229 A1 JP 2012-511274 A KR 10-2011-0097922 A US 8866760 B2 WO 2010-064162 A1	09/11/2011 12/10/2011 17/05/2012 31/08/2011 21/10/2014 10/06/2010
US 2014-0279566 A1	18/09/2014	CN 105190661 A EP 2973279 A1 KR 10-2015-0132471 A WO 2014-142617 A1	23/12/2015 20/01/2016 25/11/2015 18/09/2014
US 2013-0142363 A1	06/06/2013	US 2015-0092962 A1 US 8908894 B2	02/04/2015 09/12/2014
US 2009-0094681 A1	09/04/2009	CA 2701676 A1 CA 2701676 C CN 101821986 A EP 2195961 A1 EP 2195961 A4 KR 10-1160750 B1 KR 10-2010-0080918 A US 2015-0052583 A1 US 8893284 B2 WO 2009-045798 A1	09/04/2009 15/10/2013 01/09/2010 16/06/2010 19/12/2012 11/07/2012 13/07/2010 19/02/2015 18/11/2014 09/04/2009
US 2013-0019292 A1	17/01/2013	US 2014-0289835 A1 US 2016-0087979 A1 US 8752200 B2 US 9197636 B2	25/09/2014 24/03/2016 10/06/2014 24/11/2015