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

(11) EP 3 037 999 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
17.06.2020 Bulletin 2020/25

(21) Application number: **15202358.6**

(22) Date of filing: **23.12.2015**

(51) Int Cl.:
G06F 21/34 *(2013.01)* ***G06F 21/35*** *(2013.01)*
H04L 29/06 *(2006.01)* ***H04W 12/06*** *(2009.01)*
A61B 5/0404 *(2006.01)* *A61B 5/0452* *(2006.01)*
A61B 5/00 *(2006.01)*

(54) **ELECTRONIC DEVICE HAVING USER IDENTIFICATION FUNCTION AND USER AUTHENTICATION METHOD**

ELEKTRONISCHE VORRICHTUNG MIT BENUTZERIDENTIFIKATIONSFUNKTION UND BENUTZERAUTHENTIFIZIERUNGSVERFAHREN

DISPOSITIF ÉLECTRONIQUE AYANT UNE FONCTION D'IDENTIFICATION D'UTILISATEUR ET PROCÉDÉ D'AUTHENTIFICATION D'UTILISATEUR

(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

(30) Priority: **24.12.2014 KR 20140188556**

(43) Date of publication of application:
29.06.2016 Bulletin 2016/26

(73) Proprietor: **Samsung Electronics Co., Ltd.**
Gyeonggi-do 16677 (KR)

(72) Inventors:
- **Yoo, Sungsik**
  Suwon-si 16677 (KR)
- **Yu, Yongju**
  Suwon-si 16677 (KR)

(74) Representative: **Nederlandsch Octrooibureau**
P.O. Box 29720
2502 LS The Hague (NL)

(56) References cited:
WO-A1-2014/089665
US-A- 5 807 267
US-A1- 2005 071 647
US-A1- 2014 085 050
US-A1- 2014 372 762
US-A1- 2015 135 310

- **Bionym: "nymi", , 19 November 2013 (2013-11-19), XP055195746, Retrieved from the Internet: URL:https://www.nymi.com/wp-content/uploads/2013/11/NymiWhitePaper-1.pdf [retrieved on 2015-06-15]**

EP 3 037 999 B1

Description

BACKGROUND

[0001] The present disclosure relates to an electronic device having a user identification function and a user authentication method.

[0002] In recent years, in various fields, for example, the inclusion of a payment and/or an entrance service in the work field, e-commerce, e-banking, e-investing, e-data protection, remote access to a resource, e-transaction, work security, a theft prevention device, identification of a criminal, security entry, and entry registration, the importance of the recognition of an identity, such as the identification and verification of a personal identity, has increased.

[0003] The recognition of a personal identity may use electro-biometric identification and a verification system independently, or may be combined with a technology, such as a smart key, an encryption key, or a digital signature.

[0004] However, a separate user identification means, such as a password, a personal identification number (PIN) or card, or an accredited certificate is necessary for the recognition of the user. The password should be changed regularly in order to maintain security, which is a considerable burden to the user.

[0005] In a wearable electronic device that is mounted on a wrist of the user in the form of a watch or a band (e.g., in an existing smart watch as the electronic device), a method of authenticating the user through electrocardiogram (ECG) recognition has been suggested.

[0006] However, the conventional electronic device should sense an electrocardiogram whenever the user is authenticated. Bionym: "nymi", 19 November 2013 (2013-11-19), Retrieved from the Internet:URL:https://www.nymi.com/wp-content/ uploads/2013/1l1NymiWhitePaper-1.pdf [retrieved on 2015-06-15] discloses a wearable electronic device with ECG based authentication and invalidation of authentication information when the device is taken of from the user.

SUMMARY

[0007] Therefore, the present disclosure has been made in an effort to solve the above-mentioned problems, and provides an electronic device that can authenticate the user as long as it is worn by the user, without using a separate user identification means, by mounting both a user identification sensor and a wearing state detection sensor on the electronic device, thereby maintaining the authentication effect, and provides a user authentication method.

[0008] The present disclosure also provides an electronic device that can be associated with various applications without performing an additional user authentication, and a user authentication method.

[0009] In accordance with an aspect of the present disclosure, an electronic device comprises: a user identification unit that detects a body signal of the user and processes authentication of the user; an in-use detection unit that detects the body signal of the user and checks whether the user uses the electronic device; and a processor that authenticates the user according to the body signal detected by the user identification unit and the body signal detected by the in-use detection unit.

[0010] The user identification unit may comprise an ECG sensor that identifies the user through ECG sensing.

[0011] The in-use detection unit may comprise a heart rate monitor (HRM) sensor that detects a wearing state of the electronic device by the user.

[0012] The electronic device may comprise a body. The ECG sensor may comprise a first identification sensor and a second identification sensor, and the first and second identification sensors may be attached to different surfaces of the body.

[0013] The first identification sensor may generate a waveform according to an ECG pattern of heartbeats of the user, and the second identification sensor may generate a waveform according to an ECG pattern when the user makes various payments or performs an authentication in a login process.

[0014] The first identification sensor may be located in a button on the body to be operated by pushing the button, and completes a human body communication loop.

[0015] The HRM sensor may detect a wearing state of the electronic device by the user in a photoplethysmography (PPG) method.

[0016] The processor may record a waveform detected through the user identification unit, compare the waveform with an ECG pattern of the user yielding in a comparison result, the ECG pattern being registered in advance, by using an ECG pattern analysis solution, and process a user authentication for the electronic device by identifying the user according to the comparison result.

[0017] The processor may comprise a memory that stores authentication contents of the user through ECG sensing.

[0018] The electronic device further may comprise: a body and a coupling detection sensor that detects whether the body is maintained at a wearing location of the user.

[0019] The processor may eliminate the authentication contents of the user through ECG sensing stored in the memory according to a detection signal of at least one of the coupling detection sensor and the in-use detection unit.

[0020] The authentication of the user may be used in association with an application, if the in-use detection unit of the electronic device determines that the electronic device is being worn by the user after the processor authenticates the user resulting in an authentication of the user.

[0021] The electronic device may furthe comprise a

body. The body further may comprise a wrongful use prevention sensor in a band that is located at a wearing position of the user.

[0022] The wrongful use prevention sensor may be a conductive body that is embedded in a band.

[0023] In accordance with another aspect of the present disclosure, a user authentication method for use with an electronic device having a body may comprise: registering an ECG pattern of a user resulting in a registered ECG pattern; sensing an ECG pattern of the user; comparing the registered ECG pattern and the ECG pattern of the user sensed, and identifying the user; if the the registered ECG pattern coincides with the ECG pattern of the user sensed based on the identification, authenticating the user and storing authentication information; and checking a wearing state of the body.

[0024] The authentication information stored may be discarded, if the wearing state of the body is released or the body is not worn.

[0025] The authentication of the user may be used in association with an application, if the wearing state of the body is identified.

[0026] The user may be identified by comparing the registered ECG pattern of the user with the ECG pattern of the user sensed using an ECG pattern analysis solution.

[0027] When the wearing state of the body is identified, the stored authentication may be automatically discarded via detecting a wrongful use of the body by a third person.

BRIEF DESCRIPTION OF THE DRAWINGS

[0028] For a more complete understanding of the present disclosure and its advantages, reference is now made to the following description taken in conjunction with the accompanying drawings, in which like reference numerals represent like parts:

FIG. 1 is a perspective view illustrating a front surface of an electronic device that has a user identification function according to various embodiments of the present disclosure;

FIG. 2 is a perspective view illustrating a rear surface of the electronic device of FIG. 1;

FIG. 3 is a schematic diagram illustrating a wearing state of an electronic device according to various embodiments of the present disclosure;

FIG. 4 is a schematic diagram illustrating a band of an electronic device according to various embodiments of the present disclosure;

FIG. 5 is a block diagram illustrating an electronic device having a user identification function according to various embodiments of the present disclosure;

FIG. 6 is a flowchart illustrating an operation of an electronic device having a user identification function according to various embodiments of the present disclosure;

FIG. 7 is a view illustrating an example of automatically releasing a door lock through ECG authentication of an electronic device having a user identification function according to various embodiments of the present disclosure; and

FIG. 8 is a view illustrating an example of an automatic login through ECG authentication of an electronic device having a user identification function according to various embodiments of the present disclosure.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

[0029] The following description with reference to the accompanying drawings is provided to assist in a comprehensive understanding of various embodiments of the present disclosure as defined by the claims and their equivalents. It includes various specific details to assist in that understanding but these are to be regarded as merely exemplary. Accordingly, those of ordinary skill in the art will recognize that various changes and modifications can be made to the various embodiments described herein without departing from the scope and spirit of the present disclosure. In addition, descriptions of well-known functions and constructions may be omitted for clarity and conciseness.

[0030] The terms and words used in the following description and claims are merely used by the inventor to enable a clear and consistent understanding of the present disclosure. Accordingly, it should be apparent to those skilled in the art that the following description of various embodiments of the present disclosure is provided for illustration purpose only and not for the purpose of limiting the present disclosure as defined by the appended claims and their equivalents.

[0031] It is to be understood that the singular forms "a," "an," and "the" include plural referents unless the context clearly dictates otherwise. Thus, for example, reference to "a component surface" includes reference to one or more of such surfaces.

[0032] By the term "substantially" it is meant that the recited characteristic, parameter, or value need not be achieved exactly, but that deviations or variations, including for example, tolerances, measurement error, measurement accuracy limitations and other factors known to those of skill in the art, may occur in amounts that do not preclude the effect the characteristic was intended to provide.

[0033] As used in embodiments of the present disclosure, the expression "include" or "may include" or "can include" refers to the existence of a corresponding func-

tion, operation, or constituent element, and does not limit one or more additional functions, operations, or constituent elements. Further, as used in embodiments of the present disclosure, the term, such as "include" or "have" may be construed to denote a certain characteristic, number, operation, constituent element, component or a combination thereof, but may not be construed to exclude the existence of or a possibility of addition of one or more other characteristics, numbers, operations, constituent elements, components or combinations thereof.

[0034] As used in embodiments of the present disclosure, the expression "and/or" includes any or all combinations of words enumerated together. For example, the expression "A or B" or "at least one of A and B" may include A, may include B, or may include both A and B.

[0035] While expressions including ordinal numbers, such as "first" and "second", as used in the present disclosure may modify various constituent elements, such constituent elements are not limited by the above expressions. For example, the above expressions may not indicate a specific order and/or relative importance of the corresponding constituent elements. The above expressions may be used merely for the purpose of distinguishing a constituent element from other constituent elements. For example, a first user device and a second user device indicate different user devices although both are user devices. For example, a first constituent element may be termed a second constituent element, and likewise a second constituent element may also be termed a first constituent element without departing from the scope of the present disclosure.

[0036] When a first component is referred to as being "connected" or "accessed" to a second component, it should be understood that the first component may be directly connected or accessed to the second component, but also that a third component may be interposed between the first and second components. Contrarily, when the first component is referred to as being "directly connected" or "directly accessed" to the second component, it should be understood that there is no other component between the first component and the second component.

[0037] In various embodiments of the present disclosure, an electronic device may be a device that involves a communication function. Accordingly, an electronic device may be, for example, a smart phone, personal computer (PC), a tablet PC, a mobile phone, a video phone, an e-book reader, a desktop PC, a laptop PC, a netbook computer, a Personal Digital Assistant (PDA), a Portable Multimedia Player (PMP), a Moving Picture Experts Group (MPEG-1 or MPEG-2) Audio Layer-3 (MP3) player, a portable medical device, a digital camera, or a wearable device (e.g., a Head-Mounted Device (HMD), such as electronic glasses, electronic clothes, an electronic bracelet, an electronic necklace, electronic tattoos, an electronic appcessory, a smart watch, and the like).

[0038] FIGS. 1 and 2 illustrate an electronic device 100 that has a user identification function according to various embodiments of the present disclosure. FIG. 3 illustrates a wearing state of the electronic device 100 of FIG. 1.

[0039] The electronic device 100 that has a user identification function according to various embodiments of the present disclosure is, for example, a smart watch, and includes a housing or body 120, a band 140 for mounting or securing the body 120 on a wrist of the user, and a buckle assembly 160 that couples opposite ends of the band 140 to maintain a desired mounting position of the body 120.

[0040] The electronic device 100 may include an ECG sensor 200 (as shown in FIG. 5) for identifying the user, and a heart rate monitor (HRM) sensor, or HRM sensor 300 for detecting a wearing state of the electronic device by the user.

[0041] The ECG sensor 200 may include a first identification sensor 220 that is operated when user authentication is desired, and a second identification sensor 240 that is attached to a wrist of the user. For example, the first identification sensor 220 may be in the form of a button on an upper surface or an upper portion 154 of the body 120 and the second identification sensor 240 may be located in a lower portion or a lower surface 158 of the body 120.

[0042] The first identification sensor 220 may generate a waveform of a voltage according to an ECG pattern when the user is authenticated to perform payments and login processes, and the second identification sensor 240 may generate a waveform of a voltage according to an ECG pattern of the heart beats of the user.

[0043] The first identification sensor 220 is operated, for example, by pushing a button associated with the first identification sensor 220 for a predetermined time period, which may generate a human body communication loop.

[0044] The HRM sensor 300 may periodically detect a wearing state of the electronic device 100 by the user. For example, the HRM sensor 300 may be attached to the lower portion or the lower surface 158 of the body 120 adjacent to the second identification sensor 240, and it may be preferable to use a PPG method in which variations of reflection of light are sensed according to a flow of blood to measure heart beats or heart rates.

[0045] The buckle assembly 160 may further include a coupling detection sensor 620 (as shown in FIG. 5) that detects that a first end 162 of the opposite ends of the band 140 is coupled to a second end 166 of the opposite ends of the band 140, which enters the buckle assembly 160 into an in-use state of the electronic device 100.

[0046] The coupling detection sensor 620 may detect if the user releases the wearing (the in-use) state of the electronic device 100 thus also exiting the in-use state of the electronic device 100. For example, the electronic device 100 may include the buckle assembly 160, into which the first end 162 of the band 140 is inserted to be coupled to the buckle assembly 160 on the second end 166 such that the electronic device 100 is mounted or secured on a wrist of the user. Conversely, the electronic device 100 may use the coupling detection sensor 620,

such as, for example, a general photo sensor, a magnet, or a lead switch, to detect if the user releases the band 140 from the buckle assembly 160 to exit the in-use state of the electronic device 100.

[0047] After the electronic device 100 having a user identification function, according to various embodiments of the present disclosure, is worn by the user, the user may be identified by comparing ECG patterns according to waveforms of the voltages detected through the first identification sensor 220 and the second identification sensor 240 of the ECG sensor 200 in order to perform a user authentication for the electronic device 100. Results of the user authentication performed may be stored in an ECG authentication storage.

[0048] As long as the user maintains the wearing state of the electronic device 100, after the user authentication has been performed through the ECG sensor 200, the electronic device 100 may achieve an authentication maintaining effect.

[0049] To achieve an authentication maintaining effect, the electronic device 100 of the present disclosure checks whether the coupling detection sensor 620, which includes the buckle assembly 160, is being kept in the wearing state, and also periodically checks the wearing state of the electronic device 100 by the user through the HRM sensor 300.

[0050] Accordingly, the electronic device 100 of the present disclosure may continue to authenticate the user as long as the user wears the electronic device 100, without using a separate user identification means. It may also be unnecessary to perform ECG sensing again whenever the authentication is performed.

[0051] FIG. 4 illustrates the band 140 of the electronic device 100 according to various embodiments of the present disclosure.

[0052] Referring to FIG. 4, the band 140 of the electronic device 100 may further include a tamperproof or wrongful use prevention sensor 640 (shown in FIG. 5) that may prevent the wrongful use of the electronic device 100, on which an authentication has already been performed. For example, if the electronic device 100, on which an authentication of the user has been performed, is used after the band 140 of the electronic device 100 is cut off by a third person, the third person may wrongfully use the electronic device 100 without performing ECG sensing again because the electronic device 100 may be stolen without permission while the wearing state of the electronic device 100 based on the coupling detection sensor 620 has not been reset by the user.

[0053] In order to provide such a tamperproof function, the wrongful use prevention sensor 640 may include a conductive body 642 that is embedded in the band 140 in the shape of a stripe.

[0054] According to an embodiment of the present disclosure, because the conductive body 642 is also cut off if a third person cuts off the band 140, a processor 700 (as shown in FIG. 5) may detect a sign of wrongful use accordingly, and then the wrongful use by the third person may be prevented by commanding the elimination or discarding of ECG authentication information of the user that is stored in a security memory 720 (as shown in FIG. 5) in the processor 700.

[0055] FIG. 5 illustrates the electronic device 100 having a user identification function according to various embodiments of the present disclosure.

[0056] Referring to FIG. 5, the electronic device 100 having a user identification function, according to the present disclosure, may include the body 120 (e.g., as shown in FIG. 4), a user identification unit 500 that detects a body signal of the user and performs an authentication of the user of the electronic device 100, an in-use detection unit 600 that detects a body signal of the user and checks an in-use state of the electronic device 100 by the user, and a processor 700 that authenticates the user according to a detection signal of the user identification unit 500.

[0057] The user identification unit 500 may include an ECG sensor 200 for identifying the user, and the in-use detection unit 600 may include an HRM sensor 300 for detecting a wearing state of the electronic device 100 by the user, as described above.

[0058] The processor 700 compares ECG patterns according to waveforms of voltages detected through the first identification sensor 220 and the second identification sensor 240 (acting as a pair of ECG sensors) of the user identification unit 500 using an ECG pattern analysis solution 740 to yield in a comparison result. The processor 700 also authenticates the user of the electronic device 100 by identifying the user according to the comparison result.

[0059] The processor 700 may include a security memory 720 that stores and preserves authentication contents of the user through ECG sensing.

[0060] When the user does not release the wearing state of the electronic device 100 after the user is authenticated (ECG authentication) through ECG sensing, the processed user authentication information may be stored in the security memory 720 in the processor 700, which is an ECG authentication storage.

[0061] The electronic device 100, according to various embodiments of the present disclosure, may identify the wearing state of the electronic device 100 by the user according to a signal of the coupling detection sensor 620.

[0062] Furthermore, because the coupling detection sensor 620 detects the wearing state of the electronic device 100, and the HRM sensor 300 of the in-use detection unit 600 periodically monitors the wearing state of the electronic device 100, the processor 700 may command the security memory 720 in the processor 700 to eliminate or discard ECG authentication information that is stored and preserved in the security memory 720 according to a detection signal of the coupling detection sensor 400 or the in-use detection unit 600 when the electronic device 100 is taken off from the user.

[0063] In another embodiment, ECG authentication in-

formation may be stored in an external memory 722 external to the processor 700. In such embodiments, the security memory 720 is embedded in the processor 700.

[0064] If the wearing state of the electronic device 100 is not released, but the user continues to wear the electronic device 100, the processed ECG authentication is available and may be used in various authentication procedures.

[0065] Differently, because the ECG authentication information stored in the security memory 720 or the external memory 722 is eliminated or discarded, automatically or selectively, if the wearing state of the electronic device 100 is released or the electronic device 100 is not worn, the electronic device 100 may prompt for a new ECG authentication procedure.

[0066] Furthermore, even though a third person cuts off the band 140 for the purpose of theft while the wearing state of the electronic device 100 is not released, the wrongful use by a third person can be prevented because the processor commands the security memory 720 or the external memory 722 to eliminate or discard, automatically or selectively, the ECG authentication information stored in the security memory 720 or the external memory 722 according to a detection signal of the wrongful use prevention sensor 640 for detecting a sign of a wrongful use of the electronic device 100 by cutting-off the conductive body 642 in the band 140.

[0067] A user authentication procedure of the electronic device 100 having a user identification function, according to the present disclosure, will be described with reference to FIG. 6.

[0068] First, an authentication registering step (S 100) of registering an ECG pattern of the user is performed before the user puts on the electronic device 100.

[0069] Next, while the user wears the electronic device 100 such that the second identification sensor 240 (of FIG. 2) is placed onto a wrist of the user, ECG sensing at S200 is started by pushing or touching the first identification sensor 220 (of FIG. 1) at the upper portion 154 (of FIG. 1) of the body 120 for a predetermined time period (as shown in FIG. 3).

[0070] In S300, the processor 700 (of FIG. 5) records waveforms detected by electrodes of the first identification sensor 220 and the second identification sensor 240, and identifies the user by comparing the waveforms detected with the ECG pattern of the user (of S 100), which has been registered in advance, by using an ECG pattern analysis solution 740.

[0071] If the ECG pattern of the user coincides with the ECG pattern of the registrant in the identification result, as determined in S300, user authentication is performed in S400, and the authentication information is stored in the security memory 720 in the processor 700 or the external memory 722 in S500. If the ECG pattern of the user does not coincide with the ECG pattern of the registrant in the identification result, as determined in S300, authentication is denied and the user is considered an non-registrant in S600.

[0072] In S700, whether the user continues to wear the electronic device 100 is checked. Specifically, the processor 700 detects the wearing state of the electronic device 100 with the coupling detection sensor 620 and continuously monitors the wearing state of the electronic device 100 via the HRM sensor 300, as shown in S650. The authentication information stored in the security memory 720 or the external memory 722 is eliminated or discarded, automatically or selectively, if the electronic device 100 is released or not mounted or worn in S800. Thereafter, accordingly, the user may perform a new user authentication operation, thus repeating S100.

[0073] Differently, if the user continues to wear the electronic device 100, the ECG authentication is available and accordingly, may be variously used in association with applications in S1000.

[0074] According to an embodiment of the present disclosure, in S900, the processor 700 checks whether the conductive body 642 of the band 140 is cut off through a detection signal of the wrongful use prevention sensor 640 even though the user continues to wear the electronic device 100. The processor 700 also may eliminate or discard, automatically or selectively, the ECG authentication information stored in the security memory 720 or the external memory 722 in S800, if it is determined that the band 140 is cut off in S900. Otherwise, the processor 700 may in S1000 variously use the ECG authentication in association with an application 790 (of FIG. 5) because the ECG authentication remains to be available if it is identified that the user continues to wear the electronic device 100 while the band 140 is not cut off.

[0075] FIGS. 7 and 8 exemplify a process of automatically releasing a door lock through an ECG authentication of the electronic device 100 having a user identification function according to an embodiment of the present disclosure, and an application (e.g., the application 790 of FGI. 5) for the automatic login of a PC or a smartphone.

[0076] Referring to FIGS. 7 and 8, if the user continues to wear the electronic device 100, the user may enter a building without inputting a separate key or a password using the user authentication information stored in the security memory 720 or the external memory 722, and may automatically log in a PC or a smartphone by linking the user authentication information to a terminal or a service through Bluetooth or Wi-Fi Direct.

[0077] Furthermore, although not exemplified in detail, an application associated with an ECG authentication may unlock a vehicle without using a separate smart key, may open a safe without inputting a separate key or a password, may immediately perform a payment without a separate approval through a Point-Of-Sales (POS) or the like, and may be applied to other various applications.

[0078] As described above, according to various embodiments of the present disclosure, because a user identifying ECG sensor and a wearing state detecting HRM sensor are simultaneously mounted, an authentication may be made as long as the user wears the electronic device through the user identifying ECG sensor

without using a separate user identifying means, and an authentication effect can be maintained through the wearing state detecting HRM sensor.

[0079] In addition, through the fact that the user is not changed as long as the user does not release the wearing state, the user authentication can continue the authentication effect and can be associated with various applications such as a PC, a smartphone, a door lock, a vehicle, a safe, a payment, and the like without an additional user authentication.

[0080] While the present disclosure has been shown and described with reference to various embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the scope of the present disclosure as defined by the appended claims.

Claims

1. An electronic device (100) comprising:

a body (120);
a band (140) having a first end (162) and a second end (166);
a user identification unit (500) that is configured to detect a body signal of the user and to process authentication of the user, wherein the user identification unit comprises an electrocardiogram, ECG, sensor(200) that identifies the user through ECG sensing;
an in-use detection unit (600) that is configured to detect the body signal of the user and to check whether the user uses the electronic device;
a coupling detection sensor (620) configured to detect that the first end is coupled to the second end,
a processor (700) that is configured to authenticate the user according to the body signal detected by the user identification unit and the body signal detected by the in-use detection unit, and
a memory (720,722) that is configured to store ECG authentication information of the user authenticated by the processor,
wherein the in-use detection unit comprises a heart rate monitor, HRM, sensor (300), the HRM sensor being configured to detect that the user wears the electronic device,
characterized in that
the processor is configured to eliminate the ECG authentication information of the user stored in the memory according to a detection signal of the coupling detection sensor or the in-use detection unit when the electronic device is taken off from the user.

2. The electronic device of claim 1, further comprising a body, and wherein the ECG sensor comprises a first identification sensor and a second identification sensor, and the first and second identification sensors are attached to different surfaces of the body.

3. The electronic device of claim 2, wherein the first identification sensor generates a waveform according to an ECG pattern of heartbeats of the user, and the second identification sensor generates a waveform according to an ECG pattern when the user makes various payments or performs an authentication in a login process, and
wherein the first identification sensor is located in a button on the body to be operated by pushing the button, and completes a human body communication loop.

4. The electronic device of claim 1, wherein the HRM sensor is configured to detect (S650) a wearing state of the electronic device by the user in a photoplethysmography, PPG, method.

5. The electronic device of claim 1, wherein the processor is configured to record (S200) a waveform detected through the user identification unit, to compare (S300) the waveform with an ECG pattern of the user yielding in a comparison result, the ECG pattern being registered in advance, by using an ECG pattern analysis solution, and to process (S400) a user authentication for the electronic device by identifying the user according to the comparison result.

6. The electronic device of claim 1, the coupling detection sensor (620) that is configured to detect (S650) whether the body is maintained at a wearing location of the user.

7. The electronic device of claim 6, wherein the processor is configured to eliminate (S800) the ECG authentication information of the user through ECG sensing stored in the memory according to a detection signal of at least one of the coupling detection sensor and the in-use detection unit.

8. The electronic device of claim 1, wherein if the in-use detection unit of the electronic device is configured to determine (S650) that the electronic device is being worn by the user after the processor authenticates (S400) the user resulting in an authentication of the user, the authentication of the user is configured to be used in association with an application.

9. The electronic device of claim 1, wherein the body further comprises a wrongful use prevention sensor (640) that is located at a wearing position of the user, the wrongful use prevention sensor being a conductive body (642) that is embedded in the band.

10. A user authentication method for use with an electronic device having a body (120) and a band (140), the method comprising:

registering (S100) an electrocardiogram, ECG, pattern of a user resulting in a registered ECG pattern;
sensing an ECG pattern of the user;
comparing (S300) the registered ECG pattern and the ECG pattern of the user sensed, and identifying the user;
if the the registered ECG pattern coincides with the ECG pattern of the user sensed based on the identification, authenticating the user and storing (S500) ECG authentication information; and
checking (S650) a wearing state of the body by a coupling detection sensor detecting that a first end of the band is coupled to a second end of the band and a heart rate monitor, HRM, sensor detecting that the user wears the electronic device, and
eliminating the ECG authentication information stored according to a detection signal of the coupling detection sensor or an in-use detection unit when the electronic device is taken off from the user.

11. The user authentication method of claim 10, wherein if the wearing state of the body is released or the body is not worn, the ECG authentication information that is stored is discarded, and
when the wearing state of the body is identified, the ECG authentication information that is stored is discarded (S800)via detecting the wrongful use of the body.

12. The user authentication method of claim 10, wherein if the wearing state of the body is identified, the authentication of the user is used in association with an application.

13. The user authentication method of claim 10, wherein the user is identified by comparing (S300) the registered ECG pattern of the user with the ECG pattern of the user sensed using an ECG pattern analysis solution.

Patentansprüche

1. Elektronische Vorrichtung (100) umfassend:

einen Körper (120);
ein Band (140), das ein erstes Ende (162) und ein zweites Ende (166) aufweist;
eine Benutzeridentifikationseinheit (500), die konfiguriert ist, um ein Körpersignal des Benutzers zu erkennen und die Authentifizierung des Benutzers zu verarbeiten, wobei die Benutzeridentifikationseinheit einen Elektrokardiogramm (ECG) -Sensor (200) umfasst, der den Benutzer durch ECG-Erfassung identifiziert;
eine verwendete Erkennungseinheit (600), die konfiguriert ist, um das Körpersignal des Benutzers zu erkennen und zu prüfen, ob der Benutzer die elektronische Vorrichtung verwendet;
einen Kupplungserkennungssensor (620), der konfiguriert ist, um zu erkennen, dass das erste Ende mit dem zweiten Ende gekoppelt ist,
einen Prozessor (700), der konfiguriert ist, um den Benutzer gemäß dem Körpersignal, das von der Benutzer-Identifizierungseinheit erkannt wird und dem Körpersignal, das durch die verwendete Erkennungseinheit erkannt wird, zu authentifizieren und
einen Speicher (720,722), der konfiguriert ist, um ECG-Authentifizierungsinformationen des Benutzers, der durch den Prozessor authentifiziert wurde, zu speichern,
wobei die verwendete Erkennungseinheit einen Herzfrequenzmessgerät (HRM)- Sensor (300) umfasst, wobei der HRM-Sensor konfiguriert ist, um zu erkennen, dass der Benutzer die elektronische Vorrichtung trägt,
dadurch gekennzeichnet, dass
der Prozessor konfiguriert ist, um die ECG-Authentifizierungsinformationen des Benutzers, die in dem Speicher gespeichert sind, gemäß einem Erkennungssignal des Kupplungserkennungssensors oder der verwendeten Erkennungseinheit zu beseitigen, wenn die elektronische Vorrichtung von dem Benutzer abgenommen wird.

2. Elektronische Vorrichtung nach Anspruch 1, ferner umfassend einen Körper, und wobei der ECG-Sensor einen ersten Identifizierungssensor und einen zweiten Identifizierungssensor umfasst, und die ersten und zweiten Identifizierungssensoren an verschiedenen Oberflächen des Körpers befestigt sind.

3. Elektronische Vorrichtung nach Anspruch 2, wobei der erste Identifizierungssensor eine Wellenform gemäß einem ECG-Muster von Herzschlägen des Benutzers erzeugt, und der zweite Identifizierungssensor eine Wellenform gemäß einem ECG-Muster erzeugt, wenn der Benutzer verschiedene Zahlungen leistet oder eine Authentifizierung in einem Login-Verfahren vornimmt, und
wobei sich der erste Identifizierungssensor in einem Knopf am Körper befindet, der durch Drücken des Knopfes betätigt werden soll, und einen Kommunikations-Kreislauf des menschlichen Körpers vervollständigt.

4. Elektronische Vorrichtung nach Anspruch 1, wobei der HRM-Sensor konfiguriert ist, um ein Tragezustand der elektronischen Vorrichtung vom Benutzer in einem Photoplethysmografie (PPG) -Verfahren zu erkennen (S650).

5. Elektronische Vorrichtung nach Anspruch 1, wobei der Prozessor konfiguriert ist, um eine Wellenform, die durch die Benutzeridentifikationseinheit erkannt wird, aufzuzeichnen (S200), um die Wellenform mit einem ECG-Muster des Benutzers zu vergleichen (S300), das ein Vergleichsergebnis ergibt, wobei das ECG-Muster im voraus registriert wird, unter Verwendung von einer ECG- Musteranalyselösung, und um eine Benutzerauthentifizierung für die elektronische Vorrichtung durch Identifizierung des Benutzers gemäß dem Vergleichsergebnis zu verarbeiten (S400).

6. Elektronische Vorrichtung nach Anspruch 1, wobei der Kupplungserkennungssensor (620) konfiguriert ist, um zu erkennen (S650), ob der Körper auf einem Tragepunkt des Benutzers gehalten wird.

7. Elektronische Vorrichtung nach Anspruch 6, wobei der Prozessor konfiguriert ist, um die ECG-Authentifizierungsinformationen des Benutzers, die im Speicher über ECG-Erkennung gespeichert sind, gemäß einem Erkennungssignal eines Kupplungserkennungssensors und/oder der verwendeten Erfassungseinheit zu beseitigen (S800).

8. Elektronische Vorrichtung nach Anspruch 1, wobei, wenn die verwendete Erfassungseinheit der elektronischen Vorrichtung konfiguriert ist, um zu bestimmen (S650), dass die elektronische Vorrichtung vom Benutzer getragen wird, nachdem der Prozessor den Benutzer authentifiziert (S400), was zu einer Authentifizierung des Benutzers führt, die Authentifizierung des Nutzers konfiguriert ist, um in Verbindung mit einer Anwendung verwendet zu werden.

9. Elektronische Vorrichtung nach Anspruch 1, wobei der Körper des Weiteren einen Sensor zur Verhinderung einer missbräuchlichen Benutzung (640) umfasst, der sich an einer Trageposition des Benutzers befindet, wobei der Sensor zur Verhinderung einer missbräuchlichen Benutzung ein leitfähiger Körper (642) ist, der in dem Band eingebettet wird.

10. Benutzerauthentifizierungsverfahren zum Einsatz in einer elektronischen Vorrichtung, die einen Körper (120) und ein Band (140) aufweist, wobei das Verfahren Folgendes umfasst:

    Registrieren (S100) eines Elektrokardiogramm (ECG)-Musters eines Benutzers, das ein registriertes ECG-Muster ergibt;
    Erfassen eines ECG-Musters des Benutzers;
    Vergleichen (S300) des registrierten ECG-Musters und des ECG-Musters des erfassten Benutzers, und Identifizieren des Benutzers;

        wenn das registrierte ECG-Muster mit dem ECG-Muster des abgetasteten Benutzers basierend auf der Identifizierung übereinstimmt, Authentifizieren des Benutzers und Speichern (S500) der ECG-Authentifizierungsinformationen; und
        Kontrollieren (S650) eines Tragezustands des Körpers durch einen Kupplungserkennungssensor, der erkennt, dass ein erstes Ende des Bandes mit einem zweiten Ende des Bandes verbunden ist und einen Herzfrequenzmessgerät (HRM)-Sensor, der erfasst, dass der Benutzer die elektronische Vorrichtung trägt, und
        Beseitigen der ECG-Authentifizierungsinformationen, die gemäß einem Erkennungssignal des Kupplungserkennungssensors oder einer verwendeten Erkennungseinheit gespeichert sind, wenn die elektronische Vorrichtung von dem Benutzer abgelegt wird.

11. Benutzerauthentifizierungsverfahren nach Anspruch 10, wobei, wenn der Tragezustand des Körpers freigegeben wird oder der Körper nicht getragen wird, die ECG-Authentifizierungsinformationen, die gespeichert sind, verworfen werden, und wenn der Tragezustand des Körpers identifiziert wird, die gespeicherten ECG-Authentifizierungsinformationen verworfen (S800) werden, indem die missbräuchliche Verwendung des Körpers erkannt wird.

12. Benutzerauthentifizierungsverfahren nach Anspruch 10, wobei, wenn der Tragezustand des Körpers identifiziert wird, die Authentifizierung des Benutzers in Verbindung mit einer Anwendung benutzt wird.

13. Benutzerauthentifizierungsverfahren nach Anspruch 10, wobei der Benutzer identifiziert wird, indem das registrierte ECG-Muster des Benutzers mit dem ECG-Muster des erfassten Benutzers unter Verwendung einer ECG-Musteranalyselösung verglichen wird (S300).

Revendications

1. Dispositif électronique (100) comprenant :

    un corps (120) ;
    une bande (140) ayant une première extrémité (162) et une deuxième extrémité (166) ;

une unité d'identification d'utilisateur (500) qui est configurée pour détecter un signal du corps de l'utilisateur et pour traiter l'authentification de l'utilisateur, où l'unité d'identification d'utilisateur comprend un capteur d'électrocardiogramme, ECG, (200) qui identifie l'utilisateur par la détection d'ECG ;
une unité de détection d'utilisation (600) qui est configurée pour détecter le signal du corps de l'utilisateur et pour contrôler si l'utilisateur utilise le dispositif électronique ;
un capteur de détection de couplage (620) configuré pour détecter que la première extrémité est couplée à la deuxième extrémité,
un processeur (700) qui est configuré pour authentifier l'utilisateur selon le signal du corps détecté par l'unité d'identification d'utilisateur et le signal du corps détecté par l'unité de détection d'utilisation, et
une mémoire (720, 722) qui est configurée pour stocker des informations d'authentification d'ECG de l'utilisateur authentifié par le processeur,
où l'unité de détection d'utilisation comprend un capteur de moniteur de fréquence cardiaque, HRM, (300), le capteur de HRM étant configuré pour détecter que l'utilisateur porte le dispositif électronique,
caractérisé en ce que
le processeur est configuré pour éliminer les informations d'authentification d'ECG de l'utilisateur stockées dans la mémoire selon un signal de détection du capteur de détection de couplage ou de l'unité de détection d'utilisation lorsque le dispositif électronique est retiré de l'utilisateur.

2. Dispositif électronique selon la revendication 1, comprenant en outre un corps, et où le capteur d'ECG comprend un premier capteur d'identification et un deuxième capteur d'identification, et les premier et deuxième capteurs d'identification sont fixés à des surfaces différentes du corps.

3. Dispositif électronique selon la revendication 2, où le premier capteur d'identification génère une forme d'onde selon un motif d'ECG de battements cardiaques de l'utilisateur, et le deuxième capteur d'identification génère une forme d'onde selon un motif d'ECG lorsque l'utilisateur fait divers paiements ou effectue une authentification dans un processus d'ouverture de session, et
où le premier capteur d'identification est situé dans un bouton sur le corps à être activé en poussant le bouton, et complète une boucle de communication de corps humain.

4. Dispositif électronique selon la revendication 1, où le capteur de HRM est configuré pour détecter (S650) un état de port du dispositif électronique par l'utilisateur dans un procédé de photopléthysmographie, PPG.

5. Dispositif électronique selon la revendication 1, où le processeur est configuré pour enregistrer (S200) une forme d'onde détectée par l'intermédiaire de l'unité d'identification d'utilisateur, pour comparer (S300) la forme d'onde avec un motif d'ECG de l'utilisateur donnant lieu à un résultat de comparaison, le motif d'ECG étant enregistré à l'avance, en utilisant une solution d'analyse de motif d'ECG, et pour traiter (S400) une authentification d'utilisateur pour le dispositif électronique en identifiant l'utilisateur selon le résultat de comparaison.

6. Dispositif électronique selon la revendication 1, où le capteur de détection de couplage (620) est configuré pour détecter (S650) si le corps est maintenu à une position de port de l'utilisateur.

7. Dispositif électronique selon la revendication 6, où le processeur est configuré pour éliminer (S800) les informations d'authentification d'ECG de l'utilisateur à travers la détection d'ECG stockés dans la mémoire selon un signal de détection d'au moins l'un parmi le capteur de détection de couplage et l'unité de détection d'utilisation.

8. Dispositif électronique selon la revendication 1, où, si l'unité de détection d'utilisation du dispositif électronique est configurée pour déterminer (S650) que le dispositif électronique est porté par l'utilisateur après que le processeur a authentifié (S400) l'utilisateur donnant lieu à une authentification de l'utilisateur, l'authentification de l'utilisateur est configurée pour être utilisé en association avec une application.

9. Dispositif électronique selon la revendication 1, où le corps comprend en outre un capteur de prévention d'utilisation incorrecte (640) qui est situé à une position de port de l'utilisateur, le capteur de prévention d'utilisation incorrecte étant un corps conducteur (642) qui est intégré dans la bande.

10. Procédé d'authentification d'utilisateur à être utilisé avec un dispositif électronique ayant un corps (120) et une bande (140), le procédé comprenant :

enregistrer (S100) un motif d'électrocardiogramme, ECG, d'un utilisateur donnant lieu à un motif d' ECG enregistré ;
détecter un motif d'ECG de l'utilisateur ;
comparer (S300) le motif d'ECG enregistré et le motif d'ECG de l'utilisateur détecté et identifier l'utilisateur ;

si le motif d'ECG enregistré coïncide avec le motif d'ECG de l'utilisateur détecté sur la base de l'identification, authentifier l'utilisateur et stocker (S500) les informations d'authentification d'ECG ; et

vérifier (S650) un état de port du corps par un capteur de détection de couplage détectant qu'une première extrémité de la bande est couplée à une deuxième extrémité de la bande et un capteur de moniteur de fréquence cardiaque, HRM, détectant que l'utilisateur porte le dispositif électronique, et

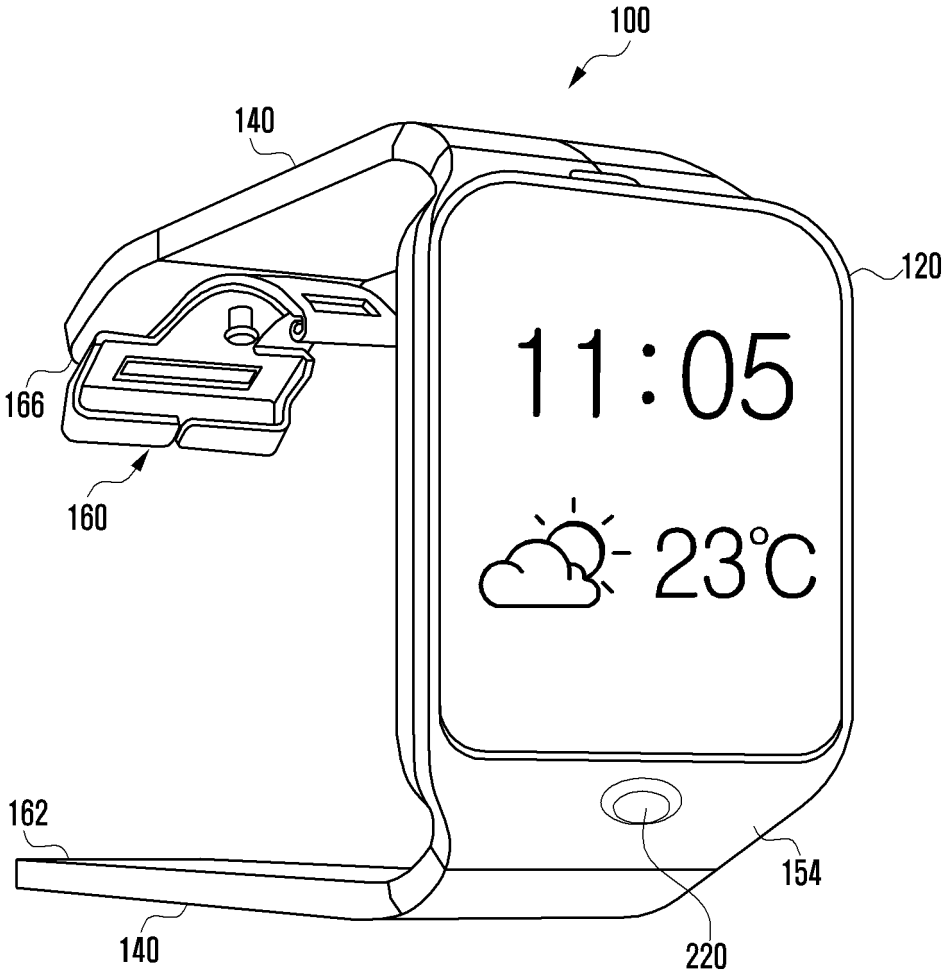
éliminer les informations d'authentification d'ECG stockées selon un signal de détection du capteur de détection de couplage ou d'une unité de détection d'utilisation lorsque le dispositif électronique est retiré de l'utilisateur.

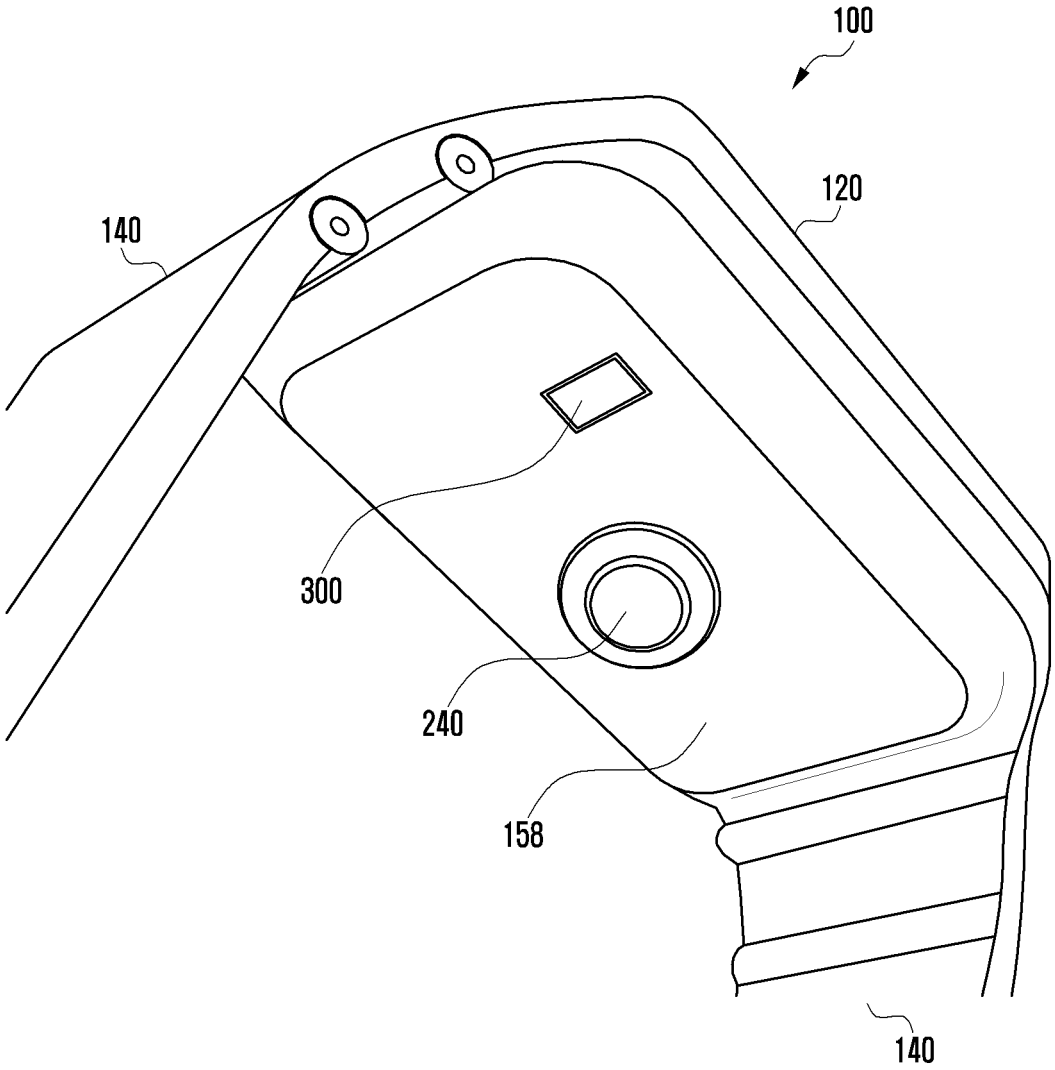
11. Procédé d'authentification d'utilisateur selon la revendication 10, où, si l'état de port du corps est libéré ou le corps n'est pas porté, les informations d'authentification d'ECG qui sont stockées sont rejetées, et

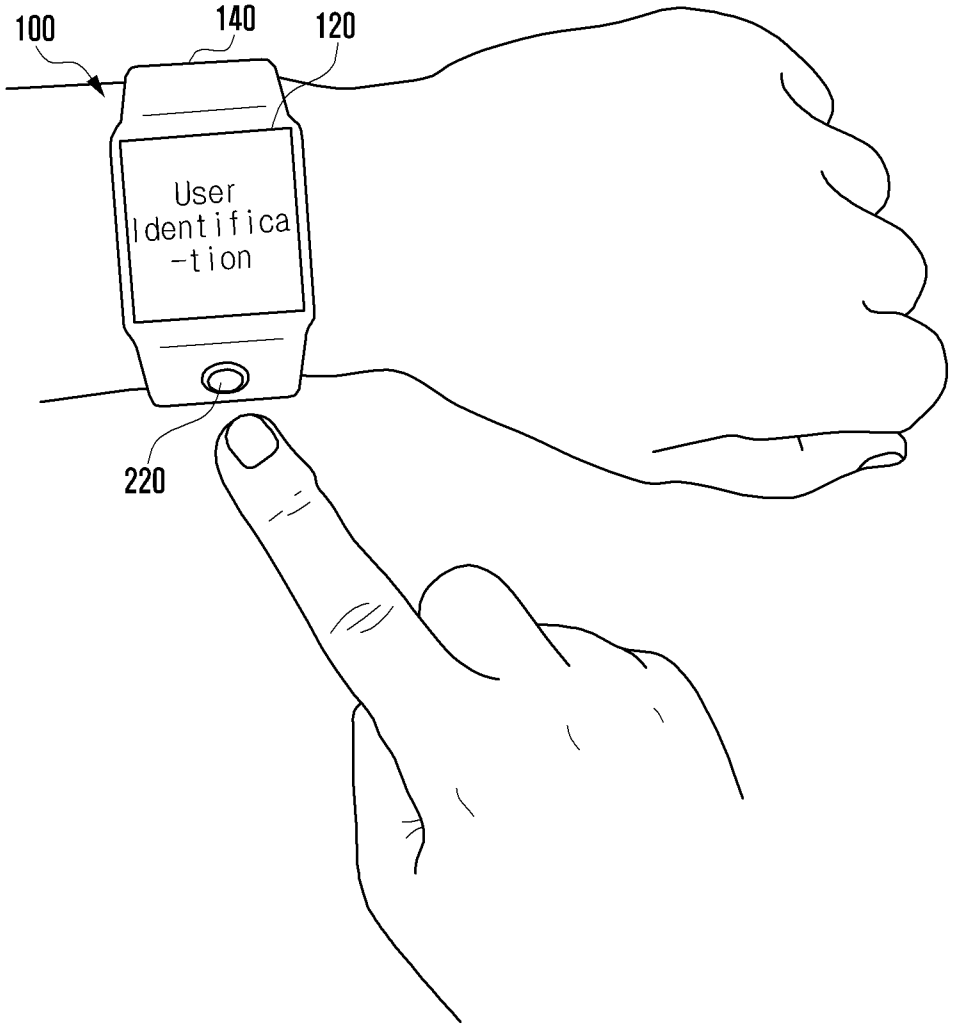
lorsque l'état de port du corps est identifié, les informations d'authentification d'ECG qui sont stockées sont rejetées (S800) par la détection de l'utilisation incorrecte du corps.

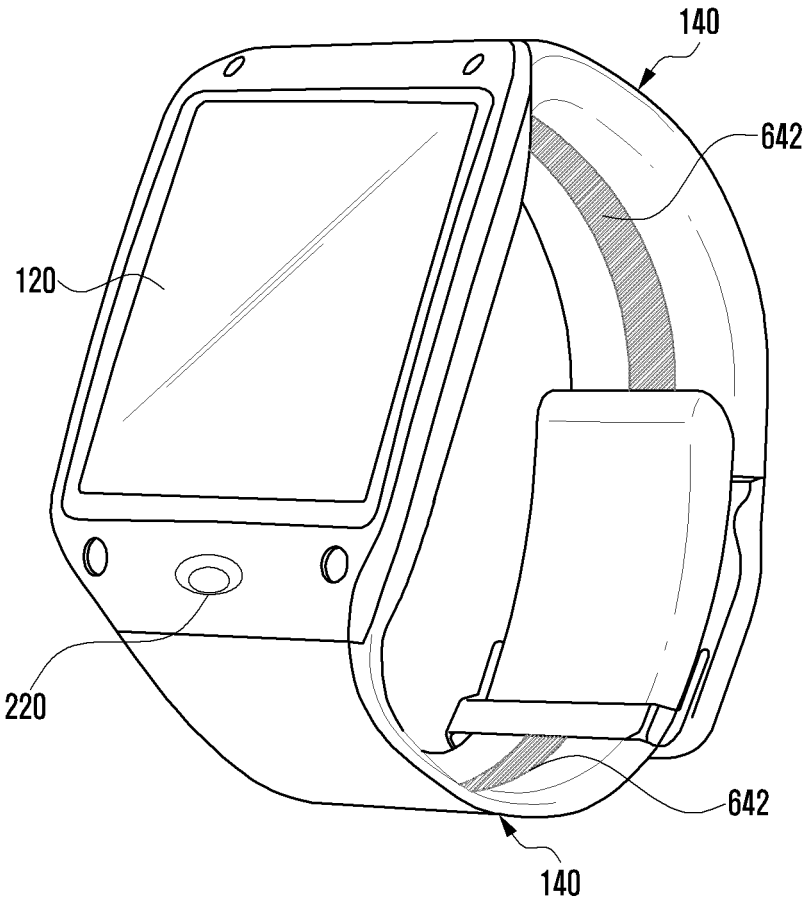
12. Procédé d'authentification d'utilisateur selon la revendication 10, où, si l'état de port du corps est identifié, l'authentification de l'utilisateur est utilisée en association avec une application.

13. Procédé d'authentification d'utilisateur selon la revendication 10, où l'utilisateur est identifié en comparant (S300) le motif d'ECG enregistré de l'utilisateur avec le motif d'ECG de l'utilisateur détecté en utilisant une solution d'analyse de motif d'ECG.


100
140
120
11:05
23°C
166
160
162
154
140
220


100
120
140
300
240
158
140


100
140
120
User
Identifica
-tion
220


140
642
120
220
642
140

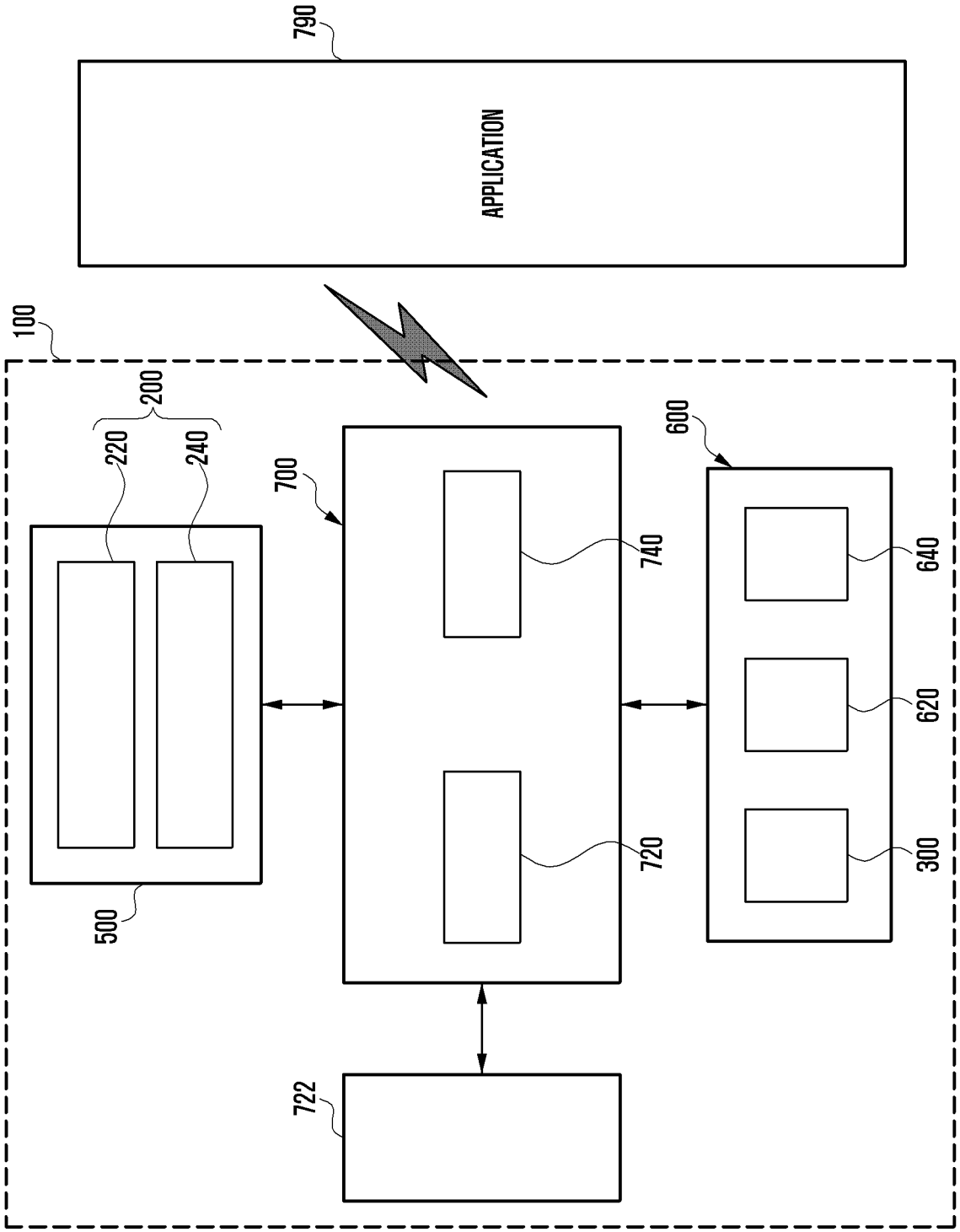

790
APPLICATION
100
200
220
240
700
740
600
640
620
300
720
500
722

FIG. 5

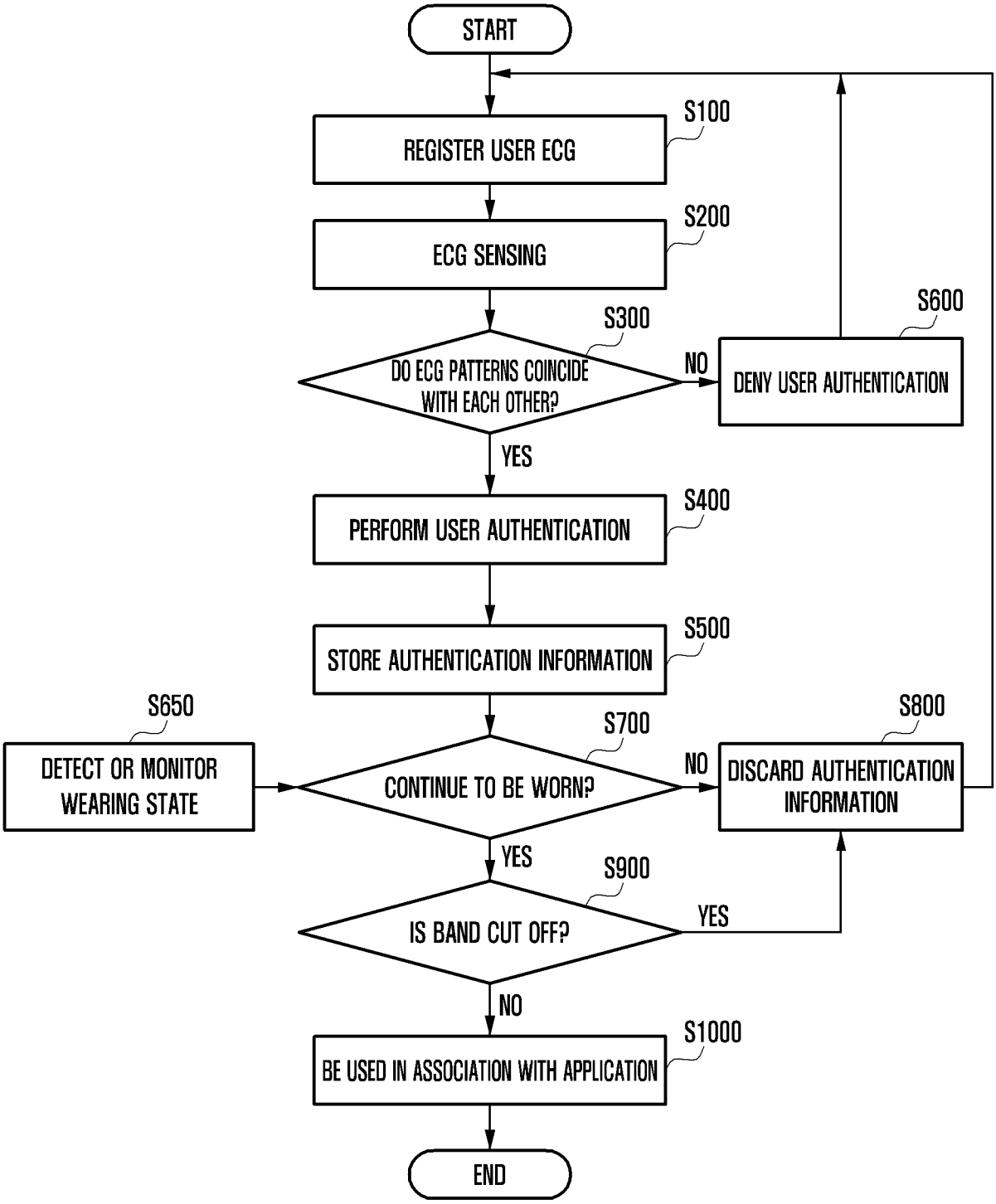

START
S100
REGISTER USER ECG
S200
ECG SENSING
S300
DO ECG PATTERNS COINCIDE WITH EACH OTHER?
NO
S600
DENY USER AUTHENTICATION
YES
S400
PERFORM USER AUTHENTICATION
S500
STORE AUTHENTICATION INFORMATION
S650
DETECT OR MONITOR WEARING STATE
S700
CONTINUE TO BE WORN?
NO
S800
DISCARD AUTHENTICATION INFORMATION
YES
S900
IS BAND CUT OFF?
YES
NO
S1000
BE USED IN ASSOCIATION WITH APPLICATION
END

FIG. 6

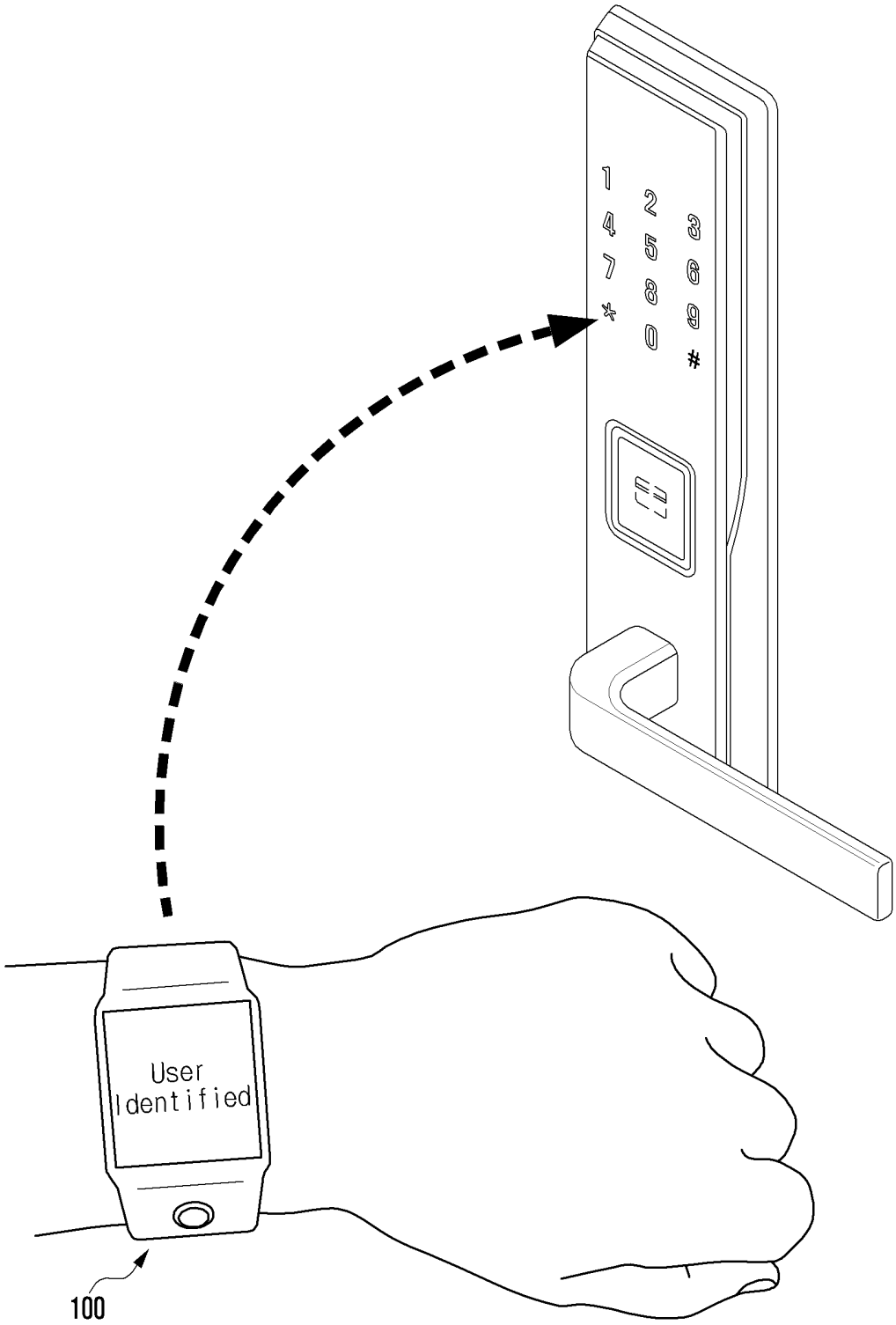


FIG. 7

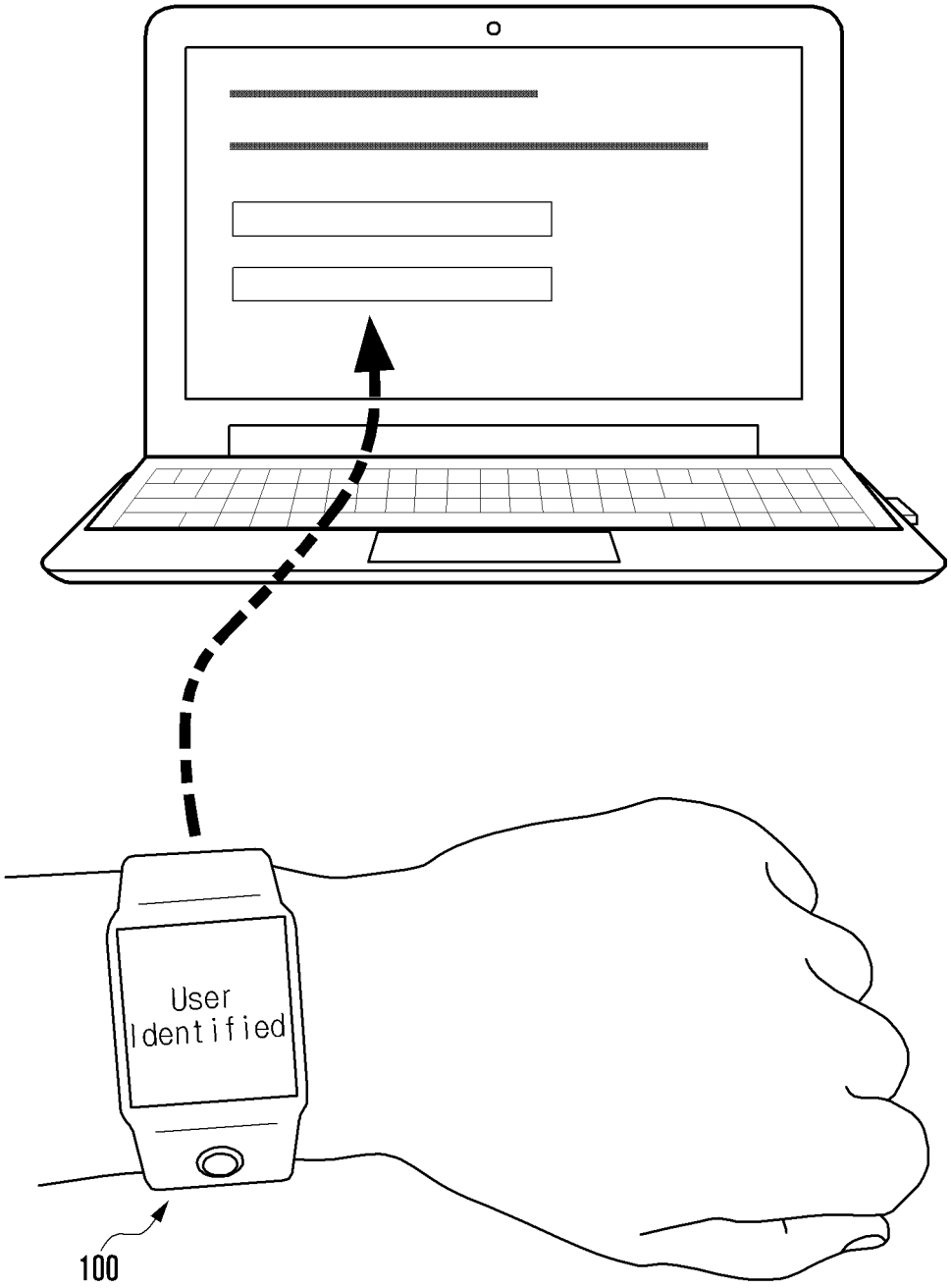


FIG. 8

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.

Non-patent literature cited in the description

- *Bionym: ''nymi,* 19 November 2013, URL:https://www.nymi.com/wp-content/uploads/2013/1l1NymiWhitePaper-1.pdf **[0006]**

专利名称(译)	具有用户识别功能和用户认证方法的电子设备		
公开(公告)号	EP3037999B1	公开(公告)日	2020-06-17
申请号	EP2015202358	申请日	2015-12-23
[标]申请(专利权)人(译)	三星电子株式会社		
申请(专利权)人(译)	三星电子有限公司		
当前申请(专利权)人(译)	SAMSUNG ELECTRONICS CO.，LTD.		
[标]发明人	YOO SUNGSIK YU YONGJU		
发明人	YOO, SUNGSIK YU, YONGJU		
IPC分类号	G06F21/34 G06F21/35 H04L29/06 H04W12/06 A61B5/0404 A61B5/0452 A61B5/00		
CPC分类号	G06F21/32 G06F21/34 A61B5/0404 A61B5/04525 A61B5/117 A61B5/681 G06F21/35 H04L63/0853 H04L63/0861 H04W12/003 H04W12/06 Y10S707/99939 G07C9/257 G07C9/26		
代理机构(译)	NEDERLANDSCH OCTROOIBUREAU		
优先权	1020140188556 2014-12-24 KR		
其他公开文献	EP3037999A1		
外部链接	Espacenet		

摘要(译)

提供了具有用户识别功能的电子设备和用户认证方法。 所述电子设备包括：主体； 用户识别单元，其检测用户的身体信号并处理用户的认证；使用中检测单元检测用户的身体信号并检查用户是否使用电子设备； 处理器根据用户标识单元和使用中检测单元的检测信号对用户进行认证。