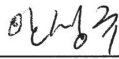


VERIFICATION OF TRANSLATION

I, Seong-Gyu AHN of c/o Jeongdong Building, 17F, 21-15 Jeongdong-gil, Jung-gu, Seoul 04518, Republic of Korea, hereby declare that I am conversant in the Korean and the English languages and that I am the translator of the document attached and certify that to the best of my knowledge and belief the following is a true and correct English translation of the Korean Patent No. 10-2136836.



Signed by Seong-Gyu AHN

Date: 2023. 1. 18

(19) Korean Intellectual Property Office (KR)	(45) Publication Date: August 13, 2020
(12) Registration Patent Publication (B1)	(11) Registration No: 10-2136836
	(24) Registration Date: July 16, 2020
(51) Int. Cl. G06F 21/32 (January 2013) G06F 21/44 (January 2013)	(73) Patentee: SAMSUNG ELECTRONICS CO., LTD. 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do, Republic of Korea
(21) Application No: 10-2013-0107833	(72) Inventors:
(22) Filing Date: September 9, 2013	CHOI, Chang Mok
Examination Request Date: September 4, 2018	No. 802, Nonhyeon-ro 111-gil 3, Gangnam-gu, Seoul, Republic of Korea (Nonhyeon-dong, HumanSpaceVill)
(65) Laid-Open No: 10-2015-0029105	KIM, Sang Joon
(43) Laid-Open Date: March 18, 2015	321-204, Dongtanmunhwaseo-ro 39, Hwaseong-si, Gyeonggi-do, Republic of Korea (Bansong-dong, Sibum Daunmaeul PoscoTheSharp Apartment)
(56) Prior Arts	YOON, Seung Keun
KR200120590 Y1*	10-1303, Seochojungang-ro 200, Seocho-gu, Seoul, Republic of Korea Seocho-dong, Sampoong Apartment.)
US06720860 B1*	(74) Agent:
US20060215883 A1*	MUHANN PATENT & LAW FIRM
US20100331649 A1*	
US20130159705 A1*	
* are the documents referred to by the Examiner	

Total claims: 26

Examiner: Moon, Nam Du

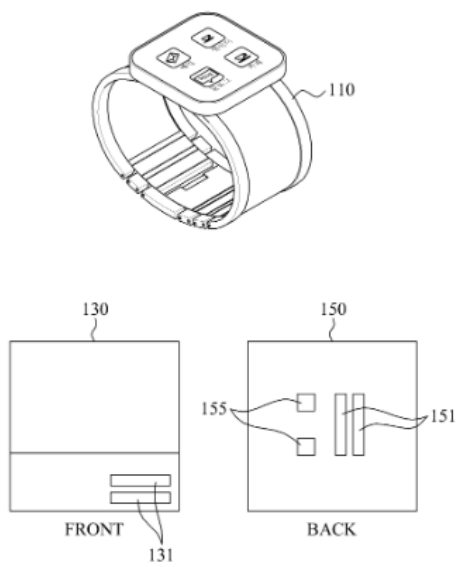
(54) Title of Invention: **WEARABLE DEVICE PERFORMING USER AUTHENTICATION USING BIO-SIGNALS AND AUTHENTICATION METHOD OF THE SAME**

(57) Abstract

A wearable device is disclosed. The wearable device includes a first sensor configured to detect a first biosignal generated in response to a gesture performed by a user, a second sensor configured to detect a second biosignal of the user, a memory configured to store, with respect to at least one user, at least one information representing directly or indirectly the first biosignal and the second biosignal, and a processor configured to initiate user authentication by determining whether the first biosignal detected by the first sensor corresponds to the information stored in the memory, and authenticate the user by comparing the second biosignal detected by the second sensor with the information stored in the memory.

Representative Figure – Fig. 1

[Translation]



Claims

[Claim 1]

A wearable device, comprising: a first sensor configured to detect a first biosignal generated in response to a gesture performed by a user; a second sensor configured to detect a second biosignal of the user; a memory configured to store, with respect to at least one user, at least one piece of information directly or indirectly representing the first biosignal and the second biosignal; and a processor configured to initiate user authentication by determining whether the first biosignal detected by the first sensor corresponds to the information stored in the memory, and authenticate the user by comparing the second biosignal detected by the second sensor with the information stored in the memory, wherein the second biosignal is unique to the user, and the second biosignal and the first biosignal are different to each other.

[Claim 2]

The device of claim 1, wherein the first biosignal is generated in response to a muscle movement performed by the user to input the gesture.

[Claim 3]

The device of claim 2, wherein the first biosignal is at least one of an electromyogram (EMG) signal generated before and after the muscle movement, a light signal penetrating a muscle of the user, and a force signal generated by the muscle of the user.

[Claim 4]

The device of claim 1, wherein the second biosignal is at least one of an electrocardiogram (ECG) signal, a photoplethysmogram (PPG) signal, a voice of the user, and an impedance signal generated by a body of the user.

[Claim 5]

The device of claim 1, wherein the information stored in the memory comprises at least one piece of feature point information obtained by performing signal processing on the first biosignal and the second biosignal.

[Claim 6]

The device of claim 1, wherein the information stored in the memory is encoded.

[Claim 7]

The device of claim 1, wherein the processor is configured to: when comparing the second biosignal detected by the second sensor to the information stored in the memory, operate based on a predetermined error range.

[Claim 8]

The device of claim 1, further comprising: an initial authenticator configured to receive the gesture and the second biosignal from the user; and store, in the memory, the first biosignal corresponding to the received gesture, and the second biosignal.

[Claim 9]

The device of claim 1, wherein the memory is further configured to store access right information on one or more functions executable in the wearable device; and in response to a command to execute the functions being input to the wearable device by the user, the processor is configured to read, by referring to the memory, the access right information on the functions, and provide, to the user, at least one of a visual feedback, an auditory feedback, and a tactile feedback based on the access right information.

[Claim 10]

The device of claim 9, wherein the feedback is a request for the user authentication.

[Claim 11]

The device of claim 1, further comprising: a wearing detection sensor configured to detect whether the wearable device is detached from the user, wherein the processor is configured to control the user authentication to be invalid in response to the wearable device being detected to be detached from the user.

[Claim 12]

The device of claim 11, wherein the wearing detection sensor is configured to be connected to the wearable device and detect a mechanical movement of a band attached to a portion of a body of the user or detect an electrical signal generated by attaching and detaching of the band.

[Claim 13]

The device of claim 1, wherein the memory is further configured to store device setting information corresponding to each of the at least one user; and in response to the user being authenticated, the processor is further configured to read, by referring to the memory, the device setting information of the authenticated user, and provide a user interface based on the device setting information.

[Claim 14]

The device of claim 1, wherein the wearable device is a watch-type smartphone.

[Claim 15]

A wearable device, comprising: a first sensor configured to detect a first biosignal generated in response to a muscle movement performed by a user to input a gesture ; a second sensor configured to detect a second biosignal of the user, the second biosignal being unique to the user, the second biosignal and the first biosignal being different to each other, and the second biosignal being at least one of an electrocardiogram (ECG) signal, a photoplethysmogram (PPG) signal, a voice of the user, and an impedance signal generated by a body of the user; a memory configured to store, with respect to at least

one user, at least one piece of information directly or indirectly representing the first biosignal and the second biosignal; and a processor configured to trigger user authentication by determining whether the first biosignal detected by the first sensor corresponds to the information stored in the memory, and authenticate the user by comparing the second biosignal detected by the second sensor with the information stored in the memory.

[Claim 16]

A user authentication method of a wearable device, the method comprising: detecting a first biosignal generated in response to a gesture performed by a user; detecting a second biosignal of the user; storing, in a memory, with respect to at least one user, at least one piece of information directly or indirectly representing the first biosignal and the second biosignal; initiating user authentication by determining whether the first biosignal detected by a first sensor corresponds to the information stored in the memory; and authenticating the user by comparing the second biosignal detected by a second sensor to the information stored in the memory, wherein the second biosignal is unique to the user, and the second biosignal and the first biosignal are different to each other.

[Claim 17]

The method of claim 16, wherein the information stored in the memory comprises at least one piece of feature point information obtained by performing signal processing on the first biosignal and the second biosignal.

[Claim 18]

The method of claim 16, wherein authenticating the user comprises: comparing the second biosignal detected by the second sensor to the information stored in the memory, based on a predetermined error range.

[Claim 19]

The method of claim 16, further comprising: receiving the gesture and the second biosignal from the user; and storing in the memory the first biosignal corresponding to the received gesture, and the second biosignal.

[Claim 20]

The method of claim 16, wherein storing the at least one piece of information comprises storing access right information on one or more functions executable in the wearable device.

[Claim 21]

The method of claim 20, comprising: receiving a command to execute the functions from the user; in response to receiving the command, reading, by referring to the memory, the access right information on the functions; and providing, to the user, at least one of a visual feedback, an auditory feedback, and a tactile feedback, based on the access right information.

[Claim 22]

The method of claim 16, comprising detecting whether the wearable device is detached from the user; and controlling the user authentication to be invalid in response to the wearable device being detected to be detached from the user.

[Claim 23]

The method of claim 22, wherein detecting whether the wearable device is detached from the user comprises connecting to the wearable device and detecting a mechanical movement of a band attached to a portion of a body of the user or an electrical signal generated by attaching and detaching of the band.

[Claim 24]

The method of claim 16, storing the at least one piece of information comprises further storing device setting information corresponding to each of the at least one user.

[Claim 25]

The method of claim 24, authenticating the user comprises: in response to the user being authenticated, reading, by referring to the memory, the device setting information of the authenticated user; and providing a user interface based on the device setting information.

[Claim 26]

A computer-readable storage medium storing a program comprising instructions to cause a computer to perform the method according to any one of claims 16 to 25.

Technical Field

[1]

The following description relates to a wearable device performing user authentication using biosignals and an authentication method of the wearable device.

Background Art

[2]

Amid the proliferation of smart phones, a variety of mobile devices are being developed, and a wearable type mobile device has been emerging.

[3]

A mobile device may provide a great deal of convenience for modern life. A growing computing power of the mobile device may enable users to handle tasks previously performed using a personal computer (PC). However, due to widespread use of the mobile device, protecting personal information stored on the mobile device, such as, contact information, personal multimedia contents, for example, photos and videos, messages, and financial information has become more important. In a case in which a user loses a

mobile device and another unspecified user uses the mobile device, there is a high risk of personal information of the user being unintentionally exposed. Accordingly, there is a desire for a method of authenticating a user for whom use of a mobile device is intended and controlling an access to various types of personal information stored on the mobile device.

Disclosure of Invention

Solution to Problem

[4]

In one general aspect, there is provided a wearable device, comprising: a first sensor configured to detect a first biosignal generated in response to a gesture performed by a user; a second sensor configured to detect a second biosignal of the user; a memory configured to store, with respect to at least one user, at least one piece of information directly or indirectly representing the first biosignal and the second biosignal; and a processor configured to initiate user authentication by determining whether the first biosignal detected by the first sensor corresponds to the information stored in the memory, and authenticate the user by comparing the second biosignal detected by the second sensor with the information stored in the memory.

[5]

The first biosignal may be generated in response to a muscle movement performed by the user to input the gesture.

[6]

The first biosignal may be at least one of an electromyogram (EMG) signal generated before and after the muscle movement, a light signal penetrating a muscle of the user, and a force signal generated by the muscle of the user.

[7]

The second biosignal may be at least one of an electrocardiogram (ECG) signal, a photoplethysmogram (PPG) signal, a voice of the user, and an impedance signal generated by a body of the user.

[8]

The information stored in the memory may include at least one piece of feature point information obtained by performing signal processing on the first biosignal and the second biosignal.

[9]

When comparing the second biosignal detected by the second sensor to the information stored in the memory, the processor may operate based on a predetermined error range.

[10]

The device may further include an initial authenticator configured to receive the gesture and the second biosignal from the user, and store, in the memory, the first biosignal corresponding to the received gesture, and the second biosignal.

[11]

The memory may be further configured to store access right information on one or more functions executable in the wearable device; and in response to a command to execute the functions being input to the wearable device by the user, the processor is configured to read, by referring to the memory, the access right information on the functions, and provide, to the user, at least one of a visual feedback, an auditory feedback, and a tactile feedback based on the access right information.

[12]

The feedback may be a request for the user authentication.

[13]

The device may further include a wearing detection sensor configured to detect whether the wearable device is detached from the user, wherein the processor is configured to control the user authentication to be invalid in response to the wearable device being detected to be detached from the user.

[14]

The wearing detection sensor may be configured to be connected to the wearable device and detect a mechanical movement of a band attached to a portion of a body of the user or detect an electrical signal generated by attaching and detaching of the band.

[15]

The memory may be further configured to store device setting information corresponding to each of the at least one user; and in response to the user being authenticated, the processor is further configured to read, by referring to the memory, the device setting information of the authenticated user, and provide a user interface based on the device setting information.

[16]

The wearable device may be a watch-type smartphone.

[17]

In another general aspect, there is provided a wearable device, including a first sensor configured to detect a first biosignal generated in response to a muscle movement performed by a user to input a gesture ; a second sensor configured to detect a second biosignal of the user, the second biosignal being unique to the user, the second biosignal and the first biosignal being different to each other, and the second biosignal being at least one of an electrocardiogram (ECG) signal, a photoplethysmogram (PPG) signal, a voice of the user, and an impedance signal generated by a body of the user; a memory configured to store, with

respect to at least one user, at least one piece of information directly or indirectly representing the first biosignal and the second biosignal; and a processor configured to trigger user authentication by determining whether the first biosignal detected by the first sensor corresponds to the information stored in the memory, and authenticate the user by comparing the second biosignal detected by the second sensor with the information stored in the memory.

[18]

In still another general aspect, there is provided a user authentication method of a wearable device, the method including detecting a first biosignal generated in response to a gesture performed by a user; detecting a second biosignal of the user; storing, in a memory, with respect to at least one user, at least one piece of information directly or indirectly representing the first biosignal and the second biosignal; initiating user authentication by determining whether the first biosignal detected by a first sensor corresponds to the information stored in the memory; and authenticating the user by comparing the second biosignal detected by a second sensor to the information stored in the memory.

[19]

The information stored in the memory may comprise at least one piece of feature point information obtained by performing signal processing on the first biosignal and the second biosignal.

[20]

The authenticating the user may comprise comparing the second biosignal detected by the second sensor to the information stored in the memory, based on a predetermined error range.

[21]

The method may further include receiving the gesture and the second biosignal from the user; and storing in the memory the first biosignal corresponding to the received gesture, and the second biosignal.

[22]

The storing the at least one piece of information may comprise storing access right information on one or more functions executable in the wearable device.

[23]

The method may further include receiving a command to execute the functions from the user; in response to receiving the command, reading, by referring to the memory, the access right information on the functions; and providing, to the user, at least one of a visual feedback, an auditory feedback, and a tactile feedback, based on the access right information.

[24]

The method may further include detecting whether the wearable device is detached from the user; and controlling the user authentication to be invalid in response to the wearable device being detected to be detached from the user.

[25]

The detecting whether the wearable device is detached from the user may comprise connecting to the wearable device and detecting a mechanical movement of a band attached to a portion of a body of the user or an electrical signal generated by attaching and detaching of the band.

[26]

The storing the at least one piece of information may comprise further storing device setting information corresponding to each of the at least one user.

[27]

The authenticating the user may comprise: in response to the user being authenticated, reading, by referring to the memory, the device setting information of the authenticated user; and providing a user interface based on the device setting information.

Brief Description of Drawings

[28]

FIG. 1 is a diagram illustrating an example of a wearable device.

FIG. 2 is a block diagram illustrating an example of a wearable device.

FIG. 3 is a block diagram illustrating another example of a wearable device.

FIG. 4 is a flowchart illustrating an example of an authentication method of a wearable device.

FIG. 5 is a flowchart illustrating another example of an authentication method of a wearable device.

FIG. 6 is a flowchart illustrating an example of an authentication method used to provide different functions based on access right information of a user in a wearable device.

FIG. 7 is a flowchart illustrating an example of an operational method used when a wearable device is detached from a user.

FIG. 8 is a diagram illustrating an example of access right information on executable functions, which are stored in a memory of a wearable device.

Mode for the Invention

[29]

The embodiments of the invention are now described with reference to the drawings. However, the invention is not limited by the embodiments. The identical reference symbols designate the identical or similar elements throughout the drawings.

[30]

FIG. 1 is a diagram illustrating an example of a wearable device.

[31]

Referring to FIG. 1, the wearable device may be attachable to, wearable on, and detachable from a portion of a body of a user, using an arm band, a wrist band, and/or other fixing devices known to one of ordinary skill in the art.

[32]

For convenience of description, a surface of the wearable device that is provided with a display visible to the user, for example, a touch display, will be described as a front 130, and another surface of the wearable device that faces the body of the user when the wearable device is attached or worn will be described as a back 150. Based on a design of the wearable device, a mechanically or electrically openable and closeable protector may be disposed on the front 130 to protect the display. In this example, the front 130 may refer to, for example, the surface of the actual display or a surface of the protector, on which a sensor to be described later is provided.

[33]

The wearable device includes a plurality of sensors 131, 151, and 155 provided on the front 130 and the back 150, respectively. The wearable device detects, using at least one of the sensors 131, 151, and 155, a trigger signal triggering a process of user authentication, and initiates the user authentication based on the detected trigger signal.

[34]

The user may generate the trigger signal by performing a predetermined gesture, for example, opening a hand, clenching a fist, rotating a wrist, and/or other gestures known to one of ordinary skill in the art. The wearable device may detect, using at least one of the sensors 131, 151, and 155, the trigger signal generated in response to the gesture. When the trigger signal is detected, the wearable device may initiate the process of the user authentication. According to an example, the gesture may be intentionally inputted by the user while the user is wearing the wearable device, although the gesture may not be performed by the user in a process of putting on the wearable device.

[35]

When the user performs the gesture while the user is wearing the wearable device, the sensor 155 provided on the back 150 of the wearable device may detect a biosignal generated in response to a muscle movement of the user, which is generated by the gesture. The biosignal generated in response to the gesture performed by the user may be the trigger signal used to initiate the user authentication, and be referred to as a first biosignal.

[36]

The first biosignal may include, for example, an electromyogram (EMG) signal generated before and after the muscle movement of the user, a light signal penetrating a muscle of the user, and/or a force signal

generated by the muscle of the user. The first biosignal may be generated only in response to a predetermined gesture input from the user.

[37]

When the process of user authentication with respect to the user is initiated by the first biosignal detected by the sensor 155 provided on the back 150 of the wearable device, the wearable device may authenticate the user, using a second biosignal detected by the sensor 131 provided on the front 130 and/or the sensor 151 provided on the back 150.

[38]

The second biosignal may be unique to each user, and be distinguished from the first biosignal. The second biosignal may include, for example, an electrocardiogram (ECG) signal, a photoplethysmogram (PPG) signal, a voice of the user, and/or an impedance signal generated by a body of the user. Based on implementation, the second biosignal may be unique to each user, and thus, recognizing an iris or a fingerprint may be used to obtain the second biosignal.

[39]

As shown in FIG. 1, the wearable device may be a watch-type smartphone 110. The watch-type smartphone 110 may be an example of the wearable device, and thus, it may be obvious to those skilled in the art that various applications and design modifications may be possible.

[40] (None)

[41]

Described hereinafter is an example of an operation of the wearable device used when the user wears the wearable device around a left wrist.

[42]

The user wearing the wearable device around the left wrist may perform a predetermined gesture, for example, opening a left hand and/or rotating the left hand upwards. Due to the gesture, a first biosignal, as a trigger signal, may be generated, and the wearable device may detect the first biosignal. The wearable device may initiate a process of user authentication in response to the detecting of the first biosignal. The detecting of the first biosignal and the initiating of the process of user authentication may be performed inconsecutively or consecutively in terms of time based on implementation.

[43]

According to an example, the first biosignal generated in response to a muscle movement of the user, due to the gesture, may be detected by the sensor 155 provided on the back 150 of the wearable device. The first biosignal detected by the sensor 155 may be compared to a trigger signal stored in a memory of the wearable device and predetermined by the user. As a result of the comparison, when the first biosignal is

determined to be identical to the trigger signal or within a predetermined error range of the trigger signal, the process of user authentication may be initiated.

[44]

After the process of user authentication is initiated, the user may place a finger of a right hand on the sensor 131 provided on the front 130 of the wearable device, and the wearable device may detect a second biosignal of the user, using the sensor 131. The sensor 151 provided on the back 150 of the wearable device and in contact with skin of the user may also detect the second biosignal in the same way as the sensor 131 provided on the front 130. For example, the sensor 155 may detect an EMG signal of the user, and the sensor 131 and the sensor 151 may detect an ECG signal of the user.

[45]

To detect the ECG signal as an example of the second biosignal, a signal detected in at least two different portions of the body of the user may be needed, and thus, the sensors 131 and 151 are provided on the front 130 and on the back 150, respectively. In an example of detecting a biosignal unique to the user from a body part, for example, a voice of the user and/or an impedance signal generated by the body of the user, aside from the ECG signal, a sensor used to receive the second biosignal may be provided on either the front 130 or the back 150. A number of the sensors used to detect the first biosignal and the second biosignal may vary based on need.

[46]

FIG. 2 is a block diagram illustrating an example of a wearable device 200.

[47]

Referring to FIG. 2, the wearable device 200 may include a first sensor 210, a second sensor 220, a memory 230, and a processor 240.

[48]

The first sensor 210 detects a first biosignal generated in response to a gesture performed by a user. The first biosignal may be generated in response to a muscle movement of the user to input the gesture. The first biosignal may include, for example, an EMG signal generated before and after the muscle movement of the user, a light signal penetrating a muscle of the user, and/or a force signal generated by the muscle of the user.

[49]

The gesture performed by the user may be one of various forms, for example, a wrist rotating, a hand flailing, and/or a fist clenching, which may be performed by the user using a portion of a body on which the user wears the wearable device 200. When a higher level of user authentication is needed based on implementation, at least two gestures consecutively input by the user may initiate the user authentication.

[50]

The second sensor 220 detects a second biosignal of the user. The second biosignal may include, for example, an ECG signal, a PPG signal, a voice of the user, and/or an impedance signal generated by the body of the user.

[51]

The memory 230 stores, with respect to at least one user, information directly or indirectly representing the first biosignal and the second biosignal.

[52]

For example, when sampling the first biosignal and the second biosignal, the information directly representing the first biosignal and the second biosignal may be information representing at least a portion of a sampled data symbol, or may be a duplicated signal of the first biosignal and the second signal.

[53]

The information indirectly representing the first biosignal and the second biosignal may be information in which the first biosignal and the second biosignal are processed and represented based on various signal processing methods.

[54]

The memory 230 may store at least one piece of feature point information obtained through signal processing performed on the first biosignal and the second biosignal.

[55]

The information to be stored in the memory 230 may be encoded and stored in the memory 230. Based on implementation, in an example of irregular access to the stored information, a design to prevent the stored information from being leaked out may be applied. When the user loses the wearable device 200, various methods may be adopted to prevent a third person from decoding the stored information in an abnormal manner.

[56]

The processor 240 determines, by referring to the memory 230, whether the first biosignal detected by the first sensor 210 corresponds to the information stored in the memory 230, and initiates a process of user authentication when the first biosignal corresponds to the stored information.

[57]

The processor 240 authenticates the user by comparing the second biosignal detected by the second sensor 220 to the information stored in the memory 230. When comparing the second biosignal detected by the second sensor 220 to the information stored in the memory 230, the processor 240 may operate

based on a predetermined error range. The error range may be determined by the user or predetermined in the wearable device 200 based on a result of statistics.

[58]

For example, the error range may be predetermined, by the user, to be 7%.

[59]

When a 5% error occurs as a result of comparing the second biosignal detected by the second sensor 220 to the information stored in the memory 230, the processor 240 may determine that the second biosignal detected by the second sensor 220 corresponds to the information stored in the memory 230 because the 5% error is within the predetermined error range. In this example, the processor 240 may authenticate the user. When a 10% error occurs as a result of comparing the second biosignal detected by the second sensor 220 to the information stored in the memory 230, the processor 240 may determine that the second biosignal detected by the second sensor 220 does not correspond to the information stored in the memory 230 because the 10% error is outside the predetermined error range. In this example, the processor 240 may not authenticate the user. The processor 240 may notify the user of a result of the user authentication in a visual, audible, and/or tactile manner, for example, on a display of the wearable device 200, through a speaker of the wearable device 200, and/or through a vibration of the wearable device 200.

[60]

FIG. 3 is a block diagram illustrating another example of a wearable device 300.

[61]

Referring to FIG. 3, the wearable device 300 may include a first sensor 310, a second sensor 320, a memory 330, a processor 340, an initial authenticator 350, and a wearing detection sensor 360.

[62]

The memory 330 stores access right information on at least one function executable in the wearable device 300. The access right information on each function may be determined by an external device, for example, a personal computer (PC), a laptop computer, and/or a smartphone, which is connected to the wearable device 300 through a wire or a wireless communication, or may be self-determined by the wearable device 300.

[63]

An example of the access right information on the executable function, which is stored in the memory 330, will be described in detail by referring to following FIG. 8.

[64]

When a command to execute a function is input to the wearable device 300 from the user, the processor 340 reads the access right information on the function, by referring to the memory 330, and provides at

least one of a visual feedback, an auditory feedback, and a tactile feedback to the user based on the access right information. Each form of feedback may be a request for user authentication to the user.

[65]

The wearable device 300 may include various executable functions, for example, performing a financial task, smartphone banking, opening a personal e-mail, using the Internet, transmitting a short message service (SMS) message, and/or other executable functions known to one of ordinary skill in the art, and each function may need a different access right. The memory 330 may store the access right information on the various functions executable in the wearable device 300.

[66]

For example, functions such as smartphone banking and opening a personal e-mail may need a relatively high level of the access right information, and functions such as using the Internet and transmitting an SMS message may need a relatively low level of the access right information.

[67]

For example, when the user inputs a command to execute the function of opening a personal e-mail, the processor 340 may read the access right information on the function, by referring to the memory 330. The access right information on the function of opening a personal e-mail that is stored in the memory 330, may be at a relatively high level.

[68]

The processor 340 may provide, to the user, at least one of a visual feedback, an auditory feedback, and a tactile feedback requesting a high level of user authentication based on the access right information. For example, the visual feedback may be feedback indicated on a display of the wearable device 300, the auditory feedback may be feedback delivered in a form of sound to the user through a speaker of the wearable device 300, and the tactile feedback may be feedback delivered in a form of touch sensation to the user through vibration of the wearable device 300.

[69]

The initial authenticator 350 receives a gesture and/or a first biosignal and a second biosignal from the user through the first sensor 310 and the second sensor 320, respectively, to set up an initial authentication. The initial authenticator 350 stores, in the memory 330, the first biosignal corresponding to the input gesture and the second biosignal.

[70]

The wearing detection sensor 360 detects whether the wearable device 300 is detached from the user. The wearing detection sensor 360 may detect a mechanical movement of a band attached to a portion of a body of the user, by being connected to the wearable device 300, or may detect an electrical signal generated in association with attaching and detaching of the band.

[71]

The wearing detection sensor 360 may detect, by being connected to the wearable device 300, changes generated when the band attached to the portion of the body of the user is attached and detached.

[72]

For example, the wearing detection sensor 360 may detect a change in which tension or elasticity of the band attached to a wrist of the user increases or decreases. Also, the wearing detection sensor 360 may detect a change in an amount of light detected by a light receiving unit of a photo sensor attached to a back of the wearable device 300, and may detect a change in which an electrical signal or an impedance signal is intensified or weakened when a contact point between the wearing detection sensor 360 and a skin appears or disappears due to the attaching or detaching of the band.

[73]

Further, the wearing detection sensor 360 may include various sensors that may detect whether the wearable device 300 is worn or not, and may deliver changes detected by the sensors to the processor 340.

[74]

The processor 340 controls the user authentication to be invalid based on a signal received from the wearing detection sensor 360. For example, the signal received from the wearing detection sensor 360 may be a signal such as "the user authentication to be invalid" indicating that a usage right assigned to the user through the process of the user authentication that is performed when the user wears the wearable device 300 is withdrawn or nullified. When the user authentication is invalid, the user may need to obtain the usage right through the process of the user authentication that is performed again when the user resumes wearing the wearable device 300.

[75]

The memory 330 may further store device setting information on each of at least one user. When the user is authenticated, the processor 340 may read the device setting information on the authenticated user, by referring to the memory 330, and may provide a user interface based on the device setting information.

[76]

For example, different device setting information or different configuration information pertaining to user A and user B may be stored in the memory 330. When the authenticated user is the user A, the processor 340 may read the device setting information on the user A that is stored in the memory 330, and may provide a main display and/or an icon arrangement for application execution, for the user A.

[77]

Other operations of the first sensor 310, the second sensor 320, the memory 330, and the processor 340 of FIG. 3, which are not described in the foregoing, may be the same as the description of the first sensor

210, the second sensor 220, the memory 230, and the processor 340 of FIG. 2, respectively. Thus, a repeated detailed description of the related operations is omitted here for conciseness and ease of description.

[78]

FIG. 4 is a flowchart illustrating a user authentication method of a wearable device.

[79]

Referring to FIG. 4, in operation 410, the wearable device detects a first biosignal generated in response to a gesture performed by a user. The first biosignal may be generated in response to a muscle movement of the user to input the gesture. The first biosignal may be at least one of an EMG signal generated before and after the muscle movement of the user, a light signal penetrating a muscle of the user, and a force signal generated by the muscle of the user.

[80]

In operation 420, the wearable device detects a second biosignal of the user. The second biosignal may be a signal distinguished from the first biosignal, and at least one of an ECG signal, a PPG signal, a voice of the user, and an impedance signal generated by a body of the user.

[81]

In operation 430, the wearable device stores, with respect to at least one user, information directly or indirectly representing the first biosignal and the second biosignal, in a memory of the wearable device.

[82]

In operation 440, the wearable device determines whether the first biosignal detected by the first sensor corresponds to the information stored in the memory.

[83]

When the wearable device determines that the first biosignal does not correspond to the stored information, the wearable device ends the method.

[84]

When the wearable device determines that the first biosignal corresponds to the stored information, the wearable device continues in operation 450. In operation 450, the wearable device initiates a process of user authentication.

[85]

In operation 460, the wearable device compares the second biosignal detected by the second sensor to the stored information, and then, in operation 470, the wearable device may authenticate the user.

[86]

When the user is authenticated, the wearable device may read device setting information of the authenticated user, by referring to the memory, and provide a user interface based on the device setting information. The device setting information on each of the at least one user may be stored in the memory of the wearable device.

[87]

FIG. 5 is a flowchart illustrating another example of a user authentication method of a wearable device.

[88]

Referring to FIG. 5, in operation 510, the wearable device receives a gesture and a second biosignal from a user.

[89]

In operation 515, the wearable device stores, in a memory of the wearable device, a first biosignal corresponding to the gesture, and the second biosignal. A process of storing initial user information is performed in operations 510 and 515, and thus, the user information stored in operations 510 and 515 may be used for user authentication in the wearable device. When two or more users use the wearable device, the information stored in operations 510 and 515 may be managed with respect to each of the users.

[90]

In operation 520, the wearable device detects the first biosignal generated in response to the gesture performed by the user. The first biosignal may be generated in response to a muscle movement of the user to input the gesture. The first biosignal may include, for example, an EMG signal generated before and after the muscle movement of the user, a light signal penetrating a muscle of the user, and/or a force signal generated by the muscle of the user.

[91]

In operation 525, the wearable device detects the second biosignal of the user. The second biosignal may be a biosignal unique to each of users and distinguished from the first biosignal, and may include, for example, an ECG signal, a PPG signal, a voice of the user, and/or an impedance signal generated by a body of the user.

[92]

In operation 530, the wearable device stores, with respect to at least one user, information directly or indirectly representing the first biosignal and the second biosignal, in the memory.

[93]

In operation 535, the wearable device determines whether the first biosignal detected by the first sensor corresponds to the information stored in the memory. When the wearable device determines that the first biosignal does not correspond to the stored information, the wearable device ends the method.

[94]

When the wearable device determines that the first biosignal corresponds to the stored information, the wearable device continues in operation 540. In operation 540, the wearable device initiates a process of user authentication.

[95]

In operation 545, the wearable device compares the second biosignal detected by the second sensor to the information stored in the memory.

[96]

In operation 550, the wearable device determines whether a difference between the second biosignal detected by the second sensor and the information stored in the memory is within a predetermined error range.

[97]

When the wearable device determines that the difference between the second biosignal and the stored information is within the predetermined error range, the wearable device continues in operation 555. In operation 555, the wearable device authenticates the user.

[98]

When the wearable device determines that the difference between the second biosignal and the stored information is outside the predetermined error range, the wearable device ends the method. When the wearable device determines that the difference between the second biosignal and the stored information is beyond the predetermined error range, the wearable device may provide basic information, such as time and day, to the user.

[99]

FIG. 6 is a flowchart illustrating an example of an authentication method used to provide different functions based on access right information of a user in a wearable device.

[100]

Referring to FIG. 6, in operation 610, the wearable device stores the access right information on at least one function executable in the wearable device.

[101]

In operation 620, the wearable device receives, from the user, an input of a command to execute a function of the wearable device of the at least one function executable in the wearable device.

[102]

In operation 630, the wearable device reads, by referring to a memory of the wearable device, the access right information on the function for which the command to execute is input.

[103]

In operation 640, the wearable device provides at least one of a visual feedback, an auditory feedback, and a tactile feedback to the user based on the access right information. Each feedback may be a request sent to the user for authentication.

[104]

FIG. 7 is a flowchart illustrating an example of an operational method used when a wearable device is detached from a user. Described hereinafter is an example in which a wearing detection sensor is provided with a sensor detecting a change of impedance.

[105]

Referring to FIG. 7, in operation 710, the wearable device detects, from the wearing detection sensor, the change of the impedance input to the wearable device.

[106]

In operation 720, the wearable device determines whether the wearable device is detached from the user based on the change of the impedance.

[107]

When the wearable device determines that the wearable device is detached from the user, the wearable device continues in operation 730. For example, when a value of the impedance input to the wearable device is greater than a predetermined level or is changed to be less than the predetermined level, the wearable device may determine that the wearable device is detached from the user. When a value of the impedance input to the wearable device remains at the predetermined level or is increased to be the predetermined level, the wearable device may determine that the wearable device is not detached from the user.

[108]

When the wearable device determines that the wearable device is detached from the user, in operation 730, the wearable device controls user authentication to be invalid.

[109]

When the wearable device determines that the wearable device is not attached to the user, the wearable device continues in operation 740. In operation 740, the wearable device controls the user authentication to be maintained.

[110]

According to another example, the wearing detection sensor may include a photo sensor detecting an amount of light collected on a back of the wearable device, or a sensor detecting tension of a band. In this example, the wearable device may determine whether the wearable device is detached from the user in a same or a similar manner as described, based on a characteristic of each sensor.

[111]

FIG. 8 is a diagram illustrating an example of access right information on executable functions, which are stored in a memory of a wearable device.

[112]

Referring to FIG. 8, in the memory of the wearable device, the access right information on the executable functions may be stored along with a command code for execution of each of the executable functions, such as performing a financial task, smartphone banking, opening a personal e-mail, using the Internet, transmitting an SMS message, and providing time (clock) and weather information.

[113]

A different access right determined with respect to each of the executable functions may be stored in the memory.

[114]

For example, the access right of level 4 may be determined for functions relating to important financial information and privacy protection such as performing a financial task, smartphone banking, and opening a personal e-mail. The access right of level 3 may be determined for functions such as using the Internet and transmitting an SMS message. Also, the access right of level 0 may be determined for basic functions needing no security, such as, providing time or weather information. The functions for which the access right of level 0 is determined, may be provided even when a user does not undergo user authentication or fails the user authentication.

[115]

For example, when a command for execution is input from the user, a processor of the wearing device may verify, by referring to the memory, which function is related to the command based on an input command code for execution, and may read the access right information on the verified function.

[116]

For example, when the input command code for execution is #00011, the processor may verify that the function is a function of opening a personal e-mail, and may read that the access right information on the verified function of opening a personal e-mail is of level 4.

[117]

The processor may request, based on the access right information, for example, of level 4, an additional user authentication to the user, using a visual feedback, an auditory feedback, and/or a tactile feedback.

[118]

Described in the foregoing is the example in which the access right information on at the executable functions in the wearable device is stored in a form or order of a level of the access right. However, the access right information may be stored in other various forms or orders.

[119]

The various units, elements, and methods described above may be implemented using one or more hardware components, one or more software components, or a combination of one or more hardware components and one or more software components. A hardware component may be, for example, a physical device that physically performs one or more operations, but is not limited thereto. Examples of hardware components include microphones, amplifiers, low-pass filters, high-pass filters, band-pass filters, analog-to-digital converters, digital-to-analog converters, and processing devices. A software component may be implemented, for example, by a processing device controlled by software or instructions to perform one or more operations, but is not limited thereto. A computer, controller, or other control device may cause the processing device to run the software or execute the instructions. One software component may be implemented by one processing device, or two or more software components may be implemented by one processing device, or one software component may be implemented by two or more processing devices, or two or more software components may be implemented by two or more processing devices. A processing device may be implemented using one or more general-purpose or special-purpose computers, such as, for example, a processor, a controller and an arithmetic logic unit, a digital signal processor, a microcomputer, a field-programmable array, a programmable logic unit, a microprocessor, or any other device capable of running software or executing instructions. The processing device may run an operating system (OS), and may run one or more software applications that operate under the OS. The processing device may access, store, manipulate, process, and create data when running the software or executing the instructions. For simplicity, the singular term "processing device" may be used in the description, but one of ordinary skill in the art will appreciate that a processing device may include multiple processing elements and multiple types of processing elements. For example, a processing device may include one or more processors, or one or more processors and one or more controllers. In addition, different processing configurations are possible, such as parallel processors or multi-core processors. A processing device configured to implement a software component to perform an operation A may include a processor programmed to run software or execute instructions to control the processor to perform operation A. In addition, a processing device configured to implement a software

component to perform an operation A, an operation B, and an operation C may have various configurations, such as, for example, a processor configured to implement a software component to perform operations A, B, and C; a first processor configured to implement a software component to perform operation A, and a second processor configured to implement a software component to perform operations B and C; a first processor configured to implement a software component to perform operations A and B, and a second processor configured to implement a software component to perform operation C; a first processor configured to implement a software component to perform operation A, a second processor configured to implement a software component to perform operation B, and a third processor configured to implement a software component to perform operation C; a first processor configured to implement a software component to perform operations A, B, and C, and a second processor configured to implement a software component to perform operations A, B, and C, or any other configuration of one or more processors each implementing one or more of operations A, B, and C. Although these examples refer to three operations A, B, C, the number of operations that may be implemented is not limited to three, but may be any number of operations required to achieve a desired result or perform a desired task.

[120]

Software or instructions for controlling a processing device to implement a software component may include a computer program, a piece of code, an instruction, or some combination thereof, for independently or collectively instructing or configuring the processing device to perform one or more desired operations. The software or instructions may include machine code that may be directly executed by the processing device, such as machine code produced by a compiler, and/or higher-level code that may be executed by the processing device using an interpreter. The software or instructions and any associated data, data files, and data structures may be embodied permanently or temporarily in any type of machine, component, physical or virtual equipment, computer storage medium or device, or a propagated signal wave capable of providing instructions or data to or being interpreted by the processing device. The software or instructions and any associated data, data files, and data structures also may be distributed over network-coupled computer systems so that the software or instructions and any associated data, data files, and data structures are stored and executed in a distributed fashion. For example, the software or instructions and any associated data, data files, and data structures may be recorded, stored, or fixed in one or more non-transitory computer-readable storage media. A non-transitory computer-readable storage medium may be any data storage device that is capable of storing the software or instructions and any associated data, data files, and data structures so that they can be read by a computer system or processing device. Examples of a non-transitory computer-readable storage medium include read-only memory (ROM), random-access memory (RAM), flash memory, CD-ROMs, CD-Rs, CD+Rs, CD-RWs, CD+RWs, DVD-ROMs, DVD-Rs, DVD+Rs, DVD-RWs, DVD+RWs, DVD-RAMs, BD-ROMs, BD-Rs, BD-R LTHs, BD-REs, magnetic tapes, floppy disks, magneto-optical data storage devices, optical data storage devices, hard disks, solid-state disks, or any other non-transitory computer-readable storage medium known to one of ordinary skill in the art. Functional programs, codes, and code segments for implementing the examples disclosed herein can be easily constructed by a programmer skilled in the art

to which the examples pertain based on the drawings and their corresponding descriptions as provided herein.

[121]

As a non-exhaustive illustration only, a device described herein may refer to mobile devices such as, for example, a cellular phone, a smart phone, a wearable smart device (such as, for example, a ring, a watch, a pair of glasses, a bracelet, an ankle bracket, a belt, a necklace, an earring, a headband, a helmet, a device embedded in the cloths or the like), a personal computer (PC), a tablet personal computer (tablet), a phablet, a personal digital assistant (PDA), a digital camera, a portable game console, an MP3 player, a portable/personal multimedia player (PMP), a handheld e-book, an ultra mobile personal computer (UMPC), a portable lab-top PC, a global positioning system (GPS) navigation, and devices such as a high definition television (HDTV), an optical disc player, a DVD player, a Blue-ray player, a setup box, or any other device capable of wireless communication or network communication consistent with that disclosed herein. In a non-exhaustive example, the wearable device may be self-mountable on the body of the user, such as, for example, the glasses or the bracelet. In another non-exhaustive example, the wearable device may be mounted on the body of the user through an attaching device, such as, for example, attaching a smart phone or a tablet to the arm of a user using an armband, or hanging the wearable device around the neck of a user using a lanyard.

[122]

While this disclosure includes specific examples, it will be apparent to one of ordinary skill in the art that various changes in form and details may be made in these examples without departing from the spirit and scope of the claims and their equivalents. The examples described herein are to be considered in a descriptive sense only, and not for purposes of limitation. Descriptions of features or aspects in each example are to be considered as being applicable to similar features or aspects in other examples. Suitable results may be achieved if the described techniques are performed in a different order, and/or if components in a described system, architecture, device, or circuit are combined in a different manner and/or replaced or supplemented by other components or their equivalents.

[123]

Therefore, the scope of the disclosure is defined not by the detailed description, but by the claims and their equivalents, and all variations within the scope of the claims and their equivalents are to be construed as being included in the disclosure.

References

[124]

200: wearable device

210: first sensor

220: second sensor

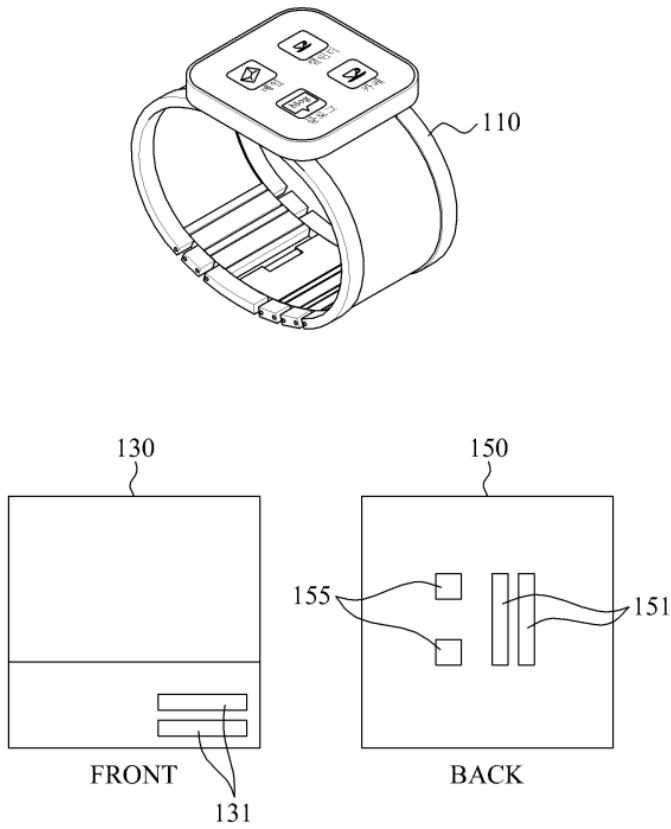
230: memory

[Translation]

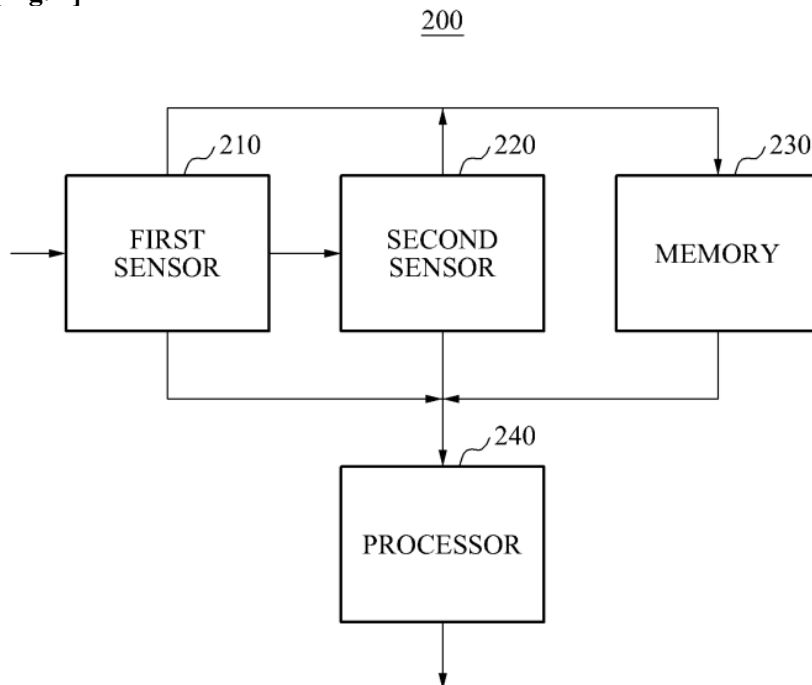
240: processor

Drawings

[Fig. 1]

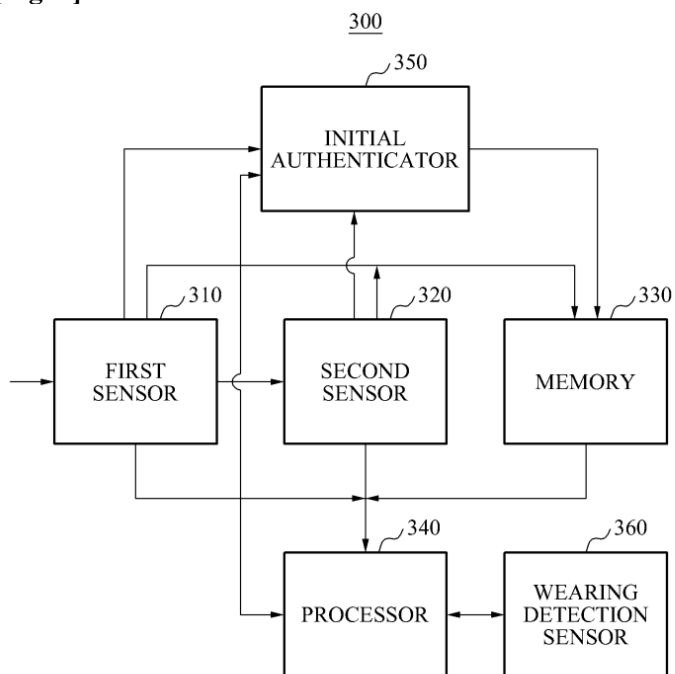


[Fig. 2]



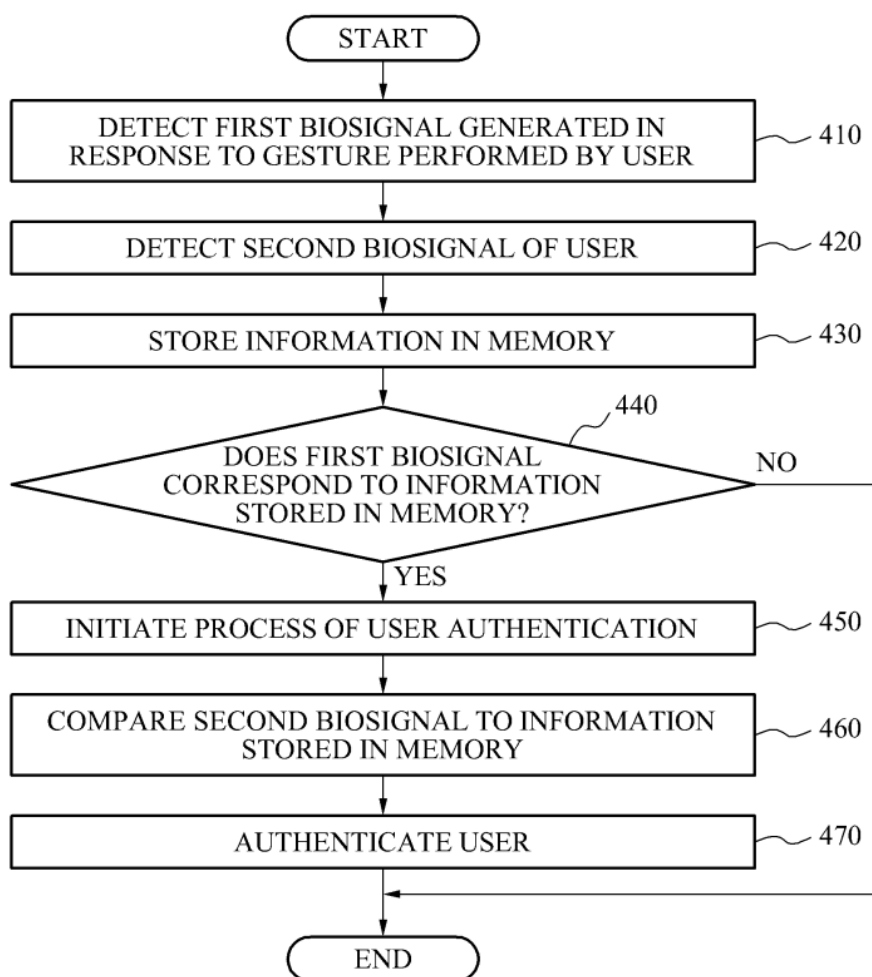
[Translation]

[Fig. 3]



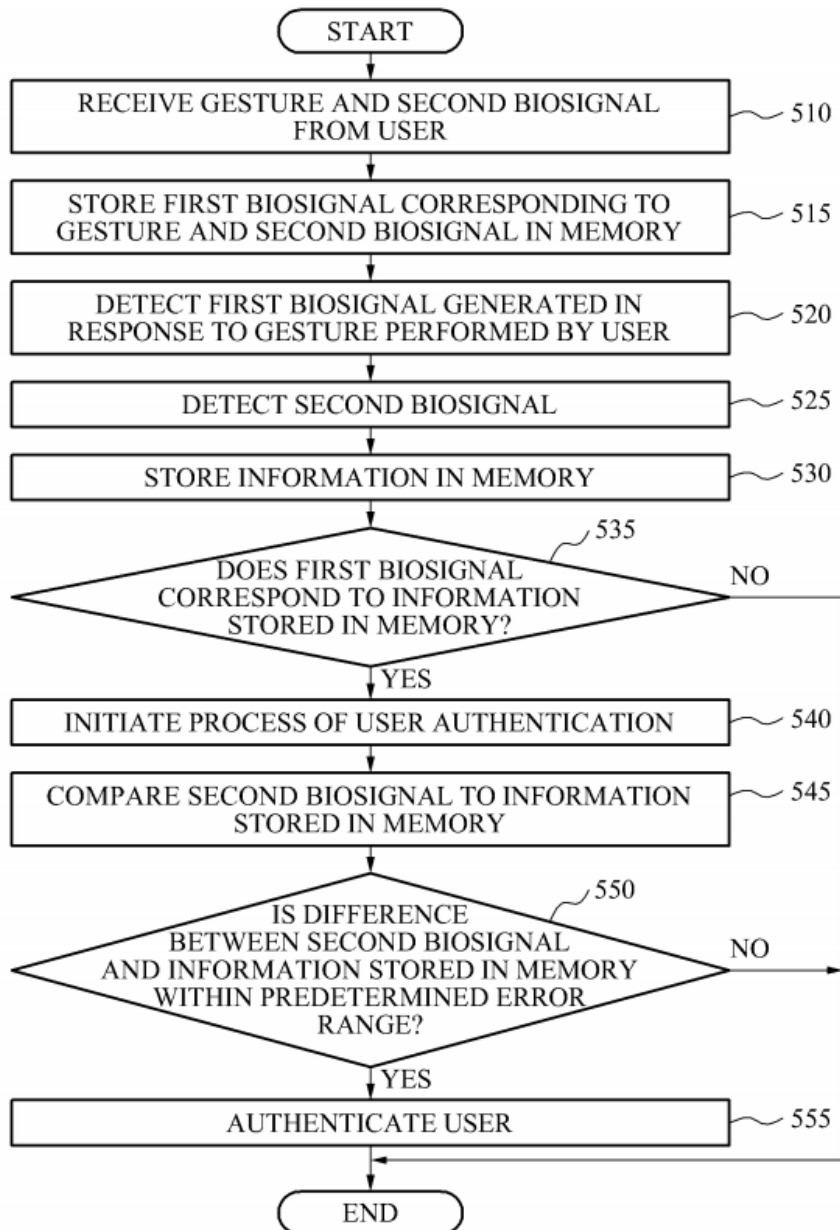
[Fig. 4]

[Translation]

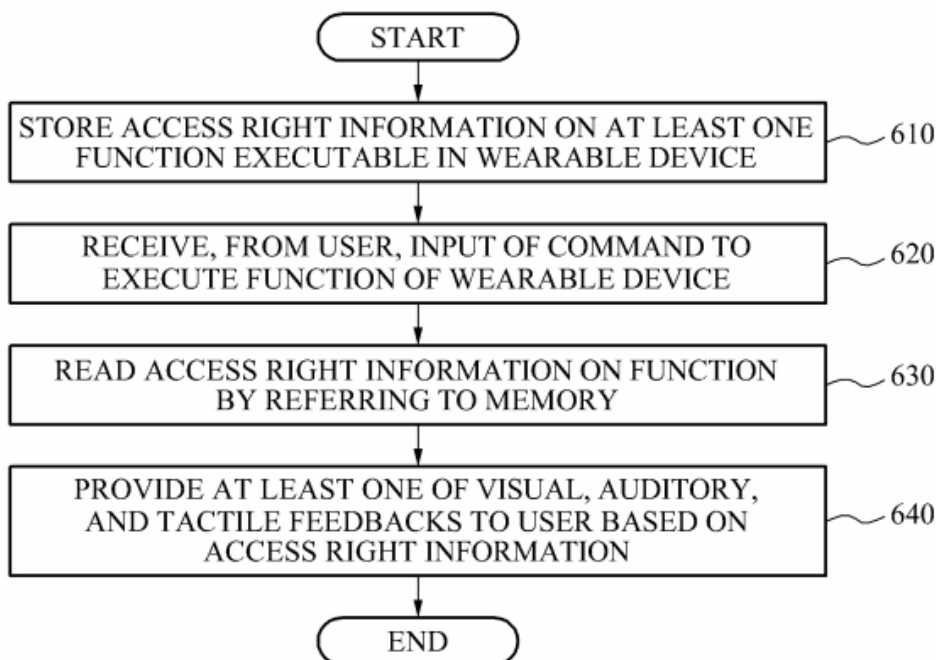


[Fig. 5]

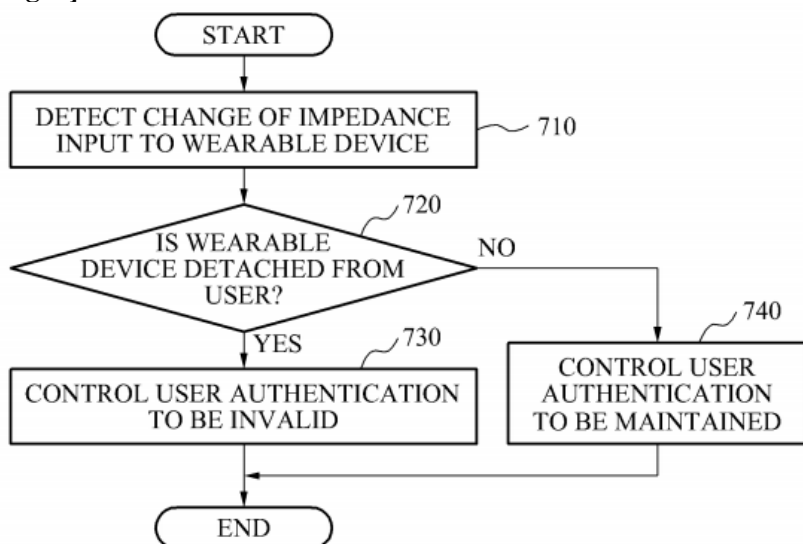
[Translation]



[Fig. 6]



[Fig. 7]



[Translation]

[Fig. 8]

FUNCTION	COMMAND CODE FOR EXECUTION	ACCESS RIGHT INFORMATION	
FINANCIAL TASK	#00001	LEVEL : 4	
PERSONAL EMAIL	#00011	LEVEL : 4	
INTERNET	#00111	LEVEL : 3	
SMS	#01111	LEVEL : 3	...
CLOCK	#11111	LEVEL : 0 (BASIC FUNCTION)	
WEATHER INFORMATION	#11110	LEVEL : 0 (BASIC FUNCTION)	

⋮



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2020년08월13일

(11) 등록번호 10-2136836

(24) 등록일자 2020년07월16일

(51) 국제특허분류(Int. Cl.)

G06F 21/32 (2013.01) G06F 21/44 (2013.01)

(21) 출원번호 10-2013-0107833

(22) 출원일자 2013년09월09일

심사청구일자 2018년09월04일

(65) 공개번호 10-2015-0029105

(43) 공개일자 2015년03월18일

(56) 선행기술조사문헌

KR200120590 Y1*

(뒷면에 계속)

(73) 특허권자

삼성전자주식회사

경기도 수원시 영통구 삼성로 129 (매탄동)

(72) 발명자

최창목

서울 강남구 논현로111길 3, 802호 (논현동, 휴먼스페이스빌)

김상준

경기 화성시 동탄문화센터로 39, 321동 204호 (반송동, 시범다운마을포스코더샵아파트)

윤승근

서울 서초구 서초중앙로 200, 10동 1303호 (서초동, 삼풍아파트)

(74) 대리인

특허법인 무한

전체 청구항 수 : 총 26 항

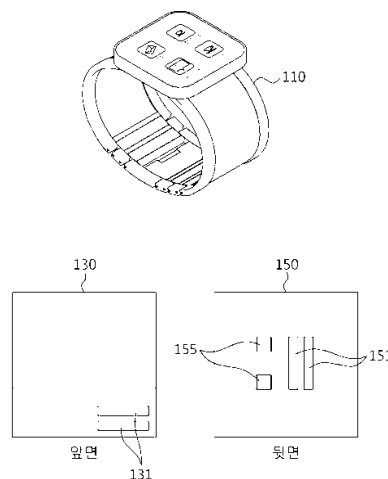
심사관 : 문남두

(54) 발명의 명칭 **생체 신호들을 이용하여 사용자 인증을 수행하는 착용형 기기 및 그 착용형 기기의 인증 방법**

(57) 요약

착용형(wearable) 기기가 개시된다. 사용자의 제스처(gesture)에 의해 발생하는 제1 생체 신호를 감지하는 제1 감지부, 사용자의 제2 생체 신호를 감지하는 제2 감지부, 하나 이상의 사용자에 대해, 제1 생체 신호 및 제2 생체 신호를 직접 또는 간접적으로 표현(represent)하는 적어도 하나의 정보를 기록하는 메모리, 및 제1 감지부에서 감지된 제1 생체 신호가 메모리에 기록된 정보와 대응되는지 판단하여 사용자 인증 절차를 개시하고, 제2 감지부에서 감지된 제2 생체 신호와 메모리에 기록된 정보를 비교하여 사용자를 인증하는 프로세서를 포함하는 착용형(wearable) 기기를 제공할 수 있다.

대표도 - 도1



(56) 선행기술조사문헌

US06720860 B1*

US20060215883 A1*

US20100331649 A1*

US20130159705 A1*

*는 심사관에 의하여 인용된 문헌

명세서

청구범위

청구항 1

사용자의 제스처(gesture)에 의해 발생하는 제1 생체 신호를 감지하는 제1 감지부;

상기 사용자의 제2 생체 신호를 감지하는 제2 감지부;

하나 이상의 사용자에 대해, 상기 제1 생체 신호 및 상기 제2 생체 신호를 직접 또는 간접적으로 표현(represent)하는 적어도 하나의 정보를 기록하는 메모리; 및

상기 제1 감지부에서 감지된 상기 제1 생체 신호가 상기 메모리에 기록된 상기 정보와 대응되는지 판단하여 사용자 인증 절차를 개시하고, 상기 제2 감지부에서 감지된 상기 제2 생체 신호와 상기 메모리에 기록된 상기 정보를 비교하여 상기 사용자를 인증하는 프로세서를 포함하고,

상기 제2 생체 신호는 상기 사용자에게 고유하고, 상기 제2 생체 신호와 상기 제1 생체 신호는 상이한 착용형(wearable) 기기.

청구항 2

제1항에 있어서,

상기 제1 생체 신호는,

상기 제스처를 입력하기 위한 상기 사용자의 근육의 움직임에 의해 발생된 것인 착용형 기기.

청구항 3

제2항에 있어서,

상기 제1 생체 신호는,

상기 사용자의 근육의 움직임 전, 후에 발생하는 근전도 신호(Electromyography; EMG), 상기 사용자의 근육을 투과한 빛 신호, 및 상기 사용자의 근육에 의해 발생하는 힘 중 적어도 하나인 착용형 기기.

청구항 4

제1항에 있어서,

상기 제2 생체 신호는,

심전도(ElectroCardioGraphy; ECG) 신호, 광용적맥파(PhotoPlethysmoGram; PPG) 신호, 상기 사용자의 음성(voice) 및 상기 사용자의 신체에서 발생하는 임피던스(impedance) 신호 중 적어도 하나인 착용형 기기.

청구항 5

제1항에 있어서,

상기 메모리에 저장되는 상기 정보는,

상기 제1 생체 신호 및 상기 제2 생체 신호에 대한 신호 처리를 통해 획득한 적어도 하나의 특징점 정보를 포함하는 착용형 기기.

청구항 6

제1항에 있어서,
상기 메모리에 저장되는 상기 정보는 암호화된,
작용형 기기.

청구항 7

제1항에 있어서,
상기 프로세서는,
상기 제2 감지부를 통해 수신한 상기 제2 생체 신호와, 상기 메모리에 기록된 상기 정보를 비교할 때, 미리 정해진 오차 범위를 고려하여 동작하는 작용형 기기.

청구항 8

제1항에 있어서,
상기 사용자로부터 상기 제스처 및 상기 제2 생체 신호를 입력 받고, 입력된 제스처에 대응하는 상기 제1 생체 신호 및 상기 제2 생체 신호를 상기 메모리에 기록하는 초기 인증부를 더 포함하는 작용형 기기.

청구항 9

제1항에 있어서,
상기 메모리는,
상기 작용형 기기에서 실행 가능한 하나 이상의 기능에 대한 접근 권한 정보를 더 기록하고,
상기 프로세서는,
상기 작용형 기기에서 상기 사용자로부터 상기 기능에 대한 실행 명령이 입력된 경우, 상기 메모리를 참조하여 상기 기능에 대응하는 상기 접근 권한 정보를 읽고, 상기 접근 권한 정보에 따라 상기 사용자에게 시각적, 청각적, 또는 촉각적 피드백 중 적어도 하나를 제공하는 작용형 기기.

청구항 10

제9항에 있어서,
상기 피드백은 사용자 인증 요청인 작용형 기기.

청구항 11

제1항에 있어서,
상기 작용형 기기가 상기 사용자로부터 분리되는지 여부를 감지하는 작용 감지부를 더 포함하고,
상기 프로세서는 상기 작용 감지부로부터 수신한 신호에 기초하여, 상기 사용자에 대한 상기 인증이 널(NULL)이

되도록 제어하는 착용형 기기.

청구항 12

제11항에 있어서,

상기 착용 감지부는, 상기 착용형 기기와 연결되어 상기 사용자의 신체 일부에 부착되는 밴드의 기계적 움직임(mechanical movement)을 감지하거나, 상기 밴드의 착탈에 대응하여 발생하는 전기적 신호를 감지하는 착용형 기기.

청구항 13

제1항에 있어서,

상기 메모리는,

상기 하나 이상의 사용자 각각에 대응하는 기기 설정 정보를 더 기록하고,

상기 프로세서는,

상기 사용자가 인증된 경우, 상기 메모리를 참조하여 상기 인증된 사용자의 상기 기기 설정 정보를 읽고, 상기 기기 설정 정보에 따라 사용자 인터페이스(User Interface)를 제공하는 착용형 기기.

청구항 14

제1항에 있어서,

상기 착용형 기기는 시계형 스마트폰인 착용형 기기.

청구항 15

사용자의 제스처(gesture)에 의해 발생하는 제1 생체 신호를 감지하는 제1 감지부;

상기 사용자의 제2 생체 신호를 감지하는 제2 감지부;

하나 이상의 사용자에 대해, 상기 제1 생체 신호 및 상기 제2 생체 신호를 직접 또는 간접적으로 표현(represent)하는 적어도 하나의 정보를 기록하는 메모리; 및

상기 제1 감지부에서 감지된 상기 제1 생체 신호가 상기 메모리에 기록된 상기 정보와 대응되는지 판단하여 사용자 인증 절차를 트리거(trigger)하고, 상기 제2 감지부에서 감지된 상기 제2 생체 신호와 상기 메모리에 기록된 상기 정보를 비교하여 상기 사용자를 인증하는 프로세서

를 포함하고,

상기 제1 생체 신호는, 상기 제스처를 입력하기 위한 상기 사용자의 근육의 움직임에 의해 발생되고,

상기 제2 생체 신호는 상기 사용자에게 고유하고, 상기 제2 생체 신호와 상기 제1 생체 신호는 상이하고,

상기 제2 생체 신호는, 심전도(ElectroCardioGraphy; ECG) 신호, 광용적맥파(PhotoPlethysmoGram; PPG) 신호, 상기 사용자의 음성(voice) 및 상기 사용자의 신체에서 발생하는 임피던스(impedance) 신호 중 적어도 하나인 착용형 기기.

청구항 16

사용자의 제스처(gesture)에 의해 발생하는 제1 생체 신호를 감지하는 단계;

상기 사용자의 제2 생체 신호를 감지하는 단계;

하나 이상의 사용자에게 대해, 상기 제1 생체 신호 및 상기 제2 생체 신호를 직접 또는 간접적으로 표현(represent)하는 적어도 하나의 정보를 메모리에 기록하는 단계;

제1 감지부에서 감지된 상기 제1 생체 신호가 상기 메모리에 기록된 상기 정보와 대응되는지 판단하여 사용자 인증 절차를 개시하는 단계; 및

제2 감지부에서 감지된 상기 제2 생체 신호와 상기 메모리에 기록된 상기 정보를 비교하여 상기 사용자를 인증하는 단계를 포함하고,

상기 제2 생체 신호는 상기 사용자에게 고유하고, 상기 제2 생체 신호와 상기 제1 생체 신호는 상이한 착용형(wearable) 기기의 사용자 인증 방법.

청구항 17

제16항에 있어서,

상기 메모리에 저장되는 상기 정보는,

상기 제1 생체 신호 및 상기 제2 생체 신호에 대한 신호 처리를 통해 획득한 적어도 하나의 특징점 정보를 포함하는 착용형 기기의 사용자 인증 방법.

청구항 18

제16항에 있어서,

상기 사용자를 인증하는 단계는

미리 정해진 오차 범위를 고려하여, 상기 제2 감지부에서 감지된 상기 제2 생체 신호와 상기 메모리에 기록된 상기 정보를 비교하는 단계

를 포함하는 착용형 기기의 사용자 인증 방법.

청구항 19

제16항에 있어서,

상기 사용자로부터 상기 제스처 및 상기 제2 생체 신호를 입력 받는 단계; 및

입력된 제스처에 대응하는 상기 제1 생체 신호 및 상기 제2 생체 신호를 상기 메모리에 기록하는 단계

를 더 포함하는 착용형 기기의 사용자 인증 방법.

청구항 20

제16항에 있어서,

상기 적어도 하나의 정보를 기록하는 단계는

상기 착용형 기기에서 실행 가능한 하나 이상의 기능에 대한 접근 권한 정보를 더 기록하는 단계

를 포함하는 착용형 기기의 사용자 인증 방법.

청구항 21

제20항에 있어서,

상기 사용자로부터 상기 기능에 대한 실행 명령을 입력 받는 단계;
 상기 실행 명령이 입력된 경우, 상기 메모리를 참조하여 상기 기능에 대응하는 상기 접근 권한 정보를 읽는 단계; 및
 상기 접근 권한 정보에 따라 상기 사용자에게 시각적, 청각적, 및 촉각적 피드백 중 적어도 하나를 제공하는 단계를 포함하는 착용형 기기의 사용자 인증 방법.

청구항 22

제16항에 있어서,
 상기 착용형 기기가 상기 사용자로부터 분리되는지 여부를 감지하는 단계; 및
 상기 착용형 기기가 상기 사용자로부터 분리된 것으로 감지되면, 상기 사용자에 대한 상기 인증이 널(NULL)이 되도록 제어하는 단계를 포함하는 착용형 기기의 사용자 인증 방법.

청구항 23

제22항에 있어서,
 상기 착용형 기기가 상기 사용자로부터 분리되는지 여부를 감지하는 단계는,
 상기 착용형 기기와 연결되어 상기 사용자의 신체 일부에 부착되는 밴드의 기계적 움직임(mechanical movement) 또는 상기 밴드의 착탈에 대응하여 발생하는 전기적 신호를 감지하는 단계를 포함하는 착용형 기기의 사용자 인증 방법.

청구항 24

제16항에 있어서,
 상기 적어도 하나의 정보를 기록하는 단계는,
 상기 하나 이상의 사용자 각각에 대응하는 기기 설정 정보를 더 기록하는 단계를 포함하는 착용형 기기의 사용자 인증 방법.

청구항 25

제24항에 있어서,
 상기 사용자를 인증하는 단계는
 상기 사용자가 인증된 경우, 상기 메모리를 참조하여 상기 인증된 사용자의 상기 기기 설정 정보를 읽는 단계; 및
 상기 기기 설정 정보에 따라 사용자 인터페이스(User Interface)를 제공하는 단계를 포함하는 착용형 기기의 사용자 인증 방법.

청구항 26

제16항 내지 제25항 중에서 어느 하나의 항의 방법을 실행시키기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록 매체.

발명의 설명

기술 분야

- [0001] 아래의 실시예들은 생체 신호들을 이용하여 사용자 인증을 수행하는 착용형 기기 및 그 착용형 기기의 사용자 인증 방법에 관한 것이다.

배경 기술

- [0002] 스마트 폰(Smart Phone)의 확산과 함께 다양한 모바일 기기들의 개발되고 있고, 착용 가능한 형태의 모바일 기기 또한 등장하고 있다.
- [0003] 모바일 기기는 현대인의 삶에 많은 편의성을 제공한다. 모바일 기기의 컴퓨팅 파워가 커지면서, 사용자들은 PC 등으로 수행하던 많은 업무를 모바일 기기를 이용하여 수행하고 있다. 모바일 기기가 널리 활용되면서, 모바일 기기에 저장된 연락처 정보, 사진, 동영상 등의 개인적인 멀티미디어 콘텐츠, 메일, 금융 관련 정보 등의 개인 정보에 대한 보호가 중요해 지고 있다. 사용자가 모바일 기기를 분실하거나, 불특정 사용자가 임의로 모바일 기기를 사용하는 경우, 개인 정보가 사용자의 의도에 반하여 노출될 위험이 있다. 따라서, 모바일 기기를 이용하고자 하는 사용자에 대한 인증 및 모바일 기기에 저장된 다양한 개인 정보에 대한 접근을 제어할 수 있는 방안이 요구된다.

발명의 내용

해결하려는 과제

과제의 해결 수단

- [0004] 일 실시예에 따르면, 착용형(wearable) 기기는 사용자의 제스처(gesture)에 의해 발생하는 제1 생체 신호를 감지하는 제1 감지부; 상기 사용자의 제2 생체 신호를 감지하는 제2 감지부; 하나 이상의 사용자에 대해, 상기 제1 생체 신호 및 상기 제2 생체 신호를 직접 또는 간접적으로 표현(represent)하는 적어도 하나의 정보를 기록하는 메모리; 및 상기 제1 감지부에서 감지된 상기 제1 생체 신호가 상기 메모리에 기록된 상기 정보와 대응되는지 판단하여 사용자 인증 절차를 개시하고, 상기 제2 감지부에서 감지된 상기 제2 생체 신호와 상기 메모리에 기록된 상기 정보를 비교하여 상기 사용자를 인증하는 프로세서를 포함한다.
- [0005] 상기 제1 생체 신호는, 상기 제스처를 입력하기 위한 상기 사용자의 근육의 움직임에 의해 발생된 것일 수 있다.
- [0006] 상기 제1 생체 신호는, 상기 사용자의 근육의 움직임 전, 후에 발생하는 근전도 신호(Electromyography; EMG), 상기 사용자의 근육을 투과한 빛 신호, 및 상기 사용자의 근육에 의해 발생하는 힘 중 적어도 하나일 수 있다.
- [0007] 상기 제2 생체 신호는, 심전도(ElectroCardioGraphy; ECG) 신호, 광용적맥파(PhotoPlethysmoGram; PPG) 신호, 상기 사용자의 음성(voice) 및 상기 사용자의 신체에서 발생하는 임피던스(impedance) 신호 중 적어도 하나일 수 있다.
- [0008] 상기 메모리에 저장되는 상기 정보는, 상기 제1 생체 신호 및 상기 제2 생체 신호에 대한 신호 처리를 통해 획득한 적어도 하나의 특징점 정보를 포함할 수 있다.
- [0009] 상기 프로세서는, 상기 제2 감지부를 통해 수신한 상기 제2 생체 신호와, 상기 메모리에 기록된 상기 정보를 비교할 때, 미리 정해진 오차 범위를 고려하여 동작할 수 있다.
- [0010] 상기 사용자로부터 상기 제스처 및 상기 제2 생체 신호를 입력 받고, 입력된 제스처에 대응하는 상기 제1 생체

신호 및 상기 제2 생체 신호를 상기 메모리에 기록하는 초기 인증부를 더 포함할 수 있다.

- [0011] 상기 메모리는, 상기 착용형 기기에서 실행 가능한 하나 이상의 기능에 대한 접근 권한 정보를 더 기록하고, 상기 프로세서는, 상기 착용형 기기에서 상기 사용자로부터 상기 기능에 대한 실행 명령이 입력된 경우, 상기 메모리를 참조하여 상기 기능에 대응하는 상기 접근 권한 정보를 읽고, 상기 접근 권한 정보에 따라 상기 사용자에게 시각적, 청각적, 또는 촉각적 피드백 중 적어도 하나를 제공할 수 있다.
- [0012] 상기 피드백은 사용자 인증 요청일 수 있다.
- [0013] 상기 착용형 기기가 상기 사용자로부터 분리되는지 여부를 감지하는 착용 감지부를 더 포함하고, 상기 프로세서는 상기 착용 감지부로부터 수신한 신호에 기초하여, 상기 사용자에게 대한 상기 인증이 널(NULL)이 되도록 제어할 수 있다.
- [0014] 상기 착용 감지부는, 상기 착용형 기기와 연결되어 상기 사용자의 신체 일부에 부착되는 밴드의 기계적 움직임(mechanical movement)을 감지하거나, 상기 밴드의 착탈에 대응하여 발생하는 전기적 신호를 감지할 수 있다.
- [0015] 상기 메모리는, 상기 하나 이상의 사용자 각각에 대응하는 기기 설정 정보를 더 기록하고, 상기 프로세서는, 상기 사용자가 인증된 경우, 상기 메모리를 참조하여 상기 인증된 사용자의 상기 기기 설정 정보를 읽고, 상기 기기 설정 정보에 따라 사용자 인터페이스(User Interface)를 제공할 수 있다.
- [0016] 상기 착용형 기기는 시계형 스마트폰일 수 있다.
- [0017] 일실시예에 따르면, 착용형 기기는 사용자의 제스처(gesture)에 의해 발생하는 제1 생체 신호를 감지하는 제1 감지부; 상기 사용자의 제2 생체 신호를 감지하는 제2 감지부; 하나 이상의 사용자에게 대해, 상기 제1 생체 신호 및 상기 제2 생체 신호를 직접 또는 간접적으로 표현(represent)하는 적어도 하나의 정보를 기록하는 메모리; 및 상기 제1 감지부에서 감지된 상기 제1 생체 신호가 상기 메모리에 기록된 상기 정보와 대응되는지 판단하여 사용자 인증 절차를 개시(initiate)하고, 상기 제2 감지부에서 감지된 상기 제2 생체 신호와 상기 메모리에 기록된 상기 정보를 비교하여 상기 사용자를 인증하는 프로세서를 포함하고, 상기 제1 생체 신호는, 상기 제스처를 입력하기 위한 상기 사용자의 근육의 움직임에 의해 발생되고, 상기 제2 생체 신호는, 심전도(ElectroCardioGraphy; ECG) 신호, 광용적맥파(PhotoPlethysmoGram; PPG) 신호, 상기 사용자의 음성(voice) 및 상기 사용자의 신체에서 발생하는 임피던스(impedance) 신호 중 적어도 하나일 수 있다.
- [0018] 일실시예에 따르면, 착용형(wearable) 기기의 사용자 인증 방법은 사용자의 제스처(gesture)에 의해 발생하는 제1 생체 신호를 감지하는 단계; 상기 사용자의 제2 생체 신호를 감지하는 단계; 하나 이상의 사용자에게 대해, 상기 제1 생체 신호 및 상기 제2 생체 신호를 직접 또는 간접적으로 표현(represent)하는 적어도 하나의 정보를 메모리에 기록하는 단계; 상기 제1 감지부에서 감지된 상기 제1 생체 신호가 상기 메모리에 기록된 상기 정보와 대응되는지 판단하여 사용자 인증 절차를 개시하는 단계; 및 상기 제2 감지부에서 감지된 상기 제2 생체 신호와 상기 메모리에 기록된 상기 정보를 비교하여 상기 사용자를 인증하는 단계를 포함한다.
- [0019] 상기 메모리에 저장되는 상기 정보는, 상기 제1 생체 신호 및 상기 제2 생체 신호에 대한 신호 처리를 통해 획득한 적어도 하나의 특징점 정보를 포함할 수 있다.
- [0020] 상기 사용자를 인증하는 단계는 미리 정해진 오차 범위를 고려하여, 상기 제2 감지부에서 감지된 상기 제2 생체 신호와 상기 메모리에 기록된 상기 정보를 비교하는 단계를 포함할 수 있다.
- [0021] 상기 사용자로부터 상기 제스처 및 상기 제2 생체 신호를 입력 받는 단계; 및 입력된 제스처에 대응하는 상기 제1 생체 신호 및 상기 제2 생체 신호를 상기 메모리에 기록하는 단계를 더 포함할 수 있다.
- [0022] 상기 적어도 하나의 정보를 기록하는 단계는 상기 착용형 기기에서 실행 가능한 하나 이상의 기능에 대한 접근 권한 정보를 더 기록하는 단계를 포함할 수 있다.
- [0023] 상기 착용형 기기에서 상기 사용자로부터 상기 기능에 대한 실행 명령을 입력 받는 단계; 상기 실행 명령이 입력된 경우, 상기 메모리를 참조하여 상기 기능에 대응하는 상기 접근 권한 정보를 읽는 단계; 및 상기 접근 권한 정보에 따라 상기 사용자에게 시각적, 청각적, 또는 촉각적 피드백 중 적어도 하나를 제공하는 단계를 포함할 수 있다.
- [0024] 상기 착용형 기기가 상기 사용자로부터 분리되는지 여부를 감지하는 단계; 및 상기 착용형 기기가 상기 사용자로부터 분리된 것으로 감지되면, 상기 사용자에게 대한 상기 인증이 널(NULL)이 되도록 제어하는 단계를 포함할 수 있다.

- [0025] 상기 착용형 기기가 상기 사용자로부터 분리되는지 여부를 감지하는 단계는 상기 착용형 기기와 연결되어 상기 사용자의 신체 일부에 부착되는 밴드의 기계적 움직임(mechanical movement) 또는 상기 밴드의 착탈에 대응하여 발생하는 전기적 신호를 감지하는 단계를 포함할 수 있다.
- [0026] 상기 적어도 하나의 정보를 기록하는 단계는, 상기 하나 이상의 사용자 각각에 대응하는 기기 설정 정보를 더 기록하는 단계를 포함할 수 있다.
- [0027] 상기 사용자를 인증하는 단계는 상기 사용자가 인증된 경우, 상기 메모리를 참조하여 상기 인증된 사용자의 상기 기기 설정 정보를 읽는 단계; 및 상기 기기 설정 정보에 따라 사용자 인터페이스(User Interface)를 제공하는 단계를 포함할 수 있다.

도면의 간단한 설명

- [0028] 도 1은 일실시예에 따른 착용형(wearable) 기기를 나타낸 도면이다.
- 도 2는 일실시예에 따른 착용형(wearable) 기기의 블록도이다.
- 도 3은 다른 실시예에 따른 착용형(wearable) 기기의 블록도이다.
- 도 4는 일실시예에 따른 착용형 기기의 인증 방법을 나타낸 플로우차트이다.
- 도 5는 다른 실시예에 따른 착용형 기기의 인증 방법을 나타낸 플로우차트이다.
- 도 6은 일실시예에 따른 착용형 기기에서 사용자의 접근 권한 정보에 따라 서로 다른 기능을 제공하기 위한 인증 방법을 나타낸 플로우차트이다.
- 도 7은 일실시예에 따른 착용형 기기가 사용자로부터 분리된 경우의 동작 방법을 나타낸 플로우차트이다.
- 도 8은 일실시예에 따른 착용형 기기의 메모리가 저장하는, 실행 가능한 하나 이상의 기능에 대한 접근 권한 정보에 대한 일 예를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0029] 이하, 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다. 그러나, 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다. 또한, 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.
- [0030] 도 1은 일실시예에 따른 착용형(wearable) 기기를 나타낸 도면이다.
- [0031] 도 1을 참조하면, 일실시예에 따른 착용형(wearable) 기기는 암 밴드(arm), 손목 밴드(wrist band) 혹은 그 밖의 고정 장치 등에 의해 신체의 일부에 부착(attachable) 또는 착용(wearable)되거나 탈착(detachable)될 수 있다.
- [0032] 이하, 설명의 편의를 위해, 착용형 기기에서 예를 들어, 터치 디스플레이 등과 같이 사용자가 볼 수 있는 화면이 제공되는 면을 '앞면(130)'으로, 부착 또는 착용 시에 사용자의 신체를 향하는 면을 '뒷면(150)'으로 설명한다. 착용형 기기의 설계에 따라, 터치 디스플레이 등의 화면을 보호하기 위해 앞면(130)에 기계적 또는 전기적으로 개폐 가능한 보호구가 위치할 수 있다. 이와 같이 설계된 착용형 기기의 경우, 앞면(130)은 후술하는 센서가 설치된 면(실제 화면 또는 보호구의 표면)을 의미할 수 있다.
- [0033] 착용형 기기는 기기의 앞면(130)과 뒷면(150)에 설치된 센서들(133, 153, 155)을 포함할 수 있다. 착용형 기기는 센서들(133, 153, 155) 중 적어도 일부를 이용하여 착용형 기기에 대한 사용자 인증 절차를 시작하는 트리거 신호(trigger signal)를 센싱하고, 사용자 인증을 개시한다.
- [0034] 사용자는 착용형 기기를 착용한 상태에서 손을 째 펴거나, 주먹을 쥐거나, 손목을 비트는 등과 같은 미리 정해진 제스처를 취함으로써 트리거 신호를 발생시킬 수 있다. 착용형 기기는 상기 제스처로 인해 발생한 트리거 신호를 센서들(133, 153, 155) 중 적어도 일부를 이용하여 센싱한다. 트리거 신호가 센싱된 경우, 착용형 기기는 사용자 인증 절차를 개시할 수 있다. 일실시예에 따르면, 상기 제스처는 사용자가 착용형 기기를 착용한 상태에서 사용자가 의도적으로(on purpose) 입력하는(착용 과정에서 잘 취하지 않는) 제스처일 수 있다.

- [0035] 사용자가 착용형 기기를 착용한 채, 손을 짹 펴거나 손목을 꺾는 등과 같은 일정한 제스처(gesture)를 취하는 경우, 착용형 기기의 뒷면(150)에 설치된 센서(155)에서는 해당 제스처에 의해 발생하는, 사용자의 근육의 움직임에 의해 발생된 생체 신호가 감지될 수 있다. 사용자의 제스처에 의해 발생하는, 사용자 인증을 개시하기 위한 트리거 신호로서의 생체 신호를 '제1 생체 신호'라고 한다.
- [0036] 제1 생체 신호는, 예를 들어, 사용자의 근육의 움직임 전, 후에 발생하는 근전도 신호(Electromyography; EMG), 사용자의 근육을 투과한 빛 신호, 및 사용자의 근육에 의해 발생하는 힘 등과 같은 신호를 포함할 수 있다. 즉, 사용자로부터 입력된, 특정 제스처에 의해서만 발생하는 생체 신호를 포함하는 개념이다.
- [0037] 착용형 기기는 기기의 뒷면(150)에 설치된 센서(155)에 의해 감지된 제1 생체 신호에 의해 해당 사용자에 대한 사용자 인증 절차가 개시(initiate)되면, 기기의 앞면(130)에 설치된 센서(133) 및 뒷면(150)에 설치된 센서(155)에 의해 감지된 제2 생체 신호를 이용하여 사용자를 인증할 수 있다.
- [0038] 제2 생체 신호는 제1 생체 신호와 구별될 수 있으며, 사용자마다 유니크(unique)한 고유의 생체 신호일 수 있다. 제2 생체 신호는 예를 들어, 심전도(ElectroCardioGraphy; ECG) 신호, 광용적맥파(PhotoPlethysmoGram; PPG) 신호, 사용자의 음성(voice), 및 사용자의 신체에서 발생하는 임피던스(impedance) 신호 등을 포함할 수 있다. 구현에 따라, 사용자마다 유니크한 고유의 생체 신호로서, 사용자의 홍채 또는 지문을 인식하여 이를 제1 생체 신호로 사용할 수 있다.
- [0039] 일실시예에 따른 착용형(wearable) 기기는 도 1에 도시된 것과 같이, 시계형 스마트폰(110)일 수 있다. 도 1에 도시된 시계형 스마트폰(110)은 착용형 기기의 일례일 뿐, 다양한 응용 및 설계 변경이 가능함은 당업자에게 자명하다.
- [0040]
- [0041] 이하에서는, 사용자가 착용형 기기를 왼쪽 손목에 착용한 경우를 예로 들어, 착용형 기기의 동작을 설명한다.
- [0042] 왼쪽 손목에 착용형 기기를 착용한 사용자가 왼손을 짹 펴거나 왼손을 위로 꺾는 등 미리 정해진 일정한 제스처를 취할 수 있다. 해당 제스처로 인해, 트리거 신호로서의 제1 생체 신호가 발생되고, 착용형 기기는 제1 생체 신호를 센싱할 수 있다. 제1 생체 신호의 센싱에 대응하여, 착용형 기기는 사용자 인증 절차를 개시할 수 있다. 제1 생체 신호의 센싱과 사용자 인증 절차의 개시는 시간적으로 이격되어 수행될 수 있고, 구현에 따라 시간적으로 연속적으로(consecutively) 수행될 수 있다.
- [0043] 일실시예에 따르면, 해당 제스처로 인한 사용자의 근육의 움직임으로 인해 발생한 제1 생체 신호는 착용형 기기의 뒷면(150)에 설치된 센서(155)에 의해 감지될 수 있다. 센서(155)에 의해 감지된 제1 생체 신호는 착용형 기기의 메모리에 기록된, 사용자가 미리 설정한 트리거 신호와 비교되고, 비교 결과 동일하거나 미리 정해진 오차 범위 내에 속하는 것으로 판단되면, 사용자 인증 절차가 개시될 수 있다.
- [0044] 사용자 인증 절차가 개시된 후, 사용자는 착용형 기기의 앞면(130)에 설치된 센서(133)에 오른손 손가락을 위치시키고, 착용형 기기는 센서(133)를 통해 사용자로부터 제2 생체 신호를 감지할 수 있다. 이때, 착용형 기기의 뒷면(150)에 설치된 센서(153) 또한 사용자의 피부에 접촉해 있으므로, 앞면(130)에 설치된 센서(133)와 마찬가지로 제2 생체 신호를 감지할 수 있다. 예를 들어, 센서(155)는 사용자의 근전도(EMG) 신호를 감지하고, 센서(133) 및 센서(153)은 사용자의 심전도(ECG) 신호를 감지할 수 있다.
- [0045] 일실시예에서, 제2 생체 신호의 일 예인 심전도(ECG) 신호를 감지하기 위해서는 사용자 신체의 서로 다른 적어도 두 부분에서 수집된 신호가 필요하므로, 착용형 기기의 앞면(130)과 뒷면에 각각 센서들(133, 153)을 설치하였다. 실시예에 따라서, 심전도(ECG) 신호 이외에 사용자의 음성(voice) 및 상기 사용자의 신체에서 발생하는 임피던스(impedance) 신호 등과 같이 신체의 한 부분을 통해서 사용자에게 유니크한 생체 신호를 감지할 수 있는 경우, 제2 생체 신호를 수신하는 센서는 착용형 기기의 앞면(130) 혹은 뒷면(150)에 하나만 설치될 수도 있다. 제1 생체 신호 및 제2 생체 신호를 감지하는 센서들의 개수는 필요에 따라 달라질 수 있다.
- [0046] 도 2는 일실시예에 따른 착용형(wearable) 기기의 블록도이다.
- [0047] 도 2를 참조하면, 일실시예에 따른 착용형(wearable) 기기(200)는 제1 감지부(210), 제2 감지부(220), 메모리(230) 및 프로세서(240)를 포함할 수 있다.
- [0048] 제1 감지부(210)는 사용자의 제스처(gesture)에 의해 발생하는 제1 생체 신호를 감지할 수 있다. 제1 생체 신

호는 제스처를 입력하기 위한 사용자의 근육의 움직임에 의해 발생할 수 있다. 상기 제1 생체 신호는, 예를 들어, 사용자의 근육의 움직임 전, 후에 발생하는 근전도 신호(Electromyography; EMG), 사용자의 근육을 투과한 빛 신호, 및 사용자의 근육에 의해 발생하는 힘 등일 수 있다.

[0049] 이때, 사용자의 제스처에는 예를 들어, 손목을 꺾거나 비트는 제스처, 손을 휘젓는 제스처, 주먹을 쥐는 제스처 등과 같이 사용자가 착용형 기기를 착용한 신체 부위를 이용하여 취할 수 있는 다양한 형태 중 어느 하나일 수 있다. 구현에 따라, 좀 더 높은 레벨의 사용자 인증이 필요한 경우, 사용자는 연속적으로 입력된 둘 이상의 제스처를 통해 사용자 인증 절차가 개시되도록 할 수 있다.

[0050] 제2 감지부(220)는 사용자의 제2 생체 신호를 감지할 수 있다. 제2 생체 신호에는 심전도(ElectroCardioGraphy; ECG) 신호, 광용적맥파(PhotoPlethysmoGram; PPG) 신호, 사용자의 음성(voice) 또는 사용자의 신체에서 발생하는 임피던스(impedance) 신호 등이 해당될 수 있다.

[0051] 메모리(230)는 하나 이상의 사용자에 대해, 제1 생체 신호 및 제2 생체 신호를 직접 또는 간접적으로 표현(represent)하는 적어도 하나의 정보를 기록(혹은 저장)할 수 있다.

[0052] 제1 생체 신호 및 제2 생체 신호를 직접적으로 표현하는 정보는, 예를 들어, 제1 생체 신호 및 제2 생체 신호를 샘플링한 경우, 샘플링된 데이터 심볼의 적어도 일부로 표현되는 정보이거나, 제1 생체 신호 및 제2 생체 신호에 대한 모사 신호(duplicated signal)일 수 있다.

[0053] 제1 생체 신호 및 제2 생체 신호를 간접적으로 표현하는 정보는, 다양한 신호 처리(signal processing) 기법에 따라 제1 생체 신호 및 제2 생체 신호가 가공되어 표현된 정보일 수 있다.

[0054] 일 실시예에서, 메모리(230)는 제1 생체 신호 및 제2 생체 신호에 대한 신호 처리를 통해 획득한 적어도 하나의 특징점 정보를 저장할 수 있다.

[0055] 메모리(230)에 저장되는 상기 정보는 암호화되어 저장될 수 있다. 구현에 따라, 메모리에 저장된 정보에 대한 정상적인 접속이 아닌 경우, 메모리에 저장된 상기 정보가 유출되지 않도록 설계될 수 있다. 사용자가 착용형 기기를 분실한 경우, 제3자가 메모리(230)에 저장된 상기 정보를 비정상적인 방법으로 판독할 수 없도록 하는 다양한 방법이 채용될 수 있다.

[0056] 프로세서(240)는 메모리(230)를 참조(refer) 하여, 제1 감지부(210)에서 감지된 제1 생체 신호가 메모리(230)에 기록된 정보와 대응되는지 판단하고, 제1 생체 신호와 상기 정보가 대응되는 경우 사용자 인증 절차를 개시한다.

[0057] 프로세서(240)는 제2 감지부(220)에서 감지된 제2 생체 신호와 메모리(230)에 기록된 정보를 비교하여 사용자를 인증할 수 있다. 프로세서(240)는 제2 감지부(220)를 통해 수신한 제2 생체 신호와, 메모리(230)에 기록된 정보를 비교할 때, 미리 정해진 오차 범위를 고려하여 동작할 수 있다. 이때, 오차 범위는 사용자에게 의해 설정되거나, 혹은 통계 결과 등에 기초하여 착용형(wearable) 기기(200)에 미리 설정되어 있을 수 있다.

[0058] 예를 들어, 사용자에게 의해 미리 설정된 오차 범위가 7%라고 가정하자.

[0059] 프로세서(240)가 제2 감지부(220)를 통해 수신한 제2 생체 신호와 메모리(230)에 기록된 정보를 비교한 결과 5%의 오차가 발생했다면, 비교 결과가 미리 정해진 오차 범위 이내이므로 프로세서(240)는 제2 감지부(220)를 통해 수신한 제2 생체 신호와 메모리(230)에 기록된 정보가 일치하는 것으로 판단할 수 있다. 프로세서(240)는 해당 사용자를 인증할 수 있다. 만약, 제2 감지부(220)를 통해 수신한 제2 생체 신호와 메모리(230)에 기록된 정보 간의 비교 결과 10%이 오차가 발생했다면, 프로세서(240)는 해당 사용자를 인증하지 않는다. 프로세서(240)는 착용형 기기의 화면, 스피커, 또는 진동 수단을 통해 인증 결과를 사용자에게 시각적, 청각적, 또는 촉각적으로 알려줄 수 있다.

[0060] 도 3은 다른 실시예에 따른 착용형(wearable) 기기의 블록도이다.

[0061] 도 3을 참조하면, 다른 실시예에 따른 착용형(wearable) 기기(300)는 제1 감지부(310), 제2 감지부(320), 메모리(330), 프로세서(340), 초기 인증부(350) 및 착용 감지부(360)를 포함할 수 있다.

[0062] 메모리(330)에는 착용형 기기(300)에서 실행 가능한 하나 이상의 기능에 대한 접근 권한 정보가 더 기록될 수 있다. 여기서, 각 기능에 대한 접근 권한은, 유선 또는 무선 통신으로 착용형 기기(300)와 연결된 외부 기기

(예를 들어, PC, 노트북, 스마트 폰 등)를 통해 설정되거나, 착용형 기기(300) 자체를 통해 설정될 수 있다.

- [0063] 메모리(330)에 저장된, 실행 가능한 하나 이상의 기능에 대한 접근 권한 정보에 대한 일 예는 도 8을 참조하여 뒤에서 상세히 설명한다.
- [0064] 프로세서(340)는 착용형 기기(300)에서 사용자로부터 기능에 대한 실행 명령이 입력된 경우, 메모리(330)를 참조하여 해당 기능에 대응하는 접근 권한 정보를 읽고, 접근 권한 정보에 따라 사용자에게 시각적, 청각적, 또는 촉각적 피드백 중 적어도 하나를 제공할 수 있다. 여기서, 각 피드백은 사용자에게 대한 인증 요청일 수 있다.
- [0065] 착용형 기기(300)는 예를 들어, 금융 업무(스마트 폰 뱅킹), 개인 메일 열람, 인터넷 사용, SMS 전송 등과 같이 실행 가능한 다양한 기능들을 구비할 수 있고, 각 기능들은 서로 다른 접근 권한을 필요로 할 수 있다. 메모리(330)는 착용형 기기(300)에서 실행 가능한 다양한 기능들에 대응하는 접근 권한 정보를 저장할 수 있다.
- [0066] 예를 들어, 스마트 폰 뱅킹 기능 및 개인 메일 열람 기능은 높은 레벨의 접근 권한 정보를 필요로 하고, 인터넷 사용, SMS 전송은 낮은 레벨의 접근 권한 정보를 필요로 한다고 하자.
- [0067] 사용자로부터 개인 메일 열람 기능에 대한 실행 명령이 입력되면, 프로세서(340)는 메모리(330)를 참조하여 해당 기능(예를 들어, 개인 메일 열람 기능)에 대응하는 접근 권한 정보를 읽는다. 이때, 메모리(330)에 저장된, 개인 메일 열람 기능에 대응하는 접근 권한 정보는 높은 레벨에 해당할 수 있다.
- [0068] 프로세서(340)는 접근 권한 정보에 따라 사용자에게 높은 수준의 사용자 인증을 요청하는 시각적, 청각적, 또는 촉각적 피드백 중 적어도 하나를 제공할 수 있다. 시각적 피드백은 예를 들어, 착용형(wearable) 기기(300)의 화면에 디스플레이에 표시되는 피드백일 수 있다. 청각적 피드백은 착용형(wearable) 기기(300)의 스피커 등을 통해 사용자에게 소리 형태로 전달되는 피드백일 수 있다. 촉각적 피드백은 착용형 기기의 진동 수단 등을 통해 사용자에게 촉각 형태로 전달되는 피드백일 수 있다.
- [0069] 초기 인증부(350)는 제1 감지부(310) 및 제2 감지부(320)를 통해, 사용자로부터 초기 인증 설정을 위한 제스처 및 제2 생체 신호를 입력 받고, 입력된 제스처에 대응하는 제1 생체 신호 및 제2 생체 신호를 메모리(300)에 기록할 수 있다.
- [0070] 착용 감지부(360)는 착용형 기기가 사용자로부터 분리되는지 여부를 감지할 수 있다. 착용 감지부(360)는 착용형 기기와 연결되어 사용자의 신체 일부에 부착되는 밴드의 기계적 움직임(mechanical movement)을 감지하거나, 밴드의 탈착에 대응하여 발생하는 전기적 신호를 감지할 수 있다.
- [0071] 착용 감지부(360)는 착용형 기기와 연결되어 사용자의 신체 일부에 부착되는 밴드의 탈착 시에 발생하는 다음과 같은 변화를 감지할 수 있다.
- [0072] 착용 감지부(360)는 예를 들어, 사용자의 손목에 부착된 밴드에 주어지는 장력 혹은 탄성력이 강해지거나 갑자기 약해지는 변화를 감지할 수 있다. 또한, 착용 감지부(360)는 예를 들어, 착용형 기기의 뒷면에 부착된 광센서의 수광부에 의해 감지되는 빛의 양의 변화를 감지하거나, 혹은 밴드의 탈착 시에 착용 감지부(360)와 피부와의 접점이 생기거나 혹은 없어짐으로 인해 전기적 신호(임피던스 신호)가 강화되거나 혹은 약화되는 등의 변화를 감지할 수 있다.
- [0073] 이 밖에도, 착용 감지부(360)는 착용형 기기의 착용 여부를 감지할 수 있는 다양한 센서들을 포함하고, 센서들에서 감지된 변화를 프로세서(340)에게 전달할 수 있다.
- [0074] 프로세서(340)는 착용 감지부(360)로부터 수신한 신호에 기초하여, 사용자에게 대한 인증이 널(NULL)이 되도록 제어할 수 있다. 여기서, '사용자에게 대한 인증이 널(NULL)이 된다'는 것은 착용형 기기를 착용할 때 수행한 사용자 인증 절차를 통해 사용자에게 부여된 사용 권한이 철회 혹은 무효화(nullify) 되는 것을 의미한다. 사용자에게 대한 인증이 널(NULL)이 된 경우, 사용자는 착용형 기기(300)를 다시 착용할 때 다시 사용자 인증 절차를 거쳐 정당한 사용 권한을 획득해야 한다.
- [0075] 메모리(330)는 하나 이상의 사용자 각각에 대응하는 기기 설정 정보를 더 기록할 수 있다. 프로세서(340)는 사용자가 인증된 경우, 메모리(330)를 참조하여 인증된 사용자의 기기 설정 정보를 읽고, 기기 설정 정보에 따라 사용자 인터페이스(User Interface)를 제공할 수 있다.
- [0076] 예를 들어, 메모리(330)에는 사용자 A 및 사용자 B 각각을 위한 서로 다른 기기 설정 정보 또는 환경 설정 정보가 저장될 수 있다. 프로세서(340)는 인증된 사용자가 사용자 A인 경우, 사용자 A에 대응하여 메모리(330)에 저장된 기기 설정 정보를 읽어 사용자 A를 위한 바탕 화면 및 어플리케이션 실행을 위한 아이콘 배치 등을 제공

할 수 있다.

- [0077] 도 3의 제1 감지부(310), 제2 감지부(320), 메모리(330), 프로세서(340)에 대하여 상술한 내용 이외의 동작은 도 2의 제1 감지부(210), 제2 감지부(220), 메모리(230) 및 프로세서(240)와 동일하므로, 상세한 설명은 생략한다.
- [0078] 도 4는 일실시예에 따른 착용형 기기의 인증 방법을 나타낸 플로우차트이다.
- [0079] 도 4를 참조하면, 일실시예에 따른 착용형 기기는 사용자의 제스처(gesture)에 의해 발생하는 제1 생체 신호를 감지할 수 있다(410). 제1 생체 신호는 제스처를 입력하기 위한 사용자의 근육의 움직임에 의해 발생될 수 있다. 제1 생체 신호는 사용자의 근육의 움직임 전, 후에 발생하는 근전도 신호(Electromyography; EMG), 사용자의 근육을 투과한 빛 신호, 및 사용자의 근육에 의해 발생하는 힘 등 중 어느 하나일 수 있다.
- [0080] 착용형 기기는 사용자의 제2 생체 신호를 감지할 수 있다(420). 제2 생체 신호는 제1 생체 신호와 구별되는 신호로서, 심전도(ElectroCardioGraphy; ECG) 신호, 광용적맥파(PhotoPlethysmoGram; PPG) 신호, 사용자의 음성(voice) 및 사용자의 신체에서 발생하는 임피던스(impedance) 신호 등 중 어느 하나일 수 있다.
- [0081] 착용형 기기는 하나 이상의 사용자에 대해, 제1 생체 신호 및 제2 생체 신호를 직접 또는 간접적으로 표현(represent)하는 적어도 하나의 정보를 메모리에 기록할 수 있다(430).
- [0082] 착용형 기기는 제1 감지부에서 감지된 제1 생체 신호가 메모리에 기록된 정보와 대응되는지 판단할 수 있다(440).
- [0083] 단계(430)에서, 제1 생체 신호가 메모리에 기록된 정보와 대응되지 않는다고 판단되면, 착용형 기기는 동작을 종료할 수 있다.
- [0084] 단계(430)에서, 제1 생체 신호가 메모리에 기록된 정보와 대응된다고 판단되면, 착용형 기기는 사용자 인증 절차를 개시할 수 있다(450).
- [0085] 착용형 기기는 제2 감지부에서 감지된 제2 생체 신호와 메모리에 기록된 정보를 비교(460)한 후, 사용자를 인증할 수 있다(470).
- [0086] 실시예에 따라서, 사용자가 인증된 경우, 착용형 기기는 메모리를 참조하여 인증된 사용자의 기기 설정 정보를 읽고, 기기 설정 정보에 따라 사용자 인터페이스(User Interface)를 제공할 수 있다. 이때, 착용형 기기의 메모리에는 하나 이상의 사용자 각각에 대응하는 기기 설정 정보가 저장될 수 있다.
- [0087] 도 5는 다른 실시예에 따른 착용형 기기의 인증 방법을 나타낸 플로우차트이다.
- [0088] 도 5를 참조하면, 일실시예에 따른 착용형 기기는 사용자로부터 제스처 및 2 생체 신호를 입력 받을 수 있다(510).
- [0089] 착용형 기기는, 단계(510)에서 입력된 제스처에 대응하는 제1 생체 신호 및 제2 생체 신호를 메모리에 기록할 수 있다(515). 단계(510) 내지 단계(515)는 초기(initial) 사용자 정보를 저장하는 과정으로서, 이 때 저장되는 사용자 정보는 이후 착용형 기기에 대한 사용자 인증에 이용된다. 착용형 기기를 사용하는 사용자들이 둘 이상인 경우, 단계(510) 내지 단계(515)에서 기록되는 정보는 각 사용자들마다에 대응하여 관리될 수 있다.
- [0090] 착용형 기기는 사용자의 제스처(gesture)에 의해 발생하는 제1 생체 신호를 감지할 수 있다(520). 제1 생체 신호는 제스처를 입력하기 위한 사용자의 근육의 움직임에 의해 발생될 수 있다. 제1 생체 신호는 사용자의 근육의 움직임 전, 후에 발생하는 근전도 신호(Electromyography; EMG), 사용자의 근육을 투과한 빛 신호, 및 사용자의 근육에 의해 발생하는 힘 등을 일 예로 들 수 있다.
- [0091] 착용형 기기는 사용자의 제2 생체 신호를 감지할 수 있다(525). 제2 생체 신호는 제1 생체 신호와 구별되는 사용자마다 유니크한 생체 신호로서, 심전도(ElectroCardioGraphy; ECG) 신호, 광용적맥파(PhotoPlethysmoGram; PPG) 신호, 사용자의 음성(voice) 및 사용자의 신체에서 발생하는 임피던스(impedance) 신호 등을 일 예로 들 수 있다.
- [0092] 착용형 기기는 하나 이상의 사용자에 대해, 제1 생체 신호 및 제2 생체 신호를 직접 또는 간접적으로 표현

(represent)하는 적어도 하나의 정보를 메모리에 기록할 수 있다(530).

- [0093] 착용형 기기는 제1 감지부에서 감지된 제1 생체 신호가 메모리에 기록된 정보와 대응되는지 판단할 수 있다(535). 단계(535)에서, 제1 생체 신호가 메모리에 기록된 정보와 대응되지 않는다고 판단되면, 착용형 기기는 동작을 종료할 수 있다.
- [0094] 단계(535)에서, 제1 생체 신호가 메모리에 기록된 정보와 대응된다고 판단되면, 착용형 기기는 사용자 인증 절차를 개시할 수 있다(540).
- [0095] 착용형 기기는 제2 감지부에서 감지된 제2 생체 신호와 메모리에 기록된 정보를 비교할 수 있다(545).
- [0096] 착용형 기기는 제2 감지부에서 감지된 제2 생체 신호와 메모리에 기록된 정보가 미리 정해진 오차 범위 내인지 여부를 판단할 수 있다(550).
- [0097] 단계(550)에서, 제2 감지부에서 감지된 제2 생체 신호와 메모리에 기록된 정보가 미리 정해진 오차 범위 내라고 판단되면, 착용형 기기는 사용자를 인증할 수 있다(555).
- [0098] 단계(550)에서, 제2 감지부에서 감지된 제2 생체 신호와 메모리에 기록된 정보가 미리 정해진 오차 범위의 밖이라고 판단되면, 착용형 기기는 동작을 종료할 수 있다. 이때, 실시예에 따라서는 제2 감지부에서 감지된 제2 생체 신호와 메모리에 기록된 정보가 미리 정해진 오차 범위 밖인 경우, 착용형 기기는 시간 또는 날짜 등과 같은 기본 정보만 사용자에게 제공하도록 구현될 수도 있다.
- [0099] 도 6은 일실시예에 따른 착용형 기기에서 사용자의 접근 권한 정보에 따라 서로 다른 기능을 제공하기 위한 인증 방법을 나타낸 플로우차트이다.
- [0100] 도 6을 참조하면, 일실시예에 따른 착용형 기기는 착용형 기기에서 실행 가능한 하나 이상의 기능에 대한 접근 권한 정보를 기록할 수 있다(610).
- [0101] 착용형 기기는 사용자로부터, 착용형 기기에서 실행 가능한 기능들 중 어느 하나의 기능에 대한 실행 명령을 입력 받을 수 있다(620).
- [0102] 단계(620)에서, 실행 명령이 입력되면, 착용형 기기는 메모리를 참조하여 실행 명령이 입력된 기능에 대응하는 접근 권한 정보를 읽을 수 있다(630).
- [0103] 착용형 기기는 접근 권한 정보에 따라 사용자에게 시각적, 청각적, 또는 촉각적 피드백 중 적어도 하나를 제공할 수 있다(640). 이때 각 피드백은 사용자 인증을 요청하는 피드백일 수 있다.
- [0104] 도 7은 일실시예에 따른 착용형 기기가 사용자로부터 분리된 경우의 동작 방법을 나타낸 플로우차트이다. 이하에서는 착용 감지부가 임피던스 변화를 감지하는 센서를 구비한 경우를 예로 들어 설명한다.
- [0105] 도 7을 참조하면, 착용형 기기는 착용 감지부로부터 입력되는 임피던스의 변화를 감지할 수 있다(710).
- [0106] 착용형 기기는 단계(710)에서 감지된 임피던스의 변화로부터 착용형 기기가 사용자로부터 분리되었는지 여부를 판단할 수 있다(720).
- [0107] 단계(720)에서, 예를 들어, 착용형 기기에 입력되는 임피던스 값이 일정 수준에 미치지 못하거나, 일정 수준에서 낮은 값으로 변화된 경우, 착용형 기기는 착용형 기기가 사용자로부터 분리된 것으로 판단할 수 있다. 단계(720)에서, 착용형 기기에 입력되는 임피던스 값이 일정 수준의 값을 유지하거나, 일정 수준의 값으로 상승한 경우, 착용형 기기는 착용형 기기가 사용자로부터 분리되지 않은 것으로 판단할 수 있다.
- [0108] 단계(720)에서, 착용형 기기가 사용자로부터 분리된 것으로 판단되면, 착용형 기기는 사용자에 대한 인증이 널(NULL)이 되도록 제어할 수 있다(730).
- [0109] 단계(720)에서, 착용형 기기가 사용자로부터 분리되지 않은 것으로 판단되면, 착용형 기기는 사용자에 대한 인증이 유지되도록 제어할 수 있다(740).
- [0110] 실시예에 따라서, 착용 감지부는 착용형 기기 뒷면에 수집되는 빛의 양을 감지하는 광 센서를 구비하거나, 밴드의 장력을 감지하는 센서를 구비할 수도 있다. 이러한 경우, 각 센서들의 특징에 따라 상술한 내용과 동일 혹은

은 유사한 방식으로 분리 여부가 판단될 수 있다.

- [0111] 도 8을 일실시예에 따른 착용형 기기의 메모리가 저장하는, 실행 가능한 하나 이상의 기능에 대한 접근 권한 정보에 대한 일 예를 나타낸 도면이다.
- [0112] 도 8을 참조하면, 일실시예에 따른 착용형 기기의 메모리에는 예를 들어, 금융 업무(스마트 폰 뱅킹), 개인 메일 열람, 인터넷 사용, SMS 전송, 시간 및 날씨 제공 등과 같이 실행 가능한 다양한 기능들에 대한 실행 명령 코드와 각 기능들에 대응하는 접근 권한 정보가 저장될 수 있다.
- [0113] 이때, 메모리에는 각 기능들에 대응하여 설정된 서로 다른 접근 권한이 기록될 수 있다.
- [0114] 예를 들어, 금융 업무(스마트 폰 뱅킹), 개인 메일 열람 등과 같이 중요한 금융 정보 및 개인의 사생활 보호와 관련된 기능에는 레벨 4의 접근 권한이 설정될 수 있고, 인터넷 사용, SMS 전송 등과 같은 기능에 대하여는 레벨 3의 접근 권한이 설정될 수 있다. 이 밖에, 날씨나 시간 제공 기능과 같이 보안이 필요 없는 기능의 경우, 레벨 0의 접근 권한이 설정될 수 있다. 실시예에 따라서, 레벨 0의 접근 권한이 설정된 기능의 경우, 해당 사용자에게 대한 인증을 거치지 않거나 인증에 실패하더라도 해당 기능을 제공하도록 할 수 있다.
- [0115] 예를 들어, 사용자로부터 실행 명령이 입력되면, 프로세서는 메모리를 참조하여 해당 실행 명령의 코드에 의해 입력된 명령이 어떠한 기능에 대한 것인지를 확인하고, 해당 기능에 대응하는 접근 권한 정보를 읽는다.
- [0116] 이때, 입력된 실행 명령이 #00011 이라면, 프로세서는 해당 기능이 개인 메일 열람 기능임을 파악하고, 개인 메일 열람 기능에 대응하는 접근 권한이 레벨 4임을 확인한다.
- [0117] 프로세서는 접근 권한 정보(레벨 4)에 따라 시각적, 청각적, 또는 촉각적 피드백 등에 의해 사용자에게 추가적인 사용자 인증을 요청할 수 있다.
- [0118] 일실시예에서는 착용형 기기에서 실행 가능한 하나 이상의 기능에 대한 접근 권한 정보가 접근 권한의 레벨 형태로 저장되는 경우에 대하여 설명하였으나, 실시예에 따라서, 접근 권한 정보는 이외의 다양한 형태로 저장될 수 있다.
- [0119] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 컨트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.
- [0120] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.
- [0121] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등

을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0122] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

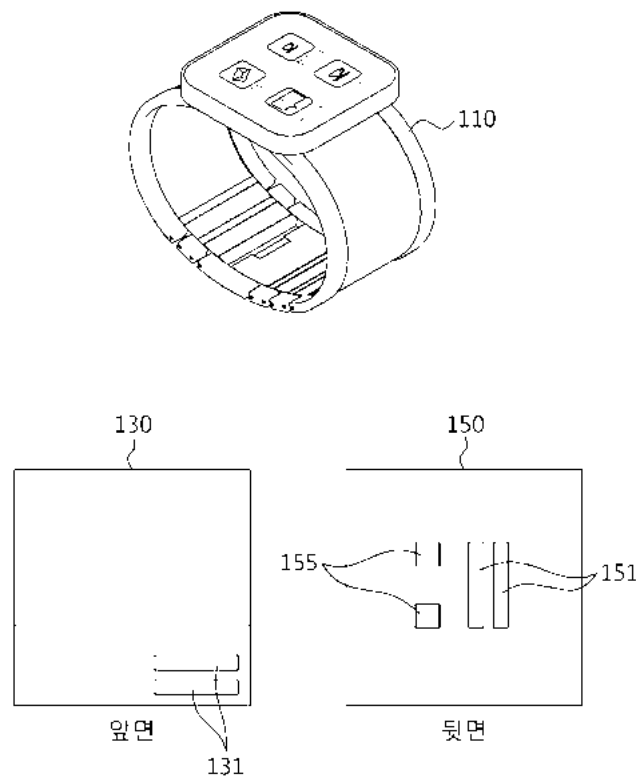
[0123] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

부호의 설명

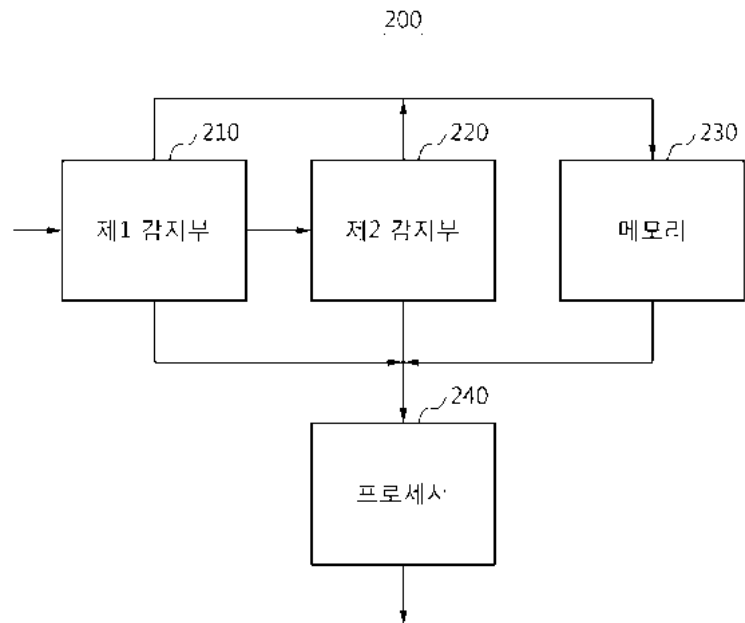
[0124] 200: 착용형 기기
210: 제1 감지부
220: 제2 감지부
230: 메모리
240: 프로세서

도면

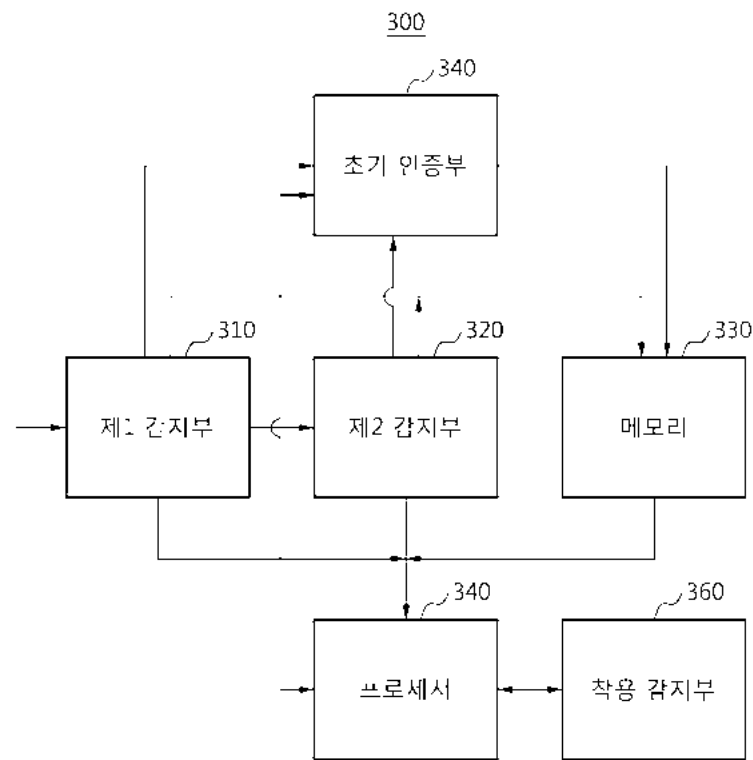
도면1



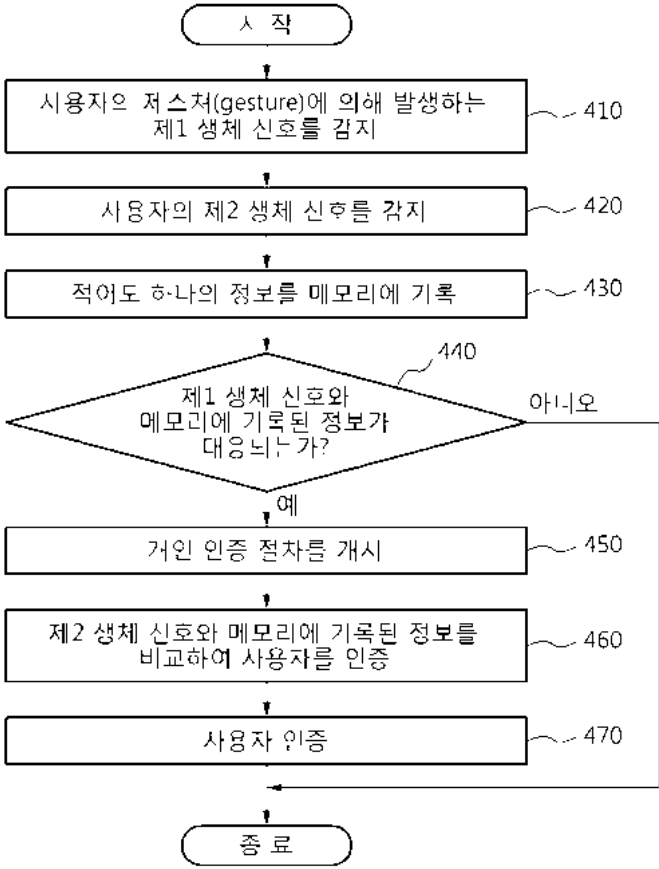
도면2



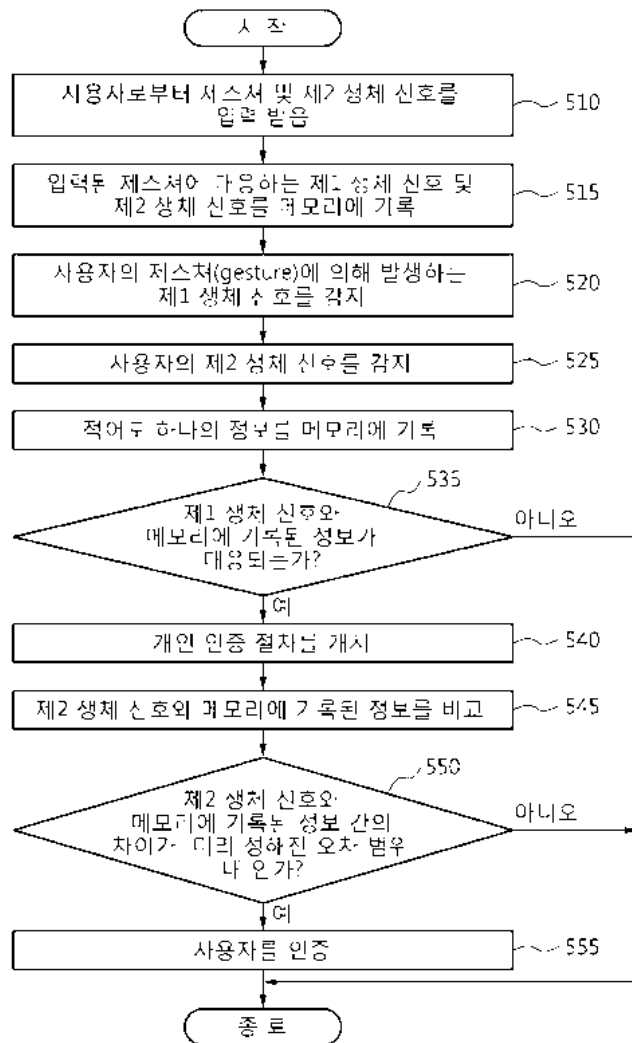
도면3



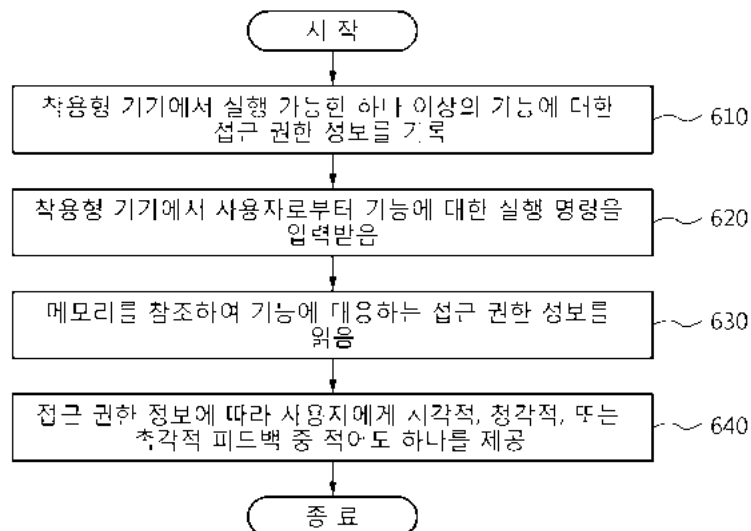
도면4



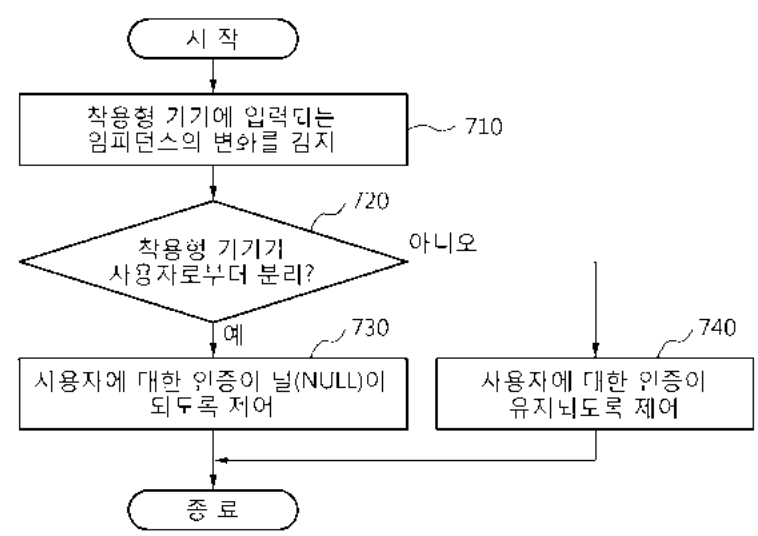
도면5



도면6



도면7



도면8

기능	실행 명령 코드	접근 권한 정보	
금융 업무	#00001	Level : 4	
개인 메일 열람	#00011	Level : 4	
인터넷 사용	#00111	Level : 3	...
SMS 전송	#01111	Level : 3	
시계	#11111	Level : 0 (기본 기능)	
날씨 확인	#11110	Level : 0 (기본 기능)	

⋮

【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 16

【변경전】

상기 제2 감지부에서

【변경후】

제2 감지부에서

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 16

【변경전】

상기 제1 감지부에서

【변경후】

제1 감지부에서