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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2019 (21.03.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/054582 A1

(51) International Patent Classification:
G06F 21/32 (2013.01) *G06F 21/45* (2013.01)
G06K 9/00 (2006.01)

(21) International Application Number:
PCT/KR2018/000664

(22) International Filing Date:
15 January 2018 (15.01.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2017-0118611 15 September 2017 (15.09.2017) KR

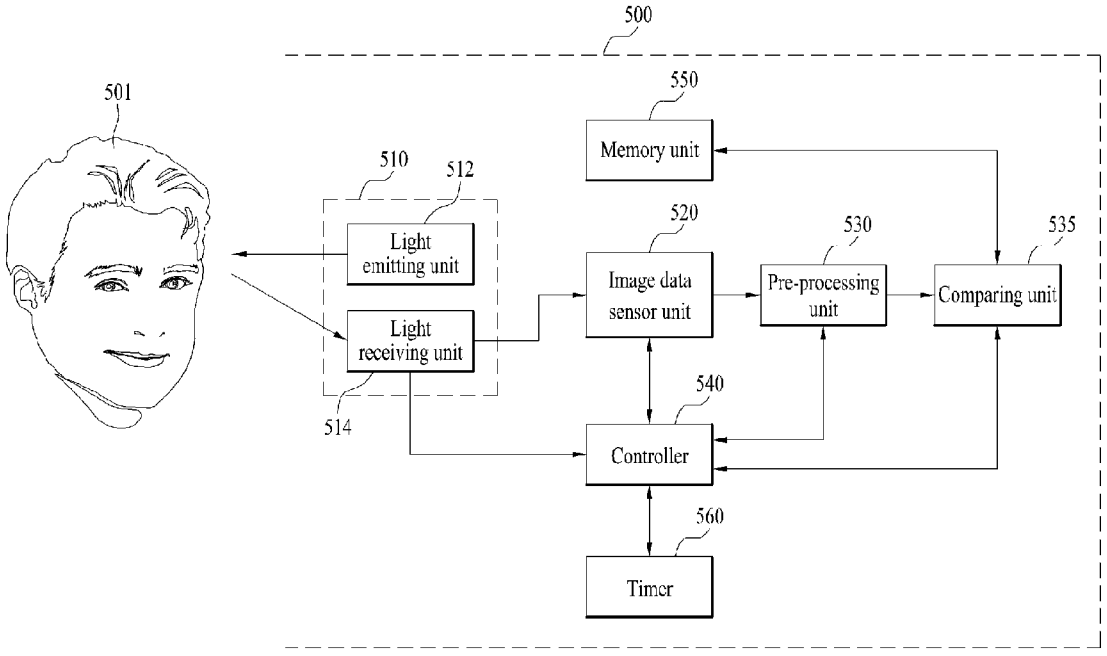
(71) Applicant: **LG ELECTRONICS INC.** [KR/KR]; 128, Yeoui-daero, Yeongdeungpo-gu, Seoul 07336 (KR).

(72) Inventors: **LEE, Chaedeok**; IP Center, LG Electronics Inc., 19, Yangjae-daero 11-gil, Seocho-gu, Seoul 06772 (KR). **PARK, Seonghong**; IP Center, LG Electronics Inc., 19, Yangjae-daero 11-gil, Seocho-gu, Seoul 06772 (KR). **LEE, Junhak**; IP Center, LG Electronics Inc., 19, Yangjae-daero 11-gil, Seocho-gu, Seoul 06772 (KR).

(74) Agent: **KIM, Yong In** et al.; KBK & Associates, 7th Floor, 82, Olympic-ro, Songpa-gu, Seoul 05556 (KR).

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

(54) Title: DIGITAL DEVICE AND BIOMETRIC AUTHENTICATION METHOD THEREIN



(57) Abstract: A digital device including a camera unit; a display unit; and a controller configured to in response to a request to execute a first application on the digital device having a first security authentication level, control the camera unit to capture face image data of a target and perform a first authentication process by comparing the captured face image data with prestored face image data; and in response to a request to execute a second application on the digital device having a second security authentication level more secure than the first authentication level, control the camera unit to capture vein image data of a particular body part of the target, and perform the first authentication process and a second authentication process by comparing the captured vein image data with prestored vein image data.

WO 2019/054582 A1

[Continued on next page]

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

Published:

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

Description

Title of Invention: DIGITAL DEVICE AND BIOMETRIC AUTHENTICATION METHOD THEREIN

Technical Field

[1] The present invention relates to a digital device, and more particularly, to a digital device and biometric authentication method therein. Although the present invention is suitable for a wide scope of applications, it is particularly suitable for performing both face authentication and vein authentication of a body part.

Background Art

[2] Generally, when financial transactions and the like are performed using a digital device such as a mobile terminal or the like, security authentication is required. Security authentication methods include entering a security authentication password, performing personal authentication by capturing a user's specific part such as a face, a fingerprint or the like through a camera, etc.

[3] Yet, since such a security authentication method can be performed by others, it causes a problem of reduced safety. Recently, a digital device adopting a biometric authentication system capable of performing authentication through biometric information of vein and the like has been developed.

[4] A digital device of processing biometric authentication can perform biometric authentication by obtaining a biometric image of a palm, a finger, or the like and analyzing unique biometric property of 'palm's vein, finger's vein or the like. Particularly, according to a vein authentication technology, infrared light of a specific wavelength is applied to a specific part of a human body, an image is photographed using an image sensor, and an image having a blood vessel pattern represented in black is then obtained. Therefore, a specific person can be authenticated by analyzing a blood vessel pattern that is different for each person.

[5] However, since the related art vein authentication is configured with a non-contact reflective or transmissive sensor module including an image sensor and an optical system, it is difficult to downsize and reduce the cost of the sensor module. Thus, the demand for developing a digital device, which can improve safety and reliability of security authentication by performing face recognition and vein authentication of a body part using a 3-dimensional (3D) camera that can be downsized and low-priced, is rising.

Disclosure of Invention

Technical Problem

[6] Accordingly, embodiments of the present invention are directed to a digital device

and biometric authentication method therein that substantially obviate one or more problems due to limitations and disadvantages of the related art.

[7] One object of the present invention is to provide a digital device and biometric authentication method therein, by which personal authentication can be performed quickly and conveniently by extracting a vein pattern of a body part by applying ToF (time of flight) employing a near infrared light source and then using the extracted vein pattern.

[8] Another object of the present invention is to provide a digital device and biometric authentication method therein, by which safety and reliability of security authentication can be improved by performing face authentication and vein authentication of a body part by applying ToF (time of flight) employing a near infrared light source.

[9] Still another object of the present invention is to provide a digital device and biometric authentication method therein, by which security can be reinforced with higher accuracy by performing face authentication and vein authentication of multiple body parts according to a security level.

[10] Technical tasks obtainable from the present invention are non-limited by the above-mentioned technical tasks. In addition, other unmentioned technical tasks can be clearly understood from the following description by those having ordinary skill in the technical field to which the present invention pertains. Additional advantages, objects, and features of the invention will be set forth in the disclosure herein as well as the accompanying drawings. Such aspects may also be appreciated by those skilled in the art based on the disclosure herein.

Solution to Problem

[11] To achieve these and other advantages and in accordance with the purpose of the present invention, as embodied and broadly described herein, the present invention provides in one aspect a digital device, including a camera unit, an image data sensor unit sensing image data of a target captured by the camera unit, a memory unit storing face image data and vein image data of a body part for authentication, a pre-processing unit determining information of the captured target from the image data sensed by the image data sensor unit, the pre-processing unit, if the determined image data is face image data or vein data of a body part, creating processed face image data or processed body vein image data for authentication, a comparing unit comparing the processed image data with at least one of the face image data or the vein image data of the body part stored in the memory unit, and a controller, if an execution mode to be executed is a security authentication mode, activating the camera unit to be ready to receive the image data of the target, the controller, if the image data is face image data, performing a primary authentication by comparing the processed face image data with the face

image data previously stored for authentication in the memory unit, the controller performing a secondary authentication by comparing the vein image data of at least one processed body part with the vein image data of at least one authentication body part previously stored for authentication in the memory unit according to a result of the primary authentication.

[12] In another aspect, the present invention provides a digital device, including a camera unit, an image data sensor unit sensing image data of a target captured by the camera unit, a memory unit storing face image data and face vein image data for authentication, a pre-processing unit determining information of the captured target from the image data sensed by the image data sensor unit, the pre-processing unit, if the determined image data is face image data or face vein data, creating processed face image data or processed face vein image data for authentication, a comparing unit comparing the processed image data with at least one of the face image data or the face vein image data stored for authentication in the memory unit, and a controller, if an execution mode to be executed is a security authentication mode, activating the camera unit to be ready to receive the image data of the target, the controller, if the image data of the target is face image data, performing a primary authentication by comparing the processed face image data with the face image data previously stored for authentication in the memory unit, the controller performing a secondary authentication by comparing the processed face vein image data with the face vein image data stored for authentication in the memory unit according to a result of the primary authentication.

[13] In another aspect, the present invention provides a biometric authentication method in a digital device including a memory and a camera unit, including receiving a security authentication mode command, capturing a target to authenticate by activating the camera unit, sensing image data of the captured target, determining whether the image data is face mage data, if the image data is the face image data, creating processed face image data from the face image data, primarily comparing the processed face image data with the face image data stored for authentication in the memory unit, checking a result of the primarily comparing, capturing the target to authenticate using the camera unit according to a result of the primarily comparing, sensing image data of the captured target, if the image data is vein image data of at least one body part, creating vein image data of a processed body part, secondarily comparing the vein image data of the at least one processed body part with the vein image data of the at least one authentication body part previously stored for authentication in the memory unit, and ending the security authentication mode according to a result of the secondarily comparing.

[14] In another aspect, the present invention provides a biometric authentication method in a digital device including a memory and a camera unit, including receiving a

security authentication mode command, capturing a target to authenticate by activating the camera unit, sensing image data of the captured target, determining whether the image data is face mage data or face vein image data, if the image data is the face image data or the face vein image data, creating processed face image data or processed face vein image data from the face image data or the face vein image data, primarily comparing the processed face image data with the face image data stored for authentication in the memory unit, secondarily comparing the processed face vein image data with the face vein image data previously stored for authentication in the memory unit, and ending the security authentication mode according to a result of the secondarily comparing.

[15] In further aspect, the present invention provides a method of updating body vein data in a digital device including a memory and a camera unit, including receiving a security update mode command, capturing a target to update by activating the camera unit, sensing image data of the captured target, determining whether the image data is face mage data, if the image data is the face image data, creating processed face image data, comparing the processed face image data with face image data stored for authentication in the memory unit, capturing a target to authenticate using the camera unit, sensing image data of the captured target, if the image data is vein image data of at least one body part, creating vein image data of a processed body part, and updating the vein image data by saving the vein image data of the processed body part to the memory unit.

[16] Further scope of applicability of the present invention will become apparent from the detailed description given hereinafter. However, it should be understood that the detailed description and specific examples, while indicating preferred embodiments of the invention, are given by illustration only, since various changes and modifications within the spirit and scope of the invention will become apparent to those skilled in the art from this detailed description.

Advantageous Effects of Invention

[17] Accordingly, the present invention provides the following advantages. According to one embodiment of the present invention, personal authentication can be performed quickly and conveniently by extracting a vein pattern of a body part by applying ToF (time of flight) employing a near infrared light source and then using the extracted vein pattern.

[18] In addition, safety and reliability of security authentication can be improved by performing face authentication and vein authentication of a body part by applying ToF (time of flight) employing a near infrared light source. Further, the security can be reinforced and accuracy can be raised by performing face authentication and vein au-

thentication of multiple body parts according to a security level.

[19] Further, the present invention can perform personal authentication with high accuracy by obtaining 3D vein blood vessel information through depth information of a ToF sensor, compensate the inaccuracy of the related art face recognition through additional vein authentication, and apply use scenes of various types.

[20] Effects obtainable from the present invention are not limited by the above mentioned effect. In addition, other unmentioned effects can be clearly understood from the following description by those having ordinary skill in the technical field to which the present invention pertains.

Brief Description of Drawings

[21] Arrangements and embodiments may be described in detail with reference to the following drawings in which like reference numerals refer to like elements and wherein:

[22] FIG. 1 is a block diagram of a digital device according to one embodiment of the present invention;

[23] FIG. 2 is a block diagram of a digital device according to another embodiment of the present invention;

[24] FIG. 3 is a block diagram of an image processor of a digital device according to an embodiment of the present invention;

[25] FIG. 4 is a block diagram of a light emitting unit of FIG. 3;

[26] FIG. 5 is a block diagram of a light receiving unit of FIG. 3;

[27] FIGS. 6 and 7 are diagrams of a detecting unit of a light receiving unit;

[28] FIG. 8 is a diagram illustrating a biometric authentication method in a digital device according to an embodiment of the present invention;

[29] FIGs. 9 to 14 are diagrams illustrating a method of authenticating a body part according to an embodiment of the present invention; and

[30] FIGs. 15 to 22 are diagrams illustrating security authentication according to security levels.

Best Mode for Carrying out the Invention

[31] Description will now be given in detail according to exemplary embodiments disclosed herein, with reference to the accompanying drawings. In general, a suffix such as “module” and “unit” can be used to refer to elements or components. Use of such a suffix herein is merely intended to facilitate description of the specification, and the suffix itself is not intended to give any special meaning or function. In addition, such an ordinal number as ‘first, ‘second’, ‘third’ and the like can have a meaning of an order. Yet, the terminologies can be used for the purpose of distinguishing one component from another component capable of being overlapped with each other.

[32] The accompanying drawings are used to help easily understand various technical features and it should be understood that the embodiments presented herein are not limited by the accompanying drawings. As such, the present disclosure should be construed to extend to any alterations, equivalents and substitutes in addition to those which are particularly set out in the accompanying drawings.

[33] A digital device according to an embodiment of the present invention as set forth herein can be any device that can handle any one of transmitting, receiving, handling and outputting data, content, servicer, application, and so forth. The digital device can be connected to other digital devices through wired network or wireless network, paired or connected to external server, and through the connections, the digital device can transmit and receive the prescribed data. Examples of the digital device can include standing devices such as a network TV, a Hybrid Broadcast Broadband TV (HBBTV), a smart TV, Internet Protocol TV (IPTV), and personal computer (PC), or mobile/handheld devices such as a Personal Digital Assistant (PDA), smart phone, tablet PC, or Notebook computer. For convenience of description, in this specification, Digital TV is used in FIG. 1 and mobile device is used in FIG. 2 depicting the digital device. Further, the digital device in this specification can be referred to configuration having only a panel, set-top box (STB), or a set including the entire system.

[34] Further, the wired or wireless network described in this specification can refer to various pairing method, standard telecommunication network protocol methods supported for transmitting and receiving data between digital devices or between digital device and external server. The wired or wireless network also includes various telecommunication network protocols supported now as well as in the future. Examples of the wired or wireless network include wired network supported by various telecommunication standard such as Universal Serial Bus (USB), Composite Video Banking Sync (CVBS), Component, S-Video (analog), Digital Visual Interface (DVI), High Definition Multimedia Interface (HDMI), RGB, D-SUB and so forth, and wireless network supported by various standards including Bluetooth, Radio Frequency Identification (RFID), infrared Data Association (IrDA), Ultra Wideband (UWB), ZigBee, Digital Living Network Alliance (DLNA), Wireless LAN (WLAN)(Wi-Fi), Wireless broadband (Wibro), World Interoperability for Microwave Access (Wimax), High Speed Downlink Packet (HSDPA), Long Term Evolution/ LTE-Advanced (LTE/LTE-A), Wi-Fi direct, and so forth.

[35] In addition, when this specification refers simply to the digital device, it can mean a standing device or a mobile device depending on the context, and when it is not referred to a specific device, the digital device referred in this specification refers to both standing and mobile device. Also, the digital device can perform intelligent functions such as receiving broadcasting program, operating computer functions, and

supporting at least one external input, and by being connected through the network wired or wirelessly, the digital device can support e-mail functions, web browsing functions, banking, gaming, and executing applications. The digital device can further include an interface for any one of input or control method (hereinafter referred as "input method") supporting handwriting input, touch-screen, and space remote control.

[36] Furthermore, the digital device can use a standard operating system (OS), however, the digital device described in this specification and the embodiments, uses Web OS. Therefore, the digital device can perform functions such as adding, deleting, amending, and updating the various services and applications for standard universal OS kernel or Linux kernel in order to construct a more user-friendly environment.

[37] When the digital device, described above, receives and handles an external input, the external input includes external input devices described above, meaning all input method or digital devices, capable of transmitting and receiving data through wired or wireless network connected to and from the digital device. For example, the external input includes High Definition Multimedia Interface (HDMI), game devices such as PlayStation or X-Box, smart phone, tablet PC, printing device such as pocket photo, digital devices such as smart TV and blue-ray device.

[38] The "server" referred to as in this application, includes digital device or system capable of transmitting and receiving data to and from client, and can also be referred to as a processor. For example, the server can be servers providing services such as portal server providing web page, web content or web service, advertising server providing advertising data, content server, Social Network Service (SNS) server providing SNS service, service server providing service to manufacturer, Multichannel Video Programming Distributor (MVPD) providing Video on Demand or streaming service, and service server providing pay services.

[39] In this application, when application is described for the convenience of explanation, the meaning of application in the context can include services as well as applications. In the following description, various embodiments according to an embodiment of the present invention are explained with reference to attached drawings.

[40] FIG. 1 is a block diagram of a digital device according to one embodiment of the present invention. The digital device 200 may include a network interface 201, a TCP/IP manager 202, a service delivery manager 203, an SI (System Information, Service Information or Signaling Information) decoder 204, a demultiplexer 205, an audio decoder 206, a video decoder 207, a display A/V and OSD (On Screen Display) module 208, a service control manager 209, a service discovery manager 210, a SI & metadata database (DB) 211, a metadata manager 212, an application manager, etc.

[41] The network interface 201 can receive or transmit IP packets including service data through a network. In other words, the network interface 201 can receive IP packets

including at least one of text data, image data, audio data, and video data, used for SNS, as well as services and applications from a server connected thereto through a network.

[42] The TCP/IP manager 202 involves delivery of IP packets transmitted to the digital device 200 and IP packets transmitted from the digital device 200, that is, packet delivery between a source and a destination. The TCP/IP manager 202 classifies received packets according to an appropriate protocol and outputs the classified packets to the service delivery manager 205, the service discovery manager 210, the service control manager 209, and the metadata manager 212.

[43] The service delivery manager 203 can control classification and processing of service data. The service delivery manager 203 can also control real-time streaming data, for example, using real-time protocol/real-time control protocol (RTP/RTCP). In other words, the service delivery manager 203 can parse a real-time streaming data packet, transmitted based on the RTP, according to the RTP and transmits the parsed data packet to the demultiplexer 205 or store the parsed data packet in the SI & metadata DB 211 under the control of the service manager 213. The service delivery manager 203 can feed back network reception information to the server based on the RTP.

[44] The demultiplexer 205 can demultiplex audio data, video data, SI from a received packet through packet identifier (PID) filtering and transmit the demultiplexed data to corresponding processors, that is, the audio/video decoder 206/207 and the SI decoder 204. The SI decoder 204 can parse and/or decode SI data such as program specific information (PSI), program and system information protocol (PSIP), digital video broadcast-service information (DVB-SI), etc. The SI decoder 204 can store the parsed and/or decoded SI data in the SI & metadata DB 211. The SI data stored in the SI & metadata DB 211 can be read or extracted and used by a component which requires the SI data. EPG data can also be read from the SI & metadata DB 211. This will be described below in detail.

[45] The audio decoder 206 and the video decoder 207 respectively can decode audio data and video data, which are demultiplexed by the demultiplexer 205. The decoded audio data and video data can be provided to the user through the display unit 208. The application manager may include a service manager 213 and a user interface (UI) manager 214, administrate the overall state of the digital device 200, provide a UI, and manage other mangers.

[46] The UI manager 214 can receive a key input from the user and provide a graphical user interface (GUI) related to a receiver operation corresponding to the key input through OSD. The service manager 213 can control and manage service-related managers such as the service delivery manager 203, the service discovery manager 210, the service control manager 209, and the metadata manager 212.

[47] The service manager 213 may configure a channel map and enable channel control at the request of the user based on the channel map. The service manager 213 can receive service information corresponding to channel from the SI decoder 204 and set audio/ video PID of a selected channel to the demultiplexer 205 so as to control the demultiplexing procedure of the demultiplexer 205.

[48] The service discovery manager 210 can provide information required to select a service provider that provides a service. Upon receipt of a signal for selecting a channel from the service manager 213, the service discovery manager 210 discovers a service based on the received signal. The service control manager 209 can select and control a service. For example, the service control manager 209 can perform service selection and control using IGMP (Internet Group Management Protocol) or real time streaming protocol (RTSP) when the user selects a live broadcast service and using RTSP when the user selects a video on demand (VOD) service.

[49] The metadata manager 212 can manage metadata regarding services and store metadata in the SI & metadata DB 211. The SI & metadata DB 211 can store SI data decoded by the SI decoder 204, metadata managed by the metadata manager 212, and information required to select a service provider, which is provided by the service discovery manager 210. In addition, the SI & metadata DB 211 can store system set-up data. The SI & metadata DB 211 can be implemented using a Non-Volatile RAM (NVRAM) or a Flash memory, and the like. An IMS (IP Multimedia Subsystem) gateway 250 may include functions required to access an IMS based IPTV services.

[50] Next, FIG. 2 is a block diagram of a digital device according to another embodiment of the present invention. In particular, FIG. 2 shows the mobile terminal 300 having various components, but implementing all of the illustrated components is not a requirement. More or fewer components may be implemented according to various embodiments.

[51] With reference to FIG. 2, the mobile terminal 300 includes a wireless communication unit 310, an A/V (audio/video) input unit 320, a user input unit 330, a sensing unit 340, an output unit 350, a memory 360, an interface unit 370, a controller 380, and a power supply unit 390. The detailed description of each component is as follows.

[52] The wireless communication unit 310 typically includes one or more components which permit wireless communication between the mobile terminal 300 and a wireless communication system or network within which the mobile terminal 300 is located. For instance, the wireless communication unit 310 can include a broadcast receiving module 311, a mobile communication module 312, a wireless Internet module 313, a short-range communication module 314, and a position-location module 315.

[53] The broadcast receiving module 311 receives a broadcast signal and/or broadcast associated information from an external broadcast managing server via a broadcast

channel. The broadcast channel may include a satellite channel and a terrestrial channel. At least two broadcast receiving modules 311 can be provided in the mobile terminal 300 to facilitate simultaneous reception of at least two broadcast channels or broadcast channel switching.

[54] The broadcast associated information includes information associated with a broadcast channel, a broadcast program, or a broadcast service provider. Furthermore, the broadcast associated information can be provided via a mobile communication network. In this instance, the broadcast associated information can be received by the mobile communication module 312.

[55] The broadcast associated information can be implemented in various forms. For instance, broadcast associated information may include an electronic program guide (EPG) of digital multimedia broadcasting (DMB) and an electronic service guide (ESG) of digital video broadcast-handheld (DVB-H).

[56] The broadcast receiving module 311 may be configured to receive broadcast signals transmitted from various types of broadcast systems. By non-limiting example, such broadcasting systems may include digital multimedia broadcasting-terrestrial (DMB-T), digital multimedia broadcasting-satellite (DMB-S), digital video broadcast-handheld (DVB-H), digital video broadcast-convergence of broadcasting and mobile services (DVB-CBMS), Open Mobile Alliance Broadcast (OMA-BCAST), the data broadcasting system known as media forward link only (MediaFLOTM) and integrated services digital broadcast-terrestrial (ISDB-T). Optionally, the broadcast receiving module 311 can be configured to be suitable for other broadcasting systems as well as the above-noted digital broadcasting systems. The broadcast signal and/or broadcast associated information received by the broadcast receiving module 311 can be stored in a suitable device, such as the memory 360.

[57] The mobile communication module 312 transmits/receives wireless signals to/from one or more network entities (e.g., a base station, an external terminal, and/or a server) via a mobile network such as GSM (Global System for Mobile communications), CDMA (Code Division Multiple Access), or WCDMA (Wideband CDMA). Such wireless signals can carry audio, video, and data according to text/multimedia messages.

[58] The wireless Internet module 313 supports Internet access for the mobile terminal 300. This module may be internally or externally coupled to the mobile terminal 300. The wireless Internet technology can include WLAN (Wireless LAN), Wi-Fi, WibroTM (Wireless broadband), WimaxTM (World Interoperability for Microwave Access), HSDPA (High Speed Downlink Packet Access), GSM, CDMA, WCDMA, or LTE (Long Term Evolution) .

[59] The short-range communication module 314 facilitates relatively short-range com-

munications. Suitable technologies for implementing this module include radio frequency identification (RFID), infrared data association (IrDA), ultra-wideband (UWB), as well as the networking technologies commonly referred to as BluetoothTM and ZigBeeTM, to name a few. The position-location module 315 identifies or otherwise obtains the location of the mobile terminal 100. According to one embodiment, this module may be implemented with a global positioning system (GPS) module.

[60] The audio/video (A/V) input unit 320 is configured to provide audio or video signal input to the mobile terminal 300. As shown, the A/V input unit 320 includes a camera 321 and a microphone 322. The camera 321 receives and processes image frames of still pictures or video, which are obtained by an image sensor in a video call mode or a photographing mode. Furthermore, the processed image frames can be displayed on the display 351.

[61] The image frames processed by the camera 321 can be stored in the memory 360 or can be transmitted to an external recipient via the wireless communication unit 310. Optionally, at least two cameras 321 can be provided in the mobile terminal 300 according to the environment of usage. The microphone 322 receives an external audio signal while the portable device is in a particular mode, such as phone call mode, recording mode and voice recognition. This audio signal is processed and converted into electronic audio data. The processed audio data is transformed into a format transmittable to a mobile communication base station via the mobile communication module 312 in a call mode. The microphone 322 typically includes assorted noise removing algorithms to remove noise generated in the course of receiving the external audio signal. The user input unit 330 generates input data responsive to user manipulation of an associated input device or devices. Examples of such devices include a keypad, a dome switch, a touchpad (e.g., static pressure/capacitance), a jog wheel, and a jog switch.

[62] The sensing unit 340 provides sensing signals for controlling operations of the mobile terminal 300 using status measurements of various aspects of the mobile terminal. For instance, the sensing unit 340 can detect an open/closed status of the mobile terminal 100, the relative positioning of components (e.g., a display and keypad) of the mobile terminal 300, a change of position (or location) of the mobile terminal 300 or a component of the mobile terminal 300, a presence or absence of user contact with the mobile terminal 300, and an orientation or acceleration/deceleration of the mobile terminal 300. As an example, a mobile terminal 300 configured as a slide-type mobile terminal is considered. In this configuration, the sensing unit 340 can sense whether a sliding portion of the mobile terminal is open or closed. According to other examples, the sensing unit 340 senses the presence or absence of power provided

by the power supply unit 390, and the presence or absence of a coupling or other connection between the interface unit 370 and an external device. According to one embodiment, the sensing unit 340 can include a proximity sensor 341.

[63] The output unit 350 generates output relevant to the senses of sight, hearing, and touch. Furthermore, the output unit 350 includes the display 351, an audio output module 352, an alarm unit 353, a haptic module 354. A projector module may also be included. The display 351 is typically implemented to visually display (output) information associated with the mobile terminal 300. For instance, if the mobile terminal is operating in a phone call mode, the display will generally provide a user interface (UI) or graphical user interface (GUI) which includes information associated with placing, conducting, and terminating a phone call. As another example, if the mobile terminal 300 is in a video call mode or a photographing mode, the display 351 may additionally or alternatively display images which are associated with these modes, the UI or the GUI.

[64] The display 351 may be implemented using known display technologies. These technologies include, for example, a liquid crystal display (LCD), a thin film transistor-liquid crystal display (TFT-LCD), an organic light-emitting diode display (OLED), a flexible display and a three-dimensional display. The mobile terminal 300 may include one or more of such displays.

[65] Some of the displays can be implemented in a transparent or optical transmittive type, i.e., a transparent display. A representative example of the transparent display is the TOLED (transparent OLED). A rear configuration of the display 351 can be implemented as the optical transmittive type as well. In this configuration, a user can see an object located at the rear of a terminal body on a portion of the display 351 of the terminal body.

[66] At least two displays 351 can be provided in the mobile terminal 300 in accordance with one embodiment of the mobile terminal 300. For instance, a plurality of displays can be arranged to be spaced apart from each other or to form a single body on a single face of the mobile terminal 300. Alternatively, a plurality of displays can be arranged on different faces of the mobile terminal 300.

[67] If the display 351 and a sensor for detecting a touch action (hereinafter called 'touch sensor') are configured as a mutual layer structure (hereinafter called 'touch screen'), the display 351 is usable as an input device as well as an output device. In this instance, the touch sensor can be configured as a touch film, a touch sheet, or a touchpad.

[68] The touch sensor can be configured to convert pressure applied to a specific portion of the display 351 or a variation of capacitance generated from a specific portion of the display 351 to an electronic input signal. Further, the touch sensor is configurable to

detect pressure of a touch as well as a touched position or size. If a touch input is made to the touch sensor, a signal(s) corresponding to the touch input is transferred to a touch controller. The touch controller processes the signal(s) and then transfers the processed signal(s) to the controller 380. Therefore, the controller 380 is made aware when a prescribed portion of the display 351 is touched.

[69] A proximity sensor 341 can be provided at an internal area of the mobile terminal 300 enclosed by the touch screen or around the touch screen. The proximity sensor is a sensor that detects a presence or non-presence of an object approaching a prescribed detecting surface or an object existing (or located) around the proximity sensor using an electromagnetic field strength or infrared ray without mechanical contact. Hence, the proximity sensor 341 is more durable than a contact type sensor and also has utility broader than the contact type sensor.

[70] The proximity sensor 341 can include one of a transmittive photoelectric sensor, a direct reflective photoelectric sensor, a mirror reflective photoelectric sensor, a radio frequency oscillation proximity sensor, an electrostatic capacity proximity sensor, a magnetic proximity sensor, and an infrared proximity sensor. If the touch screen includes the electrostatic capacity proximity sensor, it is configured to detect the proximity of a pointer using a variation of an electric field according to the proximity of the pointer. In this configuration, the touch screen (touch sensor) can be considered as the proximity sensor.

[71] For clarity and convenience of explanation, an action for enabling the pointer approaching the touch screen to be recognized as placed on the touch screen may be named 'proximity touch' and an action of enabling the pointer to actually come into contact with the touch screen may be named 'contact touch'. In addition, a position, at which the proximity touch is made to the touch screen using the pointer, may mean a position of the pointer vertically corresponding to the touch screen when the pointer makes the proximity touch.

[72] The proximity sensor detects a proximity touch and a proximity touch pattern (e.g., a proximity touch distance, a proximity touch duration, a proximity touch position, a proximity touch shift state). Information corresponding to the detected proximity touch action and the detected proximity touch pattern can be output to the touch screen.

[73] The audio output module 352 functions in various modes including a call-receiving mode, a call-placing mode, a recording mode, a voice recognition mode, and a broadcast reception mode to output audio data which is received from the wireless communication unit 310 or is stored in the memory 360. During operation, the audio output module 352 outputs audio relating to a particular function (e.g., call received, message received). The audio output module 352 may be implemented using one or more speakers, buzzers, other audio producing devices, and combinations of these

devices.

[74] The alarm unit 353 outputs a signal for announcing the occurrence of a particular event associated with the mobile terminal 300. Typical events include a call received, a message received and a touch input received. The alarm unit 353 can output a signal for announcing the event occurrence by way of vibration as well as video or audio signal. The video or audio signal can be output via the display 351 or the audio output module 352. Hence, the display 351 or the audio output module 352 can be regarded as a part of the alarm unit 353.

[75] The haptic module 354 generates various tactile effects that can be sensed by a user. Vibration is a representative one of the tactile effects generated by the haptic module 354. The strength and pattern of the vibration generated by the haptic module 354 are controllable. For instance, different vibrations can be output by being synthesized together or can be output in sequence. The haptic module 354 can generate various tactile effects as well as the vibration. For instance, the haptic module 354 can generate an effect attributed to the arrangement of pins vertically moving against a contact skin surface, an effect attributed to the injection/suction power of air though an injection/ suction hole, an effect attributed to the skim over a skin surface, an effect attributed to a contact with an electrode, an effect attributed to an electrostatic force, and an effect attributed to the representation of a hot/cold sense using an endothermic or exothermic device. The haptic module 354 can be implemented to enable a user to sense the tactile effect through a muscle sense of a finger or an arm as well as to transfer the tactile effect through direct contact. Optionally, at least two haptic modules 354 can be provided in the mobile terminal 300 in accordance with an embodiment of the mobile terminal 300.

[76] The memory 360 is generally used to store various types of data to support the processing, control, and storage requirements of the mobile terminal 300. Examples of such data include program instructions for applications operating on the mobile terminal 300, contact data, phonebook data, messages, audio, still pictures (or photo), and moving pictures. Furthermore, a recent use history or a cumulative use frequency of each data (e.g., use frequency for each phonebook, each message or each multimedia file) can be stored in the memory 360. Further, the data for various patterns of vibration and/or sound output in response to a touch input to the touch screen can be stored in the memory 360.

[77] The memory 360 may be implemented using any type or combination of suitable volatile and non-volatile memory or storage devices including hard disk, random access memory (RAM), static random access memory (SRAM), electrically erasable programmable read-only memory (EEPROM), erasable programmable read-only memory (EPROM), programmable read-only memory (PROM), read-only memory

(ROM), magnetic memory, flash memory, magnetic or optical disk, multimedia card micro type memory, card-type memory (e.g., SD memory or XD memory), or other similar memory or data storage device. Furthermore, the mobile terminal 300 can operate in association with a web storage for performing a storage function of the memory 360 on the Internet.

[78] The interface unit 370 may be implemented to couple the mobile terminal 100 with external devices. The interface unit 370 receives data from the external devices or is supplied with power and then transfers the data or power to the respective elements of the mobile terminal 300 or enables data within the mobile terminal 300 to be transferred to the external devices. The interface unit 370 may be configured using a wired/wireless headset port, an external charger port, a wired/wireless data port, a memory card port, a port for coupling to a device having an identity module, audio input/output ports, video input/output ports, and/or an earphone port.

[79] The identity module is a chip for storing various kinds of information for authenticating a usage authority of the mobile terminal 300 and can include a User Identify Module (UIM), a Subscriber Identity Module (SIM), and/or a Universal Subscriber Identity Module (USIM). A device having the identity module (hereinafter called 'identity device') can be manufactured as a smart card. Therefore, the identity device is connectible to the mobile terminal 300 via the corresponding port.

[80] When the mobile terminal 300 is connected to an external cradle, the interface unit 370 becomes a passage for supplying the mobile terminal 300 with a power from the cradle or a passage for delivering various command signals input from the cradle by a user to the mobile terminal 300. Each of the various command signals input from the cradle or the power can operate as a signal enabling the mobile terminal 300 to recognize that it is correctly loaded in the cradle.

[81] The controller 380 typically controls the overall operations of the mobile terminal 300. For example, the controller 380 performs the control and processing associated with voice calls, data communications, and video calls. The controller 380 may include a multimedia module 381 that provides multimedia playback. The multimedia module 381 may be configured as part of the controller 380, or implemented as a separate component. Further, the controller 380 can perform a pattern (or image) recognizing process for recognizing a writing input and a picture drawing input performed on the touch screen as characters or images, respectively.

[82] The power supply unit 390 provides power required by various components of the mobile terminal 300. The power may be internal power, external power, or combinations of internal and external power. Various embodiments described herein may be implemented in a computer-readable medium using, for example, computer software, hardware, or some combination of computer software and hardware.

[83] For a hardware implementation, the embodiments described herein may be implemented within one or more application specific integrated circuits (ASICs), digital signal processors (DSPs), digital signal processing devices (DSPDs), programmable logic devices (PLDs), field programmable gate arrays (FPGAs), processors, controllers, micro-controllers, microprocessors, other electronic units designed to perform the functions described herein, or a selective combination thereof. Such embodiments may also be implemented by the controller 180.

[84] For a software implementation, the embodiments described herein may be implemented with separate software modules, such as procedures and functions, each of which performs one or more of the functions and operations described herein. The software codes can be implemented with a software application written in any suitable programming language and may be stored in memory such as the memory 160, and executed by a controller or processor, such as the controller 380.

[85] FIG. 3 is a block diagram of a biometric authentication processor of a digital device according to an embodiment of the present invention. Referring to FIG. 3, a biometric authentication processor of a digital device 500 may include a camera unit 510, an image data sensor unit 520, a memory unit 550, a pre-processing unit 530, a comparing unit 535 and a controller 540.

[86] In some instances, the biometric authentication processor of the digital device may further include a timer 560 and an optical guide unit. In addition, the camera unit 510 may employ a ToF sensor that uses near infrared rays (NIR). The ToF sensor measures a distance from a target and represents a strength of a difference of a phase signal reflecting from the target as an image form, thereby checking a vein vessel pattern of a body part.

[87] The camera unit 510 may include a light emitting unit 512 projecting light onto a target 501 and a light receiving unit 514 detecting light reflecting from the target 501. In one example, the light emitting unit 512 may include a light source projecting light corresponding to an infrared region of a light spectrum.

[88] In another example, the light emitting unit 512 can project color light corresponding to a visible region of the light spectrum and infrared light corresponding to an infrared region of the light spectrum. In addition, the light source projecting the color light may include a red light source projecting red light of a red wavelength range, a green light source projecting green light of a green wavelength range, and a blue light source projecting blue light of a blue wavelength range.

[89] In addition, each of the red, green and blue light sources can use a light-emitting diode (LED) or a laser diode (LD). Also, the light receiving unit 514 may include a lens unit, a filter unit and a detecting unit. Further, the lens unit can transmit or focus the infrared light reflecting from the target 501.

[90] Also, the lens unit can move centering on the detecting unit in response to an auto focus control signal of the controller. In some instances, the lens unit can use a wideband coating lens capable of transmitting a color light of a visible wavelength range and a light of an infrared wavelength range among the lights reflecting from the target 501. In another instance, the lens unit can use a lens having wideband focusing performance capable of focusing the color light and the infrared light.

[91] The filter unit may include a single band pass filter transmitting the infrared light of the infrared (IR) wavelength range transmitted by the lens unit. In some instances, the filter unit may include a dual band pass filter simultaneously transmitting color light of red, green and blue wavelength ranges and infrared (IR) light of an infrared wavelength range, which have been transmitted by the lens unit.

[92] Hence, the filter unit can cut off the light of the UV wavelength range, the light of the wavelength range between the red, green and blue wavelength range and the IR wavelength range, and the light of the wavelength range over the IR wavelength range. The detecting unit can detect IR light only, detect color light and IR light simultaneously, or detect color light and IR light in different time slots respectively.

[93] In some instances, the camera unit 510 may include a first camera capturing the target 501 as a 2-dimnesional (2D) image and a second camera capturing the target 501 as a 3-dimnesional (3D) image. In addition, the second camera may include a light emitting unit projecting light onto the target 501 to be authenticated and a light receiving unit sensing the light reflecting from the target 501 to be authenticated.

[94] When receiving an authentication command, the controller can control the second camera to be activated to capture a face of the target 501 to be authenticated or control the second camera to be activated to capture vein of a body part of the target 501 to be authenticated. Meanwhile, the image data sensor unit 520 can sense image data of the target 501 captured by the camera unit 510. Face image data and vein image data of a body part for authentication may be already stored in the memory unit 550.

[95] The pre-processing unit 530 determines information of a shot target from the image data sensed by the image data sensor unit 520. If the determined image data is face data or vein data of a body part, the pre-processing unit 530 can create processed face image data or processed body vein data for authentication. In addition, the information of the shot target may include a size of a face, a shape (e.g., contour) of the face, and the like.

[96] For example, the pre-processing unit 530 includes a detecting unit detecting an amount of light sensed from the camera unit 510, a converting unit converting the detected amount of the light into an electric signal, and an extracting unit extracting information on an image from the electric signal, thereby determining whether the shot target is a face. According to a result of the determination, the pre-processing unit 530

can create processed image data of the face and the vein of the body part.

[97] The comparing unit 535 can compare the processed image data with at least one of the face image data and the vein image data of the body part, which were previously stored in the memory unit 550. Subsequently, if an execution mode to be executed is a security authentication mode, the controller 540 activates the camera unit 510 to be ready to receive image data of the target 501. If the image data of the target 501 is face image data, the controller 540 can perform a primary authentication by comparing the processed face image data with the face image data previously stored for authentication in the memory unit 550.

[98] In addition, the controller 540 can perform a secondary authentication by comparing vein image data of at least one processed body part according to a primary authentication result with vein image data of at least one authentication body part previously stored in the memory unit 550. In addition, the vein image data of the processed body part may include at least one of face vein image data, wrist vein image data, hand dorsum vein image data, finger vein image data, palm vein image data, and foot vein image data, by which the present invention is non-limited.

[99] Further, the according to a security level of an execution mode to be executed, the controller 540 can perform a primary authentication of comparing processed face image data with face image data previously stored in the memory unit 550 only. In some instances, according to a security level of an execution mode to be executed, the controller 540 can perform both a primary authentication of comparing processed face image data with face image data previously stored in the memory unit 550 and a secondary authentication of comparing vein image data of at least one processed body part with vein image data of at least one body part previously stored in the memory unit 550.

[100] In other instances, according to a security level of an execution mode to be executed, the controller 540 can perform a primary authentication of comparing processed face image data with face image data previously stored in the memory unit, a secondary authentication of comparing vein image data of at least one processed body part with vein image data of at least one body part previously stored in the memory unit, and a tertiary authentication of comparing vein image data of at least one processed different body part with vein image data of at least one different body part previously stored in the memory unit all.

[101] In addition, the vein image data of the processed body part may include at least one of face vein image data, wrist vein image data, hand dorsum vein image data, finger vein image data, palm vein image data, and foot vein image data, by which the present invention is non-limited.

[102] In one example, the controller 540 checks a security level of an execution mode to be

executed. If the checked security level is lower than a reference level, the controller 540 performs the primary authentication based on a face authentication image only. If the checked security level is higher than the reference level, the controller 540 performs both of the primary authentication based on a face authentication image and the secondary authentication based on a vein authentication image of a body part.

[103] Further, when checking the security level of the execution mode to be executed, the controller 540 can provide information on the checked security level to a display screen. In another example, the controller 540 checks a security level of an execution mode to be executed. If the checked security level is a special level, the controller 540 can request an additional biometric authentication after succeeding in both of the primary and secondary authentications, control the camera unit 510 to capture a body to additionally authenticate, and perform the tertiary authentication based on an additional biometric authentication image.

[104] In addition, the body to additionally authenticate may include at least one of face vein, wrist vein, hand dorsum vein, finger vein, palm vein, and foot vein, by which the present invention is non-limited. In some instances, after checking the security level of the execution mode to be executed, the controller 540 can provide information on the checked security level to the display screen.

[105] In other instances, when the primary or secondary authentication is performed, if the corresponding authentication is successful, the controller 540 can provide an authentication success notification message to the display screen and also provide a next step guide message to the display screen. In other instances, when the primary or secondary authentication is performed, if the corresponding authentication is failure, the controller 540 can provide an authentication failure notification message to the display screen and also provide a re-authentication message to the display screen.

[106] In performing the primary or secondary authentication, the controller 540 extracts an optimal authentication image from a multitude of authentication images according to an auto focus of the camera unit 510 and then calculates an error value by comparing the extracted authentication image with a previously saved registration image. If the calculated error value is within a reference range, the controller 540 can determine an authentication success.

[107] When the optimal authentication image is extracted, if a size of the extracted authentication image is different from that of the previously saved registration image, the controller 540 can control the pre-processing unit 530 to enlarge or reduce the authentication image size. When performing the secondary authentication, the controller 540 can control the lens of the camera unit 510 to capture a vein of a body part except a face with an optical zoom and control the pre-processing unit 530 to process a vein image of the body part captured with the optimal zoom into face vein image data

processed for authentication.

[108] Further, when performing the secondary authentication, the controller 540 can control the lens of the camera unit 510 to capture face vein to authenticate with an optical zoom and control the pre-processing unit 530 to create processed face vein image data for authentication from a face vein image shot with the optical zoom. In some instances, when performing the second authentication using face vein image data, without separate shooting, the controller 540 can create processed face vein image data for authentication from face vein image data extracted from an image of a target captured for the primary authentication.

[109] In some instances, when performing the second authentication, the controller 540 measures a projection time of IR light projected from the camera unit 510 using the timer 560. If the projection time of the IR light exceeds a reference time, the controller 540 can control the light emitting unit 512 of the camera unit 510 to cut off the output of the IR light. The output of the IR light is cutoff to solve the eye-safety problem. Namely, the danger due to the long-term exposure to the IR light can be reduced and safe authentication can be secured.

[110] In other instances, when performing the second authentication, the controller 540 measures a projection time of IR light projected from the camera unit 510 using the timer 560. If the projection time of the IR light exceeds a reference time, the controller 540 can control the light emitting unit 512 of the camera unit 510 to lower the strength of an output of the IR light to be smaller than a setup value.

[111] Meanwhile, if an execution mode to be executed is a biometric registration mode, the controller 540 performs a primary registration by activating the camera unit 510 to capture a face to register and saving a face authentication registration image created from the pre-processing unit 530 to the memory unit 550. If the primary registration is successfully performed, the controller 540 can perform a secondary registration by controlling the camera unit 510 to capture a face vein to register for authentication and then saving a face vein authentication registration image crated from the pre-processing unit 530 to the memory unit 550.

[112] After both of the primary and secondary registrations have been successfully completed, if there is an additional biometric authentication registration request, the controller 540 can control the camera unit 510 to capture a body part to register additionally and perform a tertiary registration based on an additional biometric authentication registration image created from the pre-processing unit 530. For example, the body to additionally register may include at least one of face vein, wrist vein, hand dorsum vein, finger vein, palm vein, and foot vein, by which the present invention is non-limited.

[113] Next, if an execution mode to be executed is an authentication registration update

mode, the controller 540 performs a primary update by activating the camera unit 510 to capture a face to update registration, saving a face registration update image created from the pre-processing unit 530 to the memory unit 550, and removing a previous face registration image. If the primary update is successfully performed, the controller 540 can perform a secondary update by controlling the camera unit 510 to capture a face vein to update registration, saving a face vein registration update image crated from the pre-processing unit 530 to the memory unit 550, and removing a previous face vein registration image.

[114] After both of the primary and secondary updates have been successfully completed, if there is an additional body registration update request, the controller 540 can control the camera unit 510 to capture a body part to additionally update registration and perform a tertiary registration based on an additional body registration update image created from the pre-processing unit 530.

[115] In addition, the body to additionally update registration may include at least one of face vein, wrist vein, hand dorsum vein, finger vein, palm vein, and foot vein, by which the present invention is non-limited. Further, the according to the body vein data update method of the present invention, if a security update mode command is received, a target is capture by activating the camera unit and image data of the captured target is then sensed.

[116] According to an embodiment of the present invention, it is determined whether the image data is face image data. If the image data is the face image data, processed face image data is created. Then, the processed face image data and face image data saved for authentication to the memory unit are compared with each other. Subsequently, according to an embodiment of the present invention, a target to be authenticated is captured by the camera unit depending on a result of the comparison and image data of the captured target is sensed. If the image data is vein image data of at least one body part, vein image data of a processed body part can be created, saved to the memory unit, and then updated.

[117] Further, the present invention can include an optical guide unit configured to calculate current location information of a face to be authenticated and guide location correction for the current location information of the face. In addition, the optical guide unit may include a light source unit projecting light onto a face to be authenticated, a detecting unit detecting light reflecting from the face, and a location calculating unit calculating current location information of the face based on the detected light.

[118] Particularly, the location calculating unit can extract coordinates of light spot points of the light detected from the detecting unit, calculate a distance value between the light spot points, and store current location information of a face including the calculated distance value. In some instances, the optical guide unit may include a

speaker unit outputting audio data for guiding location correction for the current location information of the face and a display unit displaying a face image including the current location information.

[119] In addition, the light source unit may include at least three light sources. For example, the light sources of the light source unit may be disposed by being spaced apart from each other in predetermined intervals along a periphery of the detecting unit. Further, the light sources of the light source unit can be disposed to have an angle range between 5 and 90 degrees from a surface of the optical guide unit.

[120] Thus, the present invention can perform personal authentication quickly and conveniently by extracting a vein pattern of a body part by applying ToF (time of flight) employing a near infrared light source and then using the extracted vein pattern. In addition, the present invention can improve safety and reliability of security authentication by performing face authentication and vein authentication of a body part by applying ToF (time of flight) employing a near infrared light source.

[121] Further, the present invention can reinforce security and raise accuracy by performing face authentication and vein authentication of multiple body parts according to a security level. Furthermore, the present invention can perform personal authentication with high accuracy by obtaining 3D vein blood vessel information through depth information of a ToF sensor, compensate the inaccuracy of the related art face recognition through additional vein authentication, and apply use scenes of various types.

[122] Next, FIG. 4 is a block diagram of the light emitting unit of FIG. 3, and FIG. 5 is a block diagram of the light receiving unit of FIG. 3. Referring to FIG. 4, the light emitting unit 512 of the camera unit may include an IR light source 512-2 projecting light corresponding to an IR region of an optical spectrum only.

[123] In some instances, the light emitting unit can project color light corresponding to a visible region of the optical spectrum and IR light corresponding to an IR region of the optical spectrum. In addition, the light emitting unit 512 may include a color light source 512-1, which includes a red light source 512a projecting red light of a red wavelength range, a green light source 512b projecting green light of a green wavelength range, and a blue light source 512c projecting blue light of a blue wavelength range, and an IR light source 512-2 projecting IR light.

[124] In this instance, the red light source, the green light source, the blue light source and the IR light source can use light-emitting diodes (LED) or laser diodes (LD). The light emitting unit 512 can project red light, green light and blue light simultaneously during a first time and also project IR light during a second time. The first time may be different from the second time.

[125] Referring to FIG. 5, the light receiving unit 514 may include a lens unit 514-1, a

filter unit 514-2 and a detecting unit 514-3. In addition, the lens unit 514-1 can transmit and focus IR light reflecting from the target 501. The lens unit 514-1 can move centering on the detecting unit 514-3 in response to an auto focus control signal of the controller 540.

[126] In some instances, the lens unit 514-1 can use a wideband coating lens capable of transmitting color light of a visible wavelength range and light of an infrared wavelength range among the lights reflecting from the target 501. In another instance, the lens unit 514-1 can use a lens having wideband focusing performance capable of focusing the color light and the infrared light.

[127] The filter unit 514-2 may include a single band pass filter transmitting the infrared light of the infrared (IR) wavelength range transmitted by the lens unit 514-1. In some instances, the filter unit 514-2 may include a dual band pass filter simultaneously transmitting color light of red, green and blue wavelength ranges and infrared (IR) light of an infrared wavelength range, which have been transmitted by the lens unit 514-1.

[128] Hence, the filter unit 514-2 can cut off the light of the UV wavelength range, the light of the wavelength range between the red, green and blue wavelength range and the IR wavelength range, and the light of the wavelength range over the IR wavelength range. The detecting unit 514-3 can detect IR light only, detect color light and IR light simultaneously, or detect color light and IR light in different time slots respectively.

[129] Next, FIGS. 6 and 7 are diagrams of a detecting unit of a light receiving unit. Referring to FIGS. 6 and 7, the detecting unit 514-3 can detect color light and IR light simultaneously, or detect color light and IR light in different time slots respectively. Here, as shown in FIG. 6, the detecting unit 514-3 detecting color light and IR light simultaneously may include a first pixel 514a simultaneously detecting red light of a red wavelength range and IR light of an IR wavelength range, a second pixel 514b simultaneously detecting green light of a green wavelength range and red light of a red wavelength range, and a third pixel 514c simultaneously detecting blue light of a blue wavelength range and IR light of an IR wavelength range.

[130] For example, the first pixel 514a of the detecting unit may include a first filter capable of transmitting red light of a red wavelength range and IR light of an IR wavelength range and cutting off lights of other wavelength ranges. The second pixel 514b of the detecting unit may include a second filter capable of transmitting green light of a green wavelength range and IR light of an IR wavelength range and cutting off lights of other wavelength ranges.

[131] And, the third pixel 514c of the detecting unit may include a third filter capable of transmitting blue light of a blue wavelength range and IR light of an IR wavelength range and cutting off lights of other wavelength ranges. Further, the as shown in FIG.

7, the detecting unit 514-3 detecting color light and IR light in different time slots respectively may include a first pixel 514a detecting red light of a red wavelength range, a second pixel 514b detecting green light of a green wavelength range, a third pixel 514c detecting blue light of a blue wavelength range, and a fourth pixel 514d detecting IR light of an IR wavelength range. Therefore, the controller can control the light emitting unit to project color light and IR light simultaneously or project color light and IR light in different time slots respectively.

[132] FIG. 8 is a diagram illustrating a biometric authentication method in a digital device according to an embodiment of the present invention. Referring to FIG. 8, according to an embodiment of the present invention, if receiving a security authentication mode command, the digital device can capture a target to authenticate by activating the camera unit 510.

[133] In addition, the camera unit 510 may employ a ToF sensor that uses near infrared rays (NIR). The ToF sensor is a sensor for measuring a distance from a target and represents a strength of a difference of a phase signal reflecting from the target as an image form, thereby checking a vein vessel pattern 710 of a body part 700.

[134] In this instance, the vein vessel pattern 710 of the body part can be embodied into a 3D image by extracting depth information. The digital device can sense image data of a shot target and then determine whether the image data is face image data. If the image data is the face image data, the digital device creates processed face image data from the face image data.

[135] Subsequently, the digital device performs a primary comparison step of comparing the processed face image data with face image data previously stored for authentication in the memory unit. The digital device checks a result of the primary comparison and then shoots a target to authenticate using the camera unit.

[136] The digital device senses image data of the shot target. If the image data is vein image data of at least one body part, the digital device creates vein image data of a processed body part. The digital device then performs a secondary comparison step of comparing the vein image data of the at least one processed body part with vein image data of at least one authentication body part stored in the memory unit.

[137] Subsequently, the digital device can end the security authentication mode according to a result of the second comparison. In another example, according to a biometric authentication method in a digital device, if a security authentication mode command is received, the digital device can shoot a target to authenticate by activating a camera unit, sense image data of the shot target, and determine whether the image data is face image data or face vein image data.

[138] If the image data is the face image data or the face vein image data, the digital device can create processed face image data or processed face vein image data from the face

image data or the face vein image data and then perform a primary comparison step of comparing the processed face image data with face image data stored for authentication in a memory unit.

[139] Subsequently, the digital device can perform a secondary comparison step of comparing the processed face vein image data with the face vein image data stored for the authentication in the memory unit according to a result of the primary comparison and then end the security authentication mode according to a result of the second comparison.

[140] Thus, the present invention can perform personal authentication quickly and conveniently by extracting a vein pattern of a body part by applying ToF (time of flight) employing a near infrared light source and then using the extracted vein pattern. And, the present invention can improve safety and reliability of security authentication by performing face authentication and vein authentication of a body part by applying ToF (time of flight) employing a near infrared light source.

[141] A method of registering data of a face and vein data of a body part for authentication of a digital device according to an embodiment of the present invention is described as follows. First of all, the present invention can receive a security registration mode command and shoot a target to register by activating a camera unit.

[142] Subsequently, the present invention senses image data of the shot target and then determines whether the image data is face image data and vein image data of at least one body part. If the image data is the face image data and the vein image data of the at least one body part, the present invention can create processed face image data and vein image data of at least one processed body part from the face image data and the vein image data of the at least one body part. The present invention can then register the processed face image data and the vein image fata of the at least one processed body part at the memory unit.

[143] A method of updating vein data of a body part for security authentication of a digital device according to an embodiment of the present invention is described as follows. First of all, the present invention can receive a body vein security update mode command and shoot a target to register by activating a camera unit.

[144] Subsequently, the present invention senses image data of the shot target and then determines whether the image data is face image data. If the image data is the face image data, the present invention performs authentication by comparison with face image data previously stored in the memory. According to a result from performing the authentication, the present invention captures at least one body part of the target. If the shot image is vein image data of the at least one body part of the target, the present invention creates vein image data of at least one processed body part by processing vein image data of the body part and then saves it to the memory unit, thereby

completing the update.

[145] A method of updating face data for security authentication of a digital device according to an embodiment of the present invention is described as follows. First of all, the present invention receives a face security authentication update mode command, activates a camera unit, and captures a target to register.

[146] Subsequently, the present invention senses image data of the shot target and determines whether the image data is vein image data of at least one body part of the target. If the image data is the vein image data of the body part, the present invention performs authentication by comparing the image data with vein image data of the corresponding body part of the target previously stored in the memory and then saves face data of the target to the memory unit according to a result from performing the authentication, thereby completing the update. In some instances, a procedure for performing authentication by comparison with vein image data of a body part of a target may be performed more than once.

[147] FIGs. 9 to 14 are diagrams illustrating a method of authenticating a body part according to an embodiment of the present invention. Referring to FIGs. 9 to 14, the present invention can perform face authentication primarily, shoot vein images of various body parts, and then extract vein image data of a body part from the shot images.

[148] FIG. 9 shows a process for extracting wrist vein pattern information by shooting a wrist vein image. FIG. 10 shows a process for extracting finger vein pattern information by shooting a finger vein image. FIG. 11 shows a process for extracting face vein pattern information by shooting a face vein image.

[149] In addition, FIG. 12 shows a process for extracting palm vein pattern information by shooting a palm vein image. FIG. 13 shows a process for extracting hand dorsum vein pattern information by shooting a hand dorsum vein image. And, FIG. 14 shows a process for extracting foot vein pattern information by shooting a foot vein image.

[150] Therefore, the present invention can perform a first embodiment of performing both face authentication (2D, 3D) and face vein authentication, a second embodiment of performing both face authentication (2D, 3D) and wrist vein authentication, a third embodiment of performing both face authentication (2D, 3D) and hand dorsum vein authentication, a fourth embodiment of performing both face authentication (2D, 3D) and finger vein authentication, a fifth embodiment of performing both face authentication (2D, 3D) and palm vein authentication, and a sixth embodiment of performing both face authentication (2D, 3D) and food vein authentication.

[151] Therefore, according to one embodiment of the present invention, by performing both face authentication and vein authentication of a multitude of body parts according to a security level, security can be reinforced and accuracy can be raised. Further, the

present invention can perform personal authentication with high accuracy by obtaining 3D vein blood vessel information through depth information of a ToF sensor, compensate the inaccuracy of the related art face recognition through additional vein authentication, and apply use scenes of various types.

[152] FIGs. 15 to 22 are diagrams illustrating security authentication according to security levels. Referring to FIGs. 15 to 22, the present invention can perform various authentications according to security levels of an execution mode to be executed.

[153] In one example, if a security level of an execution mode to be executed is low, the present invention can perform a primary authentication of comparing processed face image data with face image data previously stored in a memory only. In some instances, if a security level of an execution mode to be executed is middle, the present invention can perform both a primary authentication of comparing processed face image data with face image data previously stored in a memory and a secondary authentication of comparing vein image data of at least one processed body part with vein image data of at least one body part previously stored in the memory.

[154] In other instances, if a security level of an execution mode to be executed is high, the present invention can perform a primary authentication of comparing processed face image data with face image data previously stored in a memory, a secondary authentication of comparing vein image data of at least one processed body part with vein image data of at least one body part previously stored in the memory, and a tertiary authentication of comparing vein image data of at least one processed different body part with vein image data of at least one different body part previously stored in the memory all.

[155] The present invention checks a security level of an execution mode to be executed. If the checked security level is higher than a reference level, the present invention can perform both a primary authentication based on a face authentication image and a secondary authentication based on a vein authentication image of a body part.

[156] Referring to FIG. 15, if an execution mode to be executed is an electronic payment, a security level of the execution mode to be executed is checked in response to a user's touch to an electronic payment icon 620 and information on the checked security level can be provided as a notification message 630 to a display screen 610 of a digital device 600.

[157] The present invention checks a security level of an execution mode to be executed. If the checked security level is lower than a reference level, the present invention can perform a primary authentication based on a face authentication image only.

[158] Referring to FIG. 16, if an execution mode to be executed is a photo gallery, a security level of the execution mode to be executed is checked in response to a user's touch to a photo gallery icon 640 and information on the checked security level can be

provided as a notification message 650 to a display screen. The present invention checks a security level of an execution mode to be executed. If the checked security level is a special level, the present invention succeeds in both a primary authentication and a secondary authentication, requests an additional body authentication, controls the camera unit 510 to capture a body to be additionally authenticated, and then performs a tertiary authentication based on an additional body authentication image.

[159] Referring to FIG. 17, if an execution mode to be executed is a bank transaction, a security level of the execution mode to be executed is checked in response to a user's touch to a bank transaction icon 642 and information on the checked security level can be provided as a notification message 652 to a display screen.

[160] Referring to FIG. 18 and FIG. 19, when a primary or secondary authentication is performed, if it is in the middle of authentication, the present invention can provide a notification message 670/672, which indicates that authentication is in 'progress, to a display screen 610. A target 680 (face) and vein pattern 681 are also displayed.

[161] Referring to FIG. 20, if authentication is successful, the present invention can provide an authentication success notification message 674 to a display screen 610. Referring to FIG. 21, if authentication is successful, the present invention can provide a next step guide message 676 to a display screen 610. A target 690 (palm) and vein pattern 691 are also displayed.

[162] Referring to FIG. 22, when a primary or secondary authentication is performed, if it is authentication failure, the present invention can provide an authentication failure notification message to a display screen 610 and also provide a re-authentication guide message 679 to the display screen 610. A target 680 (face) and vein pattern 681 are also displayed.

[163] Accordingly, the present invention can perform personal authentication quickly and conveniently by extracting a vein pattern of a body part by applying ToF (time of flight) employing a near infrared light source and then using the extracted vein pattern. And, the present invention can improve safety and reliability of security authentication by performing face authentication and vein authentication of a body part by applying ToF (time of flight) employing a near infrared light source.

[164] Further, the present invention can reinforce security and raise accuracy by performing face authentication and vein authentication of multiple body parts according to a security level. Furthermore, the present invention can perform personal authentication with high accuracy by obtaining 3D vein blood vessel information through depth information of a ToF sensor, compensate the inaccuracy of the related art face recognition through additional vein authentication, and apply use scenes of various types.

[165] Although embodiments have been described with reference to a number of il-

lustrative embodiments thereof, it should be understood that numerous other modifications and embodiments can be devised by those skilled in the art that will fall within the spirit and scope of the principles of this disclosure. More particularly, various variations and modifications are possible in the component parts and/or arrangements of the subject combination arrangement within the scope of the disclosure, the drawings and the appended claims. In addition to variations and modifications in the component parts and/or arrangements, alternative uses will also be apparent to those skilled in the art.

Mode for the Invention

[166] Various embodiments have been described in the best mode for carrying out the invention.

[167] It will be apparent to those skilled in the art that various modification and variations can be made in the present invention without departing from the spirit or scope of the invention. Thus, it is intended that the present invention cover the modification and variations of this invention provided they come within the scope of the appended claims and their equivalents.

Industrial Applicability

[168] The present invention relates to a digital device and biometric authentication method therein. Therefore, the present invention has an industrial applicability.

Claims

[Claim 1] A digital device, comprising:
a camera unit;
a display unit; and
a controller configured to:
in response to a request to execute a first application on the digital device having a first security authentication level, control the camera unit to capture face image data of a target and perform a first authentication process by comparing the captured face image data with prestored face image data, and
in response to a request to execute a second application on the digital device having a second security authentication level more secure than the first authentication level, control the camera unit to capture vein image data of a particular body part of the target, and perform the first authentication process and a second authentication process by comparing the captured vein image data with prestored vein image data.

[Claim 2] The digital device of claim 1, wherein the camera unit comprises:
a light emitting unit including a near infrared light source configured to emit near infrared light to the target, and a color light source configured to emit color light to the target; and
a light receiving unit configured to detect light reflected from the target.

[Claim 3] The digital device of claim 2, wherein the controller is further configured to use the near infrared light source when capturing the vein image data.

[Claim 4] The digital device of claim 2, wherein the light receiving unit comprises:
a lens unit configured to transmit and focus the light reflected from the target;
a filter unit configured to only transmit infrared light from the focused light reflected from the target; and
a detecting unit configured to detect the infrared light filtered by the filter unit.

[Claim 5] The digital device of claim 4, wherein the controller is further configured to move the lens unit centering on the detecting unit in response to an auto focus control signal.

[Claim 6] The digital device of claim 1, wherein the controller is further configured to only compare the captured face image data with the prestored face image data in the first authentication process.

[Claim 7] The digital device of claim 1, wherein the controller is further configured to:
in response to a request to execute a third application on the digital device having a third security authentication level more secure than the second authentication level, control the camera unit to capture additional vein image data of an additional particular body part of the target, and perform the first and second authentication processes and a third authentication process by comparing the captured additional vein image data with prestored additional vein image data for the additional particular body part.

[Claim 8] The digital device of claim 7, wherein the first application corresponds to a payment service, the second application corresponds to a gallery application, and the third application corresponds to a banking application.

[Claim 9] The digital device of claim 1, wherein the vein image data comprises at least of face vein image data, wrist vein image data, hand dorsum vein image data, finger vein image data, palm vein image data, and foot vein image data.

[Claim 10] The digital device of claim 1, wherein the controller is further configured to:
in response to a touch input of application icon on the display unit, display information about a security authentication level of an application corresponding to the application icon.

[Claim 11] The digital device of claim 1, wherein the controller is further configured to:
display an authentication success notification message and a next step guide message on the display unit in response to a successful first authentication process and second authentication process, respectively.

[Claim 12] The digital device of claim 1, wherein the controller is further configured to:
display an authentication failure notification message and re-authentication message on the display unit in response to an unsuccessful first authentication process and second authentication process, respectively.

[Claim 13] A method of controlling a digital device, the method comprising:

in response to a request to execute a first application on the digital device having a first security authentication level, controlling a camera unit of the digital device to capture face image data of a target and performing a first authentication process by comparing the captured face image data with prestored face image data; and
in response to a request to execute a second application on the digital device having a second security authentication level more secure than the first authentication level, controlling the camera unit to capture vein image data of a particular body part of the target, and performing the first authentication process and a second authentication process by comparing the captured vein image data with prestored vein image data.

[Claim 14] The method of claim 13, wherein the camera unit comprises:
a light emitting unit including a near infrared light source configured to emit near infrared light to the target, and a color light source configured to emit color light to the target; and
a light receiving unit configured to detect light reflecting from the target.

[Claim 15] The method of claim 13, further comprising:
using the near infrared light source when capturing the vein image data.

[Claim 16] The method of claim 13, wherein the light receiving unit comprises:
a lens unit configured to transmit and focus the light reflected from the target;
a filter unit configured to only transmit infrared light from the focused light reflected from the target; and
a detecting unit configured to detect the infrared light filtered by the filter unit.

[Claim 17] The method of claim 16, further comprising moving the lens unit centering on the detecting unit in response to an auto focus control signal.

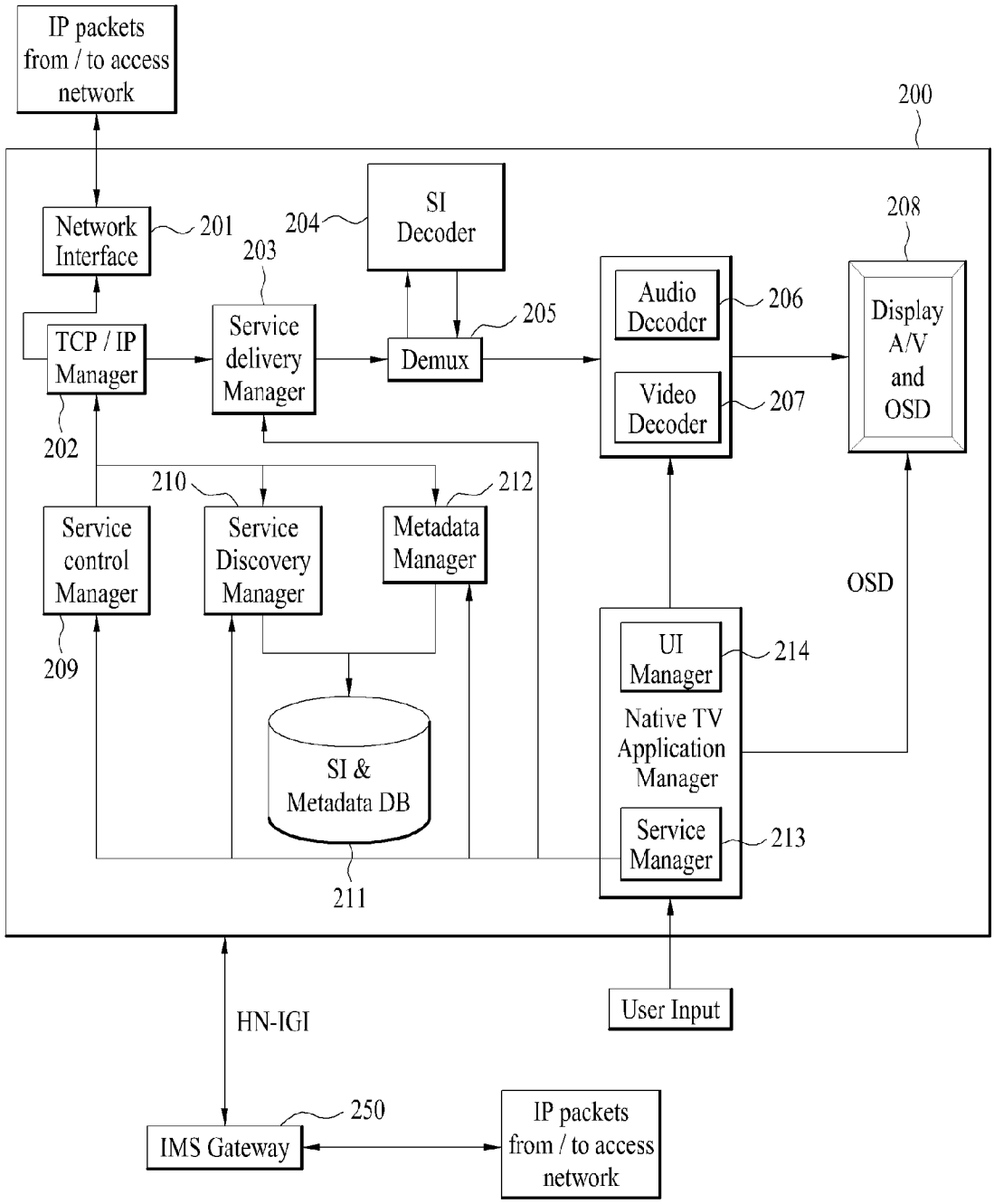
[Claim 18] The method of claim 13, further comprising only comparing the captured face image data with prestored face image data in the first authentication process.

[Claim 19] The method of claim 13, further comprising:
in response to a request to execute a third application on the digital device having a third security authentication level more secure than the second authentication level, controlling the camera unit to capture additional vein image data of an additional particular body part of the

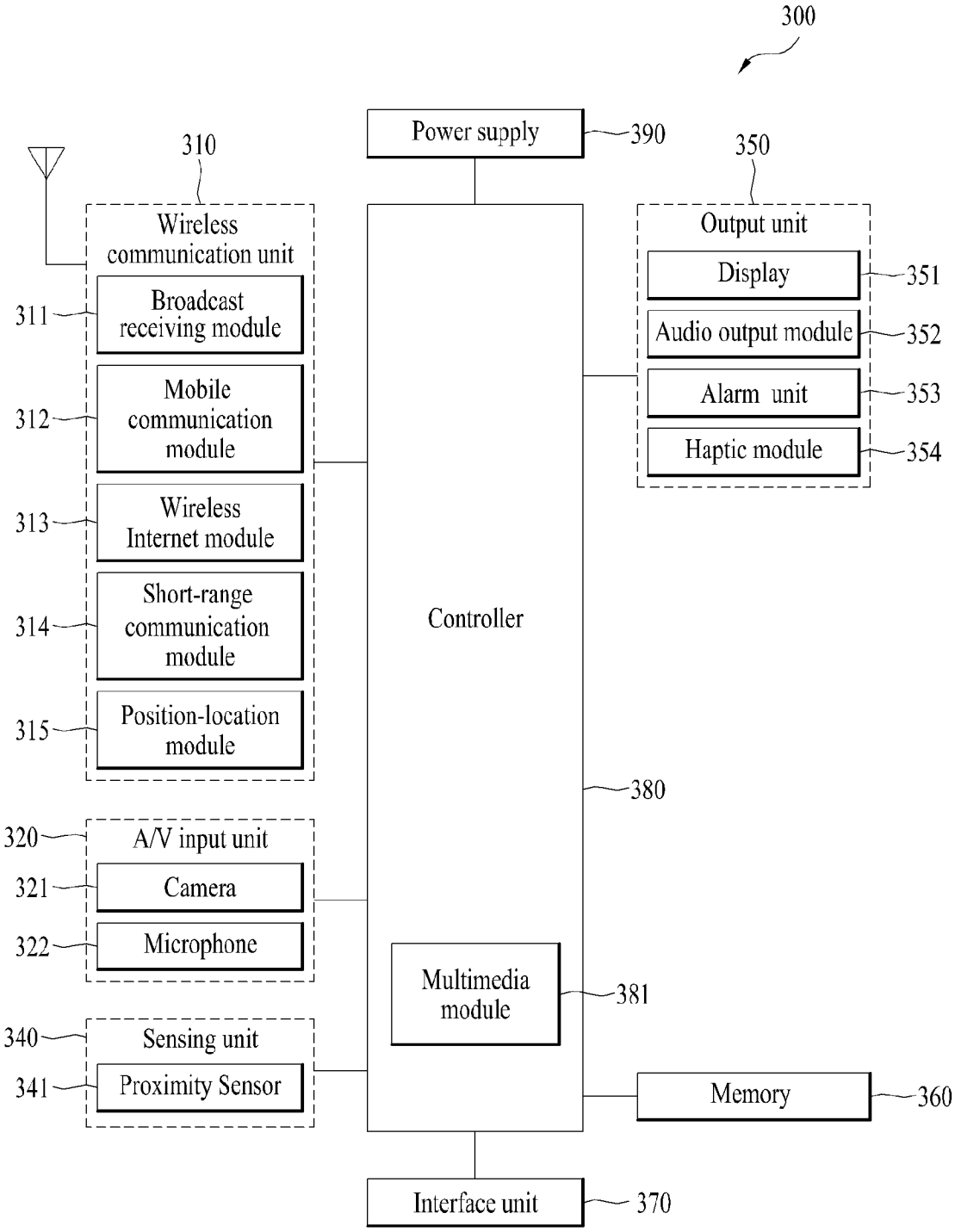
target, and performing the first and second authentication processes and a third authentication process by comparing the captured additional vein image data with prestored additional vein image data for the additional particular body part.

[Claim 20] The method of claim 19, wherein the first application corresponds to a payment service, the second application corresponds to a gallery application, and the third application corresponds to a banking application.

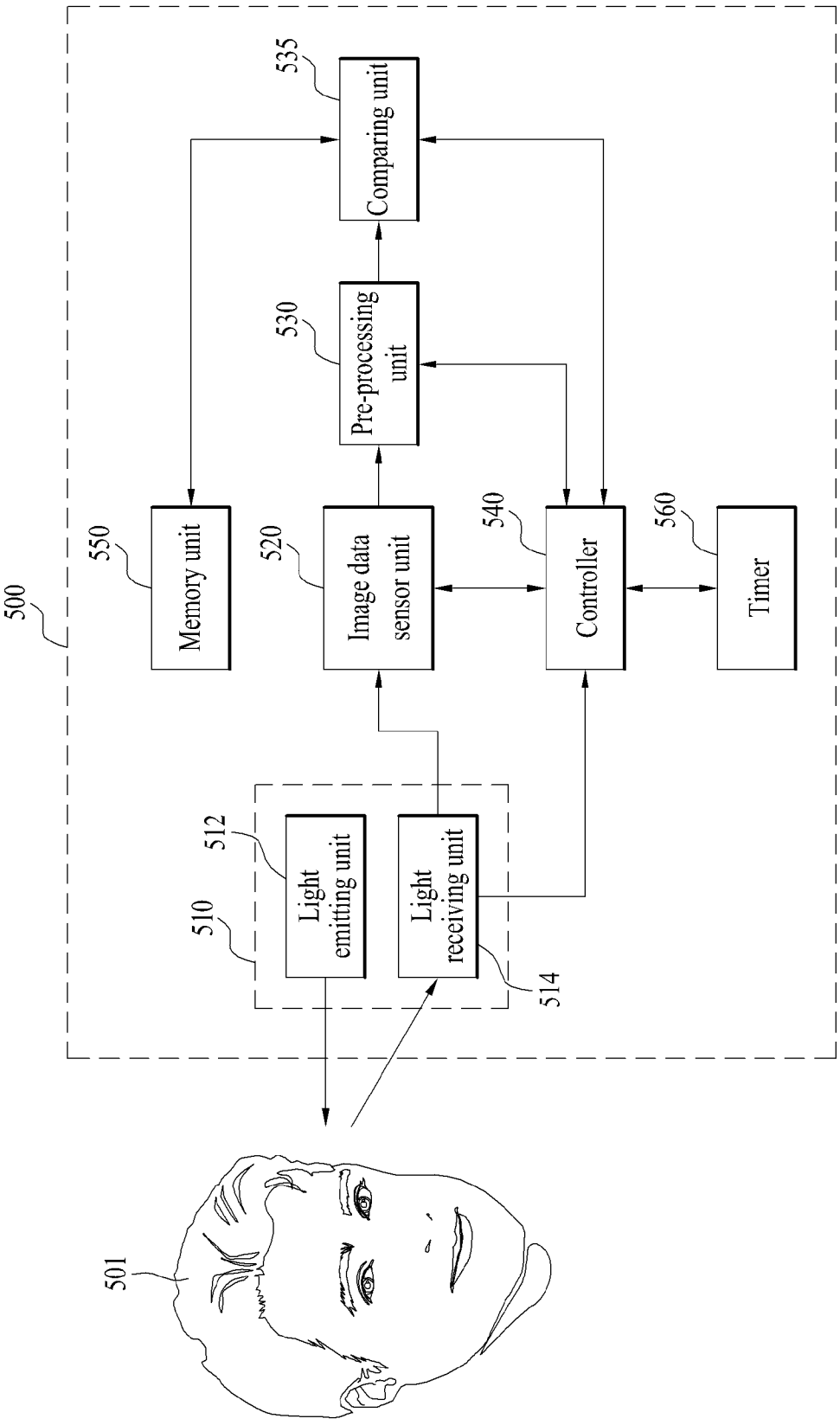
[Fig. 1]


IP packets from / to access network
200
Network Interface
201
SI Decoder
204
203
208
Audio Decoder
206
Display A/V and OSD
Service delivery Manager
205
Demux
TCP / IP Manager
Video Decoder
207
202
210
212
Service control Manager
Service Discovery Manager
Metadata Manager
OSD
209
UI Manager
214
Native TV Application Manager
SI & Metadata DB
Service Manager
213
211
HN-IGI
User Input
250
IMS Gateway
IP packets from / to access network

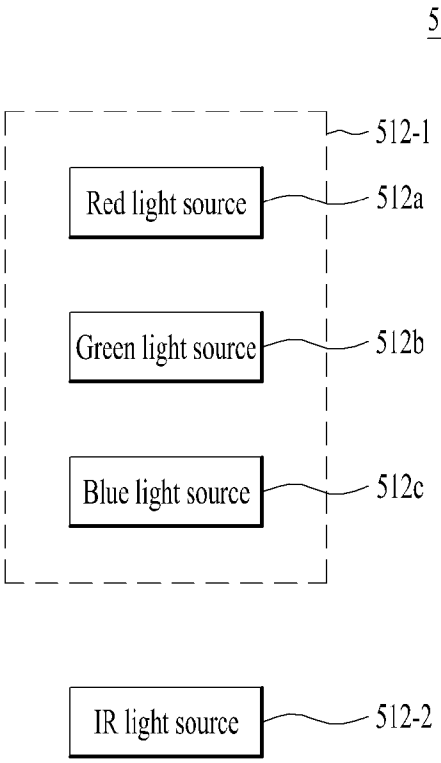
[Fig. 2]


300
Power supply
390
310
350
Wireless communication unit
Output unit
Display
351
311
Broadcast receiving module
Audio output module
352
312
Mobile communication module
Alarm unit
353
313
Wireless Internet module
Haptic module
354
314
Short-range communication module
Controller
315
Position-location module
380
320
A/V input unit
321
Camera
322
Microphone
Multimedia module
381
340
Sensing unit
341
Proximity Sensor
Memory
360
Interface unit
370

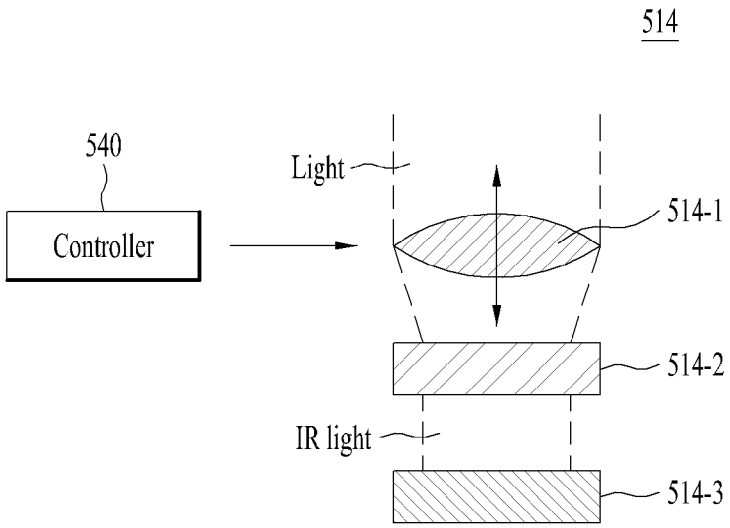
[Fig. 3]


500
535
Comparing unit
530
Pre-processing unit
550
Memory unit
520
Image data sensor unit
540
Controller
560
Timer
512
Light emitting unit
510
Light receiving unit
514
501

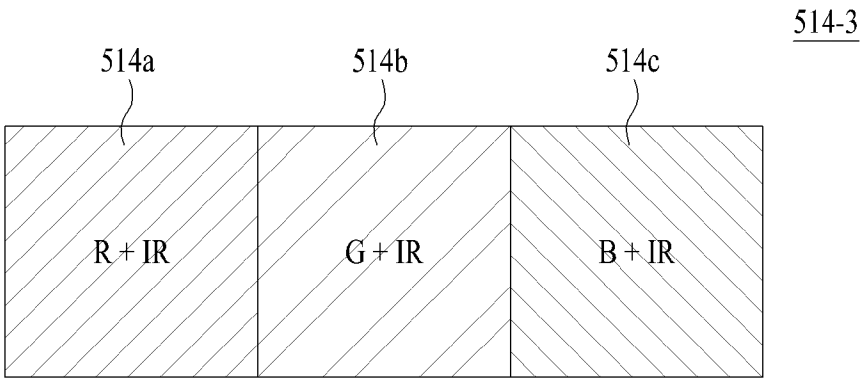
[Fig. 4]



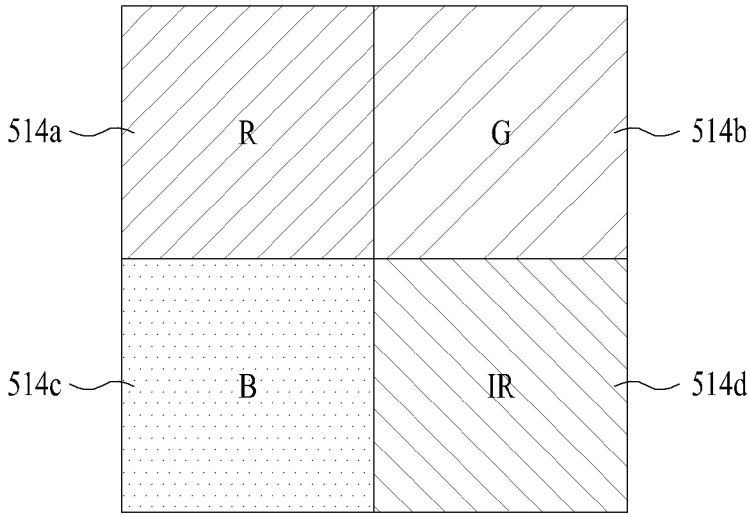
[Fig. 5]



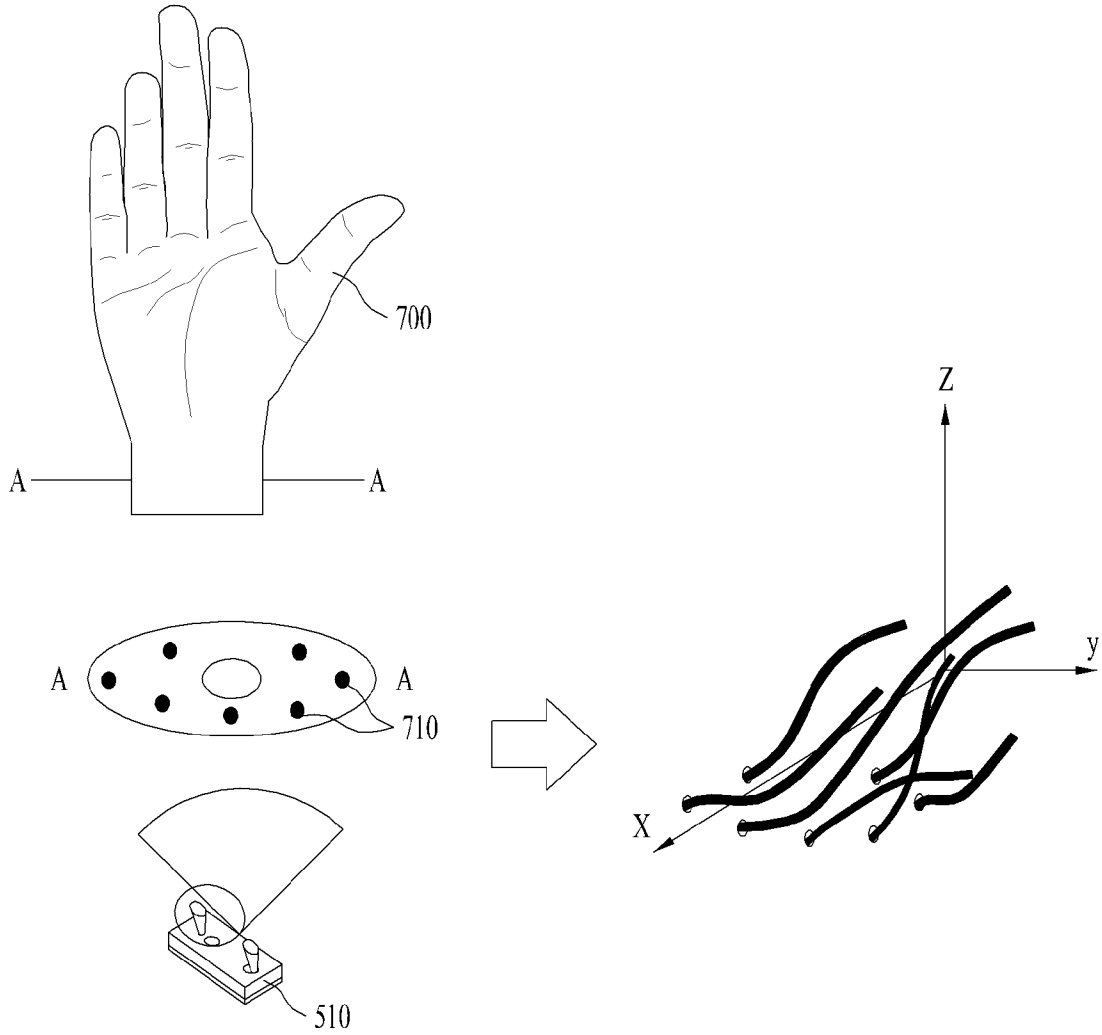
[Fig. 6]



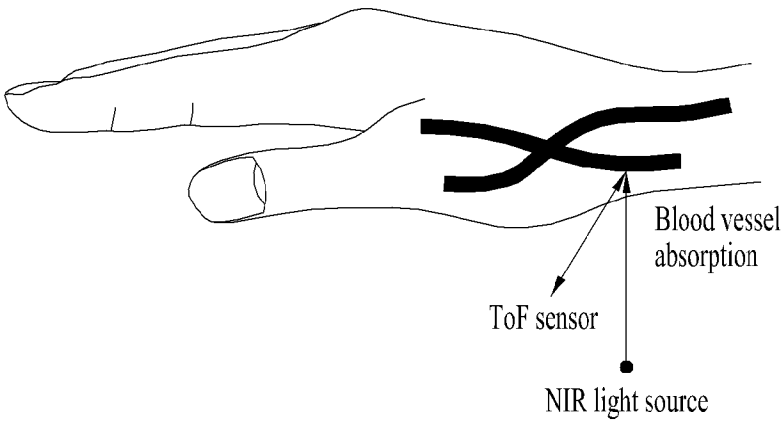
[Fig. 7]



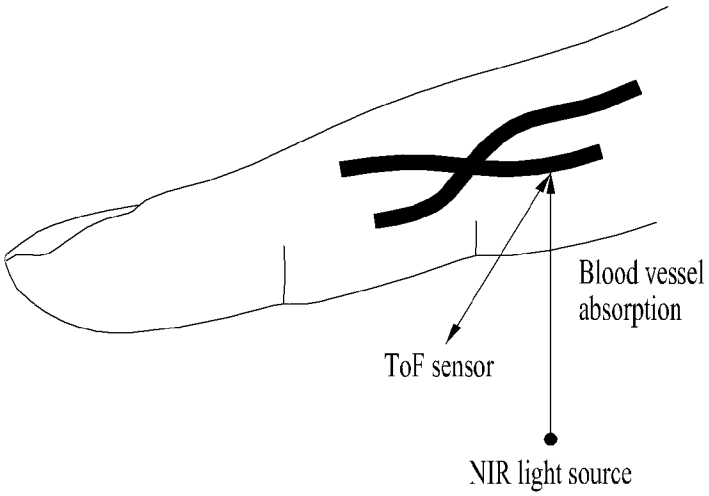
[Fig. 8]



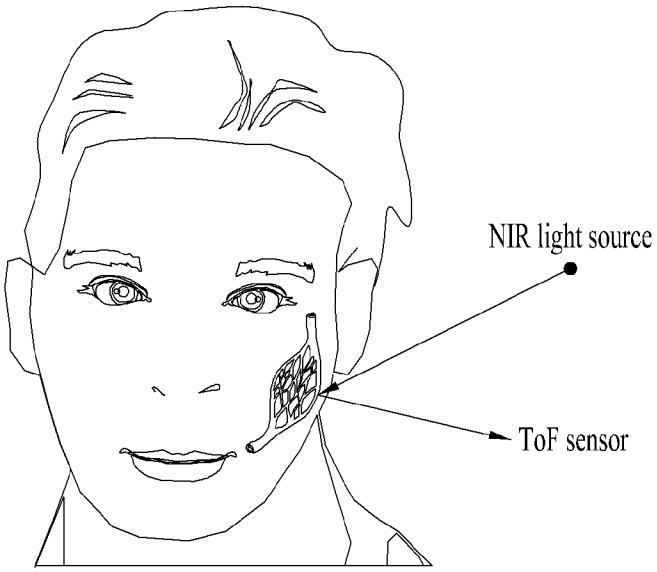
[Fig. 9]



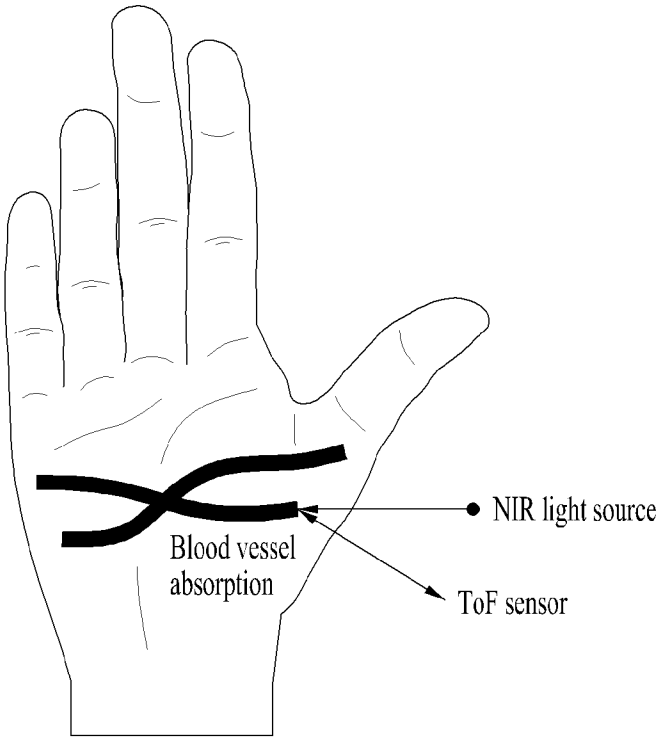
[Fig. 10]



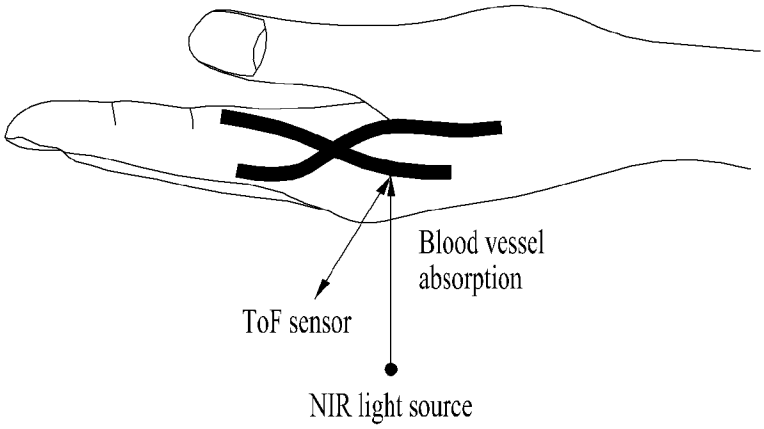
[Fig. 11]



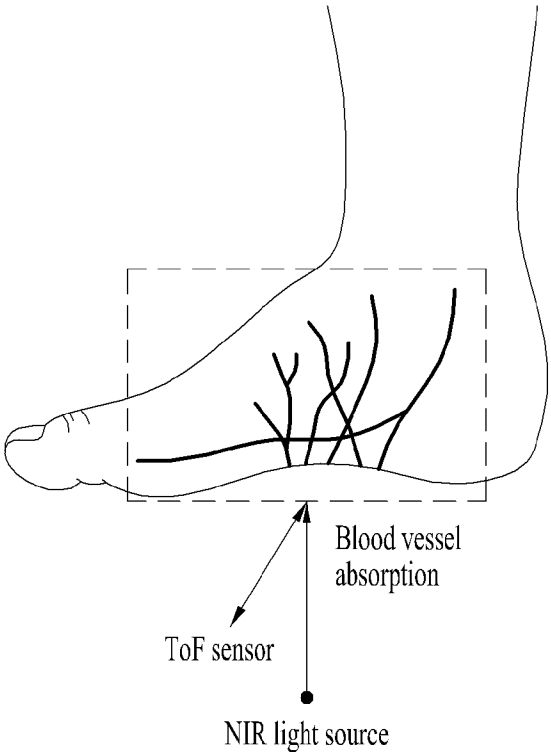
[Fig. 12]


NIR light source
Blood vessel
absorption
ToF sensor

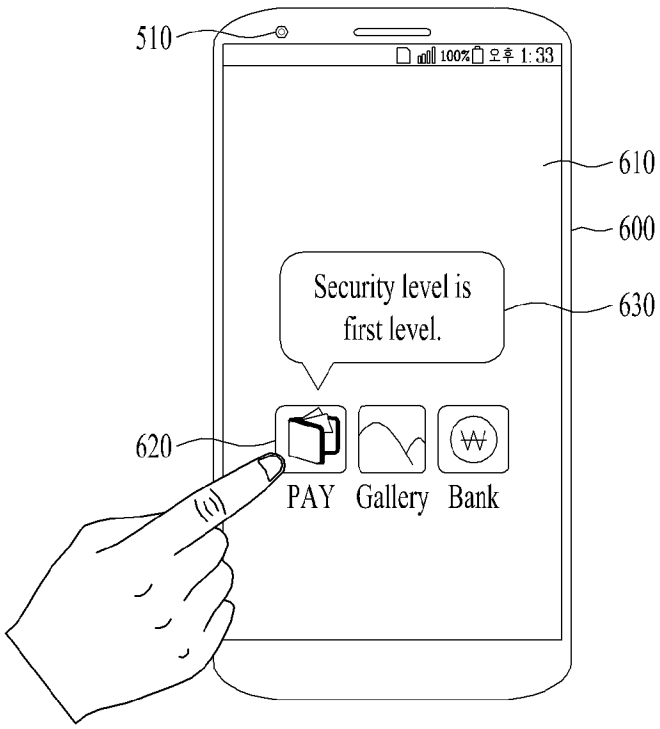
[Fig. 13]


Blood vessel
absorption
ToF sensor
NIR light source

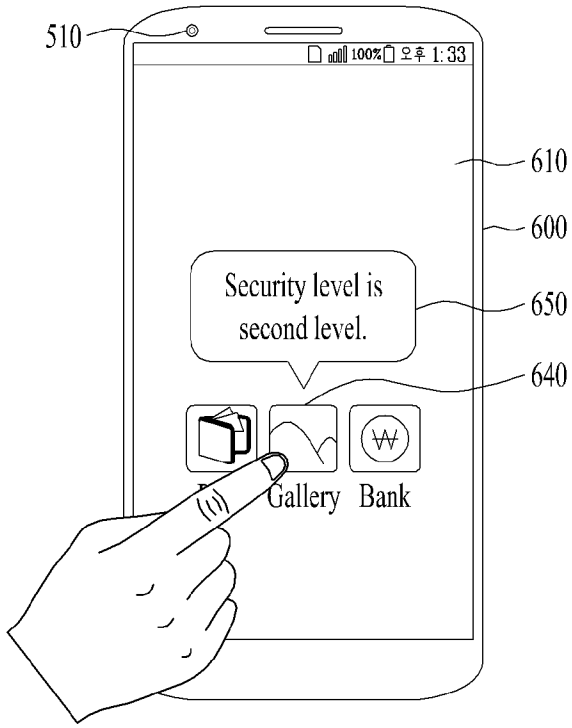
[Fig. 14]


Blood vessel absorption
ToF sensor
NIR light source

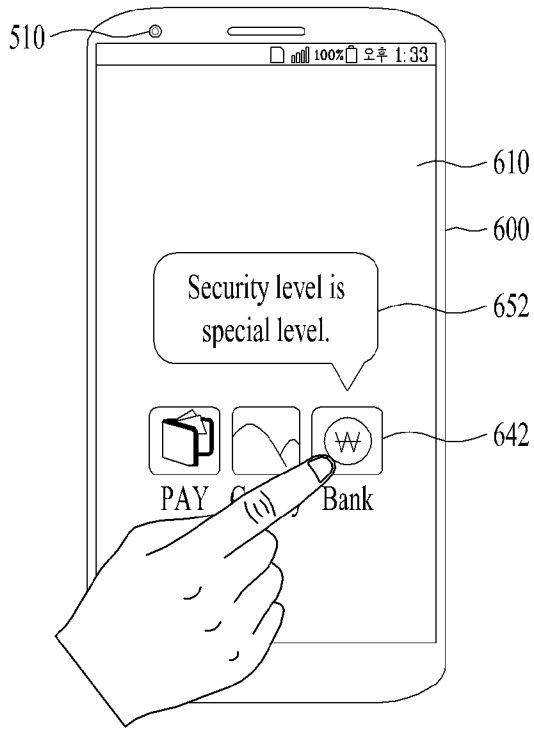
[Fig. 15]


510
610
600
Security level is first level.
630
620
PAY
Gallery
Bank

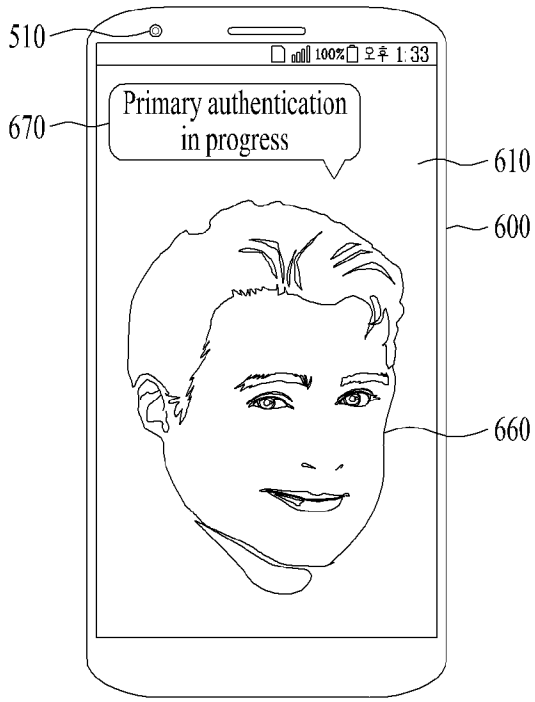
[Fig. 16]


510
100% 오후 1:33
610
600
Security level is second level.
650
640
Gallery
Bank

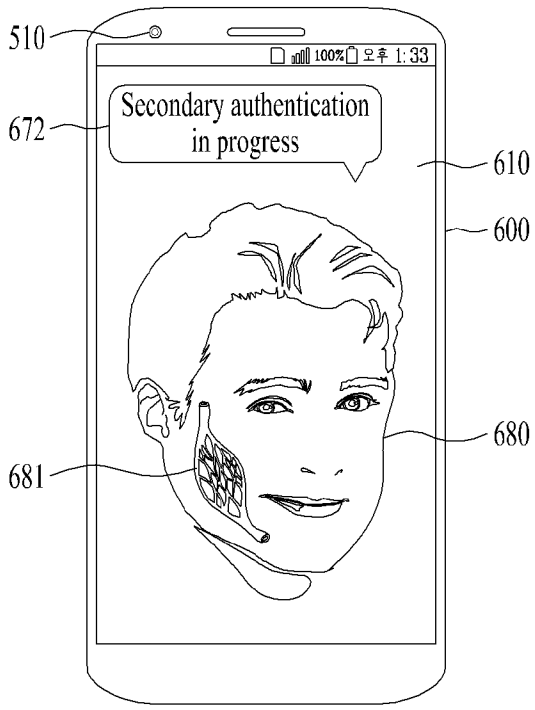
[Fig. 17]


510
100% 오후 1:33
610
600
Security level is special level.
652
642
PAY
Bank

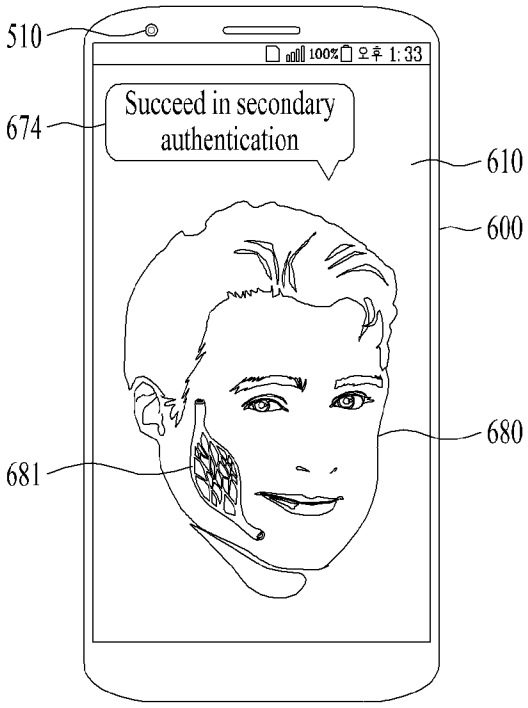
[Fig. 18]


510
100% 오후 1:33
Primary authentication in progress
670
610
600
660

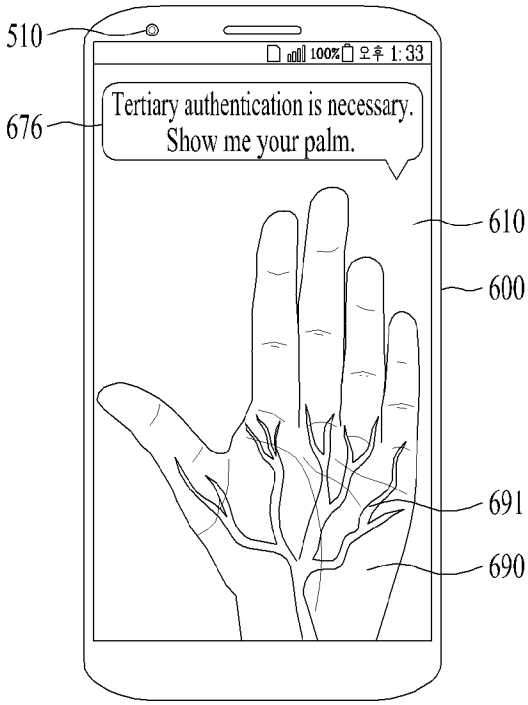
[Fig. 19]


510
100% 오후 1:33
Secondary authentication in progress
672
610
600
680
681

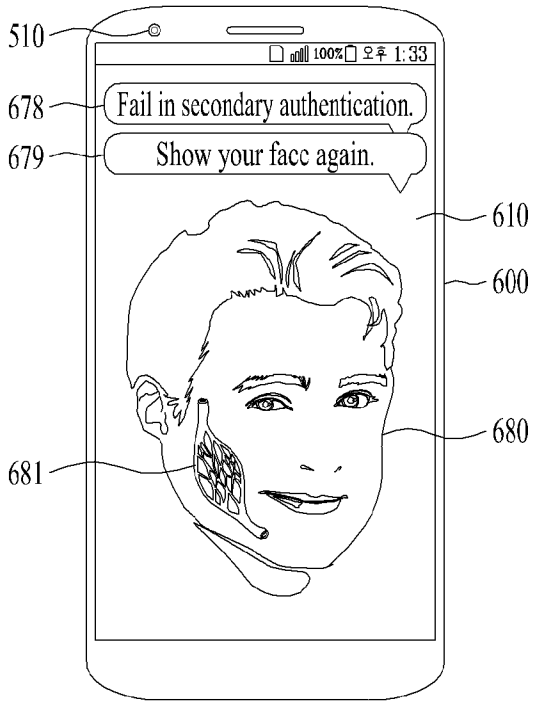
[Fig. 20]


510
100% 오후 1:33
Succeed in secondary authentication
674
610
600
680
681

[Fig. 21]


510
100% 오후 1:33
Tertiary authentication is necessary. Show me your palm.
676
610
600
691
690

[Fig. 22]


510
100% 오후 1:33
678
Fail in secondary authentication.
679
Show your face again.
610
600
680
681

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2018/000664

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32(2013.01)i, G06K 9/00(2006.01)i, G06F 21/45(2013.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/32; H04L 29/06; G06K 9/00; H04W 12/06; G05B 23/00; G06F 21/45

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: authentication, vein, face, biometric, camera

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2004-0048114 A (SECURITY INFORMATION TECHNOLOGY CO., LTD.) 07 June 2004 See pages 4, 6; claims 1-2, 8-9; and figures 1-3.	1,9,11-13
Y		2-6,14-18
A		7-8,10,19-20
Y	KR 10-2016-0099869 A (LG ELECTRONICS INC.) 23 August 2016 See paragraphs 106, 131-136, 157; and figure 6.	2-5,14-17
Y	US 2009-0214083 A1 (HIDEO SATO) 27 August 2009 See paragraph 11; and figure 7.	5,17
Y	US 2014-0366128 A1 (VINKY P. VENKATESWARAN et al.) 11 December 2014 See paragraphs 38-39; and figure 2.	6,18
A	US 2008-0211627 A1 (TAKASHI SHINZAKI) 04 September 2008 SeeSee paragraphs 31-40; and figure 1.	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 June 2018 (08.06.2018)	**11 June 2018 (11.06.2018)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
KANG, Hee Gok
Telephone No. +82-42-481-8264

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2018/000664

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-2004-0048114 A	07/06/2004	None	
KR 10-2016-0099869 A	23/08/2016	KR 10-1729563 B1	11/05/2017
US 2009-0214083 A1	27/08/2009	CN 101485570 A	22/07/2009
		CN 101485570 B	06/04/2011
		JP 2009-165630 A	30/07/2009
		JP 5292821 B2	18/09/2013
		US 8111878 B2	07/02/2012
US 2014-0366128 A1	11/12/2014	CN 105164970 A	16/12/2015
		EP 3005607 A1	13/04/2016
		EP 3005607 A4	18/01/2017
		WO 2014-193396 A1	04/12/2014
US 2008-0211627 A1	04/09/2008	CN 101256628 A	03/09/2008
		CN 101256628 B	13/10/2010
		EP 1965331 A2	03/09/2008
		EP 1965331 A3	27/01/2010
		EP 2339498 A1	29/06/2011
		EP 2339498 B1	18/12/2013
		JP 2008-217355 A	18/09/2008
		JP 5012092 B2	29/08/2012
		KR 10-1026203 B1	31/03/2011
		KR 10-2008-0080924 A	05/09/2008
		US 8797140 B2	05/08/2014