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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 August 2015 (20.08.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/123208 A1

(51) International Patent Classification:
H04M 1/725 (2006.01)

(21) International Application Number:
PCT/US2015/015238

(22) International Filing Date:
10 February 2015 (10.02.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/181,728 17 February 2014 (17.02.2014) US

(72) Inventor; and
(71) Applicant : **KIM, Seungman** [US/US]; 6908 Strata Street, McLean, VA 22101 (US).

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

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

Declarations under Rule 4.17:

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

— *of inventorship (Rule 4.17(iv))*

Published:

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

[Continued on next page]

(54) **Title**: ELECTRONIC APPARATUS AND METHOD OF SELECTIVELY APPLYING SECURITY IN MOBILE DEVICE

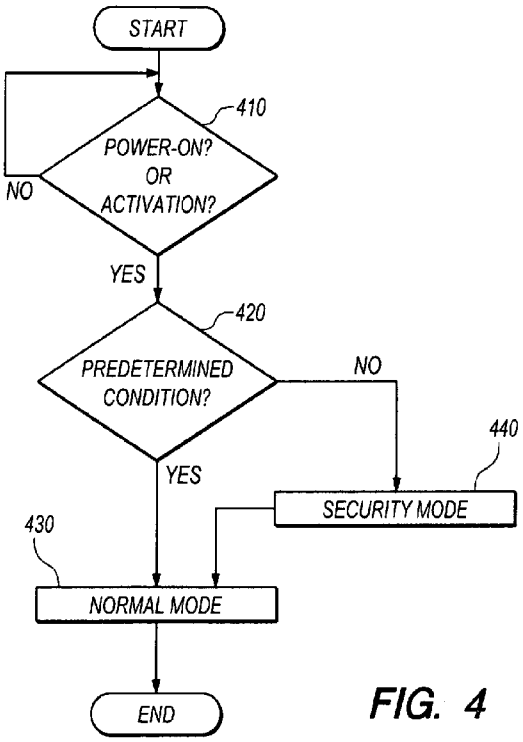

FIG. 4

(57) **Abstract**: A mobile device includes a photographing unit, a display unit, a user interface, a communication interface, and a control unit to control the display unit to display a security checking screen according to a second user input when one external device is set as a safe zone device and when there is no communication connection between the communication interface and the safe zone device, such that a deactivation mode is changed to an activation mode according to a third user input of the user interface through a security checking screen, and to change the deactivation mode to the activation mode according to the second user input without displaying the security checking screen when the one external device is set as the safe zone device and when there is a communication connection between the communication interface and the safe zone device.

WO 2015/123208 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

TITLE OF THE APPLICATION

ELECTRONIC APPARATUS AND METHOD OF SELECTIVELY APPLYING SECURITY IN MOBILE DEVICE

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The present patent application claims priority benefit of a U.S. Non-provisional Patent Application 14/181,728, filed on February 17, 2014, in the United States Patent and Trademark Office, the disclosure of which is incorporated herein in its entirety by reference.

BACKGROUND OF THE INVENTIVE CONCEPT

1. Field of the Inventive Concept

[0002] The present inventive concept relates to an electronic apparatus and method of selectively applying a security mode in a mobile device.

2. Description of the Related Art

[0003] A conventional electronic mobile device, for example, a cellular phone, is set to a security mode or a non-security mode. When the set security mode is set, a user has to input a security code by enter a password, an image, or a geniture though a user interface unit. That is, a user has to input the security code every time to access the mobile device set with the security mode.

[0004] Even if a user is in a security safe zone, the user has to enter the security code previously set in the security mode. In order for the user to avoid inconvenience in the security safe zone, a user has to disable the security mode to avoid any inconvenience to enter the security code, and then later enable the security mode.

[0005] Moreover, since the mobile device is accessed only with the security code set in the security mode, no one is allowed to access the mobile device without the set security code. That is, a person having a high priority or authorization to access the mobile device cannot access the mobile device of a person having a lower priority or authorization.

SUMMARY OF THE INVENTIVE CONCEPT

[0006] The present inventive concept provides an electronic apparatus to selectively apply a security mode in a mobile device.

[0007] The present inventive concept provides a method of selectively applying a security

mode in a mobile device.

[0008] The present inventive concept provides a computer readable medium to contain computer readable codes as a program to execute a method of selectively applying a security mode in a mobile device.

[0009] Additional features and utilities of the present inventive concept will be set forth in part in the description, which follows and, in part, will be obvious from the description, or may be learned by practice of the present inventive concept.

[0010] The foregoing and/or other features and utilities of the present inventive concept may be achieved by providing a mobile device including a display unit to display a screen to set the mobile device in a security mode and a condition as a safe zone in the security mode, a user interface to receive a user input to activate the mobile device, and a control unit to selectively apply the security mode in response to the user input when a current condition is identical to the set condition.

[0011] The foregoing and/or other features and utilities of the present inventive concept may be achieved by providing a mobile device having a photographing unit, a display unit to display a first screen to set the mobile device in a security mode and to display a second screen to set a predetermined condition as a safe zone of the security mode, a user interface to receive an activation key to provide a user input to activate the mobile device, and a control unit configured to control the display to display a third screen to provide a process for the security mode in response to the user input when a current condition of the mobile device is not same as the predetermined condition in the security mode, and to generate a fourth screen of a normal operation mode without generating the third screen for security mode in response to the user input when the current condition of the mobile device is same as the predetermined condition.

[0012] The predetermined condition may include at least one of an area condition and a time condition.

[0013] The predetermined condition may include a connectable condition to connect to an access point, a Bluetooth device, or a wireless communication station.

[0014] The predetermined condition may include a condition to be connected to an external communication apparatus.

[0015] The external communication apparatus may include at least one of a WiFi device, a Bluetooth device, a home appliance apparatus, a medical device, or a vehicle.

[0016] The control unit may control the display unit to display a fifth screen to set a non-safe zone as another condition in a non-security mode.

[0017] The control unit may apply another security mode according to the another condition in the non-security mode in response to the user input.

[0018] The fourth screen may include a state section to display one or more states including a state corresponding to the set condition, and a menu section to display one or more menus.

[0019] The menu section may include a user finger reachable area and a user finger unreachable area, and the one or more menus may be displayed in the user finger reachable area of the menu section.

[0020] The foregoing and/or other features and utilities of the present inventive concept may be achieved by providing a method of controlling a mobile device having a photographing unit, the method including displaying a first screen on a display unit to set the mobile device in a security mode, and a second screen on the display unit to set a predetermined condition as a safe zone of the security mode, providing an activation key as a user input to activate the mobile device, and controlling the display to display a third screen on the display unit to provide a process for the security mode in response to the user input when a current condition of the mobile device is not same as the predetermined condition in the security mode, and to display a fourth screen of a normal operation mode on the display unit without generating the third screen for security mode in response to the user input when the current condition of the mobile device is same as the predetermined condition.

[0021] The setting of the predetermined condition may include setting at least one of an area condition and a time condition.

[0022] The setting of the predetermined condition may include setting a connectable condition to connect to an access point, a Bluetooth device, or a wireless communication station.

[0023] The setting of the predetermined condition may include setting a condition to be connected to an external communication apparatus.

[0024] The external communication apparatus may include at least one of a WiFi device, a Bluetooth device, a home appliance apparatus, a medical device, or a vehicle.

[0025] The controlling of the display unit may include displaying a fifth screen to set a non-safe zone as another condition in a non-security mode.

[0026] The method may further include applying another security mode according to the

another condition in the non-security mode in response to the user input.

[0027] The fourth screen may include a state section to display one or more states including a state corresponding to the set condition, and a menu section to display one or more menus.

[0028] The menu section may include a user finger reachable area and a user finger unreachable area, and the displaying of the one or more menus may include displaying the one or more menus in the user finger reachable area of the menu section.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] These and/or other features and utilities of the present general inventive concept will become apparent and more readily appreciated from the following description of the exemplary embodiments, taken in conjunction with the accompanying drawings of which:

[0030] FIG. 1 is a block diagram illustrating an electronic terminal to communicate with external devices according to an embodiment of the present inventive concept;

[0031] FIG. 2 is a diagram illustrating an electronic terminal according to an embodiment of the present inventive concept;

[0032] FIGS. 3A-3D are views illustrating an electronic terminal with a display unit and a user interface unit according to an embodiment of the present inventive concept;

[0033] FIG. 4 is a flowchart illustrating a method of selectively applying a security mode in a mobile device according to an embodiment of the present inventive concept;

[0034] FIG. 5 is a flowchart illustrating a method of selectively applying a security mode in a mobile device according to an embodiment of the present inventive concept;

[0035] FIG. 6A is a flowchart illustrating a method of setting a condition for a safe zone in a password setting mode of a mobile device according to an embodiment of the present inventive concept;

[0036] FIG. 6B is a flowchart illustrating a method of setting a condition for a non-safe zone in a non-password mode of a mobile device according to an embodiment of the present inventive concept;

[0037] FIGS. 7A through 7I are views illustrating screens of a mobile device to set a condition in a mobile device according to an embodiment of the present inventive concept;

[0038] FIGS. 8A through 8F are views illustrating screens of a mobile device to perform operations in a safe zone and in a non-safe zone according to an embodiment of the present

inventive concept; and

[0039] FIG. 9 is a view illustrating a mobile device to display a user input menu within a user finger-reaching area according to an embodiment of the present inventive concept.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

[0040] Reference will now be made in detail to exemplary embodiments of the present general inventive concept, examples of which are illustrated in the accompanying drawings, wherein like reference numerals refer to the like elements throughout. The exemplary embodiments are described below in order to explain the present general inventive concept while referring to the figures.

[0041] FIG. 1 illustrates an electronic terminal apparatus 110 to communicate with one or more external apparatuses according to an embodiment of the present inventive concept. The electronic terminal apparatus 110 may be a computer apparatus, a portable personal computer, a mobile electronic device, a mobile phone, a mobile tablet apparatus, a mobile tablet computing apparatus, an audio or video recording and/or reproducing apparatus, a photographing apparatus, a communication device, etc.

[0042] The external apparatus may be an access point (AP) 120 such as a wireless access point device to connect to a wired network using WiFi, WiFi direct, or related standards, a device 130 such as a Bluetooth device or radio frequency identification (RFID) device, etc , and a station for wireless communication such as a carrier service station for 4G, LTE, etc. However, the present general inventive concept is not limited thereto. It is possible that the external apparatus may be another electronic apparatus. It is also possible that the external apparatus may be an apparatus to communicate with the terminal 110 to transmit and receive data therebetween, and such an apparatus may be a home appliance, such as a refrigerator or air conditioner.

[0043] The terminal 110 may be disposed within an area defined by a line 120a distanced from the AP 120 or an area defined by a line 130a distanced from the device 130. The terminal 110 may communicate with the AP 120 using the AP-related technology when being disposed within the area defined by the line 120a, and may also communicate with the device using the device-related technology when being disposed within the area defined by the line 130a.

[0044] The terminal 110 may have menus and/or functions to correspond to data (signal) of the AP 120, the device 130, and the station 140. The terminal 110 may have menus and

functions to correspond to data (signal) stored in a storage unit of the terminal 110.

[0045] FIG. 2 illustrates a block diagram of an electronic terminal according to an embodiment of the present inventive concept. The terminal may include a control unit 210, a network interface 220, a user interface 230, a display unit 240, an audio unit 250, one or more functional unit 260, a power supply unit 270 including a battery and a battery charging unit. The above components may be disposed in or on a housing of the terminal.

[0046] The control unit 110 may control operations of the terminal and may include a data storage unit, for example, a semiconductor memory unit. The control unit 110 may be connected to an external data storage unit disposed in the housing. The housing of the terminal may include a port such that another external data storage can be detachably attached to the port of the housing, and the port may be connected to the control unit 110 to transmit and receive data.

[0047] The network interface unit 220 may communicate with an external network apparatus, for example, the AP 120, the device 130, and the station which are illustrated in FIG. 1.

[0048] The user interface unit 230 may receive a user input to control operations of the terminal. The user interface unit 230 may include a physical button or key board such as QWERTY keyboard. The user interface unit 230 may have a sensor to detect a user gesture as a user input. The user interface unit 230 may include a microphone to detect a user voice as a user input. The user interface unit 230 may be a sensor to detect an image as a user input. The display unit 240 may include a screen to display an image corresponding to operations of the terminal. The display unit 240 may include a panel or a touch screen to perform a function to display an image and also a function to receive a user input. The user interface unit 230 and the display unit 240 may be formed as a single integrated body. The audio unit 250 may be a speaker and/or a microphone.

[0049] The functional unit 260 may be a photographing unit to photograph an object and to generate a signal corresponding to the photographing object. The signal may be processed in the control unit 210, displayed in the display unit 240, and/or transmitted to the external apparatus through the network interface unit 220.

[0050] The power supply unit 270 may be connectable to an external power source using a wired and/or wireless method.

[0051] The control unit 210 is configured to selectively perform a security mode according to a condition set by a user when the terminal receives a user input corresponding to a power-on, an activation mode in response to a deactivation mode, a wake-up mode in response to a sleep

mode, and/or a normal mode in response to a power-saving mode. The activation, wake-up, and normal mode may be usable as a common function of the terminal or may be usable differently, according to a design or user preference. The condition may be a safe zone condition in a security mode or may be a non-safe zone in a non-security mode, for example. After the condition is set in a normal mode of the terminal, the terminal is changed to the deactivation mode (the sleep mode or the power-saving mode) a predetermined time after the normal mode or a predetermined time after no user input. And then the terminal provides a process for the security mode or does not provide the process for the security mode according to the condition when being changed to the activation mode (wake-up mode or the normal mode) according to the user input.

[0052] FIGS. 3A-3D illustrating an electronic terminal 300 formed with a display unit and a user interface unit to display screens 300a-300d corresponding to operations of the electronic terminal 300 according to an embodiment of the present inventive concept.

[0053] As illustrated in FIG. 3A, the screen 300a of the terminal 300 A does not show an image according to a deactivation mode, a sleep mode, or a power saving mode. The terminal 300 may have a power switch 311 and a switch 312 as a user input. The power switch 311 may be usable to turn on and off the terminal, and the switch 312 may be usable to change a mode of the terminal 300, that is, to change from the deactivation mode, the sleep mode, or the power saving mode to an activation mode, a wake-up mode, or a normal mode. The switch 312 may be a sensor to detect a motion of the terminal 300 or to detect a motion (image) of a user as a user input.

[0054] When the switch 312 of FIG. 3A is selected, the screen 300b of FIG. 3B may be displayed on a display unit to unlock or select a security process to access the terminal 300 in a security mode. The screen 300b may include a state section 321 and a menu section 322. The state section 321 may include a communication state with the AP 120, the device 130, and/or the station 321 of FIG. 1, and may also include other states corresponding to operations or functions set in the terminal 300 or environment around the terminal 300. The other states may include a time display or a battery state display, a temperature state display, a weather state display, etc. When the terminal 300 is in a power-on state, the terminal monitors, detects, determines, and/or performs communications with external devices to correspond to the above-described states of the state section 321.

[0055] When a menu to unlock the terminal 300 is selected from the screen 300b, the screen 300c is displayed to show a security check process, for example, a password input process, as

illustrated in FIG. 3C. The screen 300c may include a state section 331 and a menu section 332 having a password indication section 332a and a password input section 332b. When a password input by the user through the password input section 332b is identical to a password previously stored therein, the terminal 300 displays the screen 300d to show a state section 341 and a menu section 342 with menus (or icons) 342a.

[0056] When a first predetermined condition is set in the terminal 300 as a safe zone in a security mode (password setting mode), the screen 300a is change to the screen 300d without displaying the screens 300b and 300c when the first predetermined condition is met. When the first predetermined condition is not met, the terminal displays the screens 200b and 300c to require a security process to enter a password. When a second predetermined condition is set in the terminal 300 as a non-safe zone in a non-security mode (no password setting), the terminal displays the screens 300a, 300b, 300c, and 300d to normally access the terminal when the second predetermined condition is met. When the second predetermined condition is not met, the terminal 300 may not display the screens 300b and 300c.

[0057] The state section of the screen 300d may include an image corresponding to the safe zone and/or the non-safe zone according to the security mode and/or non-security mode, respectively. The state section may not be selectable by a user as a user input. The menu section 342 of the screen 300d may include one or more menus selectable by a user as a user input to perform a function or operation of the terminal 300. The menu section 342 of the screen 300d may include a settings menu (icon) to set the security mode, the non-security mode, the safe zone, and/or the non-safe zone, etc.

[0058] FIG. 4 illustrates a method of selectively applying a security mode in a mobile device according to an embodiment of the present inventive concept.

[0059] A power-on or activation switch is on in operation 410, a control unit of the mobile device determines whether a predetermined condition is met in operation 420. When the predetermined condition is met, that is, the mobile device is in a safe zone, the mobile device operates a normal mode in operation 430 such that a user can access the mobile device. When the predetermined condition is not met in operation 420, that is, the mobile device is not in the safe zone, the mobile device requires a user to enter a password in operation 440 to authorize the user to access the mobile device.

[0060] FIG. 5 illustrates a method of selectively applying a security mode in a mobile device according to an embodiment of the present inventive concept

[0061] A predetermined condition is set in the mobile device in operation 510. When an activation switch is selected in operations 520A or 520B, a security mode is not performed to enter a normal mode in operation 530 or the security mode is performed in operation 540 when the predetermined condition is not met in operation 510. That is, the mobile device selectively performs the security mode according to selection of an activation switch as a user input. The mobile device selectively requires a user to perform the security mode. For example, when the mobile device is in a safe zone according to the predetermined condition, the user is not required to process the security mode to enter a password. However, the mobile device is not in the safe zone according to the predetermined condition, the user is still required to process the security mode to enter a password. Here, the password may be a character, number, motion, audio, and/or image.

[0062] FIG. 6A illustrates a method of setting a condition for a safe zone in a password setting mode of a mobile device according to an embodiment of the present inventive concept

[0063] A user selects a settings menu in operation 610, and then selects a password setting menu in operation 620 to set the mobile device as a security (password setting) mode or a non-security (no-password setting) mode.

[0064] A predetermined condition for a safe zone is selected in operation 630, and then is set in operation 640.

[0065] FIG. 6B illustrates a method of setting a condition for a non-safe zone in a non-password mode of a mobile device according to an embodiment of the present inventive concept.

[0066] When a user selects a non-security (no-password setting) mode or does not set a security mode in the settings menu in operation 650, the settings menu may further include a menu to select a non-safe zone (or password-required zone) in operation 660. The predetermined condition can be set in operation 670 such that the mobile device monitors a current condition thereof to determine whether the current condition meets the predetermined condition. When the predetermined condition is met, the mobile device requires the user to enter a password to access the mobile device in the non-security mode of the mobile device. When the predetermined condition is not met, the mobile device does not require the user to enter the password in a similar manner to the non-security mode.

[0067] FIGS. 7A through 7I illustrate screens 700a through 7I of a mobile device to set a condition for a safe zone of a security mode or a non-safe zone of a non-security mode

according to an embodiment of the present inventive concept.

[0068] When a settings menu (button or icon) 710 is selected in the screen 700a of the mobile device as a user input in FIG. 7A, the screen 700b of FIG. 7B is displayed on a display unit and/or user input unit of the mobile device to show a selection of "security setting" 721 to set a security (password) as a security mode, a selection of "all" 722 to apply the security mode to all functions or operations of the mobile device, and a selection of a "safe zone" 723 to prevent the security mode in a predetermined condition. It is possible that the selection of "all" 722 and selection of "safe zone" 723 may be displayed in a separate screen from a screen of the security setting 721, that is, the selection of "all" 722 and selection of "safe zone" 723 may be displayed, performed, or selected independently after the security setting 721 is performed to set the security mode.

[0069] When a menu of the safe zone 723 is selected, the screen 700c is displayed to show an area menu 731 and/or a time menu 732 as the predetermined condition. It is possible that both the area menu 731 and the time menu 732 can be selected and set as the predetermined condition. It is also possible that only one of the area menu 731 and the time menu 732 can be selected and set as the predetermined condition.

[0070] When the time menu 732 is selected, a specific time or a time period is set as the safe zone, using a new screen. Setting a specific time or a time period is well known, detail descriptions thereof will be omitted. When the time menu is performed to set the predetermined condition of the safe zone, the mobile device releases the security mode at the specific time or during the time period such that the user can access the mobile device without the security process according to the set time menu.

[0071] When the area menu 731 is selected, one or more area settings are displayed on the screen 700d of FIG. 7D. The one or more area settings may include a WiFi selection menu 741, a Bluetooth selection menu 742, and a communication method selection menu 743.

[0072] When the WiFi menu 741 is selected, at least one WiFi network 751 can be input, detected and then displayed, or selected as a safe zone in the screen 700e of FIG. 7E. When a user with a mobile device stays in a house of the user, for example, and an AP is located as a home use inside the house of the user, the AP as a home use may be reliable network and environment to the user and thus the home AP can be set as a safe zone. In this case, the user does not have to enter a password every time to activate or access the mobile device within an accessible area of the AP and/or inside the house. However, when a user with a mobile device

stays away from the AP, the mobile device requires the user to enter the password since the predetermined condition is not met or the mobile device cannot communicate with the AP or lost a signal from the AP.

[0073] When the Bluetooth (device) is selected, at least one device 761 can be input, detected and then displayed, or selected as a safe zone in the screen 700f of FIG. 7F. When a user with a mobile device is in a vehicle owned by the user, for example, the Bluetooth and/or the vehicle may be reliable network and environment to the user and thus the device can be set as a safe zone. In this case, the user does not have to enter a password every time to activate or access the mobile device within an access area of the device, that is, within an inside of the vehicle.

[0074] It is possible that when a user vehicle is set as the device or the AP for the safe zone and when a signal indicating an emergence, for example, traffic collision or accident to the vehicle, is generated from the vehicle and then transmitted to the mobile device through the Bluetooth or WiFi, the mobile device can recognize the received signal as a predetermined condition of a safe zone so that the user can access and/or use the mobile device without entering a password in the security mode of the mobile device. Here, the vehicle and the mobile device are configured to recognize the signal as a portion of the predetermined condition of a safe zone. In this case, a combination of the selected device and a specific or predetermined signal from the selected device can be set as the safe zone of the mobile device, and when the mobile device receives the signal from the device, so that the user can access or use the mobile device without performing a security check process in a security mode of the mobile device.

[0075] It is also possible that when a user medical device is set as the device or the AP for the safe zone and when a signal indicating an emergence for example, a life threatening situation or accident to the user, is generated from the medical device and then transmitted to the mobile device through the Bluetooth or WIFi, the mobile device can recognize the received signal as a predetermined condition of a safe zone so that the user can access and/or use the mobile device without entering a password in the security mode of the mobile device. Here, the medical device and the mobile device are configured to recognize the signal as a portion of the predetermined condition of safe zone. In this case, a combination of the selected device and a specific or predetermined signal from the selected device can be set as a predetermined condition of the safe zone of the mobile device, and when the mobile device receives the signal from the device, so that the user can access or use the mobile device without performing a

security check process in a security mode of the mobile device.

[0076] When the communication method 743 is selected, one or more communication methods (CMs) 771 and 772 can be selected and set as a safe zone on the screen 700g of FIG. 7G. In this case, a carrier name 771 and/or telephone number 772 can be reliable to the user. That is, when the user communicates with the person of the telephone number and the carrier name, the user does not have to enter a password to use the mobile device.

[0077] In the screen 700h of FIG. 7H, at least one or a combination of the Wifi, Bluetooth, and communication method can be selected and/or set in a menu 781 as safe zone.

[0078] When the security mode is not selected or set in the settings menu 710 of the screen 700a, a menu 791 of non-safe zone can be selected and set such that the mobile device is set to perform a security mode in a non-security mode of the mobile device. For example, an AP, a device, or a communication method is set as the non-safe zone using one or more non-safe zone selection processes similar to the safe zone selection processes of FIGS. 7D through 7H.

[0079] FIGS. 8A through 8F illustrate screens 800a through 800f of a mobile device to perform operations in a safe zone and in a non-safe zone according to an embodiment of the present inventive concept

[0080] FIG. 8A illustrates the screen 800a, a power on/off switch 811, and an activation switch 812. FIG. 8B illustrates the screen 800b including a state section 821 and a menu section 822. The state section 821 may be similar to the state section 321, 331, and 341 of FIGS. 3B, 3C and 3D. The state section 821 may include a state indicator 821a to indicate a predetermined state and/or a safe zone in a security mode. The states displayed on the state section 821 may not be selectable by a user as a user input. The menu section 822 may include one or more menus 822a and 822n which are displayable on a display unit and/or selectable by a user as a user input.

[0081] When a current condition matches the predetermined condition as the safe zone, the mobile device displays the screen 800b by skipping a security mode process. It is possible that the mobile device can display on the screen 800c with a state section 831 and a menu section832 including a test message 832a and selection menus 832 b relating to the displayed text 832a when the mobile device receives the test message. It is also possible that the mobile device can display on the screen 800d with a state section 841 and a menu 4 including a telephone call message 842a including selection menus relating to the telephone call message 842a when the mobile device receives the telephone call such that the user can access and use

the mobile device.

[0082] The screen 800e of FIG. 8E illustrates a state section 851 and a menu section 852 including at least one menu 852. The screen 800e may be displayed when a password is entered in a security (password-setting) mode, when a predetermined condition of a safe zone is met in the security mode, or when a password is entered in a non-security mode and in a non-safe zone. The menu 852 may be a settings menu to select, change, or modify settings of the mobile device. In this case, it is possible that the mobile device may require the user to enter a password to select, change, or modify settings when the screen 8003 is displayed when a predetermined condition of a safe zone is met in the security mode and accordingly a security mode is not preformed.

[0083] FIG. 9 illustrates a mobile device 900 to display a state section 911 and a user menu section 912 according to an embodiment of the present general inventive concept. A user U holds the mobile device 900 using one hand. At least one of user fingers UF of the user one hand can be usable to select a menu to input a user input. The user menu section 912 may include a user menu area 912b and a non-user menu area 912c which are defined by a line to be a user-finger reachable area and a user-finger unreachable area, respectively. One or more menus or images displayed within the user menu area can be selectable by a user using a finger without assistance of the other hand finger, and one or more menus or images displayed within the non-user menu area 912c may not be reachable selectable by the user using the same finger. It is possible that the non-user menu area 912c may not include a menu to be selectable by a user as a user input. Accordingly, a user can control the mobile device with one hand.

[0084] The present general inventive concept can also be embodied as computer-readable codes on a computer-readable medium. The computer-readable medium can include a computer-readable recording medium and a computer-readable transmission medium. The computer-readable recording medium is any data storage device that can store data as a program which can be thereafter read by a computer system. Examples of the computer-readable recording medium include a read-only memory (ROM), a random-access memory (RAM), a flash memory, a semiconductor chip package, CD-ROMs, magnetic tapes, floppy disks, and optical data storage devices. The computer-readable recording medium can also be distributed over network coupled computer systems so that the computer-readable code is stored and executed in a distributed fashion. The computer-readable transmission medium can transmit carrier waves or signals (e.g., wired or wireless data transmission through the Internet).

Also, functional programs, codes, and code segments to accomplish the present general inventive concept can be easily construed by programmers skilled in the art to which the present general inventive concept pertains.

[0085] As illustrated above, a mobile device can be set in a security mode and the security mode can be set with a safe zone so that a mobile device does not require a user to enter a password when a current condition matches a predetermined condition of the safe zone.

[0086] Although a few exemplary embodiments of the present general inventive concept have been shown and described, it will be appreciated by those skilled in the art that changes may be made in these exemplary embodiments without departing from the principles and spirit of the general inventive concept, the scope of which is defined in the appended claims and their equivalents.

CLAIMS

What is claimed is:

1. A mobile device having a photographing unit with a lens element to photograph an object, comprising:

a display unit to display an image corresponding to the photographed object, a menu screen, a security safe zone processing screen, and a security checking screen;

a user interface to receive a user input;

a communication interface to wirelessly communicate with one or more external devices; and

a control processor unit configured to control the display unit to display the security safe zone processing screen in an activation mode to set one of the one or more external devices as a safe zone device according to a first user input of the user interface, to set the mobile device in a deactivation mode, to control the display unit to display the security checking screen according to a second user input when the one external device is set as the safe zone device and when there is no communication connection between the communication interface and the safe zone device, to change the deactivation mode to the activation mode according to a third user input of the user interface through the security checking screen, and to change the deactivation mode to the activation mode according to the second user input without displaying the security checking screen when the one external device is set as the safe zone device and when there is a communication connection between the communication interface and the safe zone device.

2. The mobile device of claim 1, wherein the activation mode is a normal mode or a turning-on mode, and the deactivation mode is a sleep mode or a turning-off mode.

3. The mobile device of claim 1, wherein the deactivation mode includes a mode in which the control processor controls the communication interface to attempt communication with the one or more external devices to establish the communication connection.

4. The mobile device of claim 1, wherein the activation mode includes a mode in which the control processor unit controls the display unit to selectively generate the security checking screen according to status of the communication connection between the communication interface and the safe zone device.

5. The mobile device of claim 1, wherein the control processor unit controls the display unit to generate the security checking screen when the communication connection between the communication interface and the safe zone device is changed to the no communication connection.

6. The mobile device of claim 1, wherein the control processor unit controls the display unit to generate the security checking screen when the safe zone device is no longer available to provide the communication connection in the activation mode.

7. The mobile device of claim 1, wherein the control processor unit controls the display unit to generate the security checking screen when there is no communication connection between the communication interface and the safe zone device and when there is a communication connection with the communication interface and the other one of the one or more external devices than the safe zone device.

8. The mobile device of claim 1, wherein:

the control processor unit receives a condition set by a user through the security safe zone processing screen; and

the control processor unit sets the one of the one or more external devices as the safe zone device when the set condition is identical to a condition of the one of the one or more external devices.

9. The mobile device of claim 1, wherein the control processor unit determines status of the communication connection between the communication interface and the safe zone device according to identifications of the safe zone device and one of the external devices.

10. The mobile device of claim 1, wherein the control processor unit sets the one external device as the safe zone device with a predetermined condition, and the predetermined condition includes at least one of an area condition and a time condition.

11. The mobile device of claim 6, wherein the control processor unit sets the one external device as the safe zone device with a predetermined condition, and the predetermined condition includes a connectable condition to connect to an access point, a Bluetooth device, or

a wireless communication station.

12. The mobile device of claim 1, wherein the external devices comprise at least one of a WiFi device, a Bluetooth device, a home appliance apparatus, a medical device, and a vehicle.

13. The mobile device of claim 1, wherein the control processor unit controls the display unit to display a non-safe zone processing screen to set a non-safe zone device with another condition in a non-security mode such that the security checking screen is generated when the communication device and the non-safe zone device is in a connectable condition.

14. The mobile device of claim 1, wherein the control processor unit controls the display unit to display a screen to unlock and select a security process, processes the security checking screen when the security process is selected, generates a setting mode to select the security safe zone processing screen when the security process is unlocked, and processes the security safe zone processing screen when the security safe zone processing screen is selected in the setting mode.

15. The mobile device of claim 1, wherein the control processor unit controls the display unit to simultaneously display the menu screen and the security checking screen over the image.

16. The mobile device of claim 1, wherein the user interface comprises a touch input panel to detect a user touch on a first panel of the display unit, a geniture input panel to detect a user geniture with respect to a second panel of the display unit, or a sensor to detect a user image or a user sound.

17. The mobile device of claim 1, wherein the mobile device comprises a housing, and the housing accommodates the photographing unit, the display unit, the user interface, the communication unit, and the control processor unit.

18. The mobile device of claim 1, wherein:

the display unit includes a display panel formed with a screen area to display the image;

the screen area include a user finger reachable area and a user finger unreachable

area;

the user finger reachable area is disposed close to a user hand holding a housing of the mobile device;

the user finger unreachable area is disposed away from the user hand holding the housing of the mobile device; and

the menu screen is disposed in the user finger reachable area.

19. The mobile device of claim 1, wherein:

the mobile device includes a housing having two opposite sides to be held by a user hand; and

the menu screen is disposed in a side portion closer to one of the two opposite sides of the housing than a center portion between the two opposite sides of the housing.

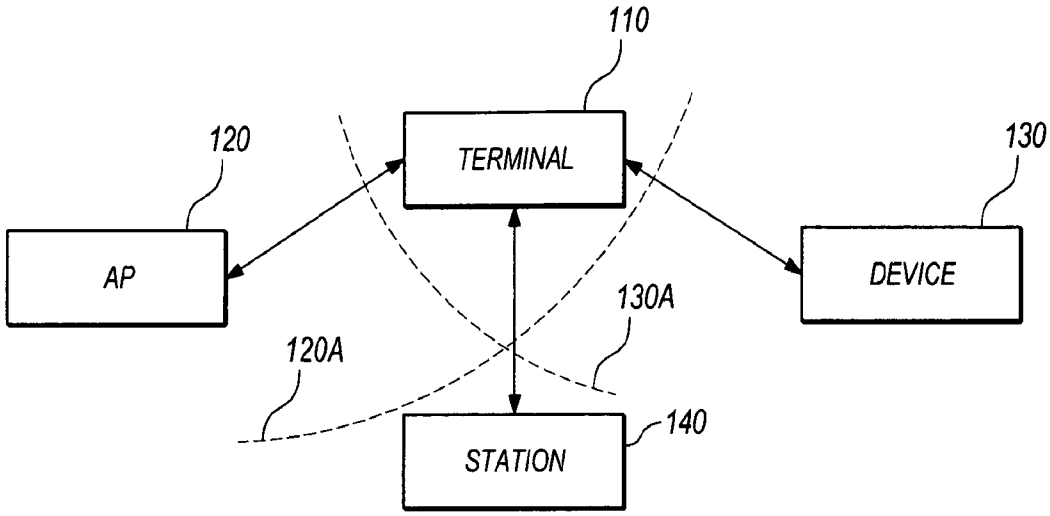
110
120
TERMINAL
130
AP
DEVICE
130A
120A
140
STATION

FIG. 1

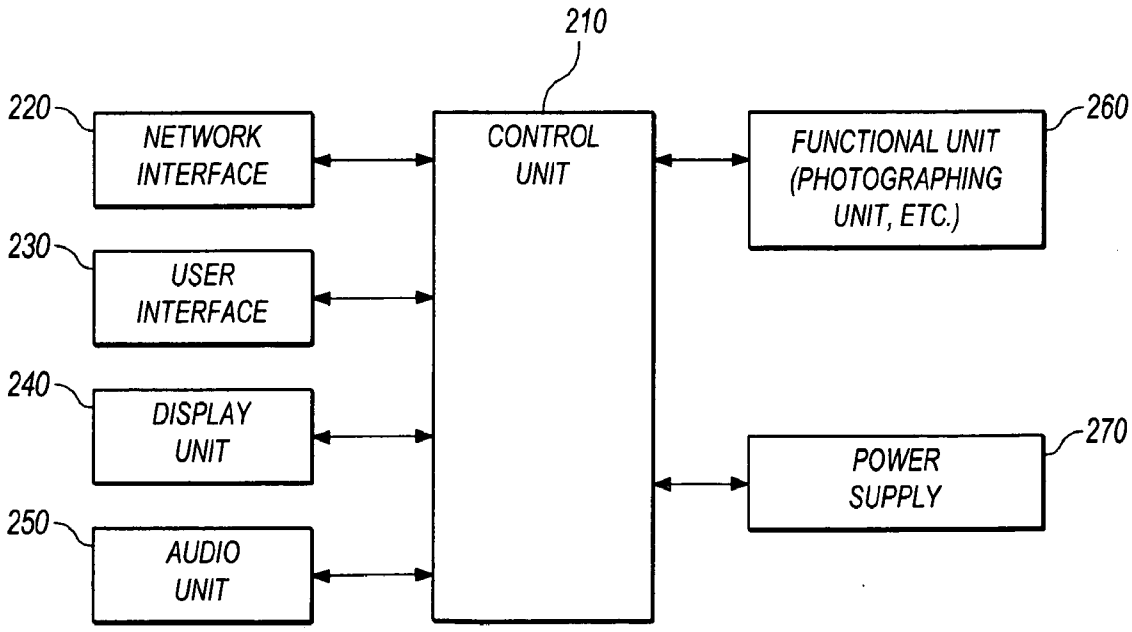
210
220
NETWORK INTERFACE
CONTROL UNIT
260
FUNCTIONAL UNIT (PHOTOGRAPHING UNIT, ETC.)
230
USER INTERFACE
240
DISPLAY UNIT
270
POWER SUPPLY
250
AUDIO UNIT

FIG. 2

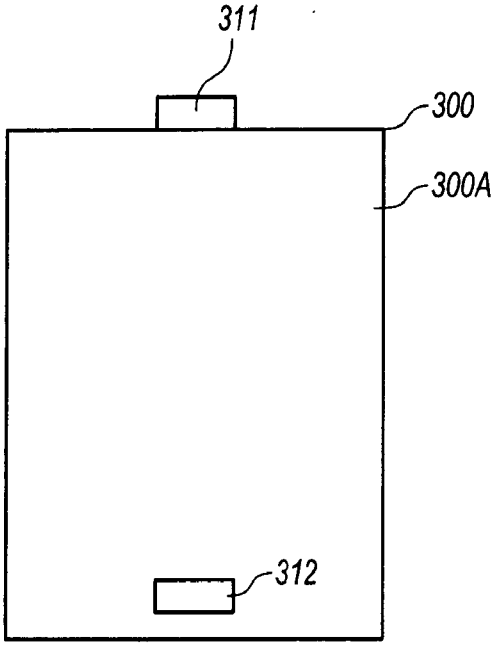

FIG. 3A

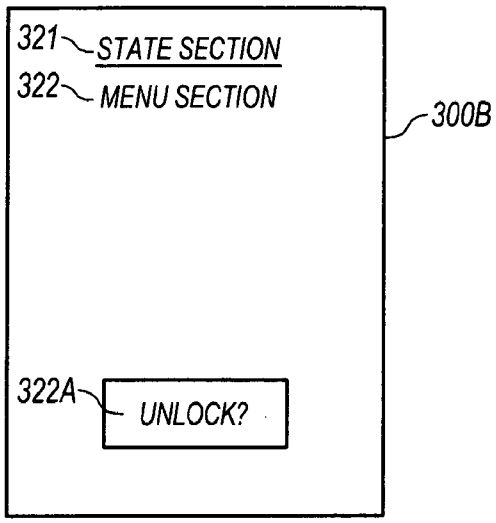

FIG. 3B

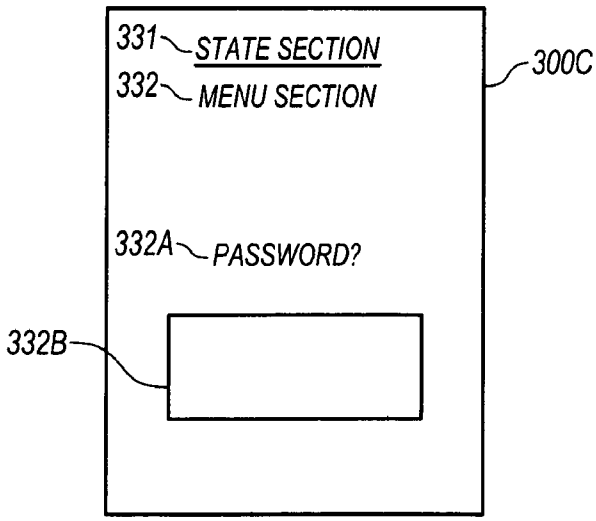

FIG. 3C

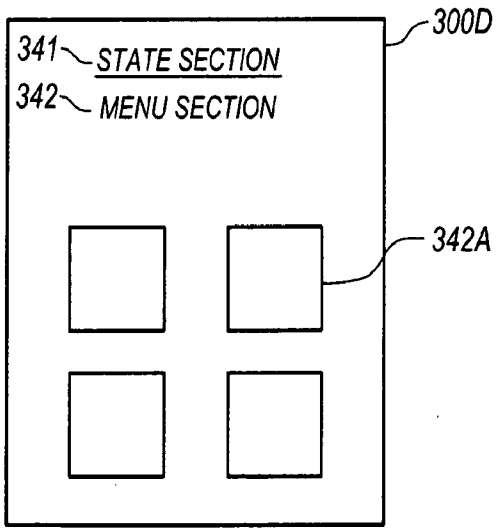

FIG. 3D

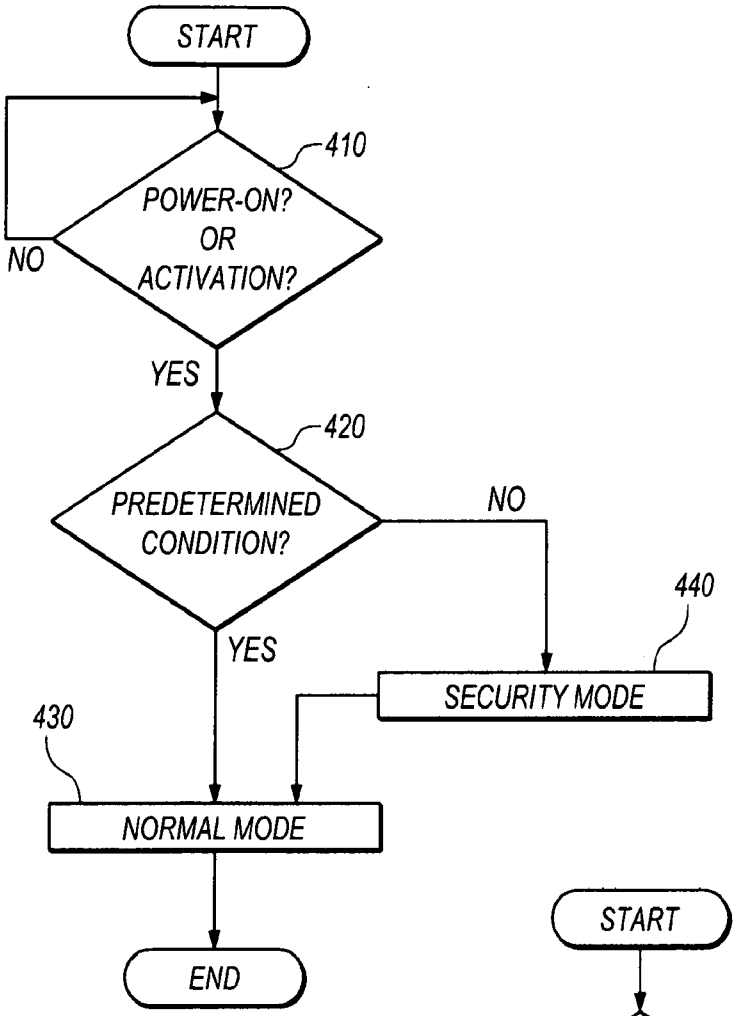
START
410
POWER-ON? OR ACTIVATION?
NO
YES
420
PREDETERMINED CONDITION?
NO
440
SECURITY MODE
YES
430
NORMAL MODE
END

FIG. 4

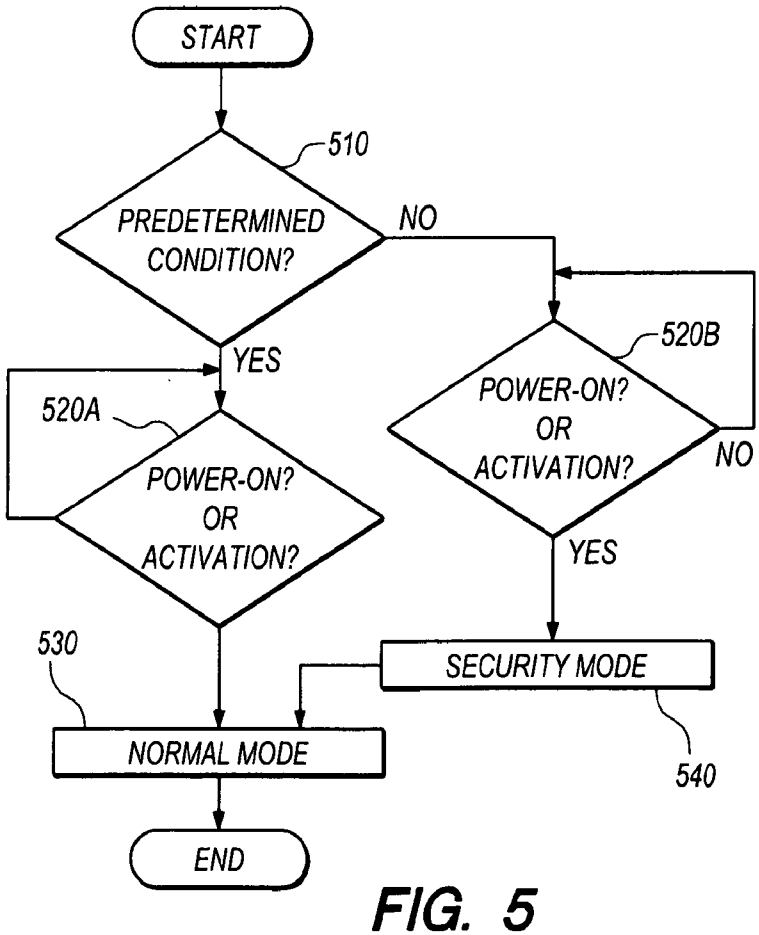
START
510
PREDETERMINED CONDITION?
NO
YES
520A
POWER-ON? OR ACTIVATION?
520B
POWER-ON? OR ACTIVATION?
NO
YES
530
SECURITY MODE
NORMAL MODE
540
END

FIG. 5

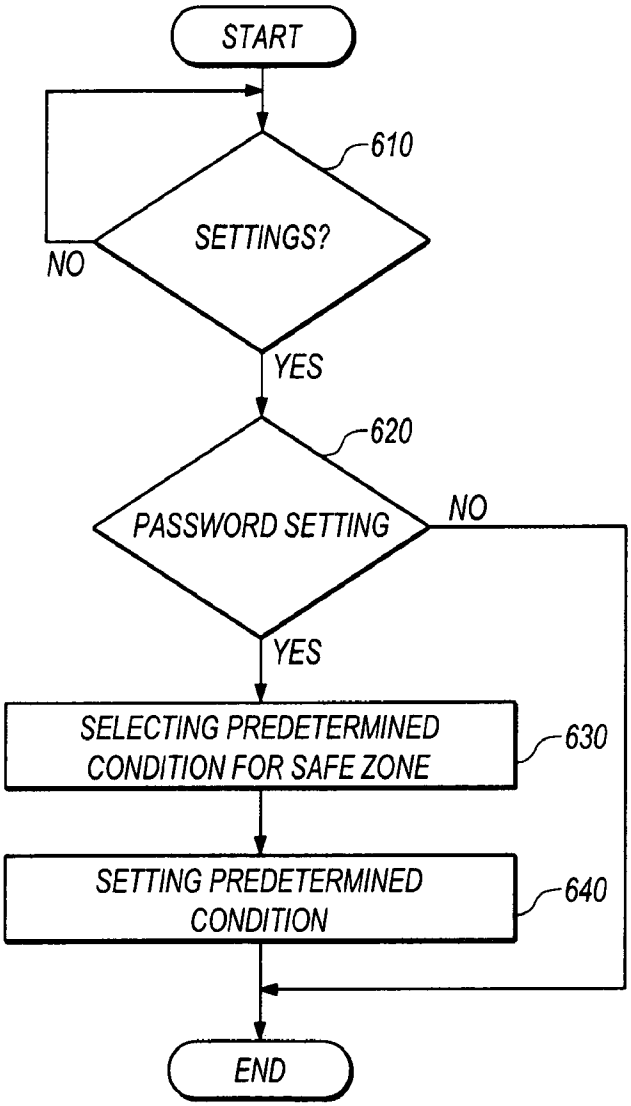
START
610
SETTINGS?
NO
YES
620
PASSWORD SETTING
NO
YES
SELECTING PREDETERMINED CONDITION FOR SAFE ZONE
630
SETTING PREDETERMINED CONDITION
640
END

FIG. 6A

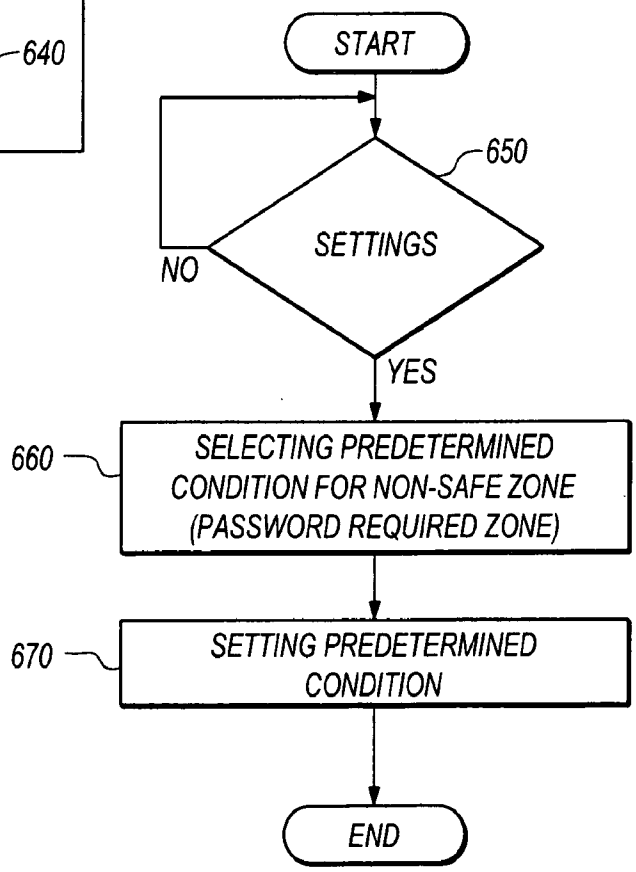
START
650
SETTINGS
NO
YES
660
SELECTING PREDETERMINED CONDITION FOR NON-SAFE ZONE (PASSWORD REQUIRED ZONE)
670
SETTING PREDETERMINED CONDITION
END

FIG. 6B

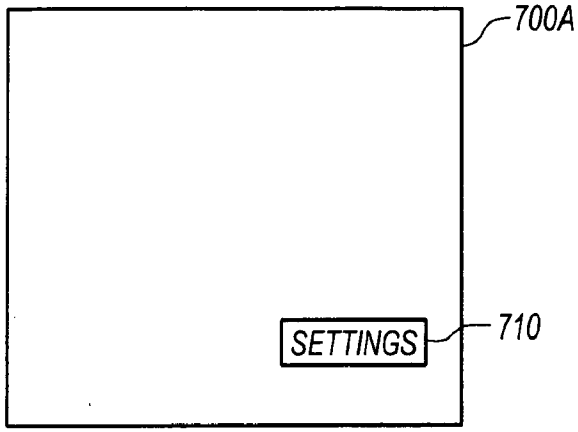

FIG. 7A

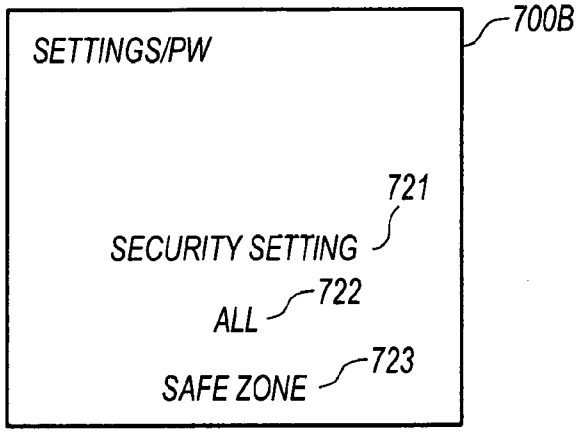

FIG. 7B

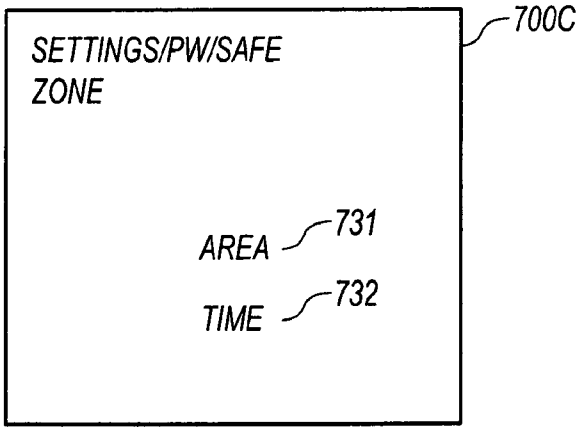

FIG. 7C

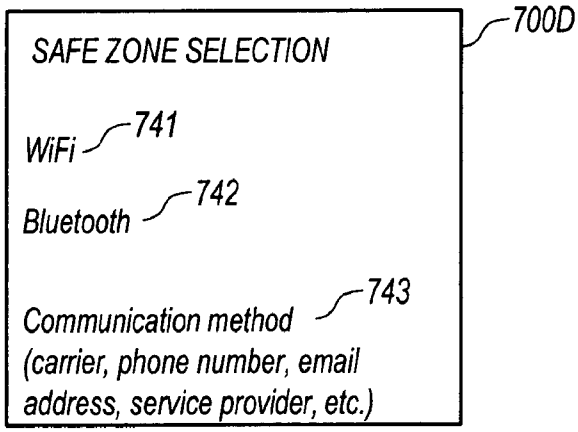

FIG. 7D

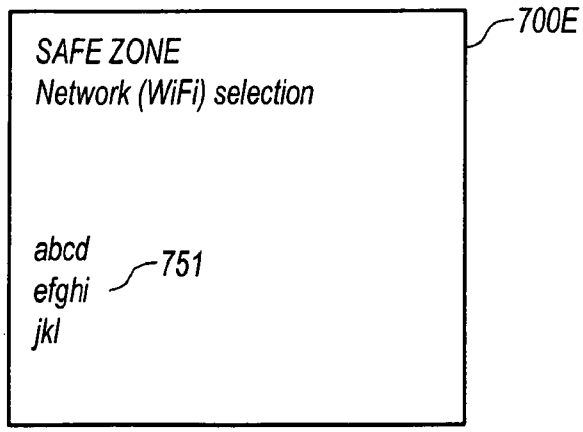

FIG. 7E

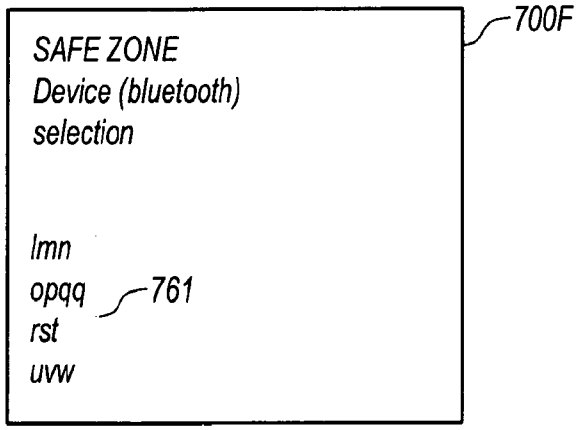

FIG. 7F

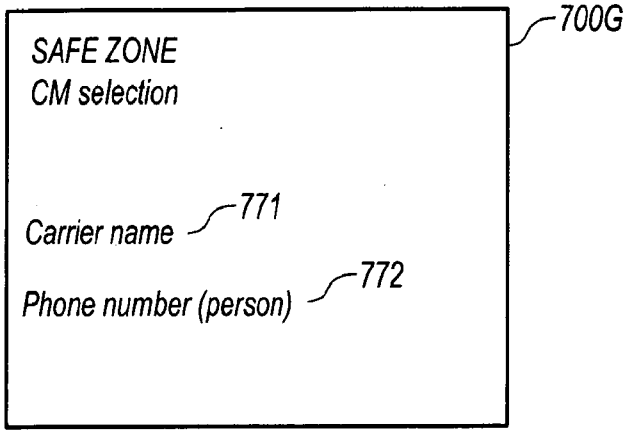

FIG. 7G

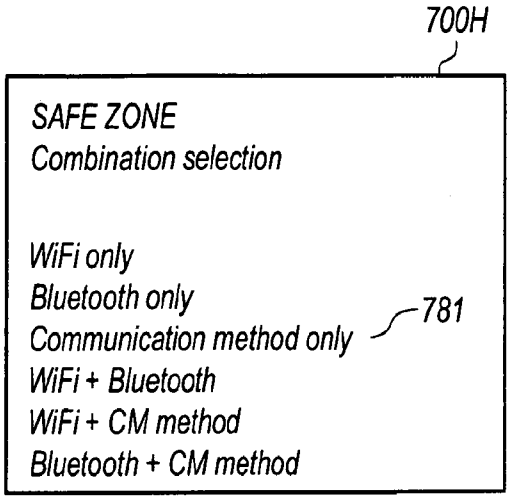

FIG. 7H

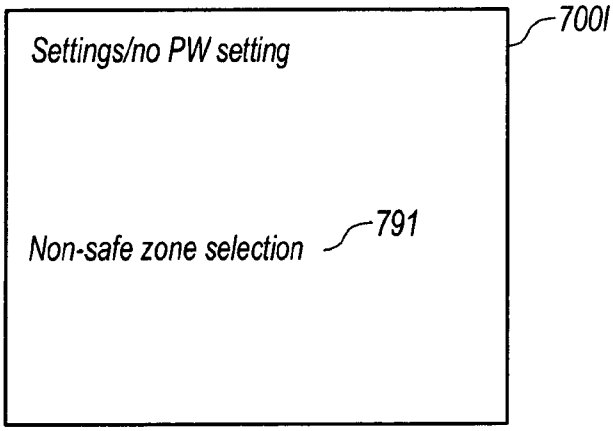

FIG. 7I

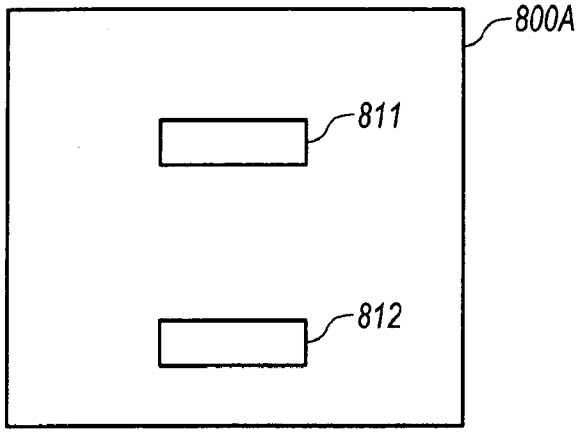

FIG. 8A

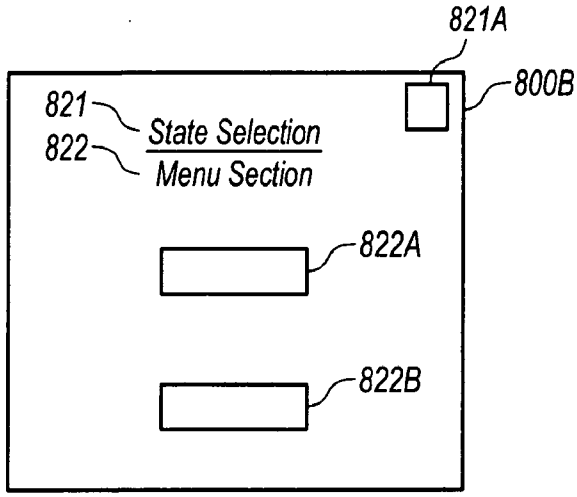

FIG. 8B

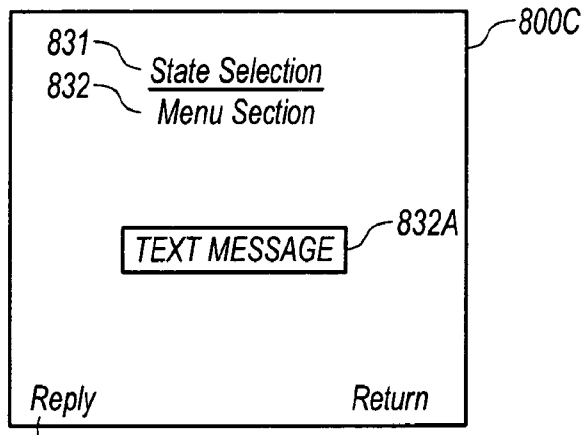

FIG. 8C

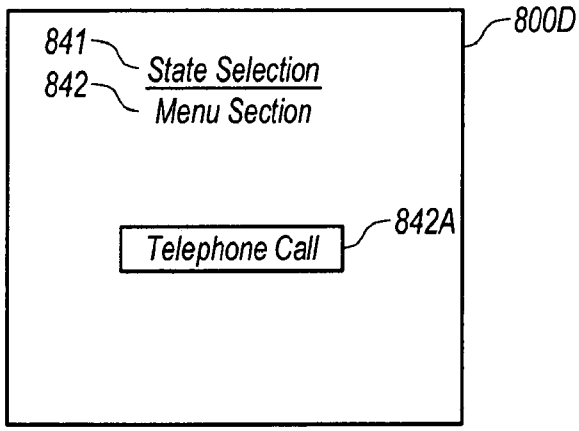

FIG. 8D

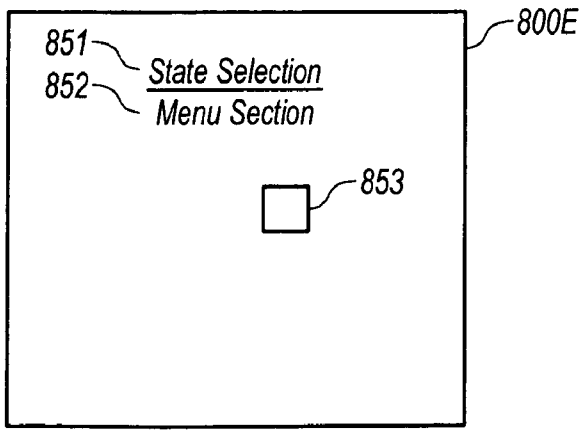

FIG. 8E

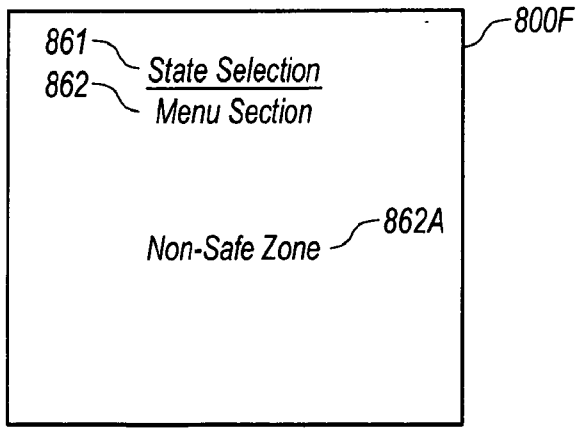

FIG. 8F

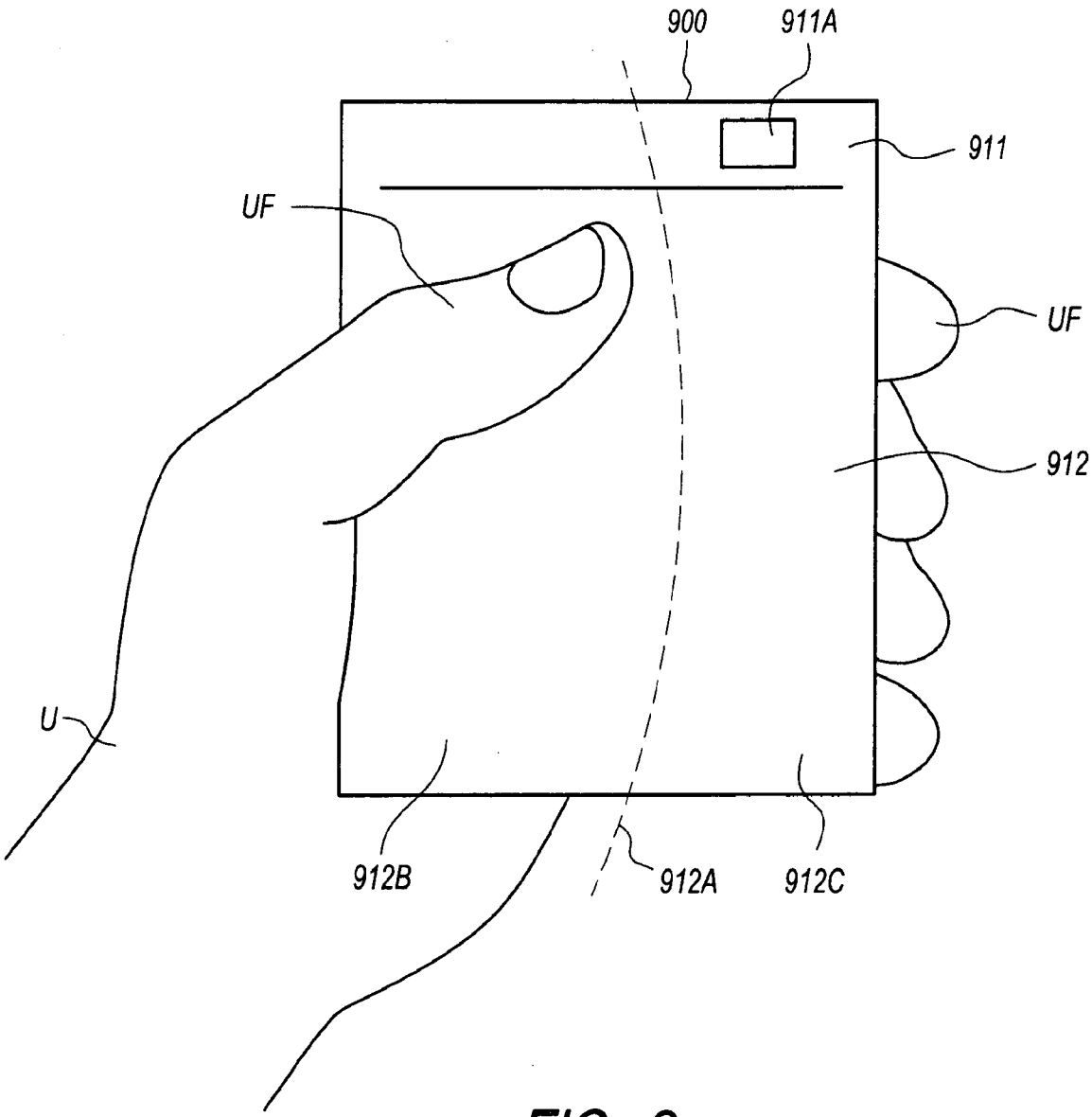

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/015238

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04M1/725
ADD.

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)
H04M H04W

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/070591 A1 (PATENTFABRIKEN AB [SE]; DELALAT HAMID [SE]) 19 August 2004 (2004-08-19) page 4, lines 7-28 page 5, lines 6-37 page 6, line 35 - page 8, line 10; figures 1,2 page 9, line 30 - page 10, line 19; figure 6 page 11, lines 10-28; figures 8,9	1-19
X	WO 2006/090899 A1 (NEC CORP [JP]; ORMSON RICHARD [GB]) 31 August 2006 (2006-08-31) pages 3-5; figure 1	1-19
X	US 2004/203895 A1 (BALASURIYA SENAKA [US]) 14 October 2004 (2004-10-14) paragraphs [0020] - [0024]; figure 1	1

-/--

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

[X] See patent family annex.

* Special categories of cited documents :

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

"E" earlier 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
4 June 2015	11/06/2015

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

1

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/015238

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 2 364 004 A1 (RESEARCH IN MOTION LTD [CA]) 7 September 2011 (2011-09-07) paragraph [0019] paragraphs [0026] - [0032] figures 1-5	1,2, 16-19
A	WO 2012/093784 A2 (LG ELECTRONICS INC [KR]; RHEE EUNWHA [KR]; CHOI YONGBONG [KR]; PARK SO) 12 July 2012 (2012-07-12) abstract; figure 1 paragraphs [0036] - [0044] paragraph [0051] paragraphs [0054] - [0056] paragraph [0079] paragraph [0084] paragraphs [0131] - [0132]; figure 5 paragraphs [0181] - [0184]; figure 13	15-19

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/015238

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004070591 A1	19-08-2004	EP 1623292 A1	08-02-2006
		US 2006128305 A1	15-06-2006
		WO 2004070591 A1	19-08-2004
WO 2006090899 A1	31-08-2006	CN 101129084 A	20-02-2008
		EP 1859641 A1	28-11-2007
		GB 2424342 A	20-09-2006
		JP 2008532336 A	14-08-2008
		US 2009011796 A1	08-01-2009
		WO 2006090899 A1	31-08-2006
US 2004203895 A1	14-10-2004	NONE	
EP 2364004 A1	07-09-2011	CA 2732554 A1	26-08-2011
		EP 2364004 A1	07-09-2011
WO 2012093784 A2	12-07-2012	CN 103329085 A	25-09-2013
		EP 2661673 A2	13-11-2013
		KR 20120079379 A	12-07-2012
		US 2013298024 A1	07-11-2013
		WO 2012093784 A2	12-07-2012