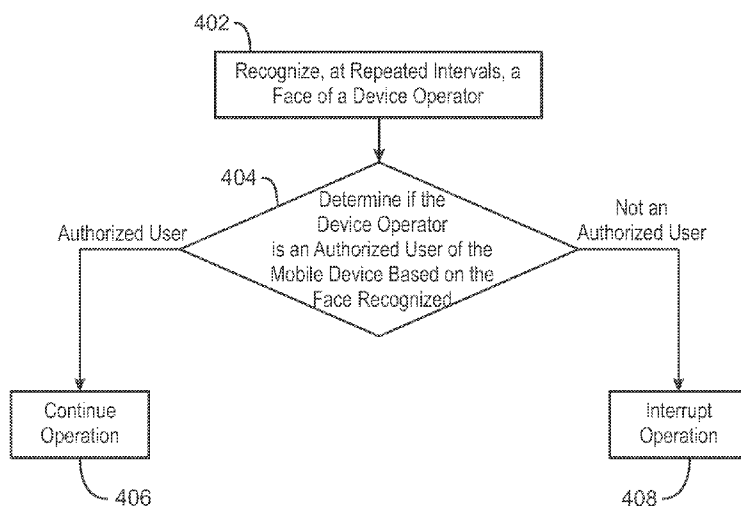




- (51) **International Patent Classification:**
H04L 29/06 (2006.01) *H04W 88/02* (2009.01)
H04W 12/06 (2009.01)
- (21) **International Application Number:**
PCT/US2013/047474
- (22) **International Filing Date:**
25 June 2013 (25.06.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** THOMSON LICENSING [FR/FR]; 1-5 rue Jeanne d'Arc, F-92130 Issy Les Moulineaux (FR).
- (72) **Inventors; and**
- (71) **Applicants :** SCHLUMBERGER, Fabian [CH/CH]; Dorfstrasse 11, Zürich, CH-8603 Schwerzenbach (CH). MEGEID, Magdy [CH/CH]; Hagenbuchrain 16b, CH-8047 Zürich (CH). DUBACH, Stefan [CH/CH]; Müliweg 76, Argau, CH-5078 Effingen (CH). SCHLATTER, André [CH/CH]; Albisriederstrasse 158, CH-8003 Zürich (CH).
- (74) **Agents:** SHEDD, Robert et al.; 2 Independence Way, Suite 200, Princeton, New Jersey 08540-6620 (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, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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).

[Continued on next page]

(54) **Title:** SECURE, UNINTERRUPTED OPERATION OF MOBILE DEVICES



400
FIG. 4

(57) **Abstract:** The disclosed embodiments relate to a system and method for secure, uninterrupted operation of a mobile device. The method includes identifying, at repeated intervals, a face of a device operator. The method also includes determining if the device operator is an authorized user of the mobile device based on the face. Additionally, the method includes continuing an operation of the mobile device if the device operator is an authorized user. The method further includes interrupting operation of the mobile device if the device operator is not an authorized user.



Published:

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

SECURE, UNINTERRUPTED OPERATION OF MOBILE DEVICES

FIELD OF THE INVENTION

The present disclosure relates generally to mobile devices. More
5 specifically, the present disclosure relates to a system for secure,
uninterrupted operation of mobile devices.

BACKGROUND OF THE INVENTION

This section is intended to introduce the reader to various aspects
10 of art, which may be related to various aspects of the present disclosure
that are described and/or claimed below. This discussion is believed to
be helpful in providing the reader with background information to
facilitate a better understanding of the various aspects of the present
disclosure. Accordingly, it should be understood that these statements
15 are to be read in this light, and not as admissions of prior art.

Mobile devices contain sensitive data, and as such, enable users
to protect this data, and associated functions, from unauthorized users.
One approach to securing mobile devices is to periodically check for the
20 presence of an authorized user, and to deny access to the device unless
an authorized user is present. Typical mobile phones, for example, use a
lock timer which prevents the activation of functions, and access to data,
after a predetermined time has elapsed. The lock timer starts to count
down when the device becomes idle, i.e., when the user stops operating
25 the device. If a user operates or touches the device, the lock timer is
reset. Then, only after the predetermined time of not operating, does the
device switch into the locked state. When in the locked state, getting
access to functions and data is prevented until the user provides a pass
code. The pass code may be spoken or typed into the device. However,

such entry methods may be observed by someone close to the user. In such a scenario, an unauthorized user may use the stolen pass code to access data and functionalities on the mobile device. A method for secure, uninterrupted operation of a mobile device is therefore desirable.

5

SUMMARY OF THE INVENTION

Certain aspects commensurate in scope with the disclosed embodiments are set forth below. It should be understood that these aspects are presented merely to provide the reader with a brief summary of certain forms the disclosure might take and that these aspects are not intended to limit the scope of the disclosure. Indeed, the disclosure may encompass a variety of aspects that may not be set forth below.

Embodiments relate to a system and method for secure, uninterrupted operation of a mobile device. The method includes identifying, at repeated intervals, a face of a device operator. The method also includes determining if the device operator is an authorized user of the mobile device based on the face. Additionally, the method includes continuing an operation of the mobile device if the device operator is an authorized user. The method further includes interrupting operation of the mobile device if the device operator is not an authorized user.

BRIEF DESCRIPTION OF THE DRAWINGS

Advantages of the disclosure may become apparent upon reading the following detailed description and upon reference to the drawings in which:

FIG. 1 is a block diagram of an exemplary mobile device in accordance with embodiments of the present disclosure;

FIG. 2 is a flow chart illustrating an exemplary mobile device
5 operating in accordance with embodiments of the present disclosure;

FIGs. 3A-3B are block diagrams of an exemplary user interface, in accordance with embodiments of the present disclosure; and

10 FIG. 4 is a flow chart illustrating operation of an exemplary mobile device in accordance with embodiments of the present disclosure.

DETAILED DESCRIPTION

One or more specific embodiments of the present disclosure will
15 be described below. In an effort to provide a concise description of these embodiments, not all features of an actual implementation are described in the specification. It should be appreciated that in the development of any such actual implementation, as in any engineering or design project, numerous implementation-specific decisions must be
20 made to achieve the developers' specific goals, such as compliance with system-related and business-related constraints, which may vary from one implementation to another. Moreover, it should be appreciated that such a development effort might be complex and time consuming, but would nevertheless be a routine undertaking of design, fabrication, and
25 manufacture for those of ordinary skill having the benefit of the present disclosure.

Mobile devices, such as mobile phones, are easy targets for theft because of their mobile nature. As such, there are numerous ways to

secure these devices, typically through infrequent requests for pass codes. In one embodiment, instead of using a password to be typed on the keyboard or touch screen, biometric information recognition, e.g. face recognition, iris recognition, and the like, is used to ensure the current user is an authorized user. Advantageously, facial biometric information recognition can be performed much more frequently, because it does not interrupt the user from operating the device.

The following discussion uses facial recognition as one example of biometric information recognition that could be used to secure mobile devices. The same techniques also apply to other biometric information recognition methods, such as iris recognition. The mobile device discussed with reference to the following figures includes a wide variety of mobile devices that store data, and enable various functionality for various users.

In one embodiment, facial recognition is used for periodic authorization of a user on a mobile device. As described herein, face recognition can be performed without having to interrupt the user from regular use of the device. The device automatically switches into a locked state if the authorized user is not present, and switches into an active state when the authorized user appears in front of the camera.

Turning initially to FIG. 1, which is a block diagram of an exemplary mobile device 100 in accordance with embodiments of the present disclosure. The mobile device 100 is a computational device, such as a laptop computer, tablet, mobile telephone, global positioning system (GPS) device, and so on.

In one embodiment, the mobile device 100 is a smartphone. The smartphone typically has the ability to send and receive phone calls and text messages, interface with the Internet either through a cellular network or local wireless network, take pictures and videos, play back audio and video content, and run applications, such as text processing programs and video games. Many smartphones include GPS capabilities, and include a touchscreen panel as part of the user interface.

For example, the smartphone includes a main processor 102 that is coupled to the other components shown. The main processor 102 routes information from the various components, such as the Bluetooth interface 104, Wifi interface 106, and 3G/4G interface 108. The main processor 102 also processes audio and video content for play back either directly on the device 100 or on an external device through the audio/video interface 110. Communication with the smartphone may be controlled through a set of antennas connected to Bluetooth interface 104, wifi interface 106, and 3G/4G interface 108. An additional antenna may be used for receiving GPS information through the GPS interface 112. A camera sensor 114 may be coupled through a camera interface 116 to the main processor 102. The camera sensor 114 and interface 116 create video content in either photo or video operational modes. An inertial sensor 118, such as one or more accelerometers, gravity sensor, magnetic sensor or gyroscopes, may be included for determining device orientation and movement.

A memory 120 and storage device 122 may be coupled to the main processor 102. The memory 120 may be used for storing specific information related to operation of the smartphone and needed by the

main processor 102. The storage device 122 may be used for storing audio, video, photos, or other data stored and retrieved by the user. A battery 124 is included for powering the smartphone and may be interfaced through a power control circuit 126 that may include a battery
5 charging interface (not shown).

The user interface includes a speaker/microphone 128 for use with phone calls, audio recording and playback, or voice activation control. The smartphone may include a touch screen 130 coupled to the main
10 processor 102 through a touch screen controller 132. The touch screen 130 may be either a single touch or multi touch screen using one or more of a capacitive and resistive touch sensor. The smartphone may also include additional user controls 134 such as but not limited to an on/off button, an activation button, volume controls, ringer controls, and a
15 multi-button keypad or keyboard.

In one embodiment, the memory 122 includes a security manager 136. The security manager 136 is software for periodic authorization of the user of the mobile device 100. Periodic authorization may be
20 performed whether or not the device 100 is being operated.

In such an embodiment, the device 100 automatically switches between active and locked states based on whether an authorized user's face is recognized in view of the camera 116. In an active state, the
25 device 100 operates without interruption. However, in a locked state, further operation is limited to operations that facilitate placing the device 100 back in possession of an authorized user.

For example, if the device 100 is lost or stolen, the device 100 may allow an unauthorized user to send a message to the owner or other authorized user. Message types include, but are not limited to, Short-Message-Service (SMS), email, a voice call, and a voice mail. In one
5 embodiment, the device 100 displays contact information, such as email-address, phone number, or the like. In this way, the unauthorized user may be enabled to call the owner's landline number, or a service provider's hotline to report the discovery. In scenarios where face recognition cannot be performed, another authorization method may also
10 be performed, such as a pass code entry.

Turning now to FIG. 2, which is a flow chart of a method 200 for an exemplary mobile device operating in accordance with embodiments of the present disclosure. The method 200 may be performed by begins at
15 step 202, where the mobile device 100 powers up. Embodiments of the present disclosure enable a user to register as an authorized user the device 100 is powered up.

For an initial registration of the first authorized user, also referred
20 to herein as the main user, a qualified picture or characteristic element of the face can be used from a certificated document or an existing face recognition database or server. Certificated documents may include, for example, biometrical passports and electronic passports. Facial recognition databases and servers are available, for example, on various
25 social media, photographic, and other image websites.

At step 204, periodic facial recognition is performed. If an authorized user is detected at step 206, the device 100 either enters an active state from a locked state, or remains in the active state at step

208. Similarly, for an unauthorized user, the device either remains in a locked state, at step 210, or enters the locked state from an active state at step 210.

5 In case the user is not authorized, the mobile device 100 is enabled to indicate an alarm by a flash-light and an acoustic alarm signal. Additionally, the mobile device 100 may capture a picture of the current user to send together with time or location information to the main user, service provider, legal authorities, as the case may arise.

10 Additionally, once the user of the mobile device 100 is out of range of the camera 116, the mobile device 100 switches automatically into the locked state at the next periodic facial recognition. To return the mobile device 100 back to the active state, an authorized user merely re-enters
15 the view of the camera 116. To preserve power consumption, the user may configure the device 100 to start the camera 116 and the circuits for facial recognition by a trigger, such as a tapped button or position on the touch screen 130. In one embodiment, facial recognition may be triggered in response to the device 100 detecting an acceleration
20 indicating movement.

 In one embodiment, the method 200 may be suspended while maintaining the active state. For example, the main user may deactivate the facial recognition security when showing the device 100 to some
25 friends or colleagues, or allowing them to use the device 100. The method 200 may be disabled entirely, or for a specified time, e.g., 3 minutes. During this period of time, the mobile device 100 does not enter the locked state because facial recognition is not performed while the method 200 is suspended.

The device 100 may also allow an unauthorized user to continue a current operation, such as, taking over an active call, or continuing viewing photos in the currently open photo album. In such an
5 embodiment, the unauthorized user's permissions are limited to the current application or document. In this way, the unauthorized user is prohibited from switching applications, dialing another phone number, opening another photo album, changing security settings, accessing messages, and so on. Further, the mobile device 100 may prevent any
10 user except an authorized user from accessing data or functions which have not been launched by the authorized user.

It is also possible to sign up further authorized users to use specific, or all, features of the device. For example, the user may
15 authorize a spouse, or executive assistant to all features and data on the mobile device 100.

In case an unauthorized user continuously fails to register, the device 100 may erase all sensitive data, such as emails, passwords, and
20 locks the device 100. In one embodiment, all sensitive data may be encrypted using a private key that is issued by a trusted party, such as a service provider, and stored securely in the mobile device. The authorized user of the device could obtain the corresponding decryption key from the trusted party after regaining the access of the mobile device
25 100.

In scenarios when user's the normal operation of the device 100 does not place or position the user's face to be fully viewable by the camera, the checking of the facial recognition could be deactivated. For

example, the checking of the facial recognition in a mobile phone is deactivated for the time when the user is in an active call, because the user's face is typically not in the viewing angle of the camera.

5 The device 100 may also determine profiles for authorized users whose pictures are stored in storage 120 or memory 122. The main user can set access rights to authorize users which have never been recognized by the camera 116, but can be recognized when in the viewing angle of the camera 116. In one embodiment, the device 100
10 may recognize only persons stored in certain albums specified by the main user.

 In one embodiment, the security manager 136 may recognize authorized users from front, side, and perspective views of their faces,
15 including a profile view, and from other angles of the face. Advantageously, the device does not accidentally enter the locked state just because the user does not look directly into the camera 116. A face tracking or object tracking function may also be used to prevent recognized users as being determined absent. Additionally, the face
20 recognition functionality of the security manager 136 may be capable of being trained, optimizing identification characteristics, and adapting to changes of the authorized users' looks.

 Additionally, the security manager 136 may identify fake users,
25 attempting to copy an authorized user's appearance. For example, if the user's face does not change for a specified time period, if the user does not appear to breathe, the recognized face may belong to a picture that is placed in front of the camera 116. Another example is when a fake

user places the camera in front of a monitor playing a video showing an authorized user in a loop.

FIGs. 3A-3B are block diagrams of an exemplary user interface 300, in accordance with embodiments of the present disclosure. In one embodiment, the user may be notified when the facial recognition is taking place. The user interface 300 includes input keys 302, a display 304, a countdown timer 306, and a camera 308. The countdown timer 306 indicates the remaining time until the device 100 is switched into the locked state unless an authorized user is recognized before the countdown has elapsed. The interface 300B shows an embodiment of the GUI display 304 including a preview 310 of the field of view of the face recognition camera, to enable the user to focus the camera 308 on the user's face. The preview field may merely be displayed when the countdown timer reaches a threshold value, e.g., 10 seconds remaining before switching into the locked state.

In one embodiment, the biometric recognition based user authorization can be combined with other user authorization mechanism such as a lock timer, password input, and voice recognition, to achieve various levels of security. For the highest security level, multiple authorization mechanisms may be used, whereas for lower security level, one or two security mechanisms may be used.

Since face recognition is typically a high-performance application, this functionality tends to consume a lot of power. In this light, the frequency of authorization by facial recognition can be adapted depending on the security area of the mobile device. Security areas for

the mobile device 100 may represent locations that have different levels of security, as designated by the main user.

For example, locations can consist of a home, an office, a public
5 location, and so on, as specified by the main user. If the mobile device
100 is at home, the frequency of facial recognition authorization is not as
high as if the user is in a public location, e.g., a restaurant. The main
user may specify various areas, with varying levels of security. Based on
the level of security, the frequency of the checking at other more or less
10 trustable places can be set by the main user.

In this way, security levels can be determined based on the
location of the mobile device 100, where the frequency of the facial
recognition of the authorized user varies based on specified security
15 levels, e.g. safe area at home, critical area in public, and intermediately
safe area in the office. In an exemplary implementation, the device 100
does not enter the locked state at home (safe area), but enters into a
locked state in public if there is no facial recognition authorization within
3 seconds. In such an implementation, the device may remain in an
20 active state for the first minute the device 100 is in an office area. After
the first minute, the device 100 may begin checking again for the
presence of the authorized user.

For higher levels of security, the time interval for re-authorization is
25 lower (e.g., 30sec) than in areas with a lower level of security, where the
interval is relatively higher, e.g., 2 minutes. The time interval may be set
infinite - to disable the periodic authorization.

Location can be determined by one of GPS-, A-GPS or WLAN-positioning methods from satellite, cell-tower or WLAN signals.

Locations may also be determined and derived from the network authentication result, such as a successful authentication in an encrypted WLAN, or a login into a network by use of username and password.

Location can also be determined by reading Near-Field-Communication (NFC) tags attached to a particular location. If a user enters the work environment, the NFC tag is read at the door, or at the user's desk to change security levels, and to read the same tag before leaving an area to change security levels back according to the specified security areas.

Security levels may be also determined based on pre-determined schedules, e.g., intermediate security during work hours. For weekends, the security levels may be set manually.

There have thus been described certain preferred embodiments of user authorization. While specific embodiments have been discussed and disclosed, it will be appreciated that other embodiments are covered by the disclosure.

FIG. 4 is a flow chart of a method 400 for operating an exemplary mobile device 100 in accordance with embodiments of the present disclosure. The method 400 begins at step 402, where the face of the device operator, i.e., the current user, is recognized periodically. At step 404, the security manager 136 determines if the device operator is an authorized user of the mobile device 100 based on the recognized face.

If the device operator is an authorized user, operation of the device continues at step 406. For an unauthorized user, the operation of the mobile device 100 is interrupted by entering the locked state.

5 It is to be understood that the present disclosure may be implemented in various forms of hardware, software, firmware, special purpose processors, or a combination thereof. Preferably, the present disclosure is implemented as a combination of hardware and software. Moreover, the software is preferably implemented as an application
10 program tangibly embodied on a program storage device. The application program may be uploaded to, and executed by, a machine comprising any suitable architecture. Preferably, the machine is implemented on a computer platform having hardware such as one or more central processing units (CPU), a random access memory (RAM),
15 and input/output (I/O) interface(s). The computer platform also includes an operating system and microinstruction code. The various processes and functions described herein may either be part of the microinstruction code or part of the application program (or a combination thereof), which is executed via the operating system. In addition, various other
20 peripheral devices may be connected to the computer platform such as an additional data storage device and a printing device.

 It is to be further understood that, because some of the constituent system components and method steps depicted in the accompanying
25 figures are preferably implemented in software, the actual connections between the system components (or the process steps) may differ depending upon the manner in which the present disclosure is programmed. Given the teachings herein, one of ordinary skill in the

related art will be able to contemplate these and similar implementations or configurations of the present disclosure.

While the disclosure may be susceptible to various modifications
5 and alternative forms, specific embodiments have been shown by way of
example in the drawings and will be described in detail herein. However,
it should be understood that the disclosure is not intended to be limited
to the particular forms disclosed. Rather, the disclosure is to cover all
modifications, equivalents and alternatives falling within the scope of the
10 disclosure.

What is claimed is:

1. A method (400) for operating a mobile device (100), comprising:
identifying, at repeated intervals, a face of a device operator;
5 determining if the device operator is an authorized user of the
mobile device (100) based on the face;
continuing an operation of the mobile device (100) if the device
operator is the authorized user; and
interrupting operation of the mobile device (100) if the device
10 operator is the an authorized user.
2. The method (400) of claim 1, comprising determining a security
zone based on a location of the mobile device (100), the security zone
being a home, the repeated intervals occurring subsequently when the
15 mobile device (100) enters the home, and when the mobile device (100)
leaves the home.
3. The method (400) of claim 2, wherein the security zone comprises
a public space, wherein the repeated intervals occur more frequently
20 than when the security zone comprises a secure space, wherein the
repeated intervals occur more frequently than when the mobile device
(100) is located in the home.
4. The method (400) of claim 1, comprising determining a beginning
25 and an end of a specific suspension period, such that the repeated
intervals occur subsequently before the beginning of the specific
suspension period, and after the end of the specific suspension period.
5. The method (400) of claim 1, comprising:

determining that a face of the device operator is not within a range of a facial recognition device for the mobile device (100); and interrupting the operation of the mobile device (100).

- 5 6. The method (400) of claim 1, comprising identifying the face of the device operator in response to a facial recognition trigger, comprising a button, a tap on the mobile device (100), and a movement of the mobile device (100).
- 10 7. The method (400) of claim 1, wherein interrupting the operation of the mobile device (100) comprises presenting contact information to contact an authorized user of the mobile device (100).
8. The method (400) of claim 1, comprising authorizing an
15 unauthorized user to place a phone call to the authorized user of the mobile device (100).
9. A mobile device (100), comprising:
a processor (102); and
20 a memory (120) comprising instructions configured to cause the processor (102) to:
identifying, at repeated intervals, a face of a device operator;
determining if the device operator is an authorized user of the
mobile device (100) based on the face;
25 continuing an operation of the mobile device (100) if the device operator is an authorized user;
interrupt operation of the mobile device (100) if the device operator is not an authorized user; and

determine a security zone based on a location of the mobile device (100), the security zone being a home, the repeated intervals occurring subsequently when the mobile device (100) enters the home, and when the mobile device (100) leaves the home.

10. The mobile device (100) of claim 9, wherein the security zone comprises a public space, wherein the repeated intervals occur more frequently than when the security zone comprises a secure space, wherein the repeated intervals occur more frequently than when the mobile device (100) is located in the home.

11. The mobile device (100) of claim 9, comprising determining a beginning and an end of a specific suspension period, such the repeated intervals occur subsequently before the beginning of the specific suspension period, and after the end of the specific suspension period.

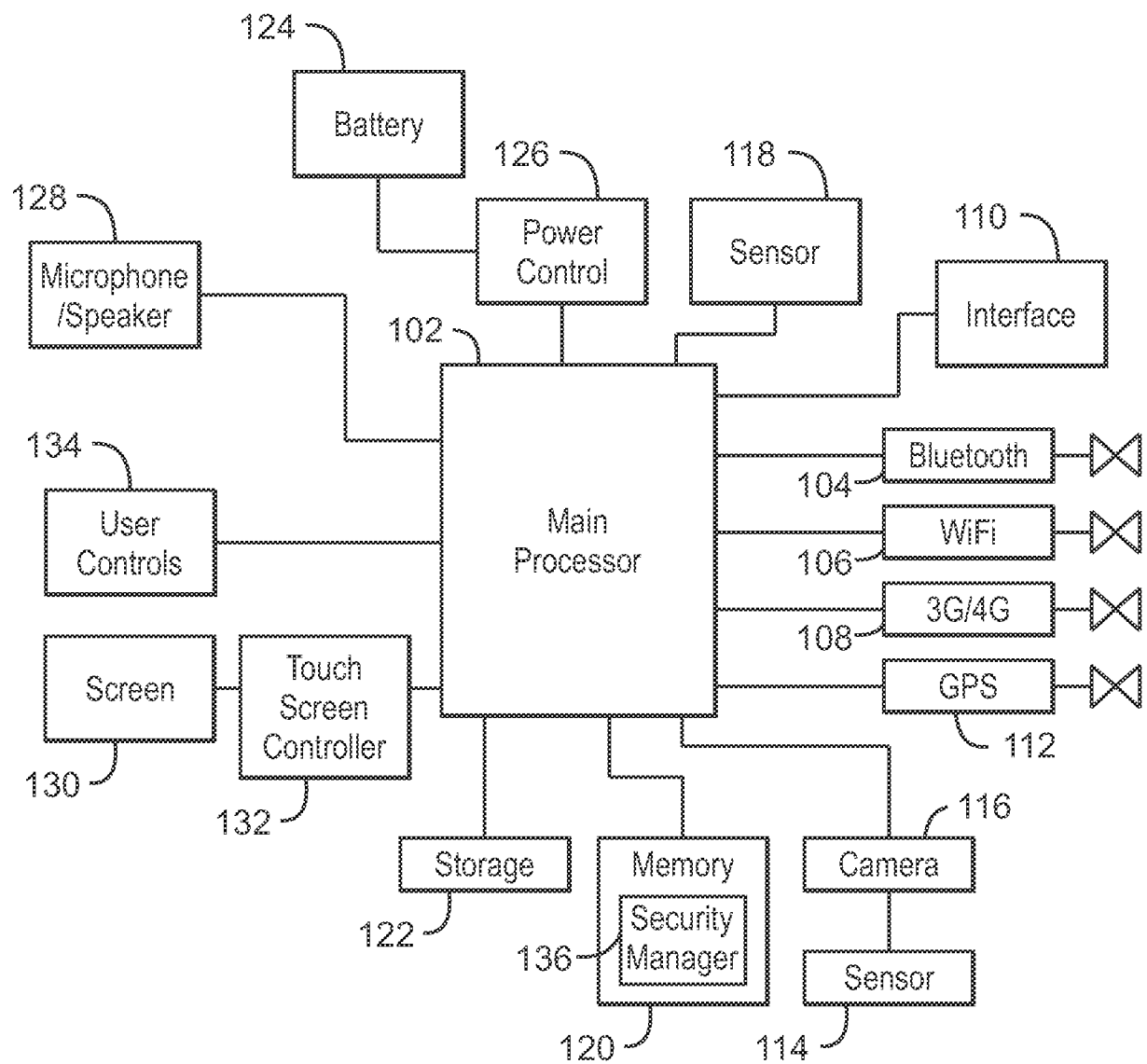
12. The mobile device (100) of claim 9, comprising:
determining that a face of the device operator is not within a range of a facial recognition device for the mobile device (100); and interrupting the operation of the mobile device (100).

13. The mobile device (100) of claim 9, comprising identifying the face of the device operator in response to a facial recognition trigger, comprising a button, a tap on the mobile device (100), and a movement of the mobile device (100).

14. The mobile device (100) of claim 9, wherein interrupting the operation of the mobile device (100) comprises presenting contact information to contact an authorized user of the mobile device (100).

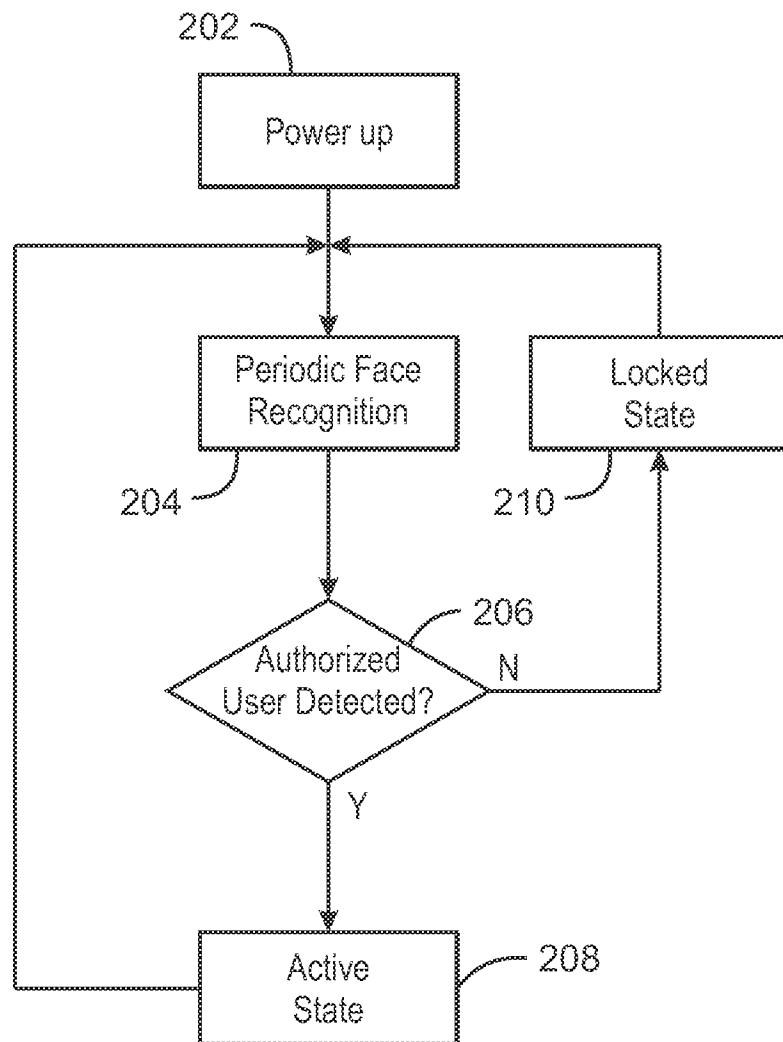
- 5 15 The mobile device (100) of claim 9, comprising authorizing an unauthorized user to place a phone call to an authorized user of the mobile device (100).

1/4



100
FIG. 1

2/4



200
FIG. 2

3/4

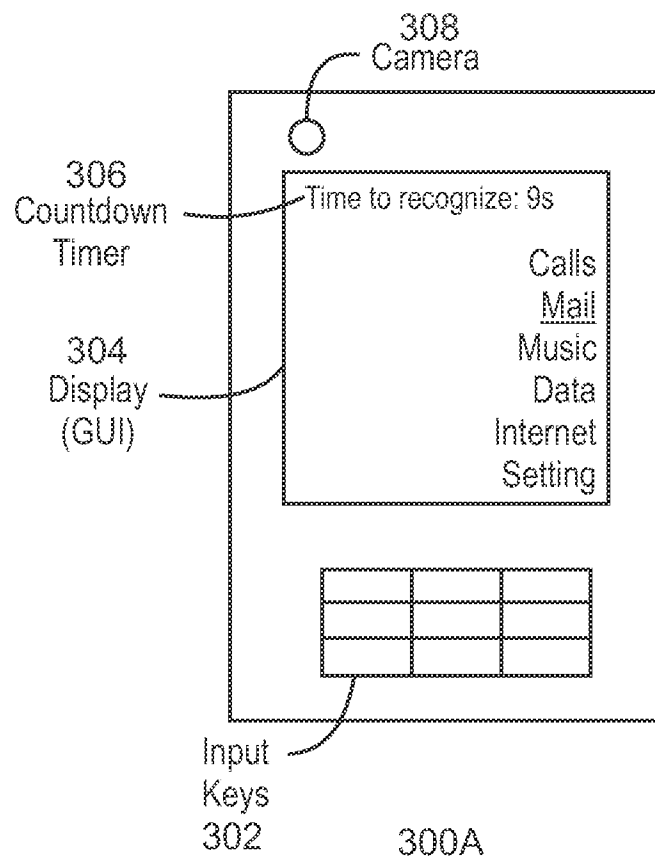


FIG. 3A

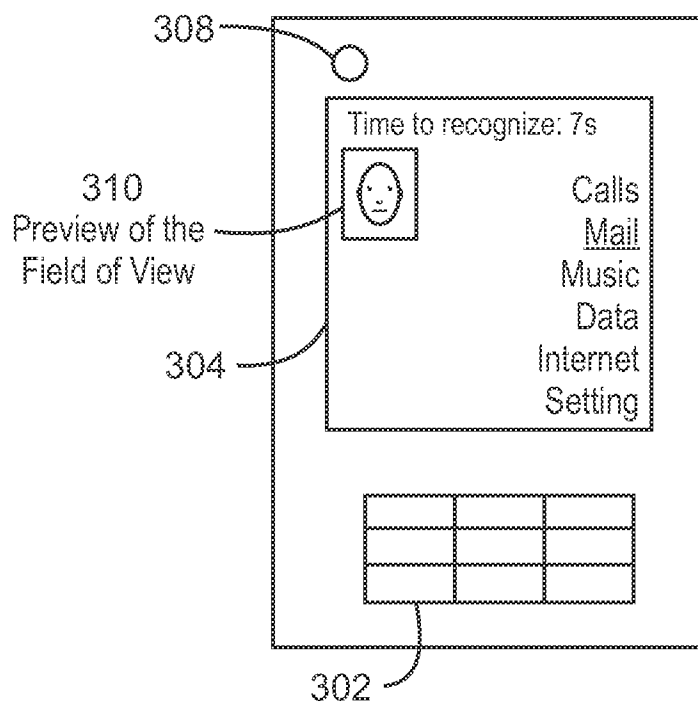
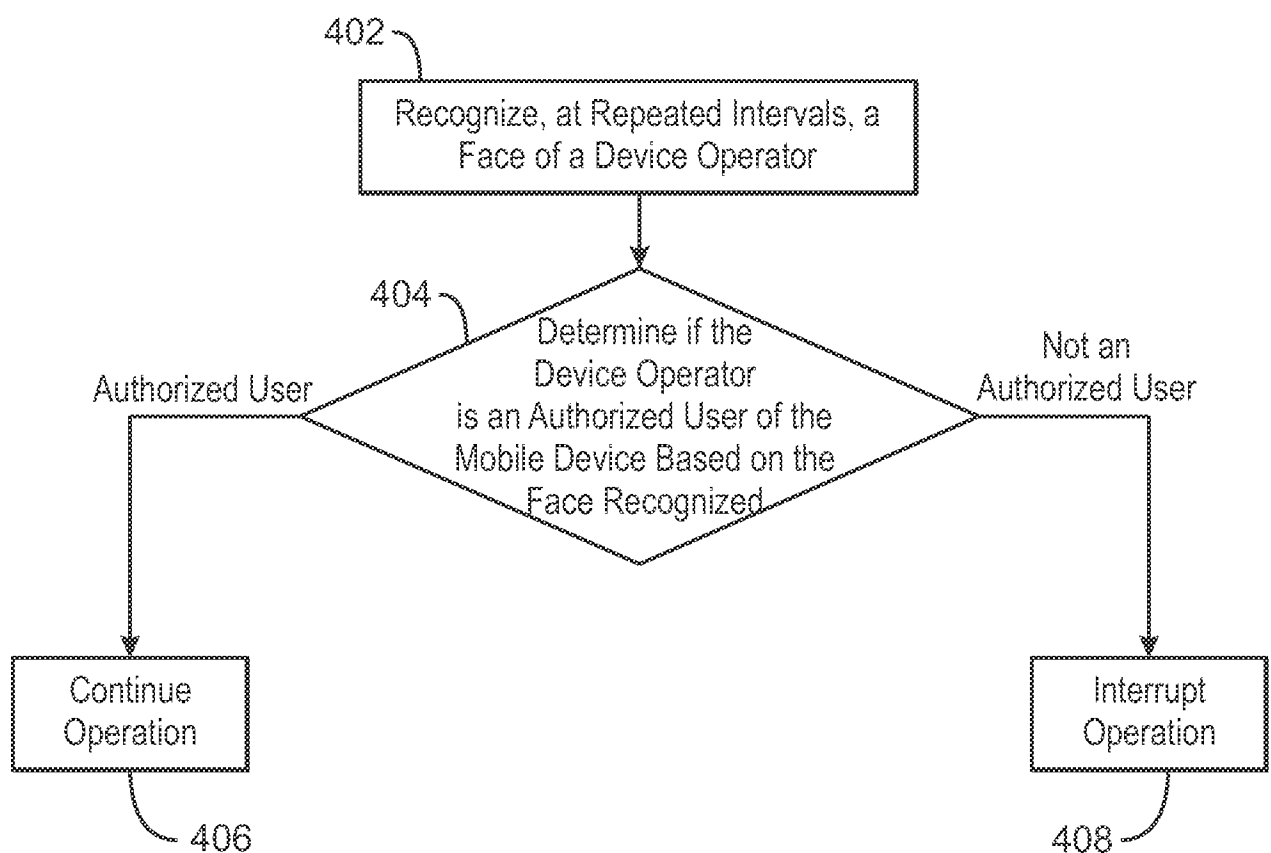


FIG. 3B

4/4



400
FIG. 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2013/047474

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06 H04W12/06
 ADD. H04W88/02

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)

H04L 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, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/235790 A1 (ZHAO LIHUA [US] ET AL) 20 September 2012 (2012-09-20)	1,4-8
Y	paragraphs [0001], [0023], [0024], [0027] - [0033] figures 1-4	2,3,9-15
X	EP 1 488 655 A1 (NOKIA CORP [FI]) 22 December 2004 (2004-12-22)	1,4-8
Y	paragraphs [0036] - [0038] paragraphs [0043] - [0047] figures 1-4	2,3,9-15
X	EP 1 521 161 A2 (MATSUSHITA ELECTRIC IND CO LTD [JP]) 6 April 2005 (2005-04-06)	1,4,8
Y	paragraphs [0001], [0008]	2,3,9-15
	----- -/-	



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

11 March 2014

Date of mailing of the international search report

18/03/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Ghomrasseni, Z

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/047474

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/252411 A1 (JOHNSGARD T J; MING S G; SHI G; SIU T; SIU T Y; SU T) 4 October 2012 (2012-10-04) paragraphs [0021] - [0026], [0030] - [0037], [0043], [0057] figures 1-5 -----	1,7,8
X	EP 2 605 180 A2 (FUJITSU LTD [JP]) 19 June 2013 (2013-06-19) paragraphs [0036], [0040], [0049] - [0056] -----	1,7,8
A	EP 1 170 969 A1 (NOKIA MOBILE PHONES LTD [FI]) 9 January 2002 (2002-01-09) paragraph [0010] -----	7,8,14, 15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2013/047474

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2012235790	A1	20-09-2012	NONE	
EP 1488655	A1	22-12-2004	AT 481838 T	15-10-2010
			AU 2002304334 A1	08-10-2003
			EP 1488655 A1	22-12-2004
			US 2005164675 A1	28-07-2005
			WO 03081932 A1	02-10-2003
EP 1521161	A2	06-04-2005	CN 1612081 A	04-05-2005
			EP 1521161 A2	06-04-2005
			US 2005071635 A1	31-03-2005
US 2012252411	A1	04-10-2012	CN 103477604 A	25-12-2013
			EP 2692106 A2	05-02-2014
			KR 20140005306 A	14-01-2014
			US 2012252411 A1	04-10-2012
			WO 2012135681 A2	04-10-2012
EP 2605180	A2	19-06-2013	EP 2605180 A2	19-06-2013
			JP 2013125341 A	24-06-2013
			US 2013147972 A1	13-06-2013
EP 1170969	A1	09-01-2002	EP 1170969 A1	09-01-2002
			JP 2002077372 A	15-03-2002
			US 6662023 B1	09-12-2003