



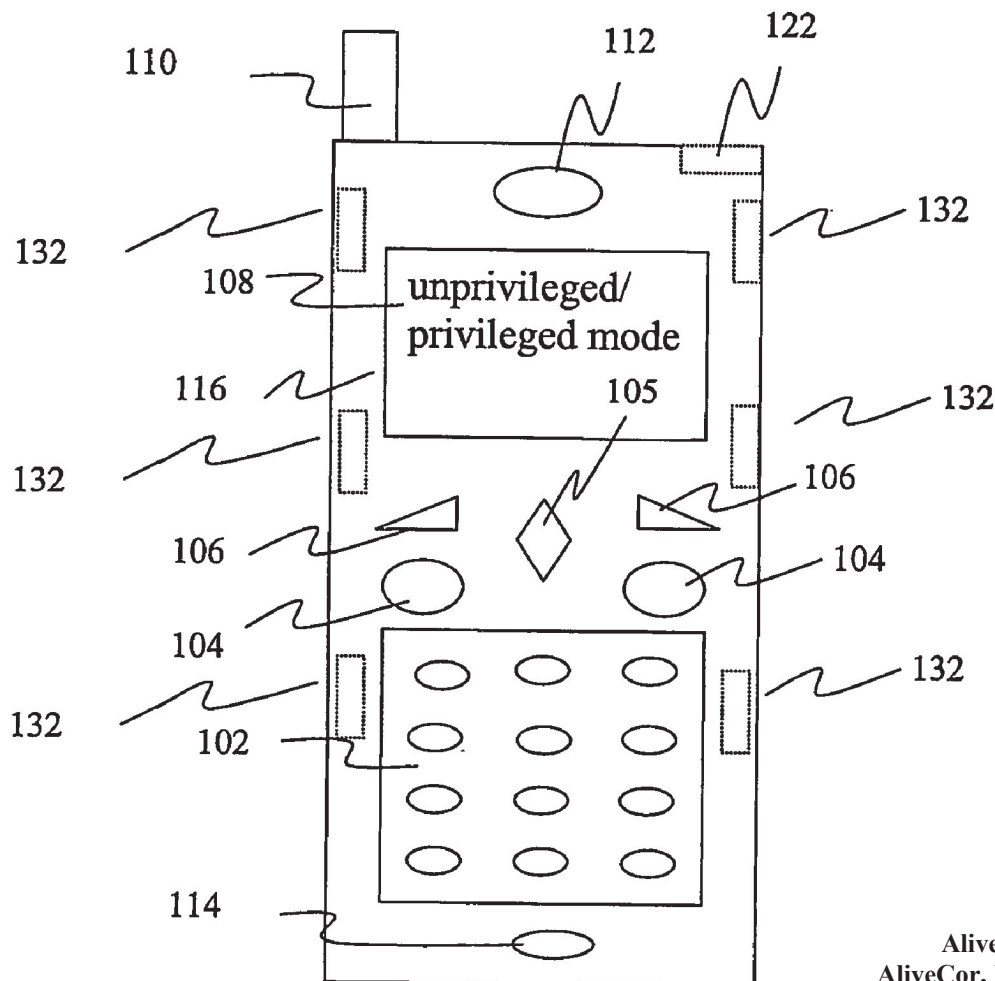
US 20080113650A1

(19) **United States**(12) **Patent Application Publication**
Engstrom(10) **Pub. No.: US 2008/0113650 A1**(43) **Pub. Date: May 15, 2008**(54) **WIRELESS MOBILE PHONE WITH
AUTHENTICATED MODE OF OPERATION
INCLUDING HEART BEAT PROFILE BASED
AUTHENTICATION****Related U.S. Application Data**

(60) Provisional application No. 60/459,281, filed on Mar. 31, 2003.

(76) Inventor: **G. Eric Engstrom, Kirkland, WA
(US)****Publication Classification**(51) **Int. Cl.**
H04M 1/66 (2006.01)
(52) **U.S. Cl.** **455/411**
(57) **ABSTRACT**Correspondence Address:
SCHWABE, WILLIAMSON & WYATT, P.C.
PACWEST CENTER, SUITE 1900
1211 SW FIFTH AVENUE
PORTLAND, OR 97204(21) Appl. No.: **10/551,254**(22) PCT Filed: **Mar. 30, 2004**(86) PCT No.: **PCT/US04/10051**§ 371 (c)(1),
(2), (4) Date: **Jun. 26, 2006**

A wireless mobile phone is equipped to operate in an unauthenticated and an authenticated mode of operation, depending on whether a user has been authenticated. In one embodiment, the wireless mobile phone includes a number of sensors to enable a user's heart beat profile to be captured and be used for authentication. In one embodiment, authentication is performed by comparing the real time captured heart beat profile against a reference heart beat profile. In one embodiment, the reference heart profile is retrieved from an identity card. The wireless mobile phone further includes a reader to retrieve the reference heart beat profile from the identity card.

**AliveCor Exhibit 1020**
AliveCor, Inc. v. Apple Inc.**IPR2023-00950, U.S. Patent No. 10,076,257****1 of 14**

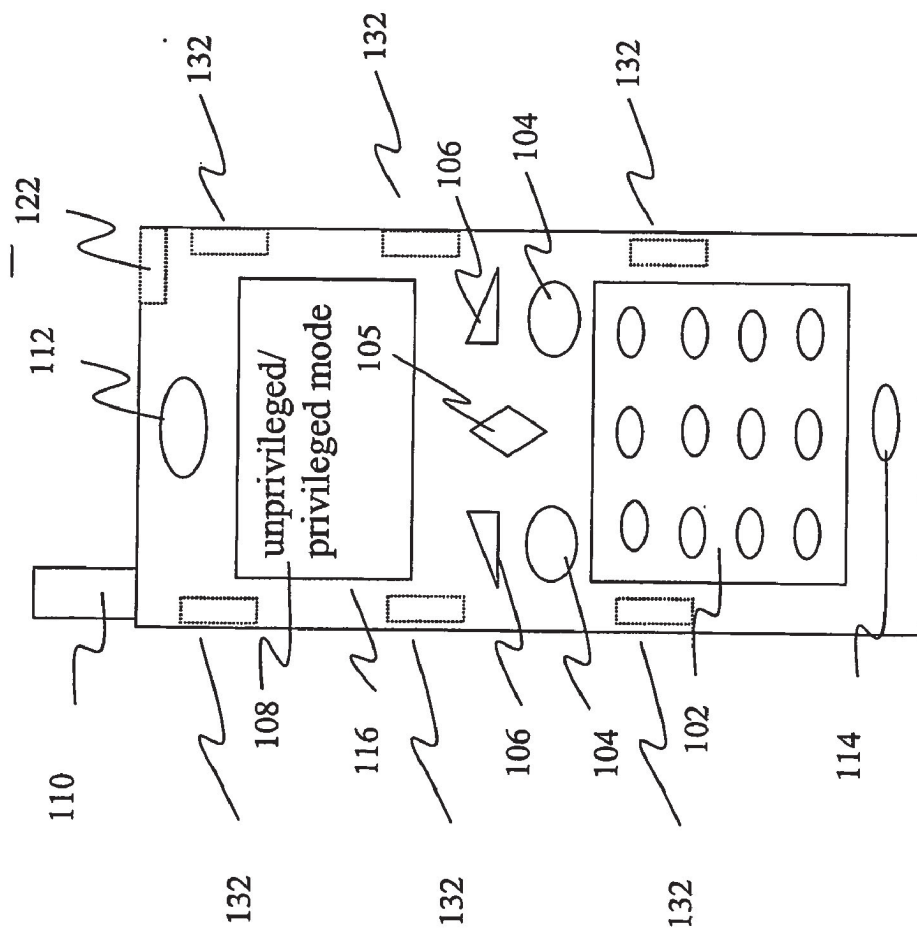


Figure 1

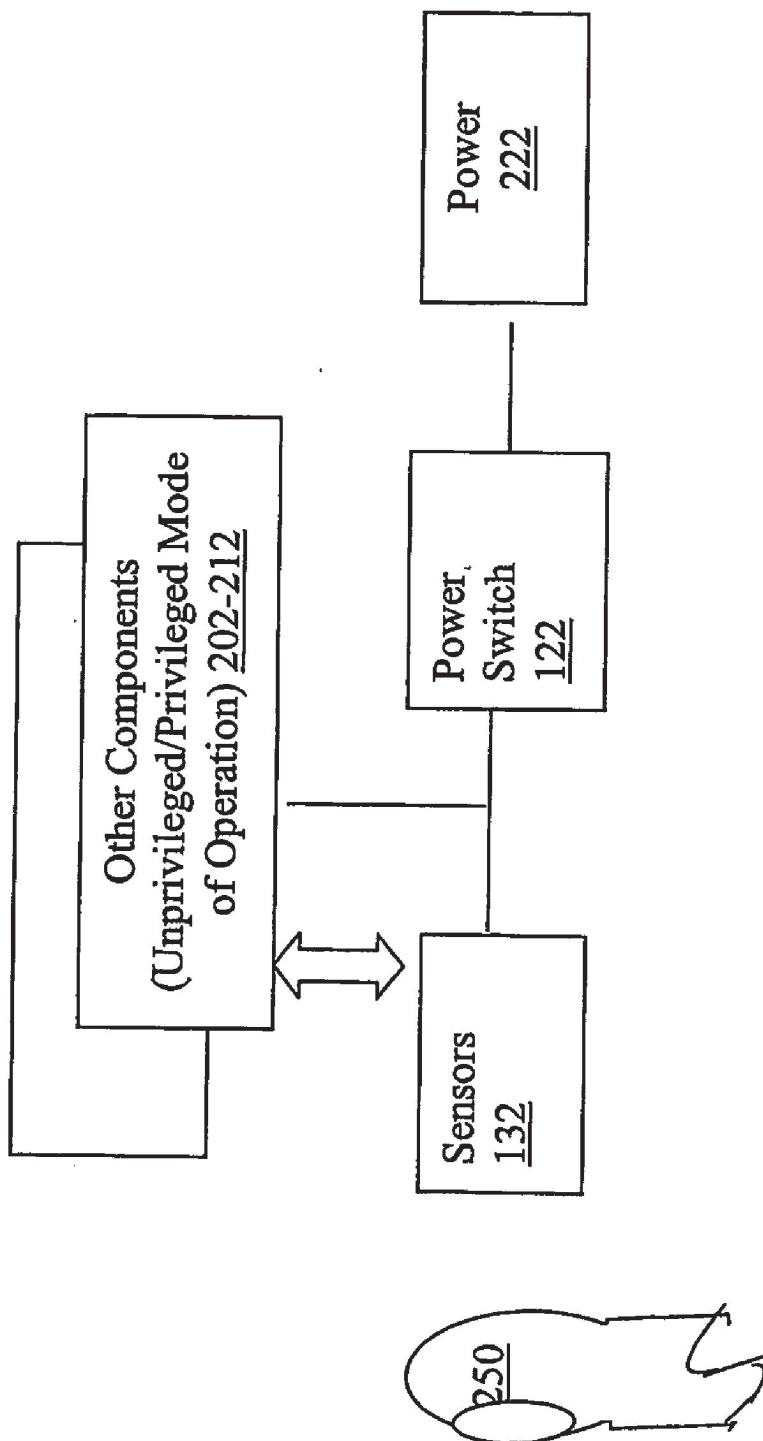


Figure 2

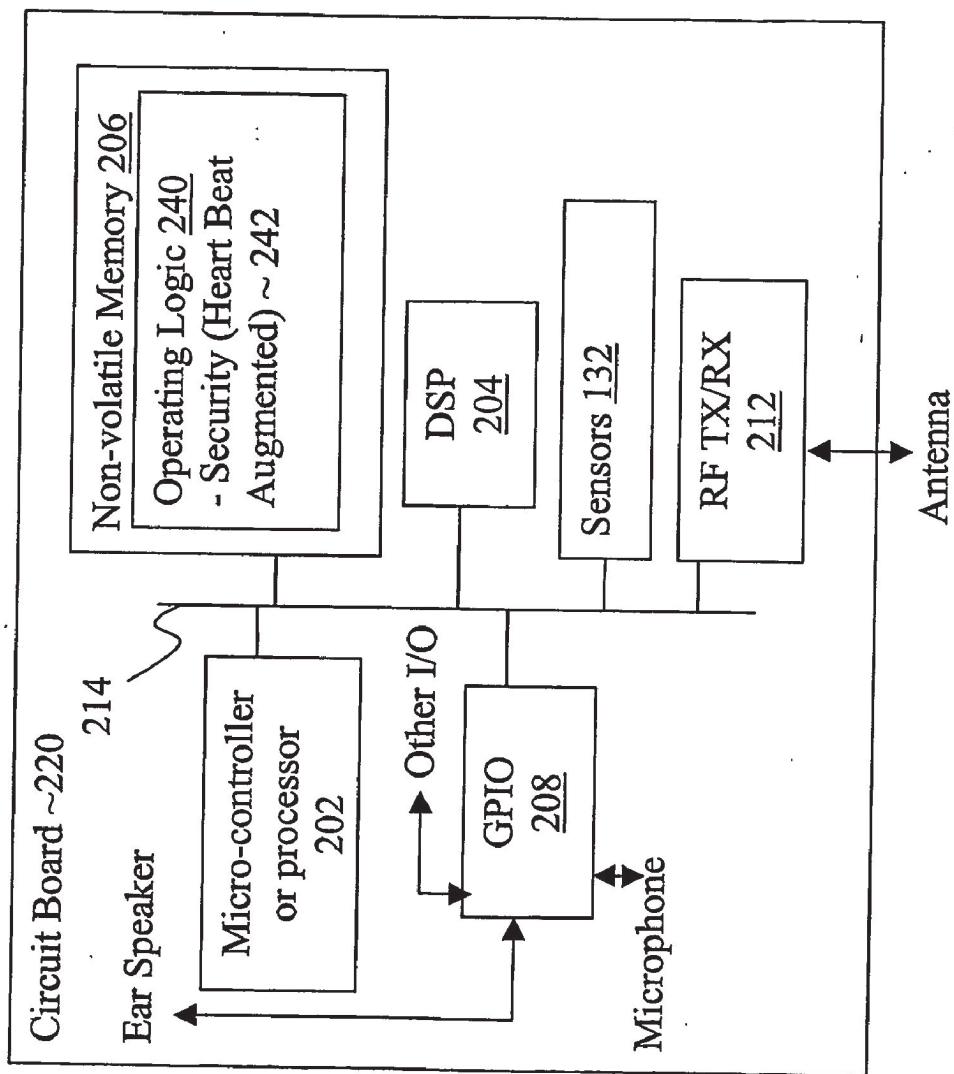


Figure 3

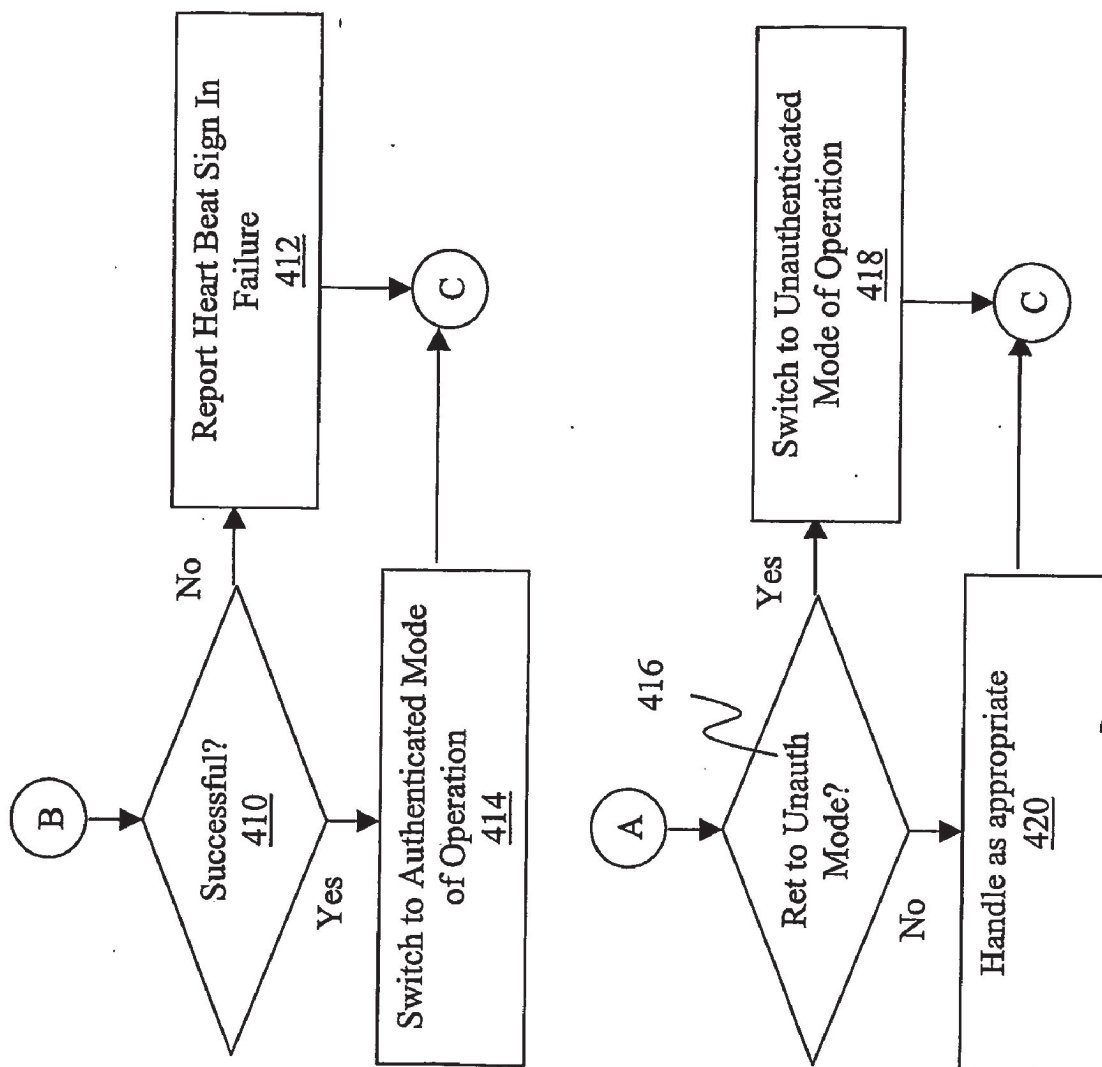


Figure 4b

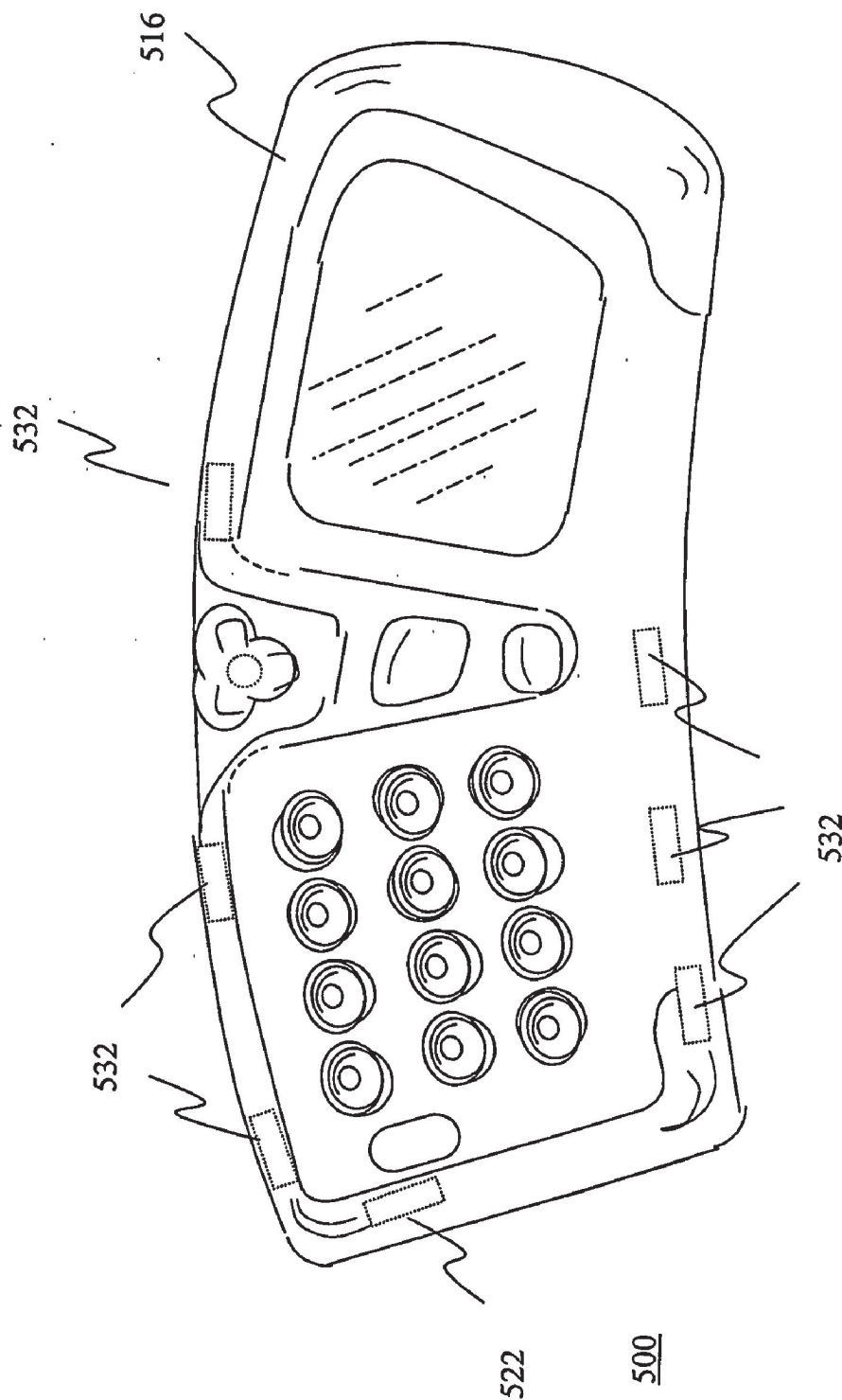


Figure 5

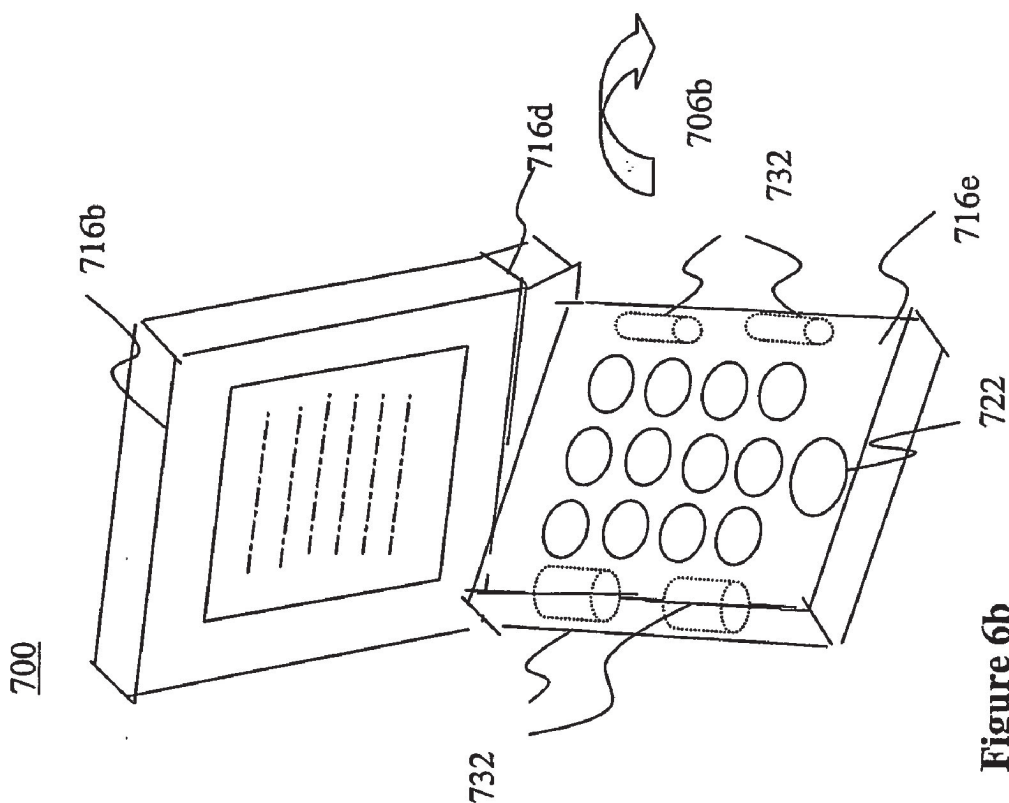


Figure 6b

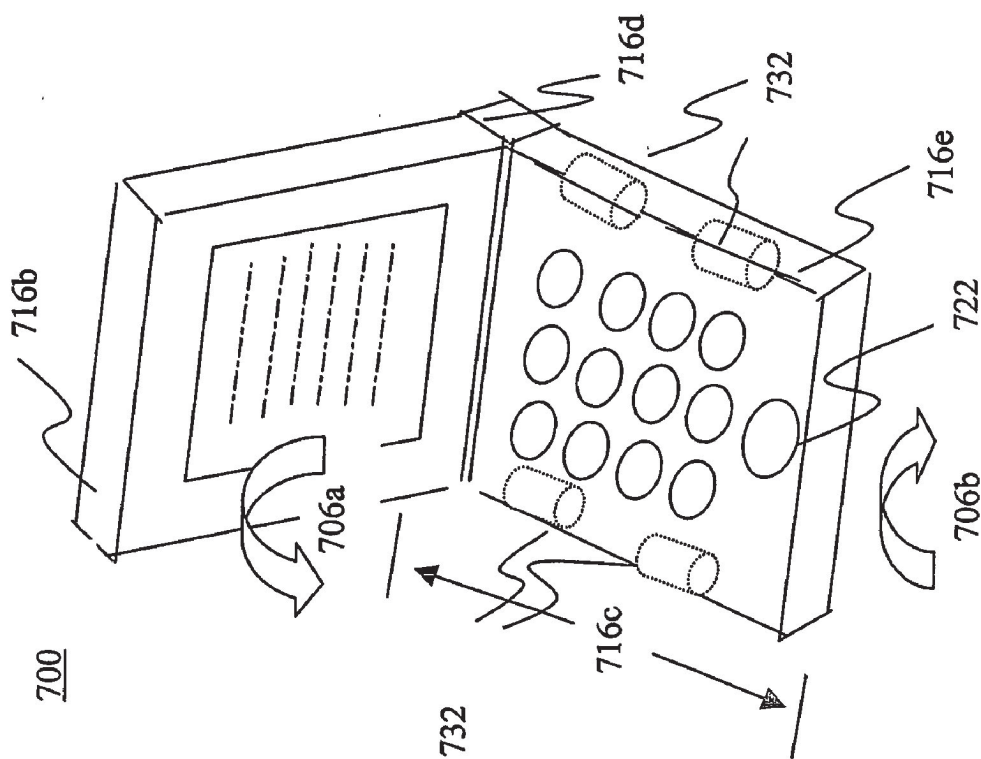


Figure 6a

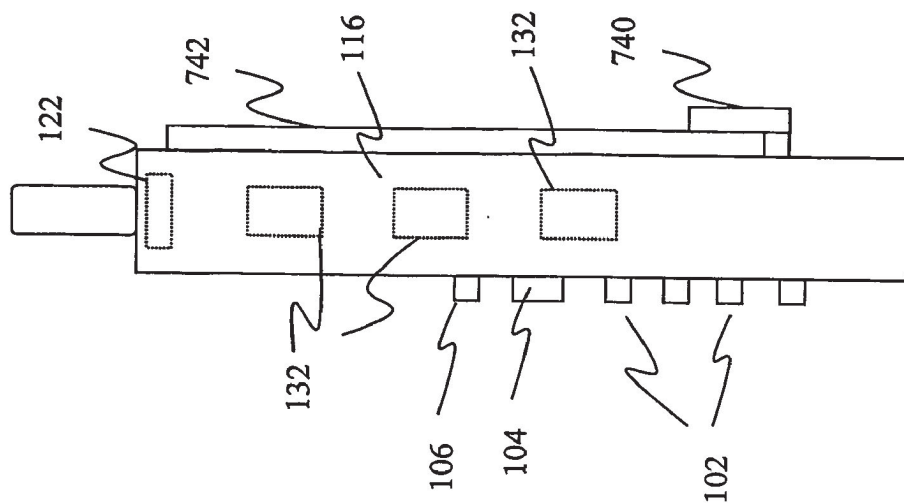


Figure 7b

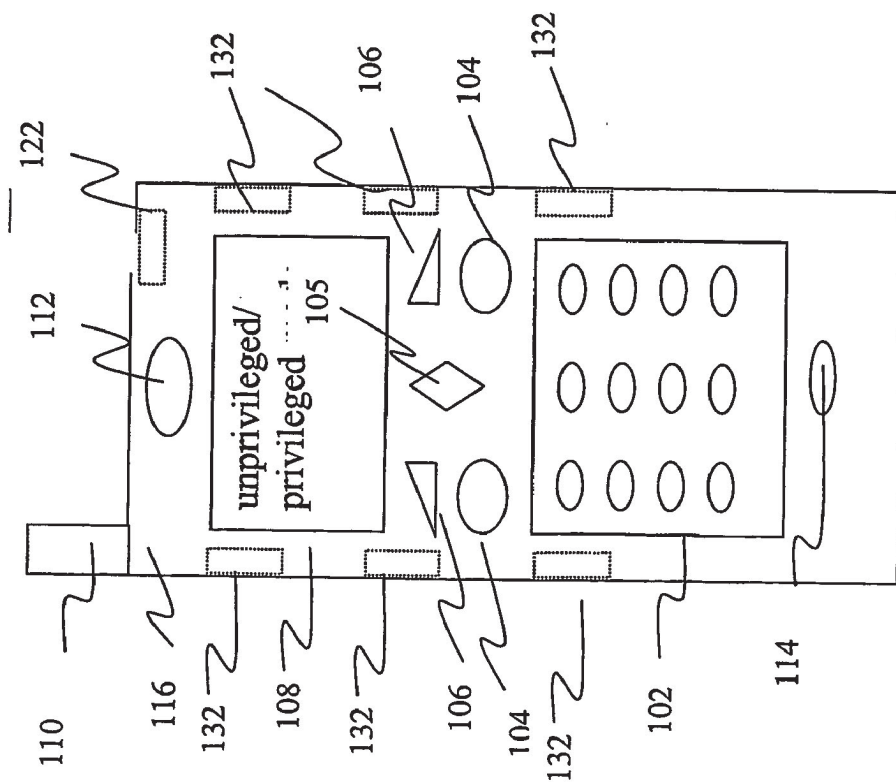


Figure 7a

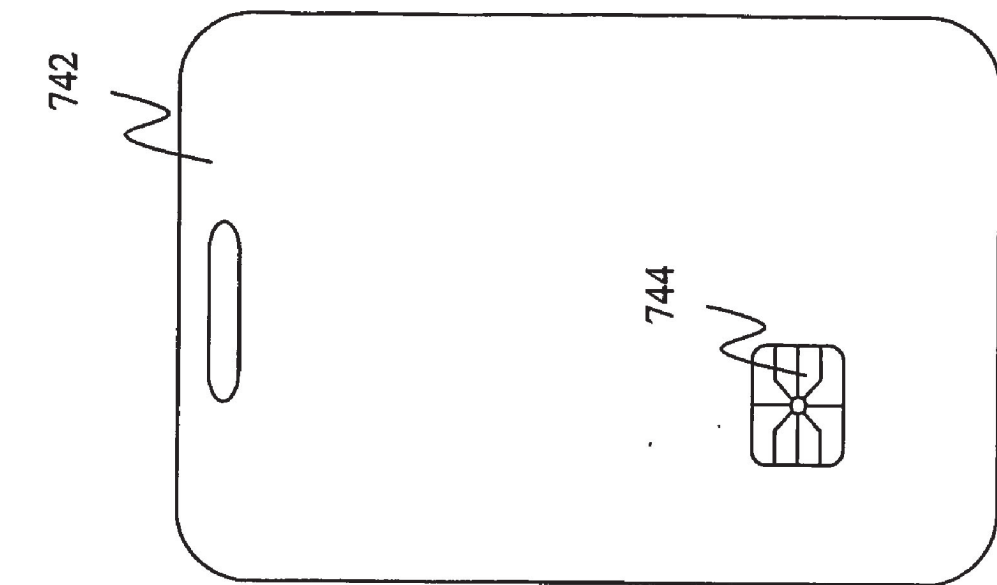


Figure 8a

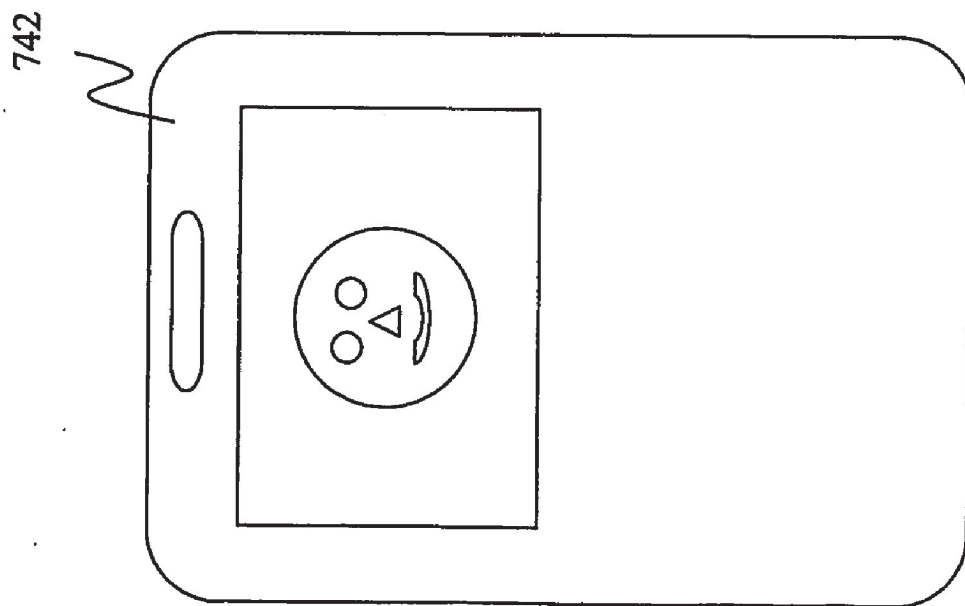


Figure 8b

WIRELESS MOBILE PHONE WITH AUTHENTICATED MODE OF OPERATION INCLUDING HEART BEAT PROFILE BASED AUTHENTICATION

RELATED APPLICATION

[0001] This application is a non-provisional application of provisional application 60/459,281, filed on Mar. 31, 2003, having the same title, and claims priority to said '281 provisional application.

[0002] Said '281 provisional application is a continuation-in-part application of U.S. Non-Provisional patent application Ser. No. 09/690,679, entitled "A Mobile Digital Communication/Computing Device Including A Heart Rate Monitor", filed on Oct. 16, 2000, and claims priority for the base materials to said '679 non-provisional application, which specification is incorporated into the '281 provisional application by reference.

[0003] Accordingly, for the U.S. version, this application also claims priority, through said '281 provisional application, to the '679 non-provisional application for the base material described in the '679 non-provisional application.

FIELD OF THE INVENTION

[0004] The present invention relates to the field of wireless communication. More specifically, the present invention is related to a wireless mobile phone having an authenticated mode of operation available only to an authenticated user, in particular, a user authenticated via a heart beat profile of the user.

BACKGROUND OF THE INVENTION

[0005] Advances in microprocessor and telecommunication technology have led to wide spread deployment and adoption of mobile devices, such as wireless mobile phones. For wireless mobile phones, in addition to wireless telephony; the late models are often equipped with advanced capabilities, such as calendar, address book, access to the World Wide Web (WWW), emails, and so forth.

[0006] Much of these functionalities are designed to increase the productivity of business users. As a result, it is not surprising that business users constitute a major user segment of wireless mobile phones, especially for the high-end function rich models. Increasingly, more business data, such as business contact information, business plans, sales/marketing strategies, financial reports, and so forth, are being stored on wireless mobile phones.

[0007] However, unlike personal computers or other computing devices, where user authentication, through e.g. user log-in, are routinely provided with virtually all operating systems, few if any operating systems of wireless mobile phones provide means to authenticate users. As a result, under the prior art, wireless mobile phones are at risk of unauthorized usage, as well as data being compromised by unauthorized accesses.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

[0009] FIG. 1 illustrates a front view of a wireless mobile phone incorporated with the teachings of the present invention, in accordance with one embodiment;

[0010] FIGS. 2-3 illustrate two architectural views of the wireless mobile phone of FIG. 1, in accordance with one embodiment;

[0011] FIGS. 4a-4b illustrate the operational flow of the relevant aspects of the operating logic of FIG. 3, in accordance with one embodiment;

[0012] FIG. 5 illustrates a front view of another wireless mobile phone incorporated with the teachings of the present invention, in accordance with an alternate embodiment;

[0013] FIGS. 6a-6b illustrate two perspective views of another wireless mobile phone incorporated with the teachings of the present invention, in accordance with yet another embodiment;

[0014] FIGS. 7a-7b illustrate a front view and a side view of another wireless mobile incorporated with another aspect of the teachings of the present invention, in accordance with yet another embodiment; and

[0015] FIGS. 8a-8b illustrate a front view and a back view of the identity card of FIG. 7b in further detail, in accordance with one embodiment.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0016] Embodiments of the present invention includes a wireless mobile phone having an authenticated mode of operation, available only to an authenticated user, in particular, a user authenticated by a heart beat profile of the user.

[0017] Parts of the description will be presented in terms commonly employed by those skilled in the art to convey the substance of their work to others skilled in the art. The term "wireless mobile phone" as used herein (in the specification and in the claims) refers to the class of telephone devices equipped to enable a user to make and receive calls wirelessly, notwithstanding the user's movement, as long as the user is within the communication reach of a service or base station of a wireless network service provider. Unless specifically excluded, the term "wireless mobile phone" is to include the analog subclass as well as the digital subclass (of all signaling protocols).

[0018] In the following description, various aspects of the present invention will be described. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention. For purposes of explanation, specific numbers, materials and configurations are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without the specific details. In other instances, well-known features are omitted or simplified in order not to obscure the present invention.

[0019] Various operations will be described as multiple discrete steps in turn, in a manner that is most helpful in understanding the present invention, however, the order of description should not be construed as to imply that these operations are necessarily order dependent. In particular, these operations need not be performed in the order of presentation.

[0020] The phrase "in one embodiment" is used repeatedly. The phrase generally means "in at least one embodiment" and is not intended to limit the scope of the present invention. The phrase "in another embodiment" is used repeatedly. The phrase generally means "in at least one other embodiment" and is not intended to limit the scope of the present invention.

AliveCor Exhibit 1020

AliveCor, Inc. v. Apple Inc.

IPR2023-00950, U.S. Patent No. 10,076,257

[0022] While operating in the unauthenticated mode of operation, i.e. without having the user authenticated, operating logic **240** makes available only a limited or reduced set of functions, whereas under the authenticated mode of operation, i.e. having the user authenticated, operating logic **240** makes available a more expanded or the entire set of functions.

[0024] In another embodiment, the limited/reduced set of functions may effectively be a null function set, excluding even the ability to make an emergency call, except for notification of the unauthenticated status of the user, and perhaps, inviting the user to authenticate himself/herself, by e.g. allowing a hear beat profile of the user to be captured in real time.

[0026] Continue to refer to FIGS. 1 and 3a-3b, for the illustrated embodiment, phone 100 is further advantageously equipped with sensors 132 to facilitate real time capturing of a heart beat profile of the user (while operating in the authenticated mode). Further, operating logic 240, or more specifically, security function 242, is endowed to facilitate such capture, and authenticate a user through the heart beat profile of the user (prior to operating phone 100 in the authenticated mode).

[0027] In particular, as will be described in more detail below, operating logic **240**, in general, is equipped to establish a reference heart beat profile of a user for authentication purpose, and automatically invokes sensors **132** to capture a heart beat profile of the user real time, during power on or reset. Further, security function **242** is endowed to use the reference and the real time captured heart beat profiles of the user to authenticate the user, and determine whether to continue to operate phone **100** in an unauthenticated mode, or operate phone **100** in an authenticated mode.

[0029] For the embodiment, sensors 132 are disposed along and underneath the side surfaces of phone 100. A dynamically determined subset of sensors 132 are employed to capture the heart beat profile of the user. The subset of sensors 132 to be employed is based on whether the user is holding phone 100 with his/her left or right hand, thereby coming into contacts with different ones of sensors 132. Discernment of the appropriate subsets of sensors 132, or more specifically, the sensing data outputted by sensors 132, to be used, is described in detail in parent U.S. patent application Ser. No. 09/690,679 set forth and incorporated by reference above.

[0031] Further, operating logic 240, more specifically, security function 242, also supports the capturing of a heart beat profile of the user, and its saving as a reference for subsequent analysis of a real time captured heart beat profile of the user to authenticate the user, before operating phone 100 in the authenticated mode.

[0033] Before proceeding with further description of phone 100, it should be noted that, while for ease of understanding, the present invention has been described referencing embodiments, where user authentication is substantially based on the heart beat profile of the user, in alternate embodiments, the present invention may be practiced with the user authentication being based on other user bio-metrics. An example of such other user bio-metrics is the user's finger print, which may e.g. collected optically, or electronically. An example of an optical collector is a camera, whereas an example of an electronic collector is capacitance sensor.

[0034] Continuing to refer to FIGS. 1 and 3a-3b, additionally, phone 100 includes conventional wireless telephony elements, including power switch 122, power 222, audio communication elements, such as ear speaker 112 and microphone 114, and non-audio communication elements, such as input key pad 102 having a number of alphanumeric input keys and display 108. Further, the non-audio input elements may further include scroll button 105, selection buttons 106, and “talk” and “end talk” buttons 104. These elements are disposed on various external surfaces of body 116.

[0035] As illustrated in FIG. 3a, upon depression by a user (optionally, for a predetermined duration), while phone 100 is in a powered down or lower power state, power switch 122 couples power 222 to sensors 132 and other components 202-212. Likewise, upon depression by a user (optionally, for a predetermined duration), power switch 122 couples power 222 to sensors 132 and other components 202-212.

state, power switch 122 cuts off or reduces power 222 to all or selected ones of sensors 132 and other components 202-212.

[0036] Externally, phone 100 may also include antenna 110. Keys of key pad 102 may be surrounded by, or otherwise include illuminable light emitting diodes (LED) in their backgrounds. For the purpose of the present specification, the terms “button” and “key” may be considered synonymous, unless the context clearly indicates otherwise.

[0037] Internally, in addition to processor 202 and DSP 204, phone 100 also includes non-volatile memory 206, general purpose input/output (GPIO) interface 208, and transmit/receive (TX/RX) 212, coupled to each other, processor 202 and DSP 204, via bus 214, and disposed on a circuit board 220.

[0038] Except for the novel manner that many of these elements, such as processor 202, DSP 204 and so forth, are used in support of making the expanded/full set of functionalities available only to an authenticated user, the enumerated elements otherwise perform their conventional functions known in the art.

[0039] Non-volatile memory 206 is employed to store programming instructions and optionally, working data, including operating logic 240 and its security function 242. Working data may include callee/messaging party or parties (e.g. their phone numbers or IP addresses) with whom user may communicate. Working data may include the reference and input heart beat profiles of the user.

[0040] Processor 202, assisted by DSP 204, is employed to operate phone 100, executing operating logic 240, including security function 242.

[0041] Keys of key pad 102 may be employed to enter alphanumeric data, including entering a sequence of alphanumeric data for the phone number or address of a “callee”. Selected sequence of the keys (such as “*#”) may also be employed to denote a user instruction to return to the unauthenticated mode of operation, if entered while operating in the authenticated mode of operation, or to return to the authenticated mode of operation, if entered while operating in the unauthenticated mode of operation (provided the user is authenticated).

[0042] Scroll key 105 and companion selection keys 106 may be employed to scroll and select various options or list items of various menu options or selection lists, including scrolling and selecting list items presented for user interactions to verify the user’s wellness. For the embodiment, scroll key 105 may be selected in one of two positions, an “up” position or a “down” position for scrolling a selection list in an “up” direction and a “down” direction respectively. Similarly, scroll and selection keys 105/106 may also be employed to select a menu item to convey a user instruction to return to the unauthenticated mode, if the selection is made while operating in the authenticated mode, or to return to the authenticated mode, if the selection is made while operating in the unauthenticated mode (provided the user is authenticated).

[0043] GPIO 208 may be employed to generate input signals, such as a corresponding “alphanumeric” signal in response to a user selection of one of the keys of key pad 102, a “scroll” signal” (or more specifically, a “scroll up” or a “scroll down” signals) in response to a user selection of scroll key 105, a “selection” signal in response to a user selection of select button 106, and so forth.

[0044] TX/RX 212 may be employed to transmit and receive communication signals for a call and/or a text mes-

sage. TX/RX 212 may be a radio frequency transceiver, and support one or more of any of the known signaling protocols, including but are not limited to CDMA, TDMA, GSM, and so forth.

[0045] The constitutions of these elements are known, and will not be further described.

[0046] As to operating logic 240, including security function 242, it may be implemented in the assembly or machine instructions of processor 202, or a high level language that can be compiled into these assembly or machine languages. In alternate embodiments, all or portions of operating logic 240, including security function 242 may be implemented in firmware and/or hardware.

[0047] Accordingly, except for the enhancements provided, phone 100 otherwise represents a broad range of wireless mobile phones, including both the analog as well as the digital types (of all signaling protocols), substantially rectangular uni-body as illustrated, or curved uni-body, as well as multi-portions, such as “flip phones” to be illustrated later.

[0048] FIG. 4 illustrates the operational flow of the relevant aspects of operating logic 240, in accordance with one embodiment. As illustrated, on start up/reset (such as depression of power on/off button 122 for the required predetermined duration by a user), operating logic 240 enables phone 100 to operate in the earlier described unauthenticated mode, making available only a limited/reduced set of functionalities, block 402. Thereafter, operating logic 240 waits for additional user input, block 404.

[0049] Recall from earlier description, upon depression by a user, while phone 100 is in powered down or low power state, power switch 122 couples power to sensors 132 and other components 202-212 of phone 100. For the embodiment, on power on/reset, operating logic 230 causes sensors 132 to sense the heart beat pattern of the user, based on the user’s fingers 250 in contact. Resultantly, after a predetermined elapsed amount of time, a heart beat profile of an authorized user who is aware of the authentication requirement, and have properly held the phone with his/her fingers in contact with sensors 132, would have a heart beat profile of the user taken or captured in real time, for authentication.

[0050] Accordingly, under the present invention, heart beat profile based authentication is seamlessly integrated with the power on/reset process.

[0051] Continuing to refer to FIG. 4, on receipt of inputs, operating logic 240 determines if the input is a heart beat profile captured by sensors 132 in real time (more specifically, by DSP 204, after it processes the signals output by sensors 132 into a heart beat profile), block 406.

[0052] If the user input is a heart beat profile, operating logic 240 (or more specifically, security function 242) further determines if phone 100 is operating in the unauthenticated mode, within the authenticated mode (including whether it is within the configuration mode of the authenticated mode), or the initial provisioning mode, block 407.

[0053] If phone 100 is determined to be operating in the configuration mode within the authenticated mode, or the initial provisioning mode, operating logic 240 (or more specifically, security function 242) saves the captured heart beat profile as a reference heart beat profile for future user authentication, block 408.

[0054] If phone 100 is determined to be operating in the unauthenticated mode, operating logic 240 (or more specifically, security function 242) initiates the heart beat profile based authentication process, block 410.

AliveCorp. Exhibit 1020

Apple Inc.

US Patent No. 10,076,257

paring the real time captured heart beat profile, against the previously saved reference heart beat profile, block 409.

[0055] If the heart beat profile does not substantially match the previously saved reference heart beat profile, block 410, operating logic 240 (or more specifically, security function 242) reports the authentication failure, block 412, and continues to operate phone 100 in the unauthenticated mode at block 404.

[0056] However, if the inputted heart beat profile substantially matches the previously saved reference heart beat profile, block 410, operating logic 240 (or more specifically, security function 242) enables phone 100 to operate in the authenticated mode, block 414. Thereafter, operating logic 240 continues operation at block 404.

[0057] The precision level at which a real time captured heart beat profile is to be considered substantially matching with a reference heart beat profile is application dependent. Preferably, different user selectable precision levels are offered. As with other user selectable options, the selection may be facilitated in any one of a number of known user selection techniques.

[0058] Back at block 408, if the input is determined not to be heart beat profile input, operating logic 240 determines if the input is a user instruction to return to the unauthenticated mode of operation (e.g. a user selecting or inputting such command using alphanumeric keys 102 and/or scroll/select keys 105 and 106 while operating in an authenticated mode of operation), block 416.

[0059] If the input is determined to be a user instruction to return to the unauthenticated mode of operation, operating logic 240 (or more specifically, security function 242) returns phone 100 to operate in the unauthenticated mode, block 418. Thereafter, operating logic 240 continues operation at block 404.

[0060] In one embodiment, before exiting to the unauthenticated mode, operating logic 240 (or more specifically, security function 242) causes a user selectable “resume” (i.e. re-authentication) option to be rendered on display 108. Selection of the option is processed as if phone 100 is being powered on or reset. That is, operating logic 240 automatically causes sensors 132 to capture another heart beat profile of the user for authentication purpose.

[0061] If the input is determined to be other user inputs, operating logic 240 handles the other user inputs in an application dependent manner, block 420. In particular, if the input is a user instruction to return to the authenticated mode of operation, operating logic 240 continues operation at block 404, and awaits for another heart beat profile input to re-authenticate the user. If the input is other conventional inputs, the inputs are processed as in the prior art. Thereafter, operating logic 240 continues operation at block 404.

[0062] FIG. 5 illustrates another embodiment of the wireless mobile phone of the present invention. More specifically, FIG. 5 illustrates a front view of the alternate embodiment. The alternate embodiment is substantially that of the embodiment of FIG. 1, except that phone 100 is substantially rectangular in shape, whereas phone 500 has a curved shape.

[0063] FIGS. 6a-6b illustrate yet another embodiment of the wireless mobile phone of the present invention. More specifically, FIGS. 6a-6b illustrate two perspective views of the embodiment. The embodiment is also substantially that of the embodiments of FIGS. 1 and 5, except that phone 100 is substantially rectangular, phone 500 has a curve shaped body, whereas phone 700 has a multi-section body. The multi-

section form factor includes a first section 716b and a second section 716c, and the second section 716c is further comprised of at least two sub-sections 716d-716e. The first and second sections 716b-716c may pivot towards each other as denoted by direction arrow 706a or away from each other opposite to the direction denoted by arrow 706a. Sub-section 716d may rotate relative to sub-section 716e as denoted by the directions denoted by arrows 706b. In other words, phone 700 may be considered as an improved version of what is commonly referred to as “flip” phones.

[0064] Similar to the earlier described embodiments, phone 700 is provided with operating logic having a security function as earlier described, and sensors 732.

[0065] In alternate embodiments, second section 716c may be a uni-section, i.e. it is not further sub-divided into to relatively pivotable sub-sections.

[0066] In yet other embodiments, the reference heart beat profile may be provided to the wireless mobile phone in a secure manner, e.g. read from an identity card, via an identity card reader additionally provided to the wireless mobile phone.

[0067] FIGS. 7a-7b illustrate one such embodiment. As illustrated in FIG. 7b, wireless mobile phone 100 is additionally endowed with an identity card reader 740. Identity card reader 740 (optionally, assisted by a device driver additionally provided to supplement operating logic 240) is equipped to retrieve the earlier described reference heart beat profile from identity card 742.

[0068] Preferably, identity card 742 has a form factor that is difficult to forge, and its issuance is governed by a secured process. Resultantly, security for wireless mobile phone 100 is further enhanced.

[0069] For the embodiment, identity card 742 comprises a smart electronic card 744 (commonly referred to as a smart card) (see FIGS. 8a-8b), and the reference heart beat profile is pre-stored in the embedded smart card 744. Operating logic 240 (optionally, supplemented by a corresponding reader device driver) retrieves the reference heart beat profile from embedded smart card 744, on detection of the presence of identity card 742.

[0070] In various embodiments, the reference heart beat profile may be further protected via encryption, requiring operating logic 240 to possess the proper decryption key to recover the reference heart beat profile after retrieval.

[0071] In yet other embodiments, the reference heart beat profile may be further protected via an authentication protocol, requiring wireless mobile phone 100 to be equipped with the appropriate credential to authenticate itself to smart card 744, before being allowed by smart card 744 to access the pre-stored reference heart beat profile in smart card 744.

[0072] In yet other embodiments, the reference heart beat profile may be imprinted on identity card 742, and identity card reader 720 is an optical reader.

[0073] In yet still other embodiments, the reference heart beat profile may be encoded via a magnetic strip disposed on a surface of identity card 742, and identity card reader 720 is a magnetic code reader.

[0074] In yet still other embodiments, the reference heart beat profile may be stored in a storage that is removably attached to the wireless mobile phone 100, such as a suitable removable storage device. **Apple Inc.**
Exhibit 1020
U.S. Patent No. 10,076,257
IPR2023-00950

[0075] These are just a few example, other equivalent encoding/storing and reading/retrieving techniques may also be employed instead.

CONCLUSION AND EPILOGUE

[0076] Thus, it can be seen from the above descriptions, a novel wireless mobile phone that can afford protection against unauthorized access to user data and/or usage of the phone, using bio-metric based authentication, has been described.

[0077] While the present invention has been described in terms of the foregoing embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described. The present invention can be practiced with modification and alteration within the spirit and scope of the appended claims.

[0078] In particular, the present invention may be practiced with employing additional and/or other means to authenticate a user.

[0079] Thus, the description is to be regarded as illustrative instead of restrictive on the present invention.

What is claimed is:

1. A wireless mobile phone comprising:
a plurality of components coupled to each other to facilitate wireless telephony communication by a user;
a plurality of sensors to facilitate real time capturing of a heart beat profile of the user; and
operating logic to receive the real time captured heart beat profile of the user and to selectively operate the components depending on whether the user is successfully authenticated via a real time captured heart beat profile of the user.
2. The wireless mobile phone of claim 1, wherein the operating logic further comprises logic to compare the real time captured heart beat profile of the user against a reference heart beat profile.
3. The wireless mobile phone of claim 1, wherein the operating logic further comprises logic to save the real time captured heart beat profile of the user as a reference heart beat profile for authentication.
4. The wireless mobile phone of claim 1, wherein the wireless mobile phone further comprises a reader to facilitate provision of the reference heart beat profile via an identity card.
5. The wireless mobile phone of claim 4, wherein the reference heart beat profile is stored on said identity card in a manner to be read by a reader selected from the reader group consisting of an electronic reader, an optical reader, and a magnetic reader, and the wireless mobile phone further comprises the selected reader.
6. The wireless mobile phone of claim 1, wherein the wireless mobile phone further comprises a reader to facilitate retrieval of the reference heart beat profile from a storage removably attached to the wireless mobile phone.
7. In a wireless mobile phone, a method of operation comprising:
capturing in real time a heart beat profile a user;
authenticating the user using the real time captured heart beat profile of the user; and

operating a plurality of components of the wireless mobile phone to facilitate wireless telephony communication by the user, beyond a set of functions not requiring user authentication, if the user is successfully authenticated via the real time captured heart beat profile of the user.

8. The method of claim 7, wherein the method further comprises comparing the real time captured heart beat profile of the user against a reference heart beat profile.

9. The method of claim 7, wherein the method further comprises saving the real time captured heart beat profile of the user as a reference heart beat profile for authentication.

10. The method of claim 7, wherein the method further comprises retrieving the reference heart beat profile from an identity card.

11. The method of claim 7, wherein the method further comprises retrieving the reference heart beat profile from a storage removably attached to the wireless mobile phone.

12. A wireless mobile phone comprising:

a plurality of components coupled to each other to facilitate wireless telephony communication by a user, with the components being equipped to operate in at least a selected one of a first mode and a second mode; and
operating logic to operate the components in said first mode without authentication of the user, and to operate the components in said second mode if the user is successfully authenticated based at least in part on a bio-metric input.

13. The wireless mobile phone of claim 12, wherein the operating logic enables the components to provide first one or more functions, including a function to retrieve a bio-metric reference from a storage removably attached to the wireless mobile phone, while operating the components in said first mode, and further enables the components to provide second additional one or more functions, while operating the components in said second mode.

14. The wireless mobile phone of claim 13, wherein the bio-metric input comprises a heart beat profile of the user to be authenticated.

15. In a wireless mobile phone, a method of operation comprising:

operating a plurality of components coupled to each other to facilitate wireless telephony communication by a user, in a first mode, prior to authenticating the user;
receiving bio-metric input for authenticating the user; and
operating the components in a second mode if the user is successfully authenticated based at least in part on the bio-metric input.

16. The method of claim 15, wherein said operating of the plurality of components in said first mode comprises enabling the components to provide first one or more functions, including retrieving a bio-metric reference from a storage device removably attached to the wireless mobile phone, and said operating of the plurality of components in said second mode comprises enabling the components to further provide second one or more functions.

17. The method of claim 15, wherein the bio-metric input comprises a heart beat profile of the user to be authenticated.

* * * * *