US 20090083847A1

(19) United States

(12) Patent Application Publication

Fadell et al.

(10) Pub. No.: US 2009/0083847 A1

(43) Pub. Date: Mar. 26, 2009

(54) EMBEDDED AUTHENTICATION SYSTEMS IN AN ELECTRONIC DEVICE

(75) Inventors: **Anthony Fadell**, Portola Valley, CA (US); **Andrew Hodge**, Palo Alto, CA (US); **Stephan Schell**, Cupertino, CA (US); **Ruben Caballero**, San Jose, CA (US); **Jesse Lee Dorogusker**, Los Altos, CA (US); **Stephen Zadesky**, Portola Valley, CA (US); **Emery Sanford**, San Francisco, CA (US)

Correspondence Address:
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, NY 10036 (US)

(73) Assignee: **Apple Inc.**, Cupertino, CA (US)

(21) Appl. No.: **12/207,370**

(22) Filed: **Sep. 9, 2008**

Related U.S. Application Data

(60) Provisional application No. 60/995,200, filed on Sep. 24, 2007.

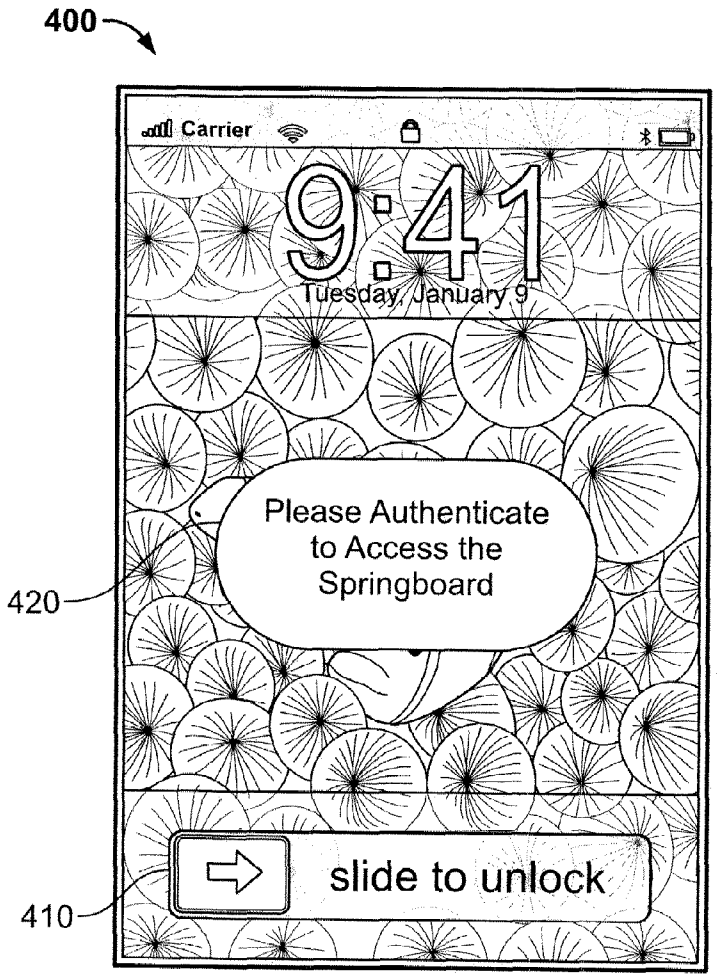
Publication Classification

(51) **Int. Cl.**
H04L 9/32 (2006.01)

(52) **U.S. Cl.** **726/16**

(57) **ABSTRACT**

This invention is directed to an electronic device with an embedded authentication system for restricting access to device resources. The authentication system may include one or more sensors operative to detect biometric information of a user. The sensors may be positioned in the device such that the sensors may detect appropriate biometric information as the user operates the device, without requiring the user to perform a step for providing the biometric information (e.g., embedding a fingerprint sensor in an input mechanism instead of providing a fingerprint sensor in a separate part of the device housing). In some embodiments, the authentication system may be operative to detect a visual or temporal pattern of inputs to authenticate a user. In response to authenticating, a user may access restricted files, applications (e.g., applications purchased by the user), or settings (e.g., application settings such as contacts or saved game profile).



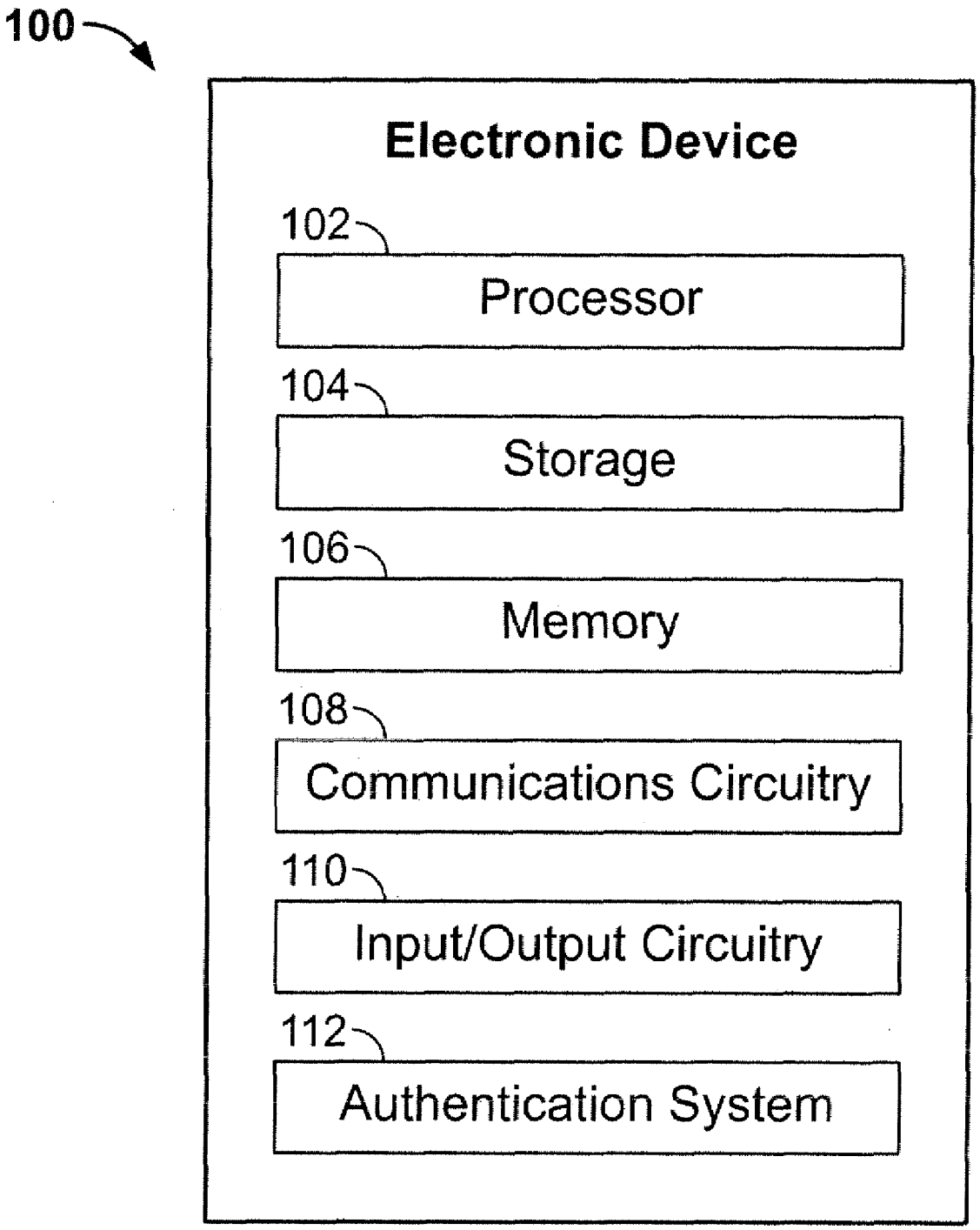

100
Electronic Device
102
Processor
104
Storage
106
Memory
108
Communications Circuitry
110
Input/Output Circuitry
112
Authentication System

FIG. 1

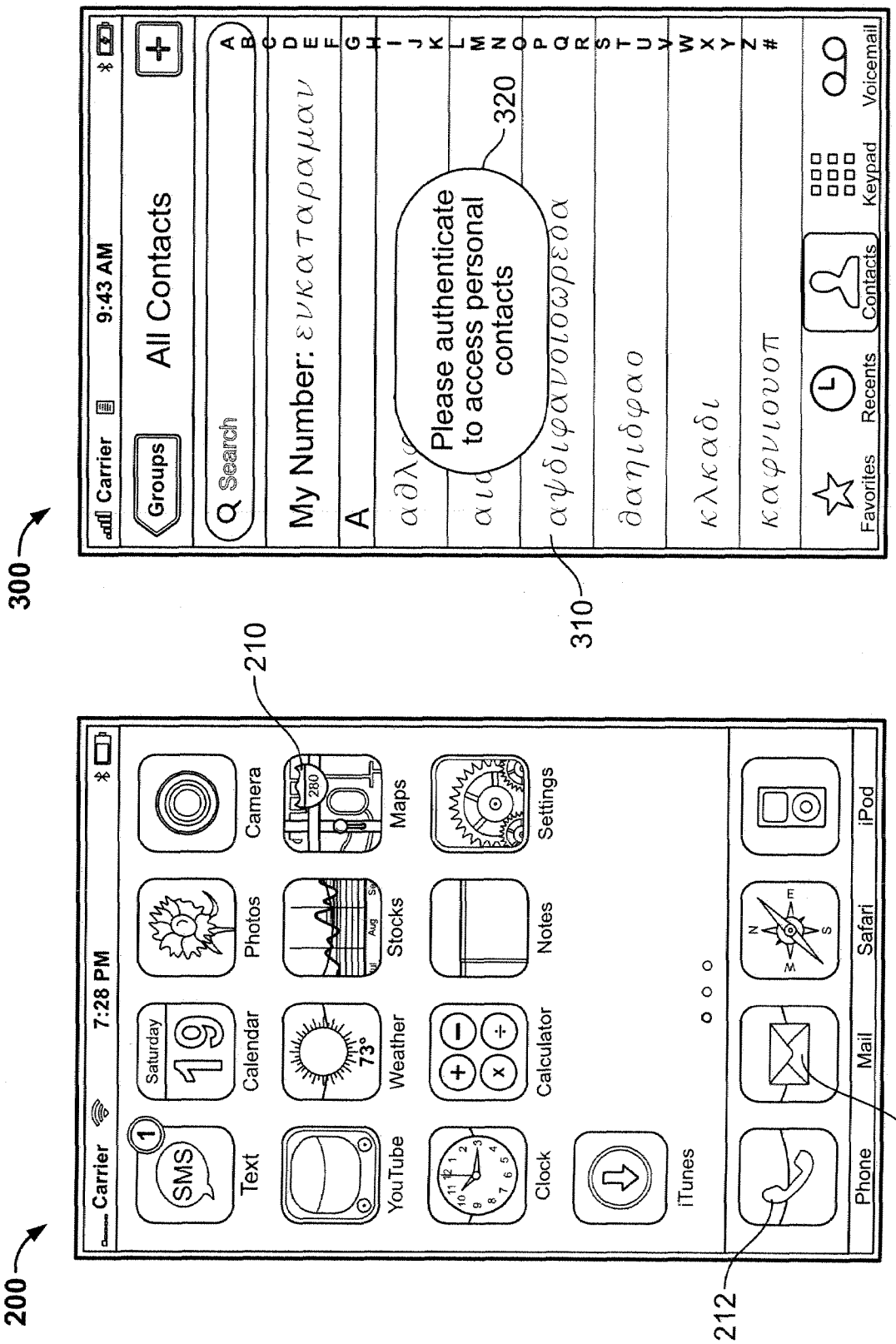

200
Carrier
7:28 PM
Text
Saturday
19
Calendar
Photos
Camera
YouTube
73°
Weather
Stocks
Maps
Clock
Calculator
Notes
Settings
iTunes
Phone
Mail
Safari
iPod
210
212
214
300
Carrier
9:43 AM
Groups
All Contacts
Search
My Number: ενκαταραμαν
A
Please authenticate to access personal contacts
320
310
Favorites
Recents
Contacts
Keypad
Voicemail

FIG. 2

FIG. 3

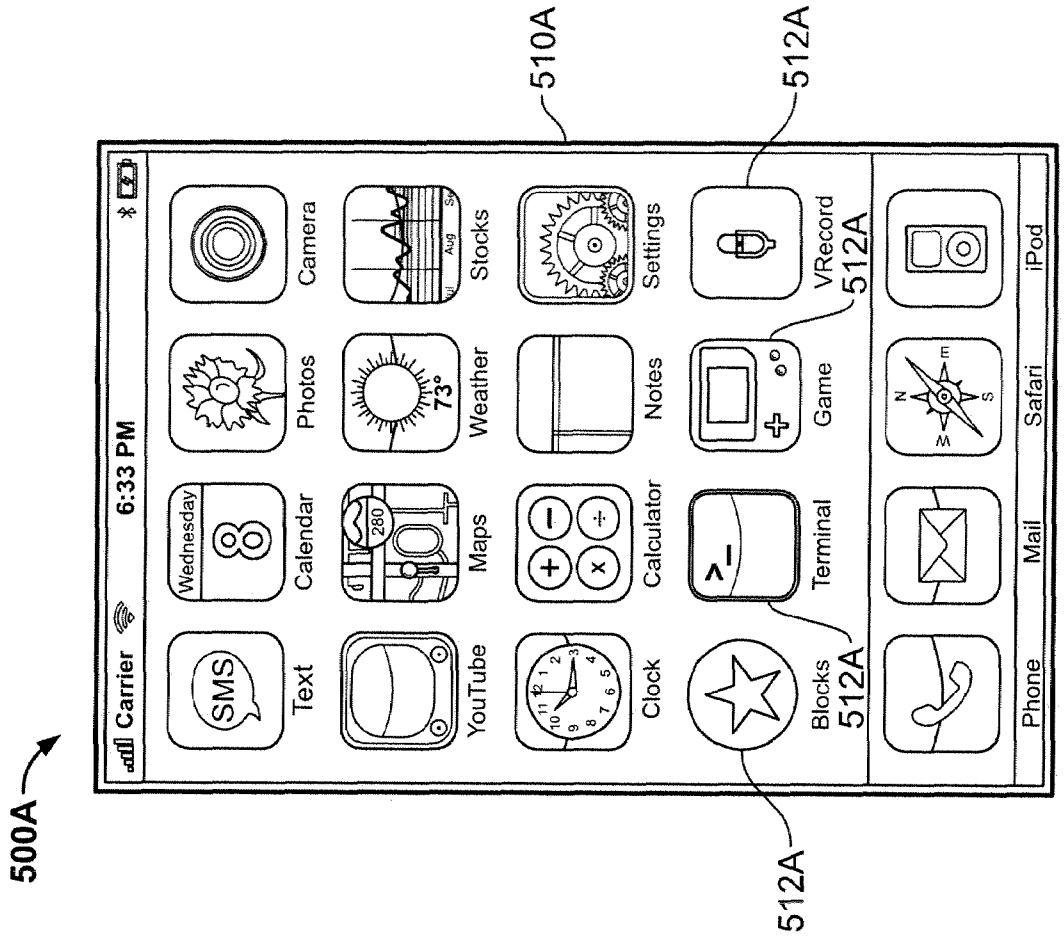

500A
510A
512A
Carrier
6:33 PM
Text
Calendar
Photos
Camera
YouTube
Maps
Weather
Stocks
Clock
Calculator
Notes
Settings
Blocks
Terminal
Game
VRecord
Phone
Mail
Safari
iPod

FIG. 5A

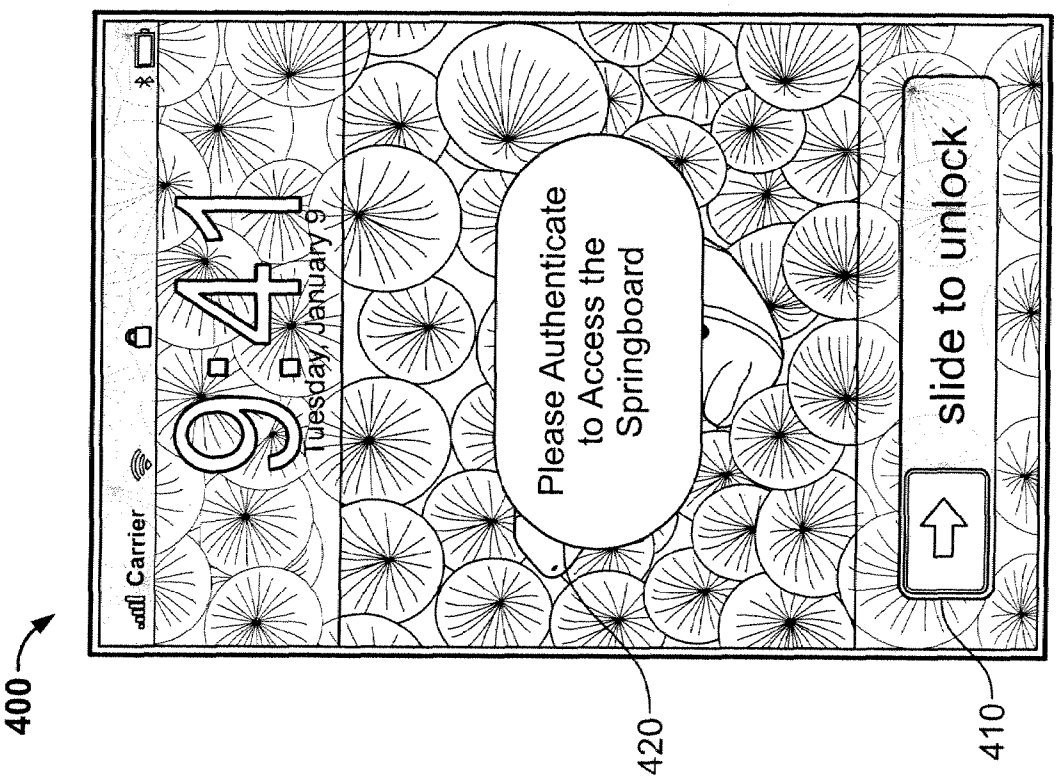

400
420
410
Carrier
9:41
Tuesday, January 9
Please Authenticate to Access the Springboard
slide to unlock

FIG. 4

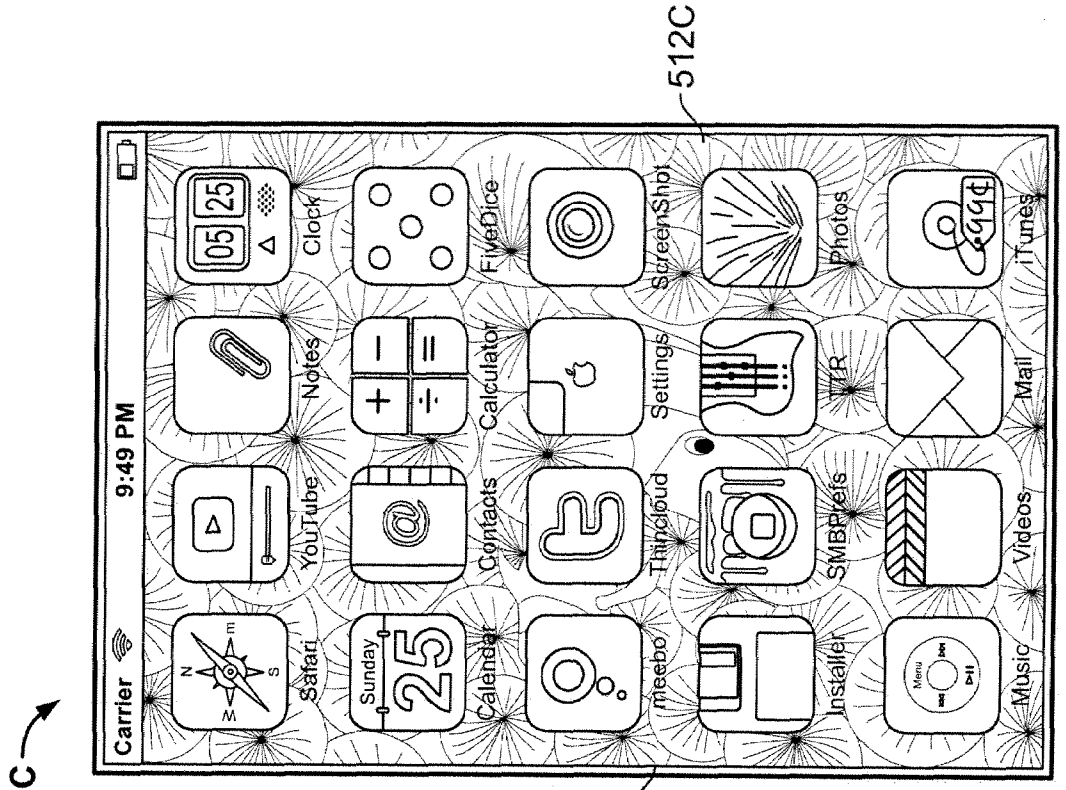

500C
Carrier
9:49 PM
Safari
YouTube
Notes
Clock
Sunday
25
Calendar
Contacts
Calculator
FiveDice
meebo
Thinkcloud
Settings
ScreenShot
Installer
SMBPrefs
TTR
Photos
Music
Videos
Mail
iTunes
510C
512C

FIG. 5C

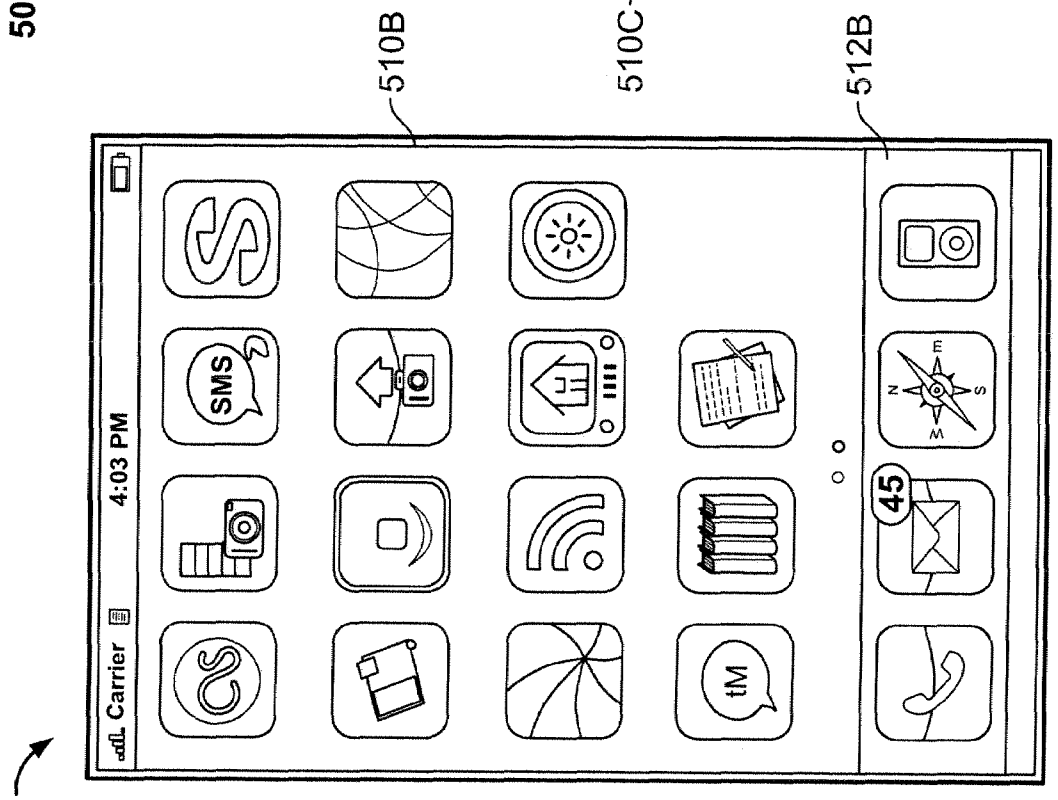

500B
Carrier
4:03 PM
SMS
tM
45
510B
512B

FIG. 5B

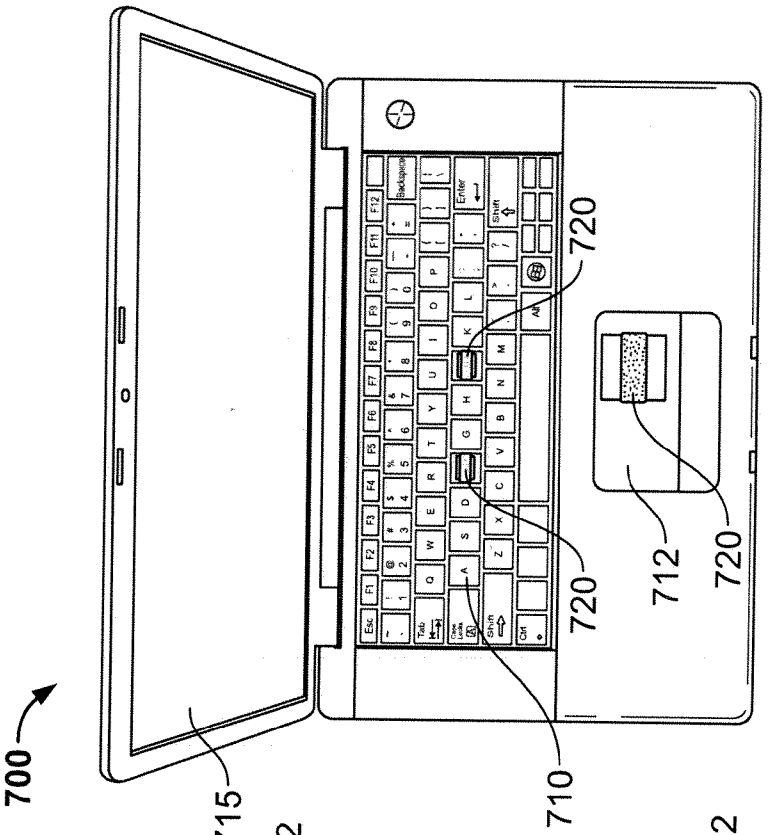

700
715
710
720
720
712
720

FIG. 7

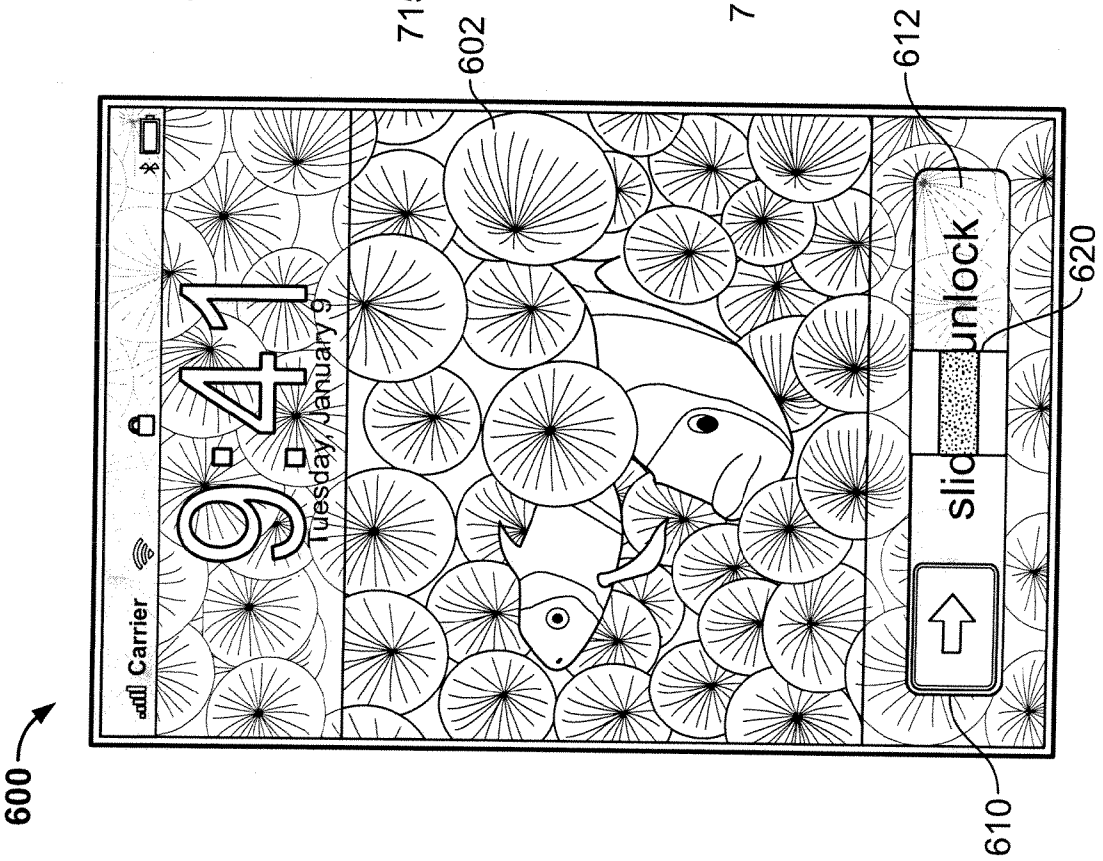

600
Carrier
9:41
Tuesday, January 9
602
612
slide to unlock
620
610

FIG. 6

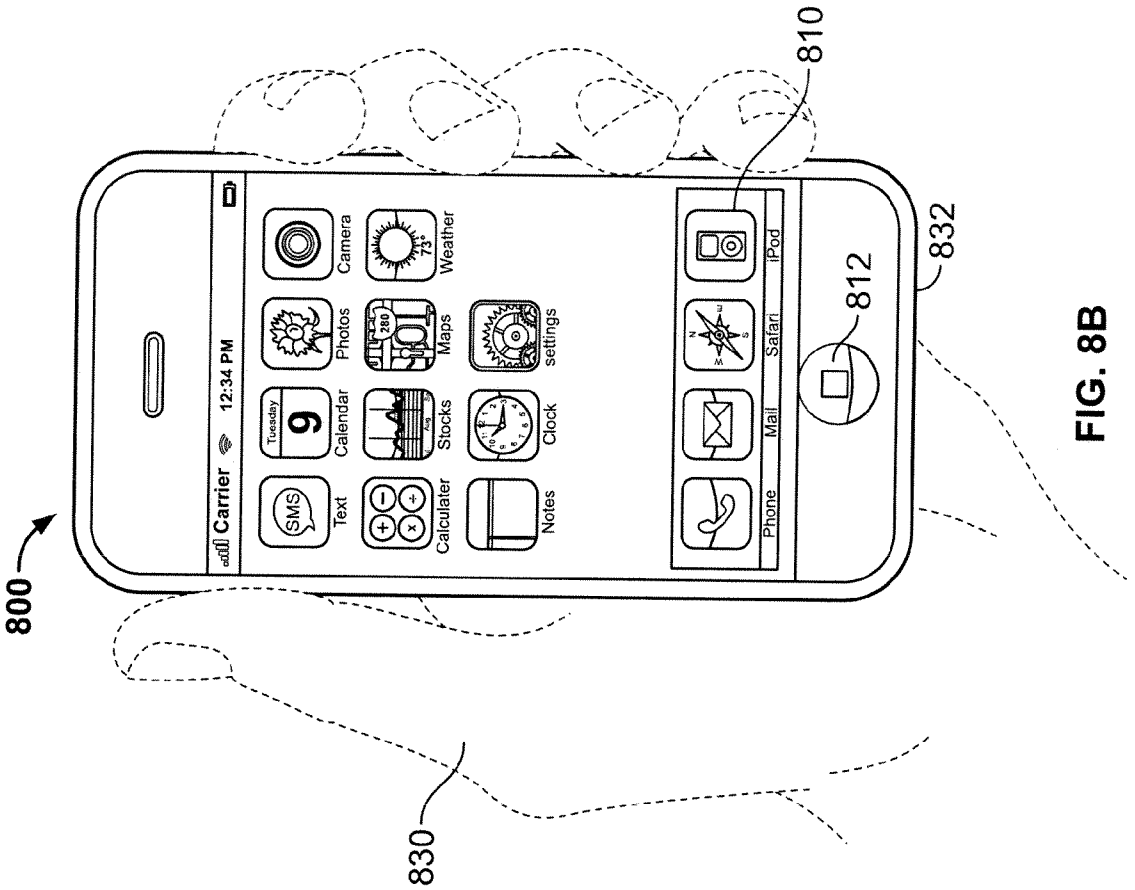

800
Carrier
12:34 PM
Text
Calendar
Photos
Camera
Calculater
Stocks
Maps
Weather
Notes
Clock
settings
Phone
Mail
Safari
iPod
810
812
830
832

FIG. 8B

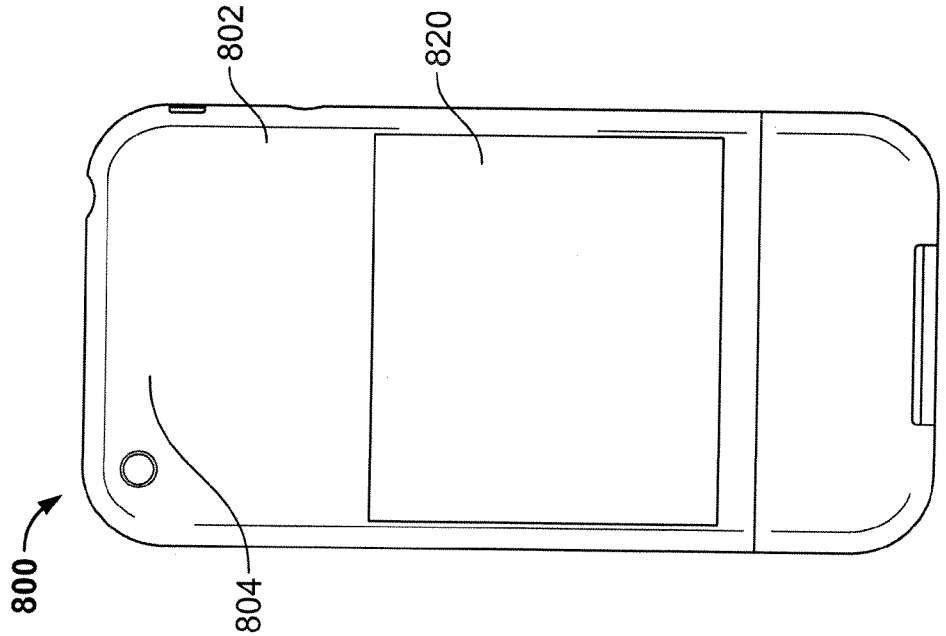

800
802
804
820

FIG. 8A

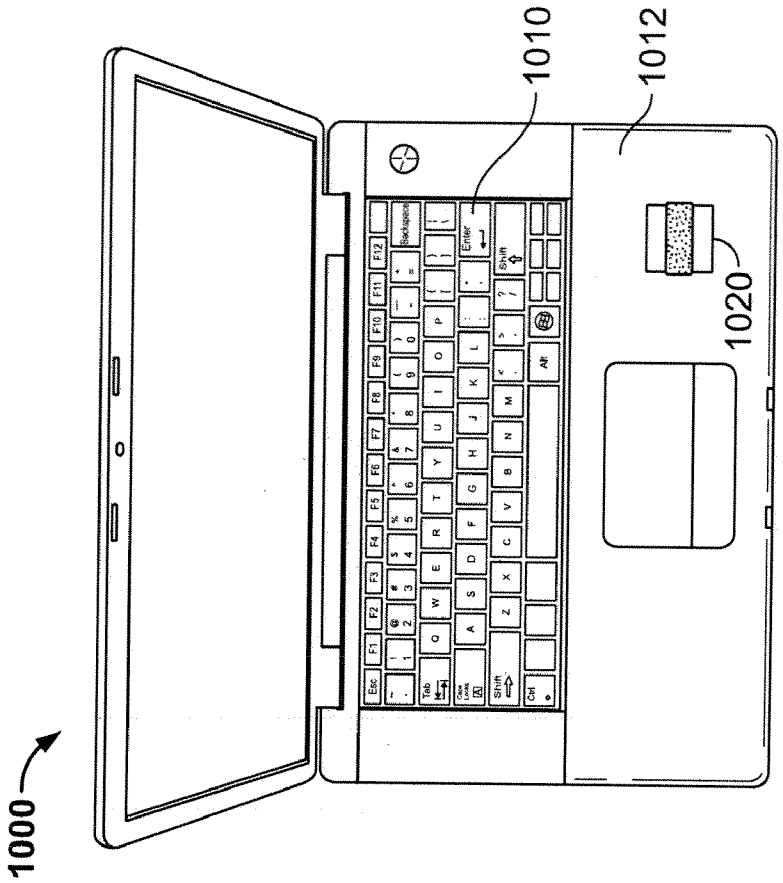


FIG. 10

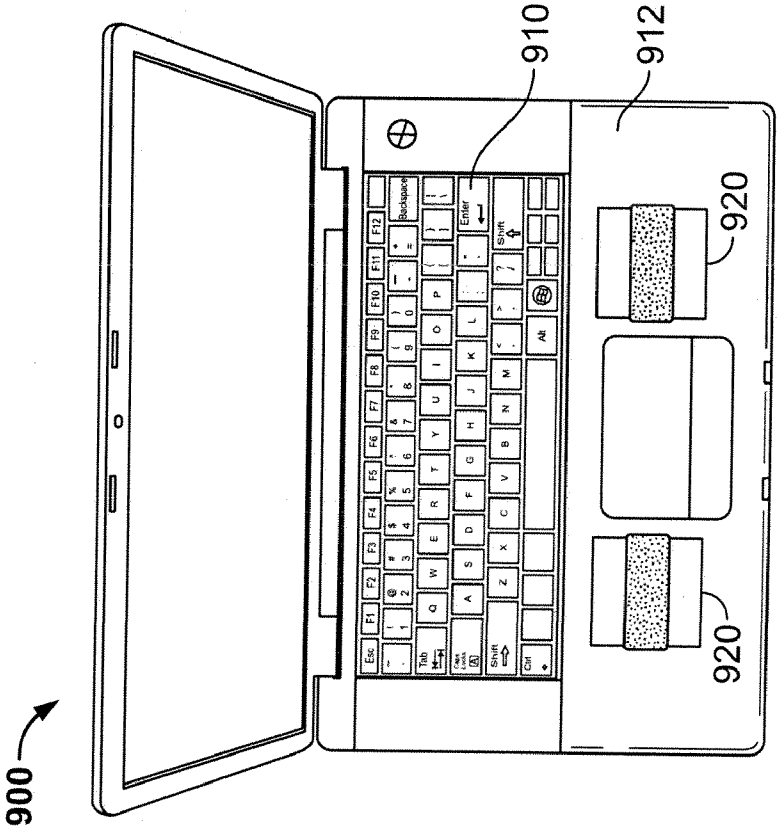


FIG.9

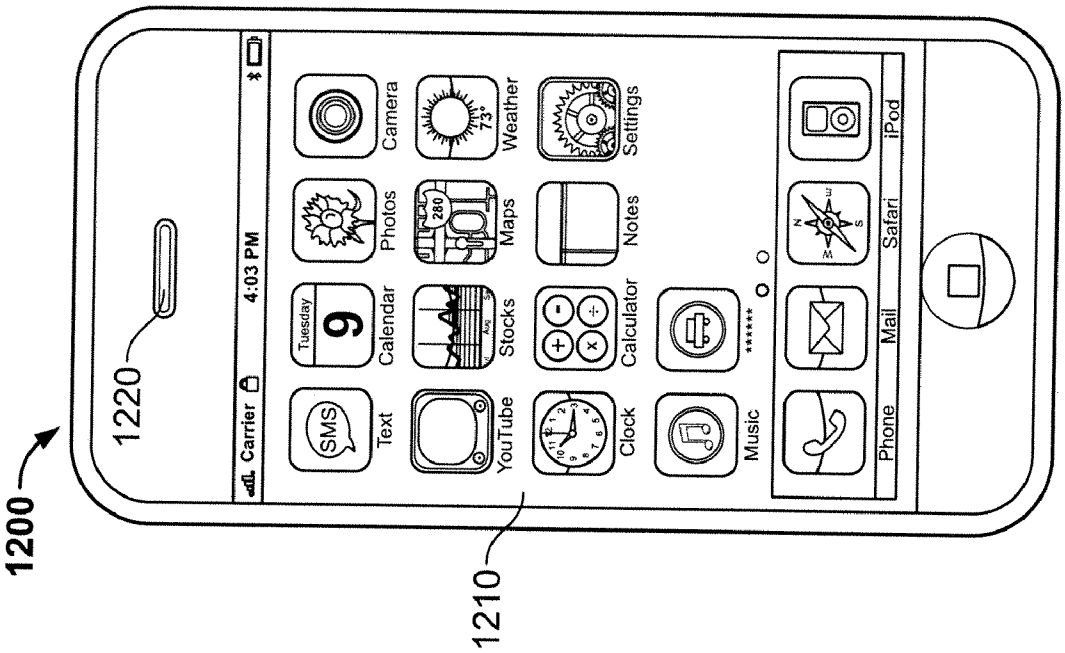

1200
1220
1210
Carrier
4:03 PM
Text
YouTube
Clock
Music
Calendar
Stocks
Calculator
Photos
Maps
Notes
Camera
Weather
Settings
Phone
Mail
Safari
iPod

FIG.12

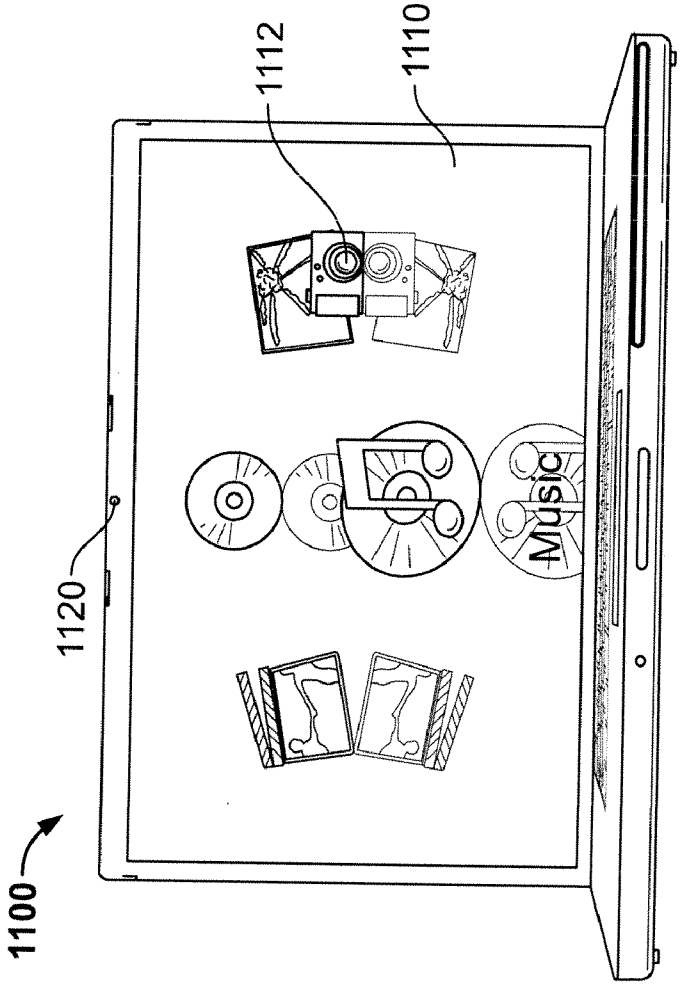

1100
1120
1112
1110
Music

FIG. 11

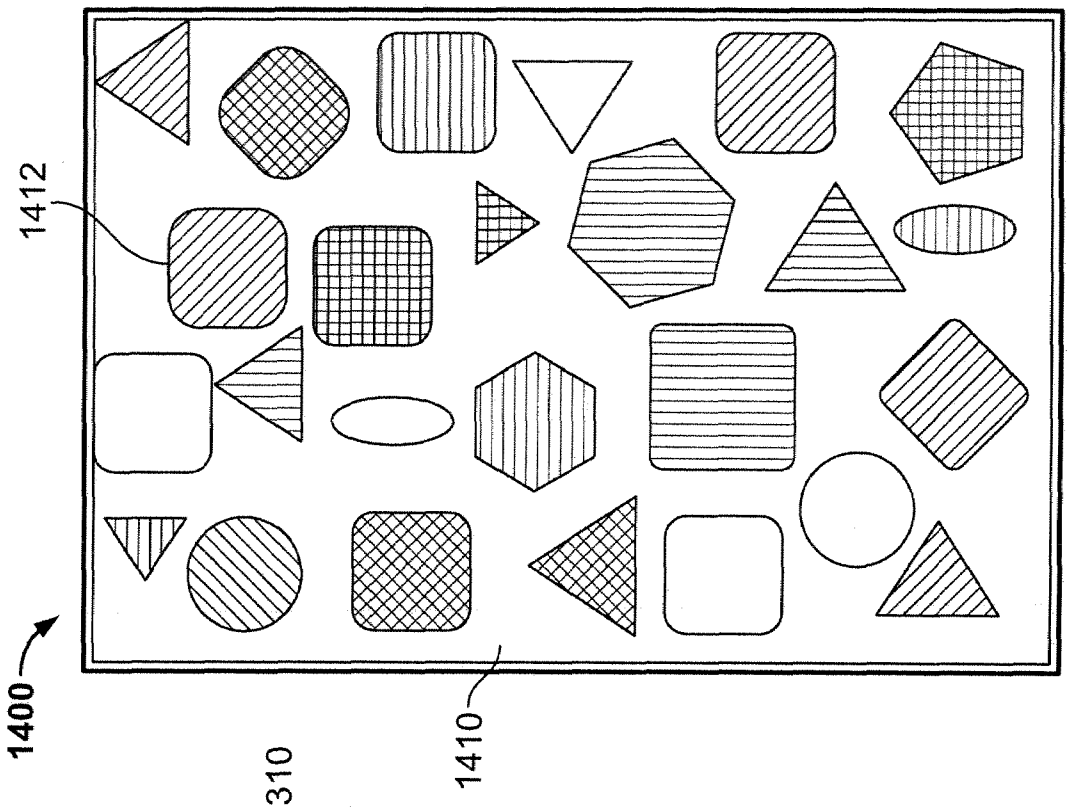


FIG.14

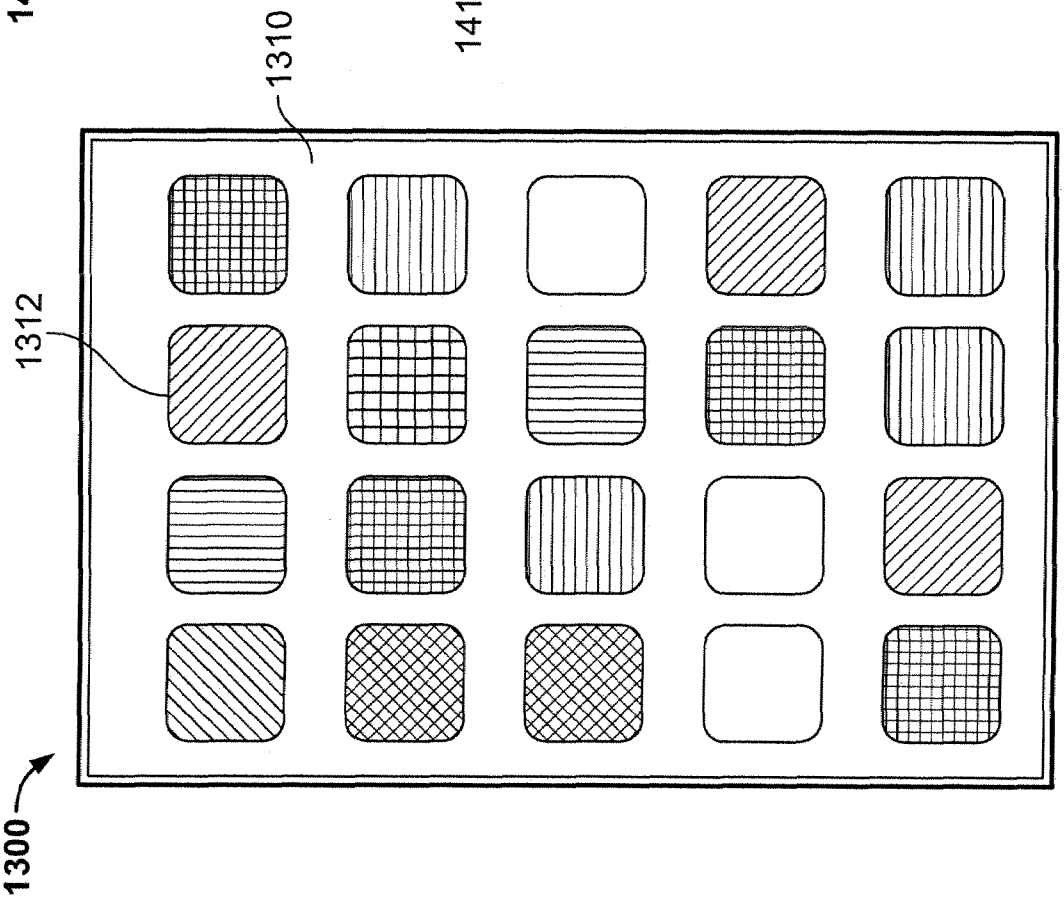


FIG.13

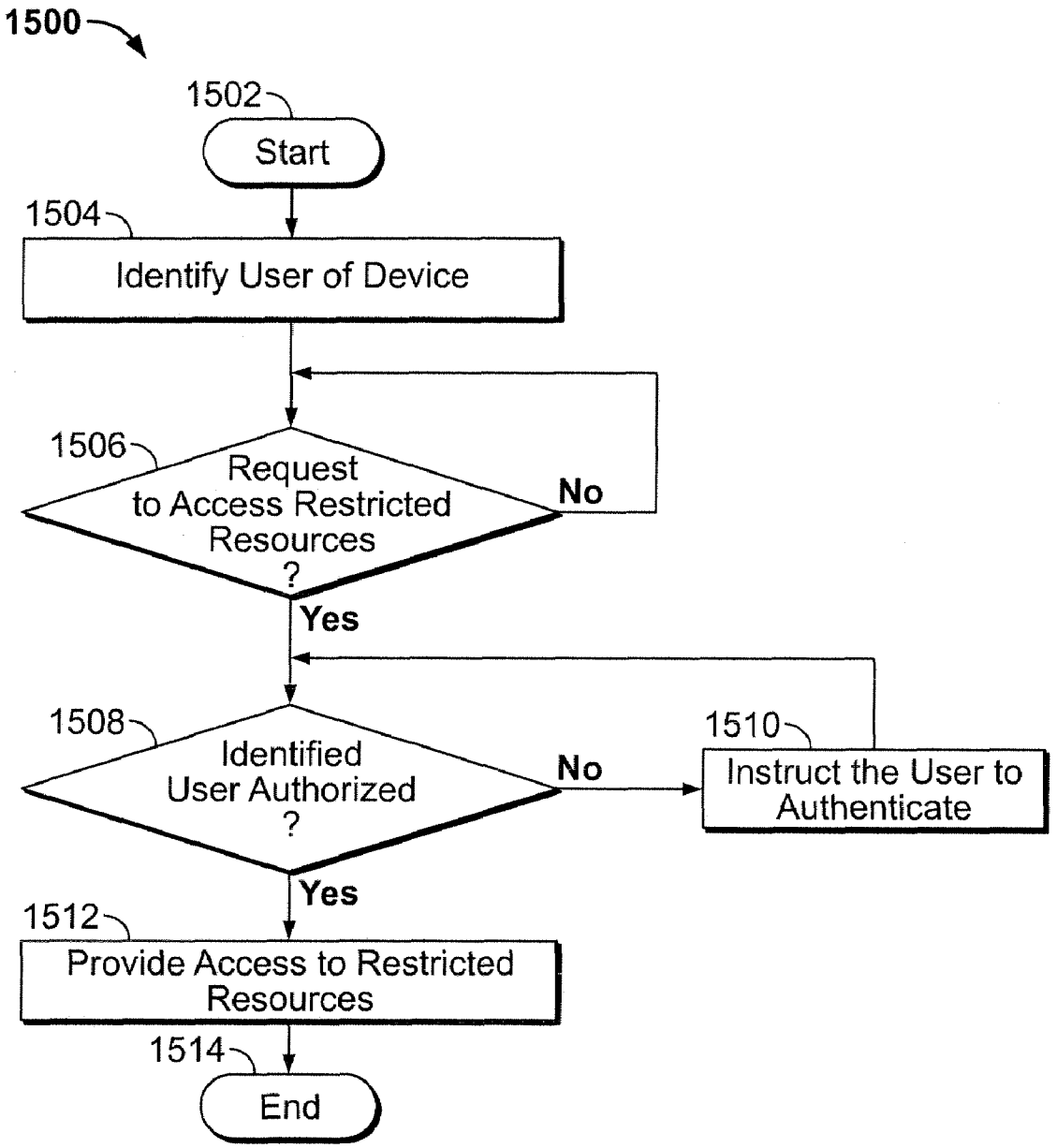

1500
1502
Start
1504
Identify User of Device
1506
Request to Access Restricted Resources ?
No
Yes
1508
Identified User Authorized ?
No
1510
Instruct the User to Authenticate
Yes
1512
Provide Access to Restricted Resources
1514
End

FIG. 15

EMBEDDED AUTHENTICATION SYSTEMS IN AN ELECTRONIC DEVICE

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority from U.S. Provisional Patent Application No. 60/995,200, filed Sep. 24, 2007, which is incorporated by reference herein in its entirety.

BACKGROUND OF THE INVENTION

[0002] This invention is directed to electronic devices with embedded authentication systems.

[0003] Electronic devices, and in particular portable electronic devices, are used to store personal information. For example, users may use cellular telephones, PDAs, smart phones, or other electronic devices to store contacts, e-mail, calendar information, documents, and other information used by the user. While this information may not necessarily be confidential, users may desire that at least some of that information be unavailable to other people. One approach for preventing unauthorized people from accessing and viewing the user's personal information may be to require users of the electronic device to provide a password or pass code prior to enabling device functions or accessing device resources. For example, the electronic device may require a user to enter a four number or four letter pin prior to displaying the device home screen (e.g., a spring board) or menus. As another example, an accessory device for detecting a user's fingerprint or for scanning a user's retina may be coupled to the device such that the user must first show an authorized fingerprint or retina before receiving access to the device.

[0004] While both of these approaches may be useful, restricting access based on a password or pass code is effective only so long as no other user knows the password or pass code. Once the password or pass code is known, the restriction mechanism may become ineffective. Also, a password or pass code may be forgotten, thus locking an authorized user out of the device. In addition, requiring a user to provide a fingerprint or submit to a retina scan may be time consuming and bothersome for the user, requiring an additional step before the user can access the device. While this approach is more secure than entering a password or pass code, it comes at a cost in hardware (e.g., the necessary scanner, detector, or reader) and time. It would be desirable therefore, to provide an electronic device by which biometric and other authentication mechanisms are implemented in the device such that the device authenticates the user quickly and seamlessly, for example as the user turns on, unlocks or wakes the device.

SUMMARY OF THE INVENTION

[0005] Methods, electronic devices and computer readable media for authenticating a user of an electronic device are provided. In some embodiments, an electronic device may seamlessly authenticate a user. The electronic device may receive an input from a user, the input provided by an input mechanism of the electronic device. The electronic device may detect identification information as the user provides the input from one or more sensors embedded in or adjacent to the input mechanism. The electronic device may authenticate the user by comparing the detected identification information with identification information stored in a library of the device. For example, the sensor may include a sensor for detecting features of a user's skin, or features underneath a user's skin. The sensor may be embedded in at least one of a touch screen, a button (e.g., of a keyboard or mouse), device housing near an input mechanism (e.g., laptop housing near keyboard), or any other suitable location.

[0006] In some embodiments, the electronic device may determine that a user is aligned with a sensing component of the device without directing the user to align with the sensing component. For example, the sensing component may be positioned such that the sensing region of the sensor includes expected positions of the user while the user operates the electronic device. The sensor may detect one or more biometric attributes of the user (e.g., facial or eye features) using the sensing component. For example the sensor may include a camera or optical sensor located adjacent to a display of the device. The user may then be authenticated by comparing the detected biometric attributes with a library of biometric attributes stored by or accessible to the electronic device.

[0007] In some embodiments, the electronic device may authenticate a user based on common attributes of options selected by a user. The electronic device may display several selectable options for selection by the user, and may receive a user selection of a subset of options. The electronic device may then identify one or more attributes common to some or all of the selected option. The attributes may include, for example at least one of, size, color, contour, fill pattern, shape, alignment with other options, the position of an option relative to other options, the source of the option, or any other suitable attribute. The electronic device may then authenticate the user based on the identified attribute. For example, if the user has selected all of the shapes sharing an attribute associated with a particular user, the electronic device may authenticate the user.

[0008] In some embodiments, the electronic device may authenticate a user based on a pattern of inputs received by the device. The electronic device may include a sensor operative to detect several inputs provided by a user. For example, the sensor may include an input mechanism operative to receive inputs provided by a user. As another example, the sensor may include an accelerometer or gyroscope operative to detect motion of or contacts with the electronic device. The electronic device may be operative to identify a pattern of the detected inputs, and to compare the identified pattern with patterns stored in memory to authenticate the user. The patterns may include temporal patterns (e.g., related to the delays between consecutive inputs), visual patterns (e.g., related to attributes of several options selected by the user or inputs provided by the user), or combinations of these. Upon authenticating the user, the electronic device may provide the user with access to restricted electronic device resources.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The above and other objects and advantages of the invention will be apparent upon consideration of the following detailed description, taken in conjunction with the accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

[0010] FIG. **1** is a schematic view of an illustrative electronic device for use with an authentication system in accordance with one embodiment of the invention;

[0011] FIG. **2** is a schematic view of an illustrative display screen of an electronic device in accordance with one embodiment of the invention;

[0012] FIG. **3** is a schematic view of an illustrative display screen directing a user to authenticate in accordance with one embodiment of the invention;

[0013] FIG. **4** is a schematic view of an illustrative display screen for directing a user to authenticate prior to accessing device resources in accordance with one embodiment of the invention;

[0014] FIGS. **5**A-C are schematic views of illustrative display screens associated with different users provided in response to authenticating the user in accordance with one embodiment of the invention;

[0015] FIG. **6** is a schematic view of an illustrative electronic device display for detecting a user's fingerprint in accordance with one embodiment of the invention;

[0016] FIG. **7** is a schematic view of another illustrative electronic device for detecting a user's fingerprint in accordance with one embodiment of the invention;

[0017] FIGS. **8**A and **8**B are schematic views of an illustrative electronic device for detecting a user's handprint in accordance with one embodiment of the invention;

[0018] FIG. **9** is a schematic view of an illustrative electronic device for detecting a user's hand print in accordance with one embodiment of the invention;

[0019] FIG. **10** is a schematic view of an illustrative device having a sensor operative to detect features underneath a user's skin in accordance with one embodiment of the invention;

[0020] FIG. **11** is a schematic view of an illustrative electronic device having a sensor for detecting features of a user's face in accordance with one embodiment of the invention;

[0021] FIG. **12** is a schematic view of an illustrative electronic device having a sensor for detecting features of a user's eyes in accordance with one embodiment of the invention;

[0022] FIGS. **13** and **14** are schematic views of an illustrative display for providing a visual pattern in one embodiment of the invention; and

[0023] FIG. **15** is a flow chart of an illustrative process for authenticating a user in accordance with one embodiment of the invention.

DETAILED DESCRIPTION

[0024] An electronic device having an authentication system for restricting access to electronic device resources is provided. Access to any suitable electronic device resource may be restricted, including for example access to files or data stored on or available to the device. As another example, access to particular applications may be restricted (e.g., applications purchased by particular users, or applications associated with administrative tasks or privileges). As still another example, access to personal settings (e.g., displayed options, background images, or the icons used for applications) may be restricted until the user authenticates.

[0025] Any suitable authentication system may be implemented. In some embodiments, the authentication system may include a system for detecting biometric features or attributes of a user. For example, the electronic device may include a system operative to detect and authenticate a user based on features of or under a user's skin, such as a finger print, hand print, palm print, knuckle print, blood vessel pattern, or any other suitable portion of or under the user's skin. As another example, the electronic device may include a system operative to detect and authenticate a user based on features of a user's eyes or face, or movements of the user's eyes. As still another example, the electronic device may include a system operative to detect features of a user's ear canal, an odor associated with the user, a user's DNA, or any other suitable biometric attribute or information associated with a user.

[0026] In some embodiments, the authentication system may include a system operative to identify a user based on a visual or temporal pattern of inputs provided by the user. For example, the electronic device may display several selectable options or shapes forming a visual pattern. The user may select any suitable predetermined subset of displayed options to authenticate. For example, the user may select one or more options that have a predetermined attribute (e.g., size, color, shape or contour) in common. As another example, the user may select one or more options positioned in predetermined areas of the display (e.g., independent of the attributes of the selected options). The user may select options simultaneously, sequentially, or as a combination of these.

[0027] As another example, the user may provide a series of inputs at a particular pace or in a particular pattern. For example, the user may select options with a particular delay (e.g., pause between two selections). Alternatively, the user may provide inputs detected by a sensor (e.g., an accelerometer or a gyroscope) of the device following a predetermined temporal pattern. The device may detect the inputs from vibrations caused by tapping the device or an area adjacent to the device, moving the device in a particular manner, or any other suitable approach for detecting inputs.

[0028] The electronic device may provide any suitable combination of authentication systems, including for example biometric authentication systems and pattern-based authentication systems, several biometric authentication systems, or several pattern-based systems. In some embodiments, different authentication systems may be associated with different resources, such that a user may provide authentication information for several systems before finally accessing particular restricted resources (e.g., private or personal information). The electronic device may use any suitable approach for selecting which authentication systems to combine. For example, a user may associate several authentication systems with particular resources, or the electronic device may instead automatically (e.g., as a default) assign particular authentication systems to particular resources.

[0029] FIG. **1** is a schematic view of an illustrative electronic device for use with an authentication system in accordance with one embodiment of the invention. Electronic device **100** may include processor **102**, storage **104**, memory **106**, communications circuitry **108**, input/output circuitry **110**, authentication system **112** and power supply **114**. In some embodiments, one or more of electronic device components **100** may be combined or omitted (e.g., combine storage **104** and memory **106**). In some embodiments, electronic device **100** may include other components not combined or included in those shown in FIG. **1** (e.g., a display, bus, or input mechanism), or several instances of the components shown in FIG. **1**. For the sake of simplicity, only one of each of the components is shown in FIG. **1**.

[0030] Processor **102** may include any processing circuitry operative to control the operations and performance of electronic device **100**. For example, processor **100** may be used to run operating system applications, firmware applications, media playback applications, media editing applications, or any other application. In some embodiments, a processor may drive a display and process inputs received from a user interface.

[0031] Storage **104** may include, for example, one or more storage mediums including a hard-drive, solid state drive, flash memory, permanent memory such as ROM, any other suitable type of storage component, or any combination thereof. Storage **104** may store, for example, media data (e.g., music and video files), application data (e.g., for implementing functions on device **100**), firmware, user preference information data (e.g., media playback preferences), authentication information (e.g. libraries of data associated with authorized users), lifestyle information data (e.g., food preferences), exercise information data (e.g., information obtained by exercise monitoring equipment), transaction information data (e.g., information such as credit card information), wireless connection information data (e.g., information that may enable electronic device **100** to establish a wireless connection), subscription information data (e.g., information that keeps track of podcasts or television shows or other media a user subscribes to), contact information data (e.g., telephone numbers and email addresses), calendar information data, and any other suitable data or any combination thereof.

[0032] Memory **106** can include cache memory, semi-permanent memory such as RAM, and/or one or more different types of memory used for temporarily storing data. In some embodiments, memory **106** can also be used for storing data used to operate electronic device applications, or any other type of data that may be stored in storage **104**. In some embodiments, memory **106** and storage **104** may be combined as a single storage medium.

[0033] Communications circuitry **108** can permit device **100** to communicate with one or more servers or other devices using any suitable communications protocol. Electronic device **100** may include one more instances of communications circuitry **108** for simultaneously performing several communications operations using different communications networks, although only one is shown in FIG. **1** to avoid overcomplicating the drawing. For example, communications circuitry **108** may support Wi-Fi (e.g., a 802.11 protocol), Ethernet, Bluetooth™ (which is a trademark owned by Bluetooth Sig, Inc.), radio frequency systems, cellular networks (e.g., GSM, AMPS, GPRS, CDMA, EV-DO, EDGE, 3GSM, DECT, IS-136/TDMA, iDen, LTE or any other suitable cellular network or protocol), infrared, TCP/IP (e.g., any of the protocols used in each of the TCP/IP layers), HTTP, BitTorrent, FTP, RTP, RTSP, SSH, Voice over IP (VOIP), any other communications protocol, or any combination thereof.

[0034] Input/output circuitry **110** may be operative to convert (and encode/decode, if necessary) analog signals and other signals into digital data. In some embodiments, input/output circuitry can also convert digital data into any other type of signal, and vice-versa. For example, input/output circuitry **110** may receive and convert physical contact inputs (e.g., from a multi-touch screen), physical movements (e.g., from a mouse or sensor), analog audio signals (e.g., from a microphone), or any other input. The digital data can be provided to and received from processor **102**, storage **104**, memory **106**, or any other component of electronic device **100**. Although input/output circuitry **110** is illustrated in FIG. **1** as a single component of electronic device **100**, several instances of input/output circuitry can be included in electronic device **100**.

[0035] Electronic device **100** may include any suitable mechanism or component for allowing a user to provide inputs to input/output circuitry **110**. For example, electronic device **100** may include any suitable input mechanism, such as for example, a button, keypad, dial, a click wheel, or a touch screen. In some embodiments, electronic device **100** may include a capacitive sensing mechanism, or a multi-touch capacitive sensing mechanism. Some sensing mechanisms are described in commonly owned U.S. patent application Ser. No. 10/902,964, filed Jul. 10, 2004, entitled "Gestures for Touch Sensitive Input Device," and U.S. patent application Ser. No. 11/028,590, filed Jan. 18, 2005, entitled "Mode-Based Graphical User Interfaces for Touch Sensitive Input Device," both of which are incorporated herein in their entirety.

[0036] In some embodiments, electronic device **100** can include specialized output circuitry associated with output devices such as, for example, one or more audio outputs. The audio output may include one or more speakers (e.g., mono or stereo speakers) built into electronic device **100**, or an audio component that is remotely coupled to electronic device **100** (e.g., a headset, headphones or earbuds that may be coupled to communications device with a wire or wirelessly).

[0037] In some embodiments, I/O circuitry **110** may include display circuitry (e.g., a screen or projection system) for providing a display visible to the user. For example, the display circuitry may include a screen (e.g., an LCD screen) that is incorporated in electronics device **100**. As another example, the display circuitry may include a movable display or a projecting system for providing a display of content on a surface remote from electronic device **100** (e.g., a video projector). In some embodiments, the display circuitry can include a coder/decoder (Codec) to convert digital media data into analog signals. For example, the display circuitry (or other appropriate circuitry within electronic device **100**) may include video Codecs, audio Codecs, or any other suitable type of Codec.

[0038] The display circuitry also can include display driver circuitry, circuitry for driving display drivers, or both. The display circuitry may be operative to display content (e.g., media playback information, application screens for applications implemented on the electronic device, information regarding ongoing communications operations, information regarding incoming communications requests, or device operation screens) under the direction of processor **102**.

[0039] Authentication system **112** may include any suitable system or sensor operative to receive or detect an input identifying the user of device **100**. For example, authentication system **112** may include a skin-pattern sensing mechanism, an optical system for identifying users based on their facial patterns, eye features (e.g., retinas), or vein patterns, or any other sensor for detecting any other unique biometric feature or attribute of a user. As another example, authentication system **112** may be operative to receive secret or confidential entries identifying the user (e.g., gestures on the device, or touching a particular pattern of objects or colors on a display). As still another example, authentication system **112** may be operative to detect particular movements or vibrations of the device caused by the user. Authentication system **112** may be combined or embedded in any other element of electronic device **112** (e.g., a display or a camera), or use events detected by various sensors of the electronic device (e.g., an accelerometer or proximity sensor). In some embodiments, several types of authentication systems may be combined or implemented in the electronic device.

[0040] In some embodiments, electronic device **100** may include a bus operative to provide a data transfer path for

transferring data to, from, or between control processor **102**, storage **104**, memory **106**, communications circuitry **108**, input/output circuitry **110** authentication system **112**, and any other component included in the electronic device.

[0041] To prevent unauthorized access to data or information stored in memory or storage, the electronic device may direct an authentication system to identify the user and authorize access to requested resources. The electronic device may require authorization prior to providing access to any electronic device resource. In some embodiments, the electronic device may require different levels of authorization before providing access to different applications or different data or files associated with different applications. For example, the electronic device may require a user to satisfy several authentication systems prior to providing access to an application or data (e.g., a secondary authentication, for example using biometrics, in addition to a first or initial authentication, for example a pass code used to unlock the device).

[0042] FIG. **2** is a schematic view of an illustrative display screen of an electronic device in accordance with one embodiment of the invention. Display screen **200** may be displayed in response to a user unlocking the electronic device. Display screen **200** may include selectable options **210** for accessing various device functions. For example, each option **210** may be associated with different applications available on the electronic device. As another example, each option may be associated with particular data or files available to the user. The electronic device may or may not require authentication to access display **200**. For example, display **200** may include basic or default applications available to the user. As another example, display **200** may include default features available to all users.

[0043] In some embodiments, one or more applications may provide access to or use data or resources that are personal to one or more users. For example, options **212** and **214**, associated with telephone and mail applications, respectively, may involve personal accounts or contacts that are not associated with every user of the electronic device. Prior to providing access to such applications, or to personal or confidential features or resources available via such applications, the electronic device may require the user to authenticate. In some embodiments, default features of applications may be available without authentication (e.g., allow all users to place telephone calls, but not to access a contact list).

[0044] FIG. **3** is a schematic view of an illustrative display screen directing a user to authenticate in accordance with one embodiment of the invention. Display screen **300** may be displayed in response to receiving an instruction from a user to access resources (e.g., information or an application) restricted by an authentication protocol. Display screen **300** may include information **310** associated with the selected resources. To prevent an unauthorized user from viewing the resources prior to authorization, information **310** may be blurred or hidden from view (e.g., entries in particular field may be unobtainable). In some embodiments, display screen **300** may instead include no information until the user is authenticated.

[0045] Display screen **300** may include notice **320** instructing the user to authenticate before accessing the requested resources. Notice **320** may include a pop-up, overlay, new display screen, or any other suitable type of display for providing an instruction to the user. Notice **320** may include any suitable instruction, including for example a manner in which the user is to authenticate (e.g., specifying a particular authentication system to use). For example, notice **320** may direct the user to provide a fingerprint or provide an input that matches a predefined visual or temporal pattern. Once the user authenticates properly, the electronic device may display information **310** in a manner discernable by the user, and enable selectable options or other functions associated with the selected resource.

[0046] In some embodiments, a user may be required to authenticate prior to unlocking the electronic device (e.g., prior to accessing any resource of the device). FIG. **4** is a schematic view of an illustrative display screen for directing a user to authenticate prior to accessing device resources in accordance with one embodiment of the invention. Display screen **400** may include option **410** for unlocking the display. For example, option **410** may include a slider operative to be dragged across a portion of the screen. As another example, option **410** may include an option or series of options for the user to select (e.g., simultaneously or sequentially press several keys or touch several areas of display screen **400**).

[0047] Display screen **400** may include notice **420** directing the user to authenticate prior to accessing the device resources (e.g., the home screen from which information and applications are launched). Notice **420** may include any suitable type of notice, including for example a pop-up, overlay, new display screen, or any other suitable type of display for providing an instruction to the user. The electronic device may display notice **420** at any suitable time, including for example when the user turns on the device (e.g., and views display screen **400**), in response to the user attempting to access device resources without first authenticating (e.g., as an error message), in response to a user request for help, or at any other suitable time. Notice **420** may include any suitable instruction, including for example a manner in which the user is to authenticate, a list of authorized users, or any other suitable information.

[0048] Once the user has been properly authenticated, the electronic device may display options associated with the authenticated user (e.g., options for applications purchased by particular users). In some embodiments, the electronic device may provide access to resources or content that was previously not available (e.g., contact lists or previous messages in a telephone or mail application). FIGS. **5**A-C are schematic views of illustrative display screens associated with different users provided in response to authenticating the user in accordance with one embodiment of the invention. Display screen **500**A may include several options **510**A. The displayed options may include some options common to a default or basic display of the electronic device (e.g., display screen **500**A shares options with display screen **200**, FIG. **2**). Display screen **500**A may include several options **512**A for additional applications or resources only available to the particular authenticated user. For example, display screen **510**A may include additional options **512**A for game, system and media applications.

[0049] Display screen **500**B may include options **510**B for resources or applications available to the users. In some embodiments, options **510**B may be entirely different from the options of a default screen (e.g., display screen **500**B shares no options display screen **200**, FIG. **2**). Display screen **500**B may be further customized to not include labels identifying the applications or resources associated with options **510**B.

[0050] Display screen **500**C may include options **510**C for resources or applications available to the users. In some

embodiments, options **510**C for the same resources as other display screens may have different appearances (e.g., different icons). For example, in FIG. **5**C, the options displayed for the Mail, Clock, Photos, YouTube, and Calculator applications may be different than those displayed in display screen **500**A of FIG. **5**A. Display screen **500**C may in addition include a custom or personal background **512**C (e.g., different background image). In some embodiments, display screen **500**C may not include a dock or other feature for maintaining some options **510**C in a fixed position (e.g., unlike options **510**B located in dock **512**B).

[0051] In some embodiments, the electronic device may provide access to different amounts of electronic device resources based on the identity of the authenticated user. For example, if an electronic device is used by several users (e.g., parents and children in the same family), the users may share some but not all of the resources (e.g., all users may have access to the family contact list, but not to other family members' e-mail). As another example, users of the electronic device may be organized in groups or tiers of users. Some resources may be associated with groups or tiers or users, instead of or in addition to particular users. When a particular user is authenticated and identified as being part of a group, the electronic device may provide the user with access to the resources associated with the group (e.g., common or shared contacts, shared communications, or shared documents) and to the resources associated with the particular user (e.g., personal contacts, e-mail accounts, and telephone call lists).

[0052] The electronic device may associate particular resources with one or more authentication systems. For example, a user may identify a resource and provide a protect or secure instruction (e.g., by selecting an appropriate option). A user may in addition select one or more authentication systems to satisfy before providing access to the resource. If the resource is not public (e.g., not a default application or file to remain available to all users), or if the resource was created or purchased by the user, the electronic device may associate the selected resource with the one or more selected authentication systems. Alternatively, if the user has sufficient privileges (e.g., an administrator), any resource may be secured using one or more selected authentication systems.

[0053] The electronic device may not require a user to authenticate each time the user unlocks or operates the electronic device. In some embodiments, the electronic device may allow a user to authenticate for a particular amount of time. For example, once authenticated, the electronic device may allow a user to access restricted resources for 10 hours from the time the user authenticated. As another example, the electronic device may retain the user's authentication for a particular amount of time after having received the user's last instruction or having entered a stand-by mode (e.g., retain authentication for thirty minutes after an input). The amount of time the electronic device retains authentication information may be set by the device or by the user, and may be based on the particular types or resources protected by the authentication information (e.g., allow for a longer authentication period for access to a game purchased by a particular user than to a user's personal contacts). Not requiring the electronic device to authenticate each time the user operates the device may save power consumption.

[0054] The electronic device may use any suitable type of authentication system to prevent unauthorized access of device resources. In some embodiments, the electronic device may include an authentication system based on a user's unique skin patterns. For example, the electronic device may include an authentication system operative to detect a user's finger, hand, palm, knuckle print, or any other suitable print or skin feature unique to the user. The authentication system may include a sensor operative to detect the user's unique skin pattern or feature.

[0055] The sensor may include any suitable type of sensor for detecting unique features or patterns of a user's skin. For example, the sensor may include an optical scanner operative to detect features of the user's skin. The optical sensor may include a charge coupled device, or any other suitable array of light-sensitive components (e.g., diodes) operative to record the light received by the sensor (e.g., a charge coupled device). For example, if a charge coupled device includes an array of light-sensitive components, the optical sensor may be operative to record, for each light sensitive component of the array, a pixel representing the light received by the particular light sensitive component. The value of each pixel may then reflect the distance from the sensor of the particular portion of the user's skin associated with the pixel (e.g., a ridge or valley). The recorded pixels may form an image, for example of a particular portion of the user's skin, that the electronic device can compare to a library of images associated with authorized users.

[0056] As another example, the sensor may include a capacitive sensor operative to detect features of a user's skin. The capacitive sensor may include one or more chips containing an array of cells, each of which may include at least two conductor plates separated by an insulating layer. The sensor may be coupled to an inverting amplifier operative to change the voltage between the at least two conductor plates of each cell in the chip. When a user's finger is placed over the array of cells, the sensor may be operative to distinguish the cells over which a valley (e.g., a fingerprint valley) and a ridge (e.g., a fingerprint ridge) are placed from the different capacitance values of each cell (i.e., cells under a valley will have a lower capacitance than cells under a ridge). Using the detected capacitance values of each cell in the chip, the sensor may generate an image or a representation of the skin placed over the sensor that can be compared to a library of images or representations available to the electronic device.

[0057] The authentication system may include any suitable countermeasure for preventing an unauthorized user from spoofing an authorized user's skin patterns, for example by placing an image (e.g., a printed image) or a three-dimensional structure (e.g., a polymer cast) adjacent to the authentication system sensor. For example, the authentication system may include a combination of optical and capacitance sensors, a sonar or radio-frequency sensor, a sensor for detecting a user's pulse, a heat sensor for determining the temperature of the object placed against the sensor (e.g., to determine if the temperature is within a range of expected human skin temperatures), or any other suitable countermeasure.

[0058] The sensor may be operative to detect features of the user's skin using any suitable approach. In some embodiments, the sensor may be operative to detect features of the user's skin when the user's skin is moved over the sensor. For example, the sensor may include a one-dimensional sensor or stagnant sensor (e.g., a line of sensing components) operative to detect features of a user's finger as it slides or rolls over the sensor. The sensor may include an orientation in which the user's skin is to move to provide an accurate representation of

the user's skin features. For example, the sensor may require a user to move a fingertip along the axis of the finger or perpendicular to the axis of the finger.

[0059] In some embodiments, the sensor may be operative to detect features of the user's skin when the skin is held immobile over the sensor. For example, the sensor may include a two-dimensional sensor or moving sensor operative to detect features of the user's finger when the finger is stationary over the sensor. The sensor may be operative to move at a regular pace or speed under the user's immobile finger, or detect an instantaneous or near-instantaneous two-dimensional representation of the user's finger at a point in time (e.g., as the user's finger moves over the sensor). Using a two-dimensional sensor may provide a more accurate representation of the user's skin features, as a two-dimensional sensor does not depend on the user moving his skin over the sensor at a regular or even pace, unlike a one-dimensional sensor.

[0060] The sensor may be placed at any suitable location within the electronic device. In some embodiments, the sensor may be placed such that it is operative to detect an appropriate portion of the user's skin as the user operates or begins to operate the electronic device. The sensor position may vary based on the portion of the user's skin to be detected (e.g., finger, hand or palm). FIG. **6** is a schematic view of an illustrative electronic device display for detecting a user's fingerprint in accordance with one embodiment of the invention. Display **600** may include screen **602** instructing the user to unlock the electronic device. For example, screen **602** may include block **610** having an arrow instructing the user to slide block **610** along track **612** to unlock the electronic device, for example by placing a finger on block **610** and dragging the finger along track **612**.

[0061] To authenticate the user during the unlocking process, display **600** may include sensor **620** in the display along track **612**. For example, sensor **620** may be embedded in the display stack (e.g., among the display stack that may include a capacitance sensing component, a light source, and a display surface). As another example, sensor **620** may be placed underneath the display stack. As still another example, sensor **620** may include an existing component of the display stack (e.g., the display stack for a touch screen display may include a capacitance sensor). In such an approach, the authentication system may use the detected output of a capacitance sensing component of the display stack (e.g., in a touch screen display) that has a sufficient resolution for distinguishing ridges and valleys of a user's skin. In some embodiments, the capacitance sensing component of the display stack may include several types or densities of capacitance sensing components to allow for authentication using particular portions of the display (e.g., use very fine sensing components in the display stack along at least a portion of track **612** for authentication and less fine sensing components in the remaining areas of display **600**).

[0062] In some embodiments, sensor **620** may be embedded in the electronic device such that it is not visible in display **600**. For example, sensor **620** may be assembled, printed or etched directly on display **600** (e.g., etched on glass) such that the user cannot see the fingerprint scanner. If a user has difficulty providing a suitable fingerprint to sensor **620**, display **600** may highlight the outlines of sensor **620** (e.g., display an icon directing the user to place a finger on the icon over sensor **620**) to assist the user in authenticating.

[0063] FIG. **7** is a schematic view of another illustrative electronic device for detecting a user's fingerprint in accordance with one embodiment of the invention. Electronic device **700** may include input mechanisms **710** and **712** that the user may actuate to provide inputs to electronic device **700**. For example, input mechanism **710** may include a keyboard, and input mechanism **712** may include a touchpad or track pad. It will be understood, however that any other input mechanism, including input mechanism remotely coupled to electronic device **700** (e.g., a wired or wireless mouse) may be used with electronic device **700**.

[0064] To provide for secure access to resources, electronic device **700** may include at least one sensor **720** operative to detect features of a user's fingerprint to identify the user. To provide a seamless user experience, the sensors **720** may be embedded in or under at least one of input mechanism **710** and **712**. In some embodiments, input mechanism **710**, which may include several distinct keys that a user may press to provide inputs to electronic device **700**, may include a sensor **720** embedded in one or more keys. For example, an optical or capacitive sensor may be placed at the top surface of a key such that when a user places a finger on the key (e.g., rests his index fingers on the "F" or "J" keys), the sensor may detect features of the user's fingertips for authenticating the user. A two-dimensional or moving sensor may be used for this implementation to authenticate the user while the user's fingers are placed over the keys.

[0065] A sensor **720** may be placed in, adjacent to or behind any button or other physical input that a user may press in an electronic device. For example, a sensor **720** may be placed behind a home button of a portable media player or cellular telephone (e.g., button **812**, FIG. **8**B). Sensor **720** may be placed between an outer cover or surface (e.g., a glass or plastic surface) and a mechanical component operative to interact with a switch or electronic circuit. For example, an fingerprint sensing mechanism may be embedded underneath a transparent surface operative through which the sensing mechanism may detect a user's fingerprint ridges and valleys. In some embodiments, no additional transparent surface may be necessary (e.g., if the sensing mechanism includes a surface on which a user may place a finger).

[0066] In some embodiments, input mechanism **712** may include a sensor **720** embedded underneath some or all of the pad such that when a user places a finger on input mechanism **712** (e.g., to move an indicator on display **715**), sensor **720** may detect the features of the user's finger for authenticating the user. Sensor **720** used may be a one-dimensional sensor, authenticating the user as the user moves his fingers across the pad, or a two-dimensional sensor operative to authenticate the user when the user's finger is immobile on the pad (e.g., when the user first places his finger on the pad). Sensor **720** may cover the entire surface of input mechanism **712** such that the user need not place his fingers over a particular portion of input mechanism **712** to be authenticated. Electronic device **700** may be operative to identify the position of each sensor **720** to assist the user in providing an adequately detectable input, for example using a highlight, indication on the display, or any other suitable approach. In some embodiments, any other suitable input mechanism may include a sensor **720** operative to seamlessly detect the user's fingerprint features (e.g. a button, wheel, key or screen).

[0067] FIGS. **8**A and **8**B are schematic views of an illustrative electronic device for detecting a user's handprint in accordance with one embodiment of the invention. Electronic

device **800** may include housing **802** operative to retain display **810**. Housing **802** may substantially constitute the back surface of electronic device **800** (e.g., the surface that does not include display **810**) to protect the components of the electronic device. When a user holds electronic device **800**, the user's hand **830** may be cupped around housing **802** leaving display **810** visible such that at least the user's palm **832** is placed against back surface **804**, as shown in FIG. **8**B. Electronic device **800** may include sensor **820** embedded in back surface **804** and operative to detect features of a user's palm or hand. By placing sensor **820** on back surface **802** (or any surface of the electronic device that is opposite the surface of display **810**), sensor **820** may authenticate the user when the user holds electronic device **800**. Sensor **820** may include a two-dimensional sensor, thus allowing electronic device **800** to seamlessly authenticate the user without requiring the user to move or slide a hand against back surface **804**.

[0068] FIG. **9** is a schematic view of an illustrative electronic device for detecting a user's hand print in accordance with one embodiment of the invention. Electronic device **900** may include input mechanism **910** with which a user may provide inputs to the device. Input mechanism **910** may be positioned such that a user's fingers are placed over input mechanism **910** while the user's palms and wrists are placed on or extend over housing **912**. Electronic device **900** may include one or more sensors **920** embedded in or placed on housing **912** to authenticate a user of the device. Sensors **920** may be located such that the user's hands, palms or wrists are aligned with sensors **920** when the user places his hands over housing **912** to operate input mechanism **910**. Sensors **920** may be operative to detect features of the user's skin when the user's hands are placed over housing **912**, for example using a two-dimensional sensor.

[0069] In some embodiments, the authentication system may instead or in addition include a sensing mechanism for detecting features underneath a user's skin. For example, the authentication system may include a sensor operative to detect the pattern of a user's veins, arteries, follicle distribution, or any other suitable feature underneath the user's skin that may be detected. The sensor may include any suitable type of sensor, including for example an optical sensor (e.g., a camera) located on the surface of the electronic device. The sensor may be positioned so as to detect a feature underneath any suitable portion of the user's skin when the electronic device is in use. For example, the sensor may be positioned to detect features underneath a user's skin in an area of the user's fingers, hand, wrist, arm, face, or any other suitable area.

[0070] FIG. **10** is a schematic view of an illustrative device having a sensor operative to detect features underneath a user's skin in accordance with one embodiment of the invention. Electronic device **1000** may include input mechanism **1010** located on or extending through a portion of housing **1012**. Input mechanism **1010** may be configured such that when in use, a user's hands and wrists are placed over housing **1012** (e.g., instead of over input mechanism **1010**). Electronic device **1000** may include sensor **1020** operative to detect features underneath a user's skin. For example, sensor **1020** may include an optical sensor operative to detect a user's vein patterns near the user's wrists. Sensor **1020** may be located on any suitable surface of electronic device **1000**, including for example on or embedded in housing **1012** such that the user's wrists may be adjacent to sensor **1020** when the user's hands are positioned to provide an input using input mechanism **1010**. Such a positioning may allow for a seamless authentication of the user by detecting features underneath the user's skin (e.g., a vein pattern by the user's wrist) while the user operates device **1000**.

[0071] In some embodiments, the authentication system may instead or in addition include a sensor operative to detect features of the user's face. For example, the authentication system may include a sensor operative to detect radiation emitted or reflected by one or more distinctive features of the user's face when the user's face is placed opposite the sensor. The sensor may be operative to detect any suitable type of radiation. For example, the sensor may include a light sensor (e.g., a camera), an infra-red sensor, an ultra-violet sensor, a scanning laser, an ultrasound sensor (e.g., sonar), or any other sensor operative to detect a desired radiation (e.g., a particular range of radiation frequencies or periods).

[0072] The authentication system may be operative to detect any suitable element of the user's face. For example, the authentication system may identify faces by analyzing the relative to position and size of a user's head, nose, mouth, ears, cheekbones, jaw, or any other attribute of the user's face. As another example, the authentication system may identify features of the user's face using a three-dimensional authentication system to capture and analyze curved surfaces or depths of a user's facial features (e.g., contour of eye sockets, chin or nose). As still another example, the authentication system may detect unique lines, patterns or spots of the user's skin (e.g., using skin texture analysis). To enhance or facilitate authentication, combinations of these approaches may be used.

[0073] The sensor for detecting features of the user's face may be located at any suitable position on the electronic device. In some embodiments, the sensor may include a camera or other sensor provided with the electronic device for a different purpose (e.g., an embedded webcam for chatting). FIG. **11** is a schematic view of an illustrative electronic device having a sensor for detecting features of a user's face in accordance with one embodiment of the invention. Electronic device **1100** may include sensor **1120** located adjacent to display **1110** such that the user's face, and the features of interest of the user's face may be aligned with sensor **1120** (e.g., in the field of view of sensor **1120**) when the user faces display **1110** to view or access electronic device resources. In response to detecting a user's face opposite sensor **1120**, electronic device **1100** may direct sensor **1120** to capture and analyze features of the user's face, and compare the analyzed features with a library of features associated with authorized users. If an authorized user is detected, electronic device **1100** may display or provide access to restricted content **1112** on display **1110**.

[0074] In some embodiments, the authentication system may instead or in addition include a sensor operative to authenticate a user based on attributes of the user's eyes. For example, the sensor may be operative to scan a user's retina, iris or retinal blood vessels to detect unique patterns of the user. The sensor may include a light source operative to emit light, for example infrared light, to be reflected by the user's eye and detected by a lens or optical sensor. The sensor may analyze the received light to create a representation of the user's eyes that can be compared with a library of authorized user's eyes.

[0075] As another example, the sensor may instead or in addition be operative to detect movements of the user's eyes, for example by tracking the position and movement of a user's retina, iris, blood vessels, or any other feature of the

user's eyes. Before providing a user with access to electronic device resources, the electronic device may direct the sensor to detect a predetermined eye movement set up by an authorized user. For example, each authorized user may create an eye movement track by moving his eyes in a particular manner (e.g., up, down, left, right, blink, blink) while looking at the sensor. When a user of the device moves his eyes in a manner that matches a predetermined eye movement, the electronic device may unlock the device or provide access to restricted resources.

[0076] The sensor may be located at any suitable position of the device, including for example adjacent to a display or other portion of the device that will face the user's eyes (e.g., a position similar to that of sensor **1120**, FIG. **11**, which may be used to authenticate a user from features of the user's eyes). FIG. **12** is a schematic view of an illustrative electronic device having a sensor for detecting features of a user's eyes in accordance with one embodiment of the invention. Electronic device **1200** may include sensor **1220** located adjacent to display **1210** such that the user's eyes may be aligned with sensor **1220** (e.g., in the field of view of sensor **1220**) when the user faces display **1210** to view or access electronic device resources. Using sensor **1220**, electronic device **1200** may detect features or movements of a user's eyes to authenticate the user and provide access to restricted device resources. In some embodiments, sensor **1220** may be implemented to authenticate a user based on features of the user's face (e.g., like sensor **1120**, FIG. **11**).

[0077] In some embodiments, the authentication may be operative to authenticate users based on attributes or qualities of their voices. For example, the authentication system may be operative to detect a particular voice pitch or voice signature. The authentication system may be text dependent (e.g., the user must say a particular phrase to authenticate, such as "my voice is my passport") or text independent (e.g., any suitable words may be said to authenticate the user). In some embodiments, the authentication system may require the user to say a secret password to authenticate, thus requiring both knowledge of the user's password and the user's voice pitch to properly authenticate. The authentication system may include any suitable component for authenticating a user, including for example a microphone. In some embodiments, the microphone may be primarily used for other purposes (e.g., telephone communications or video conferencing). In some embodiments, other types of authentication systems may be used. In some embodiments, the authentication system may be operative to identify and authenticate users from the shape of their ear canals. For example, the authentication system may include a sensor (e.g., optical, radar or sonar) operative to detect unique features of a user's ear canal (e.g., shape and length). The sensor may be located, for example, near a speaker of the device (e.g., if the device is a telephone). In some embodiments, the authentication system may be operative to identify a user based on an odor particular to the user. For example, the authentication system may include a sensor operative to detect unique attributes of the odor of a user's skin or sweat glands. The sensor may be located at any suitable position on the device, including for example at or near an input mechanism (e.g., where the user touches the device).

[0078] In some embodiments, the authentication system may be operative to identify a user based on a DNA sequence. For example, the authentication may include a sensor coupled to a processor that is operative to receive a cell having the user's DNA (e.g., from the user's skin or mouth) and determine whether a particular DNA sequence is present. The length or variation in DNA sequence may be selected to both ensure that proper authentication is provided and that the authentication process is sufficiently quick (e.g., the entire DNA strand need not be analyzed). The sensor may be positioned at any suitable location on the device, including for example on or adjacent to input mechanisms or other components that a user may touch.

[0079] The electronic device may receive biometric information reflecting authorized users using any suitable approach. For example, when a user selects an authentication system to use with particular device resources, the electronic device may direct the user to provide biometric information (e.g., a fingerprint, eye scan, or DNA sequence) to be stored in a library. The electronic device may direct the user to provide the biometric input using any suitable approach, including for example using visual cues, audio cues, and highlighting or identifying the location of the authentication system sensor. Received biometric information stored in the library may be retrieved when a user attempts to authenticate, and compared to the biometric information provided by the user. If the provided biometric authentication information matches information stored in the library (e.g., information associated with a requested resource), the electronic device may provide access to a restricted resource. In some embodiments, a similar approach may be used to receive non-biometric authentication information.

[0080] In some embodiments, the authentication system may instead or in addition not require biometric parameters to provide access to electronic device resources to users. Although non-biometric authentication systems may be, in some cases, easier to circumvent than biometric authentication systems, the non-biometric authentication systems may nevertheless be highly effective and secure. In some embodiments, the authentication system may provide access to electronic device resources in response to detecting that a key or token is within a particular distance of the electronic device. For example, a user may have a cellular telephone and a computer. One or both devices may include circuitry for detecting that the devices are within a particular range of each other (e.g., 5 feet so that a user may sit at a desk to use the computer with the cellular telephone in his pocket and authenticate). When the devices determine that they are in proximity, resources of one or both devices may become available. This approach may be particularly useful to secure access to static devices while taking advantage of the fact that a user may keep a portable device on his person. This and other embodiments are described in more detail in commonly owned U.S. patent application Ser. No. 11/823,656, filed Jun. 27, 2007 (Attorney Docket No. 104677-0059-101, P4884US1).

[0081] In some embodiments, the electronic device may authenticate a user based on a particular sequence of inputs provided by the user. For example, the electronic device may require the user to provide an input corresponding to a visual pattern provided by the electronic device. FIGS. **13** and **14** are schematic views of an illustrative display for providing a visual pattern in one embodiment of the invention. Display **1300** may include distribution **1310** of options or shapes **1312**. Display **1400** may include distribution **1410** of options or shapes **1412**. Each shape **1312** and **1412** may have a different fill pattern (e.g., different line orientations), color or colors, shape or contour, size (e.g., periphery or area), prox-

imity to or position relative to other displayed shapes, alignment with other shapes (e.g., select four yellow shapes that form a straight line), source (e.g., shapes representing pictures in a particular album or library), or any other suitable characteristic. Distributions **1310** and **1410** may include any suitable number and distribution of shapes, including for example a number of evenly distributed shapes (e.g., 20 evenly distributed shapes **1310**) or a seemingly arbitrary distribution of shapes (e.g., arbitrarily distributed shapes **1410**).

[0082] To authenticate, the user may select (e.g., as detected by an input mechanism or other sensor) any suitable subset of the displayed shapes or options. The subset may include some or all of the shapes that share one or more attributes. For example, the user may select some or all of the shapes that are of a particular color (e.g., all shapes that include a shade of yellow). As another example, the user may select some or all shapes that have the same contour (e.g. all squares). As still another example, the user may select some or all shapes that have a particular attribute in common (e.g., all 5-sided shapes, or all shapes representing pictures associated with a particular album stored by the device). As yet still another example, the user may select some or all shapes that include a particular distribution of colors (e.g., shapes that include a red portion adjacent to a blue portion). Any suitable criteria or attribute (including combinations of the examples listed above, such as selecting the top two blue shapes and the bottom two square shapes) may be used to select the particular subset of displayed shapes.

[0083] Any suitable number of shapes or options may be associated with the subset to select for authentication. For example, the number of shapes may be related to the total number of displayed shapes (e.g., select 20% of the displayed shapes). As another example, the number of shapes may be a fixed number, for example less than five (e.g., so that the user can simultaneously select all shapes using one hand) or ten (e.g., so that the user can simultaneously select all shapes using both hands). The number of shapes may be selected to optimize security (e.g., require enough shapes that it is too difficult to simply guess which shapes to select).

[0084] The user may select the subset of the shapes using any suitable approach. If a multi-touch display is provided, the authentication system may require the user to simultaneously select all of the shapes used for authentication. As another example, the authentication system may allow the user to sequentially select the shapes used for authentication. The shapes may be selected in an arbitrary or particular order (e.g., from top to bottom or left to right). As still another example, the authentication system may require the user to provide a single, moving input (e.g., dragging a finger across the display) selecting only the shapes of the authorized subset. Any other suitable approach for selecting the subset of shapes may be used.

[0085] To avoid having the user always select shapes displayed in the same relative position on the display (e.g., like entering a numeric pass code using a displayed keypad), the electronic device may change the distribution of the shapes to select for authentication. To authenticate, the user may then identify the shapes that share the attribute associated with the authentication protocol. Because the position of the shapes used to authenticate may change each time the user accesses device resources, someone looking over the user's shoulder to see the general distribution of the selected shapes may not be able to select shapes with the same distribution to authenticate (e.g., the striped shapes may not be distributed in the same areas of the device).

[0086] After each failed attempt at selecting shapes for authentication, the electronic device may change the distribution of the displayed shapes, or even change the shapes (e.g., use different colors or contours) to prevent an unauthorized user from guessing the proper subset of shapes. The electronic device may lock the device resources after a particular number of failed attempts to select the proper subset of shapes. Once locked, a user may need to couple the device with a host to re-enable the device (e.g., couple a mobile device to a fixed device) or use another authentication system (e.g., a biometric system) to re-enable the device.

[0087] In some embodiments, rather than selecting particular shapes, the user may simply select the shapes located in pre-determined portions of the screen. For example, the user may place one or more fingers over several shape positions independent of the actual displayed shape. As another example, the user may place one or more fingers over particular shapes displayed by the electronic device, and move the one or more fingers in a predetermined manner (e.g. slide one or more fingers), independent of the displayed shapes. As still another example, the user may successively select several shapes located at predetermined positions on the display (e.g., select shapes at particular locations to form a predetermined pattern). The electronic device may, in some embodiments, provide a blank or uniform display on which the user may draw one or more patterns using one or more fingers. Such an approach may confuse or distract unauthorized users by creating a visual distraction via the displayed shapes.

[0088] In some embodiments, the electronic device may authenticate a user based instead or in addition on a received temporal pattern of inputs by the user. For example, the user may provide a particular number of inputs at a particular rate to authenticate. The electronic device may detect the inputs using any suitable approach. For example, the electronic device may detect inputs provided using an input mechanism of the device (e.g., inputs received by a touch screen). As another example, the electronic device may detect inputs from motion, contacts, vibrations or other impacts detected by an appropriate sensor of the device (e.g., an accelerometer). In such an approach, a user may tap any portion of the device (or a body in contact with the device, such as a table on which the device is placed) such that the sensor in the device detects the taps and determines whether they correspond to an authorized temporal pattern. As still another example, the electronic device may detect that it has been moved in a particular manner (e.g., shaken twice then spun) using a sensor in the device (e.g., an accelerometer or gyroscope). In response to detecting a correct temporal pattern, the electronic device may provide access to restricted resources.

[0089] In some embodiments, the authentication system may combine temporal and visual patterns for authentication. For example, a user may be required to select particular displayed shapes at a certain rate (e.g., the first two shapes quickly, then a pause before simultaneously selecting the last two). As another example, the user may be required to first select the proper shapes then provide an input for a temporal pattern. As still another example the user may be required to select one or more shapes and move the device (e.g., shake the device). Any other suitable combination of inputs may be required for authentication.

[0090] The electronic device may set up visual or temporal patterns for authorized users using any suitable approach. In some embodiments, when a user selects to use a temporal or visual pattern to restrict access to particular device resources, the electronic device may direct the user to provide or select the temporal or visual pattern. For example, the electronic device may provide a list of shape attributes that the user may select to form a pattern (e.g., a color or a contour). As another example, the electronic device may direct the user to select displayed shapes or provide a temporal pattern, and extract or identify the pattern from the received inputs. The electronic device may direct the user to provide a pattern several times before it is accepted to ensure that the user intended and remembers the selected pattern.

[0091] The electronic device may include any suitable number and types of authentication systems. For example, the electronic device may include one, more or all of the authentication systems or authentication approaches described above. Access to different resources may be restricted using one or more authentication systems, which a user may select or set up. In some embodiments, several authentication systems may be used sequentially before access to particular restricted resources is provided.

[0092] FIG. **15** is a flow chart of an illustrative process for authenticating a user in accordance with one embodiment of the invention. Process **1500** may begin at step **1502**. At step **1504**, the electronic device may identify the user of the device. For example, the electronic device may receive a username or password associated with the user. As another example, the electronic device may receive authentication information using an authentication system and identify the user from the received authentication system. The electronic device may automatically receive authentication information without requiring an express input from the user, for example by placing a sensor of the authentication system in a manner that seamlessly captures authentication information as the user operates the device. As another example, the sensor may be operative to detect features of attributes of the user as soon as the user is within the field of view or sensing region of the sensor. In some embodiments, process **1500** may move directly from step **1502** to step **1506**.

[0093] At step **1506** the electronic device may determine whether a request to access restricted resources was received. For example, the electronic device may determine whether the user provided an instruction to access data associated with a particular user (e.g., a contact list or other personal information). As another example, the electronic device may determine whether the user provided an instruction to access a restricted application (e.g., an application restricted to a particular tier of users, such as administrators, or an application purchased by a particular user). If the electronic device determines that no instruction to access restricted resources was received, process **1500** may return to step **1506** and continue to monitor inputs received from the user.

[0094] If, at step **1506**, the electronic device instead determines that an instruction to access restricted resources was received, process **1500** may move to step **1508**. At step **1508**, the electronic device may determine whether the identified user is authorized to access the resources. For example, the electronic device may determine whether the user has provided suitable authentication information for accessing the restricted resources. The electronic device may receive suitable authentication information without the user's knowledge, for example by embedding an authentication sensor in the device such that authentication information is received during normal use. If the electronic device determines that the identified user is not authorized, process **1500** may move to step **1510**. At step **1510**, the electronic device may instruct the user to authenticate. For example, the electronic device may direct the user to provide authentication information to an authentication system (e.g., any of the authentication systems described above). In some embodiments, the electronic device may detect several inputs by the user, and determine whether the inputs have a pattern or share attributes associated with an authorized user (e.g., determine whether the user has provided the proper inputs that correspond to an attribute or pattern of an authorized user, or determine whether the attribute or pattern of the inputs matches an attribute or pattern associated with authorized users). Process **1500** may then return to step **1508** to determine whether the user has provided suitable authentication information.

[0095] If, at step **1508**, the electronic device instead determines that the user is authorized, process **1500** may move to step **1512**. At step **1512**, the electronic device may provider the user with access to the requested restricted resources. For example, the electronic device may provide the user with access to personal data or to applications specific to the user. Process **1500** may then end at step **1514**.

[0096] The above described embodiments of the invention are presented for the purposes of illustration and not of limitation, and the present invention is limited only by the claims which follow.

What is claimed is:

1. A method for authenticating a user of an electronic device, comprising:
- displaying a plurality of selectable options;
- receiving a user selection of a subset of the selectable options;
- determining that the selected subset of selectable options share a common attribute; and
- authenticating the user in response to determining.

2. The method of claim **1**, further comprising:
- comparing the common attribute with a selectable option attribute stored in memory; and
- authenticating in response to determining that the common attribute matches the attribute stored in memory.

3. The method of claim **1**, further comprising:
- detecting that every selectable option having a selectable option attribute stored in memory was selected; and
- authenticating in response to detecting.

4. The method of claim **1**, wherein the attribute comprises at least one of:
- size;
- color;
- contour;
- fill pattern;
- shape;
- alignment with other options;
- position relative to other options; and
- source.

5. The method of claim **1**, wherein receiving further comprises simultaneously receiving at least a portion of the subset of selectable options.

6. The method of claim **1**, wherein receiving further comprises sequentially receiving at least a portion of the subset of selectable options.

7. The method of claim **1**, further comprising providing access to a restricted resource in response to authenticating.

8. The method of claim **1**, wherein the subset of selectable options comprises a number of selectable options in the range of 4 to 8.

9. A method for authenticating a user of an electronic device, comprising:

receiving a plurality of inputs from the user;

identifying the delays between consecutive inputs;

determining that the identified delays match delays stored in a library; and

authorizing the user in response to determining.

10. The method of claim **9**, wherein receiving further comprises receiving the plurality of inputs using an input mechanism.

11. The method of claim **9**, wherein receiving further comprises detecting movements of the electronic device.

12. The method of claim **9**, wherein receiving further comprises detecting impacts to the electronic device using a sensor.

13. The method of claim **9**, further comprising:

detecting the specific plurality of inputs received; and

determining that the detected specific plurality of inputs matches inputs stored in the library.

14. The method of claim **9**, further comprising determining whether the identified delays are within an allowable range of delays stored in the library.

15. The method of claim **9**, wherein at least one delay is zero.

16. An electronic device for authenticating a user based on a pattern of inputs, comprising:

a sensor operative to detect a plurality of inputs; and

a processor operative to:

identify a pattern of the detected plurality of inputs;

determine that the pattern matches a pattern stored in a library; and

authenticate the user in response to determining.

17. The electronic device of claim **16**, wherein the processor is further operative to identify a visual patterns of inputs.

18. The electronic device of claim **16**, wherein the sensor comprises at least one of:

an input mechanism;

an accelerometer; and

a gyroscope.

19. The electronic device of claim **16**, further comprising:

a display operative to display screens; and

wherein the processor is further operative to direct the display to display a plurality of selectable options.

20. The electronic device of claim **19**, wherein the sensor is further operative to detect selections of a subset of the displayed plurality of selectable options.

21. The electronic device of claim **20**, wherein the processor is further operative to identify a common attribute associated with the selected subset of selectable options.

22. The electronic device of claim **21**, wherein the attribute comprises at least one of:

size;

color;

contour;

fill pattern;

shape;

alignment with other options;

position relative to other options; and

source.

23. The electronic device of claim **16**, wherein the processor is further operative to identify a temporal patterns of inputs.

24. The electronic device of claim **23**, wherein the processor is further operative to detect the time delays between consecutive inputs of the detected plurality of inputs.

25. A computer readable medium for authenticating a user of an electronic device, comprising computer program logic recorded thereon for:

receiving a user selection of a subset of the selectable options;

identifying a pattern of the received subset of selectable options;

determining that the identified pattern matches a pattern stored in a library; and

authenticating the user in response to determining.

* * * * *